CYBER SECURITY REPORT

Media Impact International

MII™

Revised February 14, 2017

TABLE OF CONTENTS

MII would like to acknowledge and thank 100fold and its Director for serving as the lead researcher for this report, and the countless hours committed to this important project. MII also appreciates the many cyber professionals – inside and outside of the missional world – that provided counsel and expertise for this report.

EXECUTIVE SUMMARY

Overview

While Cyber Security breaches are often in the news, the impact of cyber security breaches on field ministry is often kept secret. In our su - vey of 30 key MENA ministries, we found that mission organizations were not only experiencing financial loss (perhaps in the millions of dollars), but more than 50% had staff or seekers that experienced arrest or harassment, prison, expulsion – and even death – due to cyber security breaches. These adverse impacts raise cyber risk from a technical issue to be solved by the IT department, to an organization's board and executive team that need to put in place cyber risk mitigation strategies.

The survey also found that a third of responding organizations were being deeply impacted by cyber security breaches, and did not appear to know what to do to improve their situation. Another third were impacted, but had implemented a plan to improve their cyber security profile. The last third reported almost no cyber security problems, but often lacked the means to even detect a cyber breach.

MENA Cyber Risks

A review of the cyber risks present in the MENA region shows that both state and non-state actors have access to – and use – increasingly sophisticated cyber attack tools. In addition, network-wide tools that are common in the West for monitoring terror organizations and criminal activity (Deep Packet Inspection and Lawful Interception Gateway) are being deployed across the MENA region. These

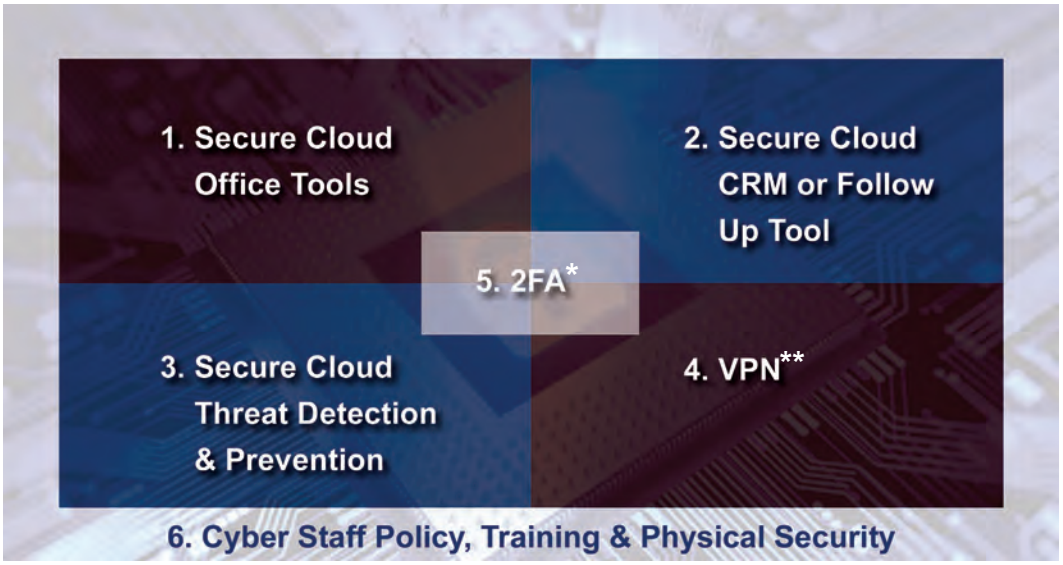
tools allow for the monitoring of all phone calls and a great deal of online activity. This creates a very challenging environment for field ministr , when the message and mission of an entity is opposed by a state actor.

The knowledge of the threats and actors in the region – and what actions they are most likely to take – makes it possible to do rational Cyber Risk Assessment. A rubric is suggested in the report that considers likely risks and matches that with appropriate mitigation steps. This process is designed to be flexible and allows organizations to have a sensible level of response based on actual risks. This in turn reduces cost and complexity of implementing a Cyber Risk Reduction program.

Cyber Risk Mitigation

A key point is that technical interventions alone will not solve cyber risk issues. Appropriate policies and strong cyber security training are crucial to a successful cyber risk reduction program. In fact, addressing staff behavior is the single most important factor in reducing cyber risk. Flexible and low-cost training tools have been identified, and the report also includes sample policies in the areas of passwords, communication, and the reduction of sensitive information to assist in this area.

CYBER RISK MITIGATION MODEL / STEPS



*** Two Factor Authentication**

****Virtual Private Network**

In the last section of the report, Cyber Risk Mitigation steps are proposed that are based on the baseline cyber risk assessment conducted in section five These mitigation steps involve policy, training and technical interventions that fulfil the Baseline Cyber Safety Profile

Cyber Response By Size of Organization

In our survey of MENA organizations, we found that roughly a third of respondents were from small organizations, with less than 50 staff. About a third were from medium-sized organizations, with more than 50 but less than 500 people. And a third were from large organizations with 500 or more staff. Each of these different-sized organizations have specific challenges, so the report proposes possible next steps with cost projections for each type. We also recognize that “one size does not fit all” and that each organization must address their unique situation and safety profile.

Small entities typically have tight budgets, highly distributed teams and little IT support. So the report proposes new cloud-based tools and training that can be implemented in stages, and that greatly improve the cyber security profile of an organization.

Medium-sized entities may have preexisting networks that need to be secured and a detailed “cookbook” has been provided (in the appendix) that has a step-by-step procedure on how to lock down a network. A cost estimate for implementing this has also been provided. An alternative proposal – similar to the one for small entities is also provided – along with cost estimates.

Large entities have much more complex network architectures and often many legacy systems. So it is not possible to recommend a single course of action that will implement a cyber safety profile for a large organization. Howeve , the report provides a cloud-based proposal similar to the one for small and medium sized organizations, along with cost estimates for implementation. For those organizations with very little in the way of cyber security, it is recommended that a Cyber Risk Assessment be conducted, and that the organization begin logging adverse impacts that are the result of cyber breaches. These two tools can then be used to inform and prioritize next steps.

A Final Word

At every step in this study, effort has been made to simplify the process and reduce cost. Missional organizations are often resource limited, so the question will often be asked “Can I afford this?” As was noted earlier, some of the negative impact that organizations reported included the loss of reputation, death of workers and seekers, and the shutdown of programs due to cyber breaches. The cost of these adverse impacts far exceeds those of implementing a baseline Cyber Safety Profile. Therefore, the question really becomes, “How can I afford NOT to do this?”

INTRODUCTION

Cyber Security in the Missional Context

It is clear that technology has strengthened the work of Christian ministries around the world. However, missiologists and missions leaders seldom consider the full implications of the rapid and pervasive adoption of so many electronic devices and online services, often by workers with little understanding of the underlying technologies. This study will focus on one aspect of the use of technology in the missional context – that of cyber security. It is important to note that this is a "point in time" report and that the whole area of cyber security is changing rapidly – both in terms of the types of risks and the potential solutions to mitigate this challenge.

Cyber security is just one piece of the over-arching security context of missional work. From the start of the Church, physical security was a recognized concern of the missional effort. This can be seen in decisions to inform local military authorities of a plot to kill a missionary (Paul), avoid a riot situation (in Ephesus), scatter away from places of intense physical persecution, as well as many other situations.

Cyber security deals with unauthorized or unexpected access to data and electronic devices. Such access can expose identities of seekers, field workers, budgets, methods, and physical locations. This can lead to death of disciples, imprisonment, expulsion, loss of visa status, counter movements, negative impact on organizational reputation, loss of funding, and other negative outcomes. Another way to consider this is to look at cyber security as a significant risk that every organization should evaluate and seek to mitigate

When we began this study, we could find no existing data on the impact of cyber breach on missional organizations. Additionally – while there are many sources for standards and best practices in cyber security – the level of detail, high technical level and high cost required to implement them appeared to have been overwhelming to many small- and medium-sized organizations.

Therefore, we have sought to help organizations reduce their cyber risk in an approachable and affordable way. This report is not a comprehensive work on cyber security in all its technical detail – such a report would be hundreds of pages long and incomprehensible to all but specialists.

There are also vast differences in context and technologies employed by missional organizations. Some small organizations are totally distributed with members using personal devices with no IT staff, much less cyber security staff. Some large organizations are utilizing cloud-based central services, are well developed and have implemented cyber security policies and full-time cyber security staff. We have chosen to focus most closely on those areas that can help the least protected improve their cyber security risk profile

> ***We have chosen to focus most closely on those areas that can help the least protected improve their cyber security risk profile.***

The core cyber security profile we have chosen for this study are the first five Critic Security Controls of the Center for Internet Security (CIS)[i], as the starting place for any cyber risk mitigation effort.

This study is also focused primarily on the cyber risk in the MENA region – how organizations can evaluate that risk and what they can do to mitigate it. However, our findings should be applicable to mission organizations in many contexts outside the MENA region.

One question that all organizations must ask – even if they don't want to ask it openly – is "what is the compelling reason for us to invest a lot of resources in this problem?" For very large corporations, it is often cheaper to deal with the adverse impacts from a cyber security breach than to implement a comprehensive and robust cyber security plan.[ii] In the corporate world there is public accountability for a financial loss that comes from cyber security breaches, so there is some ultimate accountability. However, in the mission world – not only is there no reporting – but there are seldom any internal valuations attached to

i https://www.sans.org/security-resources/posters/special/20-critical-security-controls-55
ii http://www.cbsnews.com/news/the-reason-companies-dont-fix-cybersecurity

adverse impacts due to cyber security breaches. This can make the problem invisible to senior leaders, boards and donors who all have an interest in – and a duty to – mitigate organizational risk.

Since there is no existing data on the cost of cyber security breaches in missional organizations, we have researched the cost for businesses as a surrogate. We also conducted a direct survey of 30 MENA missional organizations to gather information about the impact of cyber security breaches, attitudes and aspirations about cyber security, as well as a snapshot of current practices. The results of this survey indicate that cyber breaches are having a deep and costly impact on many organizations.

As all cyber risk originates from some threat source, it is important for organizations to identify the threats they face and seek to develop a risk mitigation strategy. To aid this process, this report provides information on known cyber risks in the MENA region as well as a flexible risk assessment tool. While it is not possible to provide comprehensive cyber risk mitigation guidance in this report – as each organization has many different issues and contexts – a section has been included on basic cyber risk mitigation. The suggestions in that section are relatively low in resource requirements, and have the potential to greatly improve the cyber security profile of an organization that is struggling with "where to start." In the appendix, additional resources are provided including a list of useful products and vendors.

It is clear from the survey we conducted with MENA ministries, that cyber security is a very significant issue for at least two-thirds of the organizations that responded. Not only are organizations suffering financial losses, but also the death and imprisonment of wor - ers due to cyber security breaches. This is coupled with a sense in several organizations of not knowing what to do to improve their cyber security situation.

This report seeks to illuminate the need, as well as provide practical information and help for missional organizations wrestling with cyber security.

> ***A wise man is full of strength, and a man of knowledge enhances his might, for by wise guidance you can wage your war, and in abundance of counselors there is victory.*** **Proverbs 24: 5-6 ESV**

CYBER THREATS

In order to effectively protect an organization, relevant and realistic Cyber Threats and Threat Actors must be identified. Once threats and threat actors have been identified, Risk Assessment can be conducted and Cyber Safety Profiles developed. Then appropriate mitigations can be put in place to fulfil the profil

In the survey of MENA ministries conducted for this study, a number of adverse impacts were reported due to cyber security breaches. These included:

1. Death of national workers or disciples
2. Imprisonment of national and expat workers
3. Arrest of national and expat workers
4. Expulsion of expat workers
5. Shut down of programs
6. Loss of organizational reputation
7. Loss of time and resources

The loss of life and imprisonment of personnel is a far greater adverse impact than is typically experienced by a for-profit compan . This type of loss actually meets the defin - tion of genuine Cyber War.[1]

What was not collected in the survey was the financial impact of cyber security breaches for missional organizations. In this study we will use data from breaches in for-profit co - panies as a surrogate for the financial impact in missional organizations

PROBABILITY OF CYBER SECURITY BREACH

In a global study of more than 380 companies, it was determined that there was a .256 probability of a Cyber Security Breach that involved at least 10,000 data records.[2] In the MENA region this was calculated at 0.31.[3] Another way to state this is that between 1 in 4 and 1 in 3 organizations would experience a cyber security breach that involved 10,000 data records or more (over any 2-year period).

In the survey conducted for this report, 23 out of 30 (or 76%) of respondents reported some type of cyber security breach. However, the time frame for those breaches was not collected in the survey.

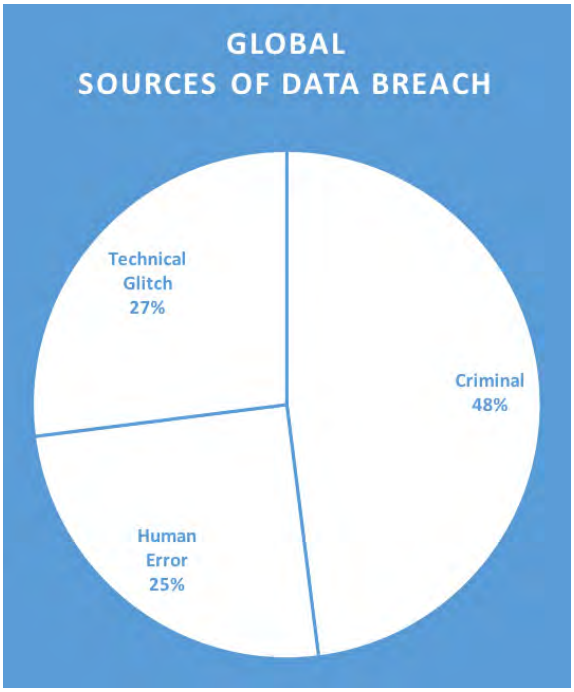
1 'Cyberwar' Is Over Hyped: It Ain't War Til Someone Dies
2 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute Research Report, p 21
3 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute Research Report, p 22

FINANCIAL LOSS DUE TO CYBER SECURITY BREACH

Financial loss for cyber breach was calculated on a cost per record basis. This cost incorporates the total cost to the entity. This differs by industry and region. The low-end cost was $61 per record and the high-end cost was $221 per record (over a 3-year span). For a loss of 10,000 records, this would range from $610,000 to $2.2 million per organization. If we model this using the eight mission organizations in the survey that had an Adverse Impact Score of 30 or above, that would yield a range of $4.8 million to $17.6 million in financial loss. Based on Adverse Impacts like Loss of Organizational Reputation, Shut Down of Programs, Expulsion of Expats and Death of National Workers, it appears likely that real financial losses experienced by missional entities could easily fall within this range.

TIME NEEDED TO IDENTIFY & CONTAIN A CYBER SECURITY BREACH

Mean Time To Identify (MTTI) represents the average time it takes a company to identify that they have had a cyber security breach. Currently, among for-profit companies the MTTI is 210 days or roughly 7 months.[4] The Mean Time To Contain (MTTC) is 70 days.[5] It is not known what the MTTI and MTTC are for missional organizations. However, based on the low level of spending on cyber security by a third of the survey respondents, it is likely that the MTTC and MTTI are greater for those entities.



Globally, at least 25% of Cyber Breaches are due to human error.

ORGANIZATIONAL STAFF

Organizational staff can present two main types of threats to an organization. The first is due to negligence and error that results in a cyber security breach. The second is malicious actions that seek to steal from the organization or do harm to the entity. This second threat is also called an "insider threat." This second type of threat is considered targeted criminal behavior. In this study we have cited data that

4 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute Research Report, p 23
5 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute Research Report, p 24

indicates that at least 25% of cyber breaches can be directly attributed to staff actions. There are multiple online sources that claim this to be as high as 90%[6], however the bulk of these claims were not substantiated with data. In any case, organizational staff training and compliance is a key factor in a successful risk mitigation program.

OPPORTUNISTIC CRIMINALS

Opportunistic Criminals use a variety of un-targeted physical and cyber attacks to steal information, equipment, funds, personal identities, hold information ransom and a range of other criminal actions.

LAWFUL INTERCEPTION GATEWAYS (LIG)

Lawful Interception Gateways are technologies built into the telecom infrastructure that allow telecoms to monitor, intercept, record and analyze all phone call and SMS traffic. This technology has become standard globally and is intended to be used to counter terrorism and criminal activity. However, the extensive invasive capabilities of these systems are only limited by the legislation of any specific countr .

All MENA countries have some version of the Lawful Interception Gateway capacity.

When built out extensively, it is possible to monitor all call and SMS traffic simultaneously and in real time. Because this monitoring can be automated it greatly reduces the “hide in the long grass” privacy defense. Lawful Interception Gateways can be configured to access GPS and telecom user location data – so that not only can the system monitor a call or SMS – but it can pinpoint the location of the person receiving the call and the person making the call (if they are both in the network). Additionally, user location data can be accessed for people within a specific distance of either caller if they have phones.

6 http://www.prnewswire.com/news-releases/employee-errors-cause-most-data-breach-incidents-in-cyber-attacks-300342879.html

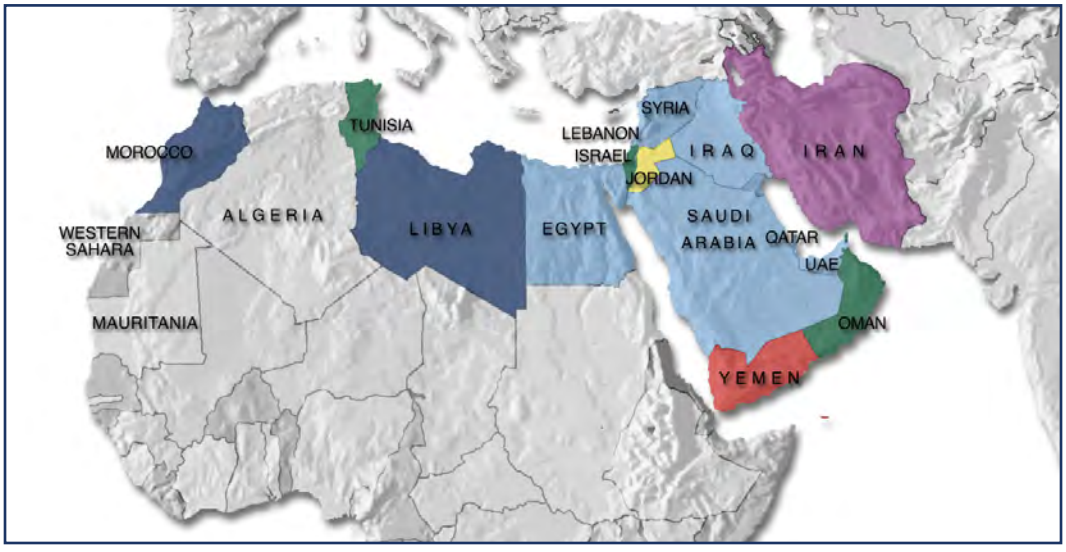
Systems can also be configured to report who a caller received a call from, and who that caller telephoned after receiving a specific call, and who each of those people called after contacted by the first calle .

SS7 GLOBAL TRACKING

SS7 is a global locator system for phones that are roaming in networks other than their own. It allows a telecom to determine what network the phone belongs to, and whether it has a way to bill that user for the use of the local phone network. SS7 is available to all cell phone networks. The system can also be misused to track individuals on a global scale.[7]

For example, if someone from France was visiting the UAE and was "roaming," the telecom in the UAE would recognize that this phone was from outside its network and would query SS7 as to where the phone was from, and if its home telecom had a roaming agreement with it. If the agreement existed, the person from France would be able to make calls without having to buy a local SIM chip. However, once the local telecom in the UAE made a record of the phone's unique equipment ID number, it would be possible to query the SS7 system in the future and request location information on that phone, even if it was back in its home network in France, or any place they were located around the globe. Therefore, if someone on the UAE telecom network traveled to another country and *even changed their SIM card*, the phone would still be trackable on the SS7 network based on the unique hardware ID number.

DEEP PACKET INSPECTION (DPI)



Countries using DPI Technology in the MENA region – DPI vendors identified for each country.

7 Webinar by Silent Circle - https://www.youtube.com/watch?v=JaxHk-QUsnE&feature=youtu.be

Deep Packet Inspection (DPI) is a technology that allows an Internet Service Provider (ISP) to examine in great detail all of the Internet traffic from an Internet use . All un-encrypted traffic can be monitored, including usernames and passwords. DPI can also be used to identify and block specific content and services. Many governments in the MENA region are documented as having DPI technology in place. Vendors are Bluecoat,[8] Amesys,[9] Raytheon,[10] Cyberroam,[11] Narus,[12] and ZTE.[13] DPI systems can be programmed to identify specific users and services automaticall , defeating in part the "hide in the long grass" privacy defense.

THE HACKING TEAM

The Hacking Team[14] is a company that specializes in producing tools that can invade a mobile device and use it to remotely monitor the user. The software is typically undetectable by the device owner and gives access to all data and communication on the device, and avoids encryption tools that allow privacy in communication. The Hacking Team typically sells their tools to governments. There are confirmed incidents of The Hacking Team tool being used to monitor human rights advocates by governments they oppose.

Map of countries in the MENA region (highlighted in red) that are known to have purchased The Hacking Team tools.[15]

8 https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/
9 https://malwaretips.com/threads/access-denied-crazy-internet-censorship-in-morocco.19319/
10 http://www.deepacketinspection.com/dpi/AS51140
11 https://lwn.net/Articles/506337/
12 http://www.pcworld.com/article/218142/article.html
13 Reuters News , 25 May 2012, U.S. probes China's ZTE over tech sales to Iran
14 https://en.wikipedia.org/wiki/Hacking_Team
15 http://mashable.com/2014/02/18/controversial-government-spyware-hacking-team/#Uj7MvVCwPEqD

MENA Cyber Threats

SUNNI, SHIA, JEWISH CYBER WAR

In the MENA region there is an active cyber war between Iran, Egypt / Saudi Arabia and Israel.[16] Initially, this consisted of website defacements and DDOS attacks of various sites. However, it has now escalated to attacks on core infrastructure and industries. This cyber war likely involves state and non-state actors with more than 30 non-state hacker groups involved. While the focus of all of these resources is the other belligerents, it is important to note that any perception that a missional group or its staff was in some way aligned with the goals of any of the attacker's interests, that missional group could be subjected to a targeted attack by the other two belligerents.

ALGERIA

While there is no public record of Algeria acquiring DPI (Deep Packet Inspection) technology, the country does have centralized systems to monitor Internet traffic and the legal power to block websites "contrary to public order and decency."[17] We did not receive specific reports of cyber attacks on ministries by Algeria, however press and government sources have reported attacks on websites and social media increased 300% – with over 500 cases – in 2015.[18] Algeria has a small but vibrant software development segment and thus a skilled pool of people that could engage in cyber activities. There have been numerous attacks on French websites by Algerian hackers.[19] The capacity of these hackers was shown in 2013 with the development of the "SpyEye" financial fraud malware package by Hazma Bendelladj. "SpyEye" was considered the most widely used financial fraud malware package in the world.[20]

Currently the most likely threats are:

1. Petty theft.
2. Government monitoring of web and phone activity.
3. Website defacement and destruction if targeted by Algerian hackers.

16 http://www.bluekaizen.org/CSCAMP2012/CONFHpdfs/EbrahimHegazy/Cyber-Warfare-in-the-middle-east.pdf
17 https://freedomhouse.org/report/freedom-world/2016/algeria - see section D.
18 https://www.osac.gov/pages/ContentReportDetails.aspx?cid=19075
19 http://www.huffingtonpost.com/2015/01/13/charlie-hebdo_n_6464318.htm
20 http://arstechnica.com/tech-policy/2013/05/alleged-mastermind-behind-spyeye-botnet-tools-extradited-to-us/

EGYPT

The national network in Egypt has had a low level of security in general, which led to widespread infestation with botnets and other criminal software. In 2010, there were hundreds of thousands of machines that were infected.[21] By 2015, the government of Egypt had Finfishe [22] software in place,[23] which is a commercial "botnet" that is used for surveillance. In the same year, the Cyber Security Council of Egypt was formed as a national-level effort to improve cyber security. However, many groups see the CSC as a means of national surveillance and suppression.[24] It is also publicly documented that Egypt has Lawful Interception Gateway (LIG) and DPI technology,[25] as well as tools from the Hacking Team. In December 2016, Egypt began to block the use of "Signal," an encrypted communications app at the network level.[26] As part of the new Cyber Security Infrastructure, Egypt has signed agreements to share cyber intelligence with South Korea, Oman, Malaysia, Uganda, Tunisia, India, Tanzania and the U.S.[27] With nine different terrorist organizations operating within the borders of Egypt[28] (ISIS being one of them) – and thirteen hacking groups[29] – Egypt presents a complex environment with many physical and cyber security challenges.

There have been no specific reports of cyber attacks targeted at missional organizations, however the well equipped and antagonistic government,[30] as well as hostile militant groups are viable threat actors. Currently the most likely threats are:

1. Monitoring of unencrypted email, SMS, VOIP, and phone calls.
2. Monitoring of unencrypted web and social media usage.
3. Untargeted malware and phishing attacks.
4. Exposure of personal information by radical Muslim hackers who operate in Egypt.
5. Petty theft.

21 https://en.wikipedia.org/wiki/Virut
22 https://en.wikipedia.org/wiki/FinFisher
23 https://citizenlab.org/2015/10/mapping-finfishers-continuin proliferation/
24 http://www.al-monitor.com/pulse/en/originals/2015/01/egypt-cyber-security-council-privacy.html
25 http://www.huffingtonpost.com/timothy-karr/congress-urges-state-depa_b_82 949.html
26 http://english.alarabiya.net/en/media/digital/2016/12/21/Egypt-blocks-encrypted-messaging-app.html
27 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Egyp .pdf
28 http://thehill.com/blogs/congress-blog/foreign-policy/239566-terror-attacks-skyrocket-in-egypt-and-across-the-globe
29 http://www.bluekaizen.org/CSCAMP2012/CONFHpdfs/EbrahimHegazy/Cyber-Warfare-in-the-middle-east.pdf
30 http://www.nytimes.com/2016/12/22/opinion/egypts-cruelty-to-christians.html?_r=0

For those that are engaged in high profile activities, work amo g suspect populations, or have drawn the attention of the government or radical groups, the following are likely threats:

1. Targeted malware and phishing attacks – which could lead to kidnapping.
2. Targeted malware and phishing attacks – which could result in exposure of a network of contacts.
3. Targeted cyber attack on personal devices.
4. Targeted network attacks.
5. Active monitoring of all communications – phone, SMS, VOIP, Chat, email, etc.

IRAN

In April 2010, there was public evidence that Nokia sold LIG equipment to Iran that could be used to monitor all calls and texts – especially mobile communications.[31] In February 2014, Iran was considered to be a first-tier cyber warfare threat to the USA [32] In April 2014, Viber – the most popular chat app in Iran at the time – was shown to have stored communications in unencrypted form,[33] and thus gives credence to claims by Iran of monitoring communications on Viber.[34] In September 2014, the Iranian high court issued orders to block Viber. This occurred after there was evidence that Viber had an opportunity to fix the security issues [35]

In September 2014, there were reports from a media ministry serving Iran that phone numbers had been blocked and high-jacked. Security personnel in Iran have also impersonated ministry counselors to gather intelligence on seekers that called a high-jacked phone number.[36] In August 2015, Iran was caught high-jacking two factor authentications of a Gmail account[37] (two factor authentication is considered a best practice in cyber security). In Winter 2015, it was reported that Psiphon VPN service was widely disrupted in Iran.[38] At the time of the attack, Psiphon was one of the most widely used VPNs in Iran. In Spring 2016, it was reported that a device in the West was compromised and data ex-

31 http://arstechnica.com/tech-policy/2010/03/how-nokia-helped-iran-persecute-and-arrest-dissidents/
32 http://foreignpolicy.com/2014/02/18/forget-china-irans-hackers-are-americas-newest-cyber-threat/
33 http://thehackernews.com/2014/04/vibers-poor-data-security-practices.html
34 https://www.iranhumanrights.org/2014/09/viber-company-refutes-tapping-claims-by-iranian-officials
35 http://www.al-monitor.com/pulse/originals/2014/09/iran-internet-communication-viber-whatsapp-judiciary.html
36 Personal conversation with ministry leaders
37 https://citizenlab.org/2015/08/iran_two_factor_phishing/
38 Bulletin from Psiphon Feb 2016

filtrated that resulted in the arrest of more than a dozen people inside Iran [39] This appears to have been a targeted cyber attack. In March 2016, the company ZTE was banned from trade in the U.S. over selling DPI and other technologies to Iran. The investigation provided public proof of long suspected capabilities to use DPI to monitor Internet use in Iran.[40] Iran is also a major sponsor of Hamas and would be able to share information gained via cyber breach with them.[41] Additionally, Iran has a very strong hacker capability[42] with many groups aligned with state purposes.[43] This has resulted in attacks on high profile Western targets and the ability of Iran to project cyber power on a global scale.

Iran is a very well equipped and aggressive state threat actor. It has also treated missional work and church planting as a national security threat. Any organization seeking to work in Iran – or partner with those who work there – needs to be diligent in their cyber security preparations. Currently the most likely threats are:

1. Targeted theft.
2. Targeted cyber attacks on personal devices.
3. Targeted network attacks.
4. Active monitoring of all communications – phone, SMS, VOIP, Chat, email, etc.
5. Exploits against two factor authentication.
6. Blocking VPN at the network level.
7. Arrest, imprisonment and possible torture of nationals in country that are exposed in a cyber breach.

IRAQ

Iraq is an active war zone with fighting between ISIS and estern powers. The Cyber Caliphate has emerged as a hacking group aligned with ISIS. The Cyber Caliphate is very social media savvy and has a large number of members monitoring and engaging with social media.[44] They have also conducted “false flag” attacks where they produce anti-ISIS media to attract their most ardent opponents.[45] This content is delivered with exploits that

39 Personal conversation with ministry leaders
40 http://www.theregister.co.uk/2016/03/08/us_trade_ban_on_zte
41 http://www.al-monitor.com/pulse/originals/2016/06/gaza-hamas-resume-relations-iran.html
42 https://en.wikipedia.org/wiki/Iranian_Cyber_Army
43 http://uk.businessinsider.com/what-its-like-to-be-a-hacker-in-iran-2016-2?r=US&IR=T
44 http://www.al-monitor.com/pulse/originals/2015/04/iraq-social-media-convey-battle-against-islamic-state.html
45 http://www.bbc.co.uk/news/technology-28418951

allow ISIS hackers to trace the physical location of the person who accessed the media, and then trace who the media was shared with. This information can then be used for targeted kidnapping,"hit lists" (for ISIS sympathizers to kill if the person lives outside Iraq), or cyber exploits to gather intelligence. As a pure hacking force, ISIS has received a good deal of publicity, but a recent analysis has determined that ISIS hackers are currently deploying standard open-source hacking tools and well-dated exploits.[46] This implies that missional workers can build a Cyber Safety Profile that will protect them against the vast majority of ISIS hacking efforts.

The central government of Iraq has advanced cyber attack and monitoring tools.[47] There is public information that Iraq has LIG and DPI technologies, as well as advanced Internet surveillance and monitoring tools. They also utilize over-the-air surveillance systems that allow for the interception, monitoring and physical tracking of cell phone calls in real time.[48] The Iraqi central government also receives cyber training and support from the U.S. and NATO.[49] The most likely threats are:

1. Monitoring of unencrypted email, SMS, VOIP, and phone calls.
2. Monitoring of unencrypted web and social media usage.
3. Untargeted malware and phishing attacks.
4. Exposure of personal information by radical Muslim hackers who operate in and outside of Iraq.
5. Social engineering on social media with attempts to identify those opposed to ISIS.
6. Petty theft.

For those that are engaged in high profile activities, work amo g suspect populations, or have drawn the attention of the government or radical groups, the following are likely threats:

1. Targeted malware and phishing attacks – which could lead to kidnapping.
2. Targeted malware and phishing attacks – which could result in exposure of a network of contacts.
3. Targeted social media malware attacks – which could lead to kidnapping or execution.
4. Targeted cyber attacks on personal devices.
5. Targeted network attacks.
6. Active monitoring of all communications – phone, SMS, VOIP, Chat, email, etc.

46 Hacking for ISIS: The Emergent Cyber Threat Landscape. Flashpoint. 2016
47 https://sii.transparencytoolkit.org/search?utf8=✓&utf8=✓&q=Iraq
48 https://sii.transparencytoolkit.org/search?utf8=✓&utf8=✓&q=Iraq
49 http://www.nato.int/cps/en/natohq/news_139179.htm

JORDAN

There are reports of Internet scams and identity theft as an ongoing concern in Jordan.[50] Petty theft and untargeted break-ins against expatriates are also reported.[51] Jordan has been attacked by elements of ISIS and there appears to be a significant ISIS pre - ence in some areas of the country.[52] There is public evidence that Jordan has DPI, LIG, FinFisher surveillance software, and remote access tools from The Hacking Team. They also have over-the-air surveillance systems that allow for the interception, monitoring and physical tracking of cell phone calls in real time.[53]

There were no reports of cyber attacks against a missional organization by Jordan. The government has a reputation of being tolerant of Christianity. Most incidents of persecution originate at the personal and family level.[54] Currently the most likely threats are:

1. Monitoring of unencrypted email, SMS, VOIP, and phone calls.
2. Monitoring of unencrypted web and social media usage.
3. Untargeted malware and phishing attacks.

For those that are engaged in high profile activities like work among refugees, or have drawn the attention of the government or radical groups, the following are likely threats:

1. Targeted malware and phishing attacks.
2. Targeted malware and phishing attacks – which could result in exposure of a network of contacts.
3. Targeted cyber attacks on personal devices.
4. Targeted network attacks.
5. Active monitoring of all communications – phone, SMS, VOIP, Chat, email, etc.

50 https://www.osac.gov/pages/ContentReportDetails.aspx?cid=19208
51 Ibid
52 http://www.middleeasteye.net/news/enemy-within-jordans-battle-stop-home-grown-terrorism-481722991
53 https://sii.transparencytoolkit.org/search?utf8=✓&utf8=✓&q=jordan
54 https://www.vomcanada.com/jordan.htm

LEBANON

Lebanon does not have a central policy nor a legislative framework for cyber security.[55] It is reported that Lebanon is subject to significant cyber crime [56] Although on the surface Lebanon does not appear to have much cyber security capacity, there is evidence that the country and non-state actors like Hezbollah have significant surveillance and cyber warfare capability. In 2015, a large and long-term cyber espionage campaign was identified as originating out of Lebanon, under the control of Hezbollah [57] This cyber espionage campaign was considered to be advanced and representative of a high level of internal capability.[58] There is public evidence that Lebanon has DPI, LIG, FinFisher surveillance software, and remote access tools from The Hacking Team. They also have over-the-air surveillance systems that allow for the interception, monitoring and physical tracking of cell phone calls in real time.[59] Petty theft, targeted theft, and kidnapping are all present risks.[60] Militant groups like ISIS, Hezbollah and at least seven other extremist groups operate within Lebanon.[61] They have specifically targeted Christian [62] in Lebanon and many have been tortured and killed.[63]

The lack of political stability, the high influx of Syrian refugees, the unrestrained presence of militant groups with proven cyber espionage capability, and the use of very sophisticated surveillance and cyber attack tools by the state, presents a very complex and challenging environment for missional organizations. Special precautions should be taken to encrypt and compartmentalize sensitive data. The most likely threats are:

1. Petty theft.
2. Monitoring of unencrypted email, SMS, VOIP, and phone calls.
3. Monitoring of unencrypted web and social media usage.
4. Untargeted malware and phishing attacks – criminal.

---

55 http://www.tra.gov.lb/Cybersecurity-in-Lebanon
56 http://www.executive-magazine.com/economics-policy/lebanon-cyber-security-telecommunications-regulatory-authority
57 http://www.csmonitor.com/World/Passcode/2015/0601/Cyberattack-tied-to-Hezbollah-ups-the-ante-for-Israel-s-digital-defenses
58 http://www.csoonline.com/article/2904396/data-protection/lebanese-cyberespionage-campaign-hits-defense-telecom-media-firms-worldwide.htm
59 https://sii.transparencytoolkit.org/search?recipient_country_facet=Lebanon
60 https://www.osac.gov/Pages/ContentReportDetails.aspx?cid=19280
61 https://www.osac.gov/Pages/ContentReportDetails.aspx?cid=19280
62 http://www.foxnews.com/opinion/2016/07/02/after-fallujah-isis-moves-to-lebanon-and-targets-christians.html?refresh=true
63 Private report of converts being tortured and killed for position of Christian media, 2016.

For those that are engaged in high profile activities – especially with refugees – or have drawn the attention of the government or radical groups, the following are likely threats:

1. Targeted theft.
2. Targeted cyber attack on personal devices.
3. Targeted network attacks.
4. Active monitoring of all communications – phone, SMS, VOIP, Chat, email, etc.
5. Exposure of personal information by radical Muslim hackers to hostile militant groups.
6. Possible kidnapping, torture and death of nationals in country that are exposed in a cyber breach.

LIBYA

The government of Libya is publicly known to have LIG and DPI Technology. During the unrest in 2011, the government shut down the Internet for the entire country. After that total shut down, there have been multiple partial shutdowns,[64] demonstrating total control of the Internet by the central government. Additionally in 2011, ten Libyan hacking groups were identified that were aligned with the central government, and at least one hacking group that was engaged in cyber jihad against the West.[65] This cyber jihad group was found to be creating viruses that were used against major corporations. A wide-ranging analysis of the national network of Libya also showed a poor state of cyber security standards, meaning that the compromise of national systems was likely.[66] This makes for a ripe environment of botnets and other cyber attack tools. In 2016, there were reports that in the active Libyan war zone, non-state actors were engaged in cyber espionage against high-profile Libyans using the remote access trojan (R T) “AlienSpy.” Using a combination of targeted phishing and social engineering, a Telegram account of a target was taken over and used to pass malware to contacts of the target. Researchers said this software – while not sophisticated – could allow the tracking and monitoring of individuals for possible kidnapping and assassination.[67]

64 Project Cyber Dawn v1.0, The Cyber Security Forum Initiative. P. 8
65 Ibid. p 21
66 Ibid. p 25
67 http://news.softpedia.com/news/libyan-scorpions-cyber-espionage-group-targets-high-profile-lybians-508664shtml

No reports have been received of direct cyber attacks on missional organizations operating in Libya. However, the most likely threats are:

1. Monitoring of unencrypted email, SMS, VOIP, and phone calls.
2. Monitoring of unencrypted web and social media usage.
3. Untargeted malware and phishing attacks.
4. Exposure of personal information by radical Muslim hackers who operate in Libya.
5. Petty theft.

For those who are engaged in high profile activities – such as work among suspect populations or ministries that have drawn the attention of the government or radical groups, the following are likely threats:

1. Targeted malware and phishing attacks – which could lead to kidnapping.
2. Targeted malware and phishing attacks – which could result in exposure of a network of contacts.

MOROCCO

The government of Morocco is publicly known to have LIG and DPI technologies, and to have purchased tools from The Hacking Team.[68] Conversations with local workers indicated that the government has monitored the use of VPNs by nationals, especially in rural areas.[69] In 2010, the government of Morocco expelled scores of Christian workers.[70] Some Christian workers reported that phone calls are being monitored, SMS messages are being hijacked, email and web usage is being monitored, and this information is used in identifying other expat workers and national Christians.[71] In 2012, 2013 and 2014, the government of Morocco used tools from The Hacking Team to gain control of mobile phones, computers, webcams, email accounts, and social network accounts of journalists and "civil society advocates."[72] Hacking groups have also been very active in Morocco. In 2013 and 2014, there were reports of cyber attacks on the Israeli government, academic and infrastructure sites by Moroccan hackers.[73] There were also ISIS-aligned radical

68 Their Eyes On Me – Stories of surveillance in Morocco, Privacy International, 2015. P 10
69 Private conversation with local worker.
70 http://www.christianpost.com/news/morocco-begins-large-scale-expulsion-of-foreign-christians-44271/
71 Debrief with Christian worker who was expelled. Unpublished paper 2010.
72 https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/
73 https://www.moroccoworldnews.com/2015/02/152136/moroccan-hackers-behind-cyber-attacks-on-israeli-targets/

Muslim hackers that attacked media outlets in 2014.[74] After more than 100 workers were expelled in 2010, those who attempt to work in Morocco should be using sound cyber security practices. Currently the most likely threats are:

1. Monitoring of unencrypted email, SMS, VOIP, and phone calls.
2. Monitoring of unencrypted web and social media usage.
3. Untargeted malware and phishing attacks.
4. Exposure of personal information by radical Muslim hackers that operate in Morocco.
5. Petty theft.

For those that are engaged in high profile activities, work amo g suspect populations, or have drawn the attention of the government or radical groups, the following are likely threats:

1. Targeted malware and phishing attacks.
2. Monitoring of encrypted email and VOIP.
3. Monitoring of encrypted web and social media usage.
4. Remote entry to computers and mobile devices, allowing access to encrypted files, webcam and microphones on those devices.
5. Physical search of premises.
6. Targeted effort to circumvent VPN protections.

SAUDI ARABIA

Saudi Arabia conducts raids on private Christian meetings on a regular basis.[75] These raids are reported to be initiated by anonymous tips, but could be the result of surveillance.[76] Expats caught up in raids are expelled, while local people can be arrested, imprisoned, tortured and killed. The government of Saudi Arabia spends more than $37 billion a year on cyber security.[77] The country has one of the most active social media environments in the world.[78] Because of its prevalence, the government is thought to employ a “Social

74 http://themoroccantimes.com/2014/09/10779/cyber-attacks-isils-new-deadly-weapon
75 https://www.jihadwatch.org/2016/09/saudi-arabia-27-christians-arrested-and-deported-for-conducting-christian-prayers-in-private-residence
76 http://www.dailymail.co.uk/news/article-2756134/Dozens-Christians-including-women-children-arrested-Saudi-Arabia-tip-state-s-Islamist-police-force.html
77 http://www.oxfordbusinessgroup.com/news/saudi-arabia-strengthen-defences-against-cyberattacks
78 http://www.economist.com/news/middle-east-and-africa/21617064-why-social-media-have-greater-impact-kingdom-elsewhere-virtual

Media Army"[79] to monitor, interact with and subvert online discussions. The government also seeks to block or monitor all VOIP traffic [80] All web use is monitored and many sites are blocked.[81] There is also public evidence of government capability to circumvent the encryption of SSL connections, as well as most "secure" chat apps.[82] There is public information that Saudi Arabia has LIG and DPI technologies, as well has tools from The Hacking Team for taking over mobile devices.[83] The most common cyber crime in Saudi Arabia is cyber blackmail – where compromising details are acquired through a cyber attack and used as leverage to receive a payment.[84]

With a virtually unlimited budget for cyber security and top-end surveillance technology,[85] as well as a close partnership with the U.S. in intelligence, Saudi Arabia presents a very challenging environment for Christian workers. Special precautions should be taken to encrypt and compartmentalize sensitive data. Currently the most likely threats are:

1. Targeted theft.
2. Targeted cyber attack on personal devices.
3. Targeted network attacks.
4. Active monitoring of all communications – phone, SMS, VOIP, Chat, email, etc.
5. Exploits against two factor authentication.
6. Cyber blackmail.
7. Arrest, imprisonment and possible torture of those in country who are exposed in a cyber breach.

SYRIA

At the time of this study, Syria is an active war zone that involves not just regional, but global powers. The same is true for the cyber war that is being waged there. The Syrian Electronic Army (SEA) is a hacker group that is aligned with the central government. It has hijacked social media accounts of the opposition, gathered critical intelligence, and changed the outcome of military campaigns. To do this it has used RAT's (Remote Access

79 https://freedomhouse.org/report/freedom-net/2015/saudi-arabia
80 Ibid
81 https://en.wikipedia.org/wiki/Censorship_in_Saudi_Arabia
82 https://moxie.org/blog/saudi-surveillance/
83 http://www.economist.com/blogs/pomegranate/2014/07/internet-monitoring-gulf
84 http://www.arabnews.com/online-blackmail-main-cyber-crime
85 https://www.issworldtraining.com/ISS_MEA/index.htm

Trojan) software as well as spear phishing (targeted phishing), and social engineering techniques.[86] There are reports that the SEA receives help and training not just from the central government, but also from Russia and Iran (both of which are major cyber warfare powers).[87] The central government, while possessing the capacity to heavily filter or cut off the Internet, chooses to lightly filter – but heavily surveil – Internet and social media usage, and gathering user names and passwords of Facebook accounts so that it can access those for intelligence purposes.[88] There are also reports that Russia has sent technical resources that allow it to tap into the core sub-oceanic fiber optic cable that feeds more than 60% of the Internet access for Syria.[89]

It has also been reported that surveillance technology was used to discover the IP addresses of activists opposed to the central government, and that these people were arrested and tortured.[90] The opposition also has a significant cyber warfare capabilit , and some elements of that opposition received training and funding from the U.S. and other Western powers opposed to the central government of Syria. Other elements of the opposition – ISIS and al-Qaeda – are not aligned with any Western governments and have their own cyber attack capabilities.

There is public information that Syria has LIG and DPI technologies, and advanced Internet surveillance and monitoring tools.[91] There is also evidence that they utilize satellite phone interception and tracking technology as well. The combination of both active physical and cyber warfare – along with the involvement of major militant groups and global cyber warfare powers – makes for an extremely hazardous and complex environment. Currently the most likely threats are:

1. Monitoring of unencrypted email, SMS, VOIP, and phone calls.
2. Monitoring of unencrypted web and social media usage.

For those that are engaged in high profile activities, work amo g suspect populations, or have drawn the attention of the government or radical groups, the following are likely threats:

1. Targeted malware and phishing attacks.
2. Targeted malware and phishing attacks – which could result in exposure of a network of contacts.
3. Targeted cyber attack on personal devices.
4. Targeted network attacks.
5. Active monitoring of all communications – phone, SMS, VOIP, Chat, email, etc.

---

86 http://www.aljazeera.com/programmes/peopleandpower/2015/06/syria-electronic-armies-150617151503360.html
87 Ibid
88 http://europe.newsweek.com/syria-grants-free-internet-access-so-it-can-snoop-230442?rm=eu
89 https://www.alaraby.co.uk/english/news/2016/10/20/syrian-regime-internet-network-repairs-guise-for-more-surveillance
90 http://www.aljazeera.com/programmes/peopleandpower/2015/06/syria-electronic-armies-150617151503360.html
91 https://sii.transparencytoolkit.org/search?utf8=✓&utf8=✓&q=syria

TUNISIA

The government of Tunisia is publicly known to have LIG and DPI technologies. In 2011 during the Arab Spring uprisings, the government was stealing Facebook users' IDs and passwords on a massive scale through ISPs (Internet Service Providers). This resulted in counter actions by Facebook to restore control of accounts to their rightful users.[92] Some Tunisian hackers have been identified as aligned with ISIS, and have attacked U.S. government websites as well as banking and infrastructure sites in 2014.[93] The Falaga hacking group from Tunisia is also engaged in attacking targets in France and Israel.[94]

While the government of Tunisia has significant cyber attack capabilities – and radical Islamic hacker groups have a history of operating in the country – there have been no direct reports of missional organizations being directly attacked by either group. Currently the most likely threats are:

1. Petty theft.
2. Government monitoring of web, social media and phone activity.
3. Website defacement and destruction if targeted by Tunisian hackers.
4. Possible DDOS attacks on websites.
5. Exposure of identity information by radical Islamic hackers who operate in Tunisia.

92 http://www.theatlantic.com/technology/archive/2011/01/the-inside-story-of-how-facebook-responded-to-tunisian-hacks/70044/

93 http://www.hstoday.us/briefings/daily-news-analysis/single-article/exclusive-tuni ian-hackers-announce-cyber-jihad-against-us-banks-airport-computer-systems/7c3d2373e69fa9319e521816ce539b7d.html

94 http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/fallaga-team-tunisian-hacker-group-engages-in-jihadi-hacktivism-active-on-twitter-facebook-youtube/

UNITED ARAB EMIRATES (UAE)

The UAE recently upgraded their laws concerning the use of VPNs. Many missional workers in Dubai stopped using VPNs out of concern that the use would make them subject to heavy fines or expulsion. Howeve , at least one legal opinion holds that their core law is no different from a year ago, only the level of fine has changed. Therefore it is likely that missional workers would not be charged under this law for normal use of a VPN. However, until there is a test case on the matter it remains uncertain.[95]

VOIP services are “unlicensed” and the use of them is subject to heavy fines [96] There is evidence to indicate that the UAE monitors all communications and web usage. The cyber crime law also contains punishments for offending the state, its rulers, its symbols, or for insulting Islam and other religions. Violating this law can result in arrest. Imprisonment, expulsion, and harsh physical punishment can also be applied.[97] A KPMG cyber survey of UAE in 2015, showed the country to be one of the top ten global locations for cyber crime, with over a third of those surveyed indicating they had been hacked in the last 12 months.[98]

The public record indicates that the UAE is investing in world class surveillance and cyber attack tools.[99] There is additional public information that the UAE has LIG and DPI technologies, advanced video surveillance and facial recognition technology, as well as tools from The Hacking Team for taking over mobile devices.[100] No reports have been received of direct cyber attacks on missional organizations operating in the UAE. The most likely threats are:

1. Monitoring of unencrypted email, SMS, and phone calls.
2. Monitoring of unencrypted web and social media usage.
3. Untargeted malware and phishing attacks – criminal.

For those that are engaged in high profile activities, like wor among refugees, or have drawn the attention of the government or radical groups, the following are likely threats:

95 http://www.lexology.com/library/detail.aspx?g=60307f30-2f86-4aae-88fe-0cdae6c427dc
96 https://freedomhouse.org/report/freedom-net/2015/united-arab-emirates
97 Ibid
98 https://home.kpmg.com/ae/en/home/media/press-releases/2015/12/kpmg-uae-cyber-security-survey-2015.html
99 http://www.middleeasteye.net/news/exclusive-uae-elite-task-force-security-secret-surveillance-state-135285760
100 https://sii.transparencytoolkit.org/search?utf8=✓&utf8=✓&q=UAE

1. Targeted malware and phishing attacks.
2. Targeted malware and phishing attacks – which could result in exposure of a network of contacts.
3. Targeted theft.
4. Targeted cyber attack on personal devices.
5. Targeted network attacks.
6. Active monitoring of all communications – phone, SMS, Chat, email, etc.

For additional Country Profiles, please see Appendix N.

CYBER SECURITY SURVEY

The Cyber Security Survey was conducted in July and August of 2016. It sought to determine if cyber security breaches were having a detrimental impact on missional organizations – especially those working in the MENA region. The survey was conducted as an anonymous assessment and no identifying information was collected on respondents. The anonymous survey was chosen to increase the likelihood that organizations would report adverse impacts.[101] The survey was "advertised" through a cyber security affinity g oup in the missions community and via a private mailing list of participants in a regional ministry conference. Thirty respondents completed the on-line survey utilizing Survey Monkey.[102]

SURVEY LIMITATIONS

Before the survey was conducted, we sought out existing data on cyber security breaches in missional organizations to help establish a baseline, but we didn't find an . As in any survey, we were somewhat limited by the perceptions of the respondents. It is possible for two organizations to have cyber security programs that are vastly different technically, yet both report that they have effective programs. We sought to mitigate this through questions about outcomes and spending that helped to identify gaps in effectiveness.

While preparing the survey, we received feedback from potential survey participants that long and detailed surveys would be rejected or only answered in part. Therefore, we endeavored to keep the survey concise, thus limiting its scope. We also recognized that it was possible for survey respondents to be unaware of cyber attacks that had penetrated their organization, and have a false sense of security. This issue could not be resolved in the survey as it was an "unknown unknown" for the respondents. We did seek to address this gap in the section of the report on risk mitigations.

SURVEY DATA

The survey collected data about the following issues:

- Adverse impacts of cyber security breaches
- Details about the cyber security program of the organization
- Attitudes about cyber security / cyber risk
- Felt needs in cyber security
- Organizational demographics
- Additional cyber security needs

101 Multiple anecdotal reports of adverse impacts have been shared with the author "off the record," thus indicating that adverse impacts are occurring and that organizations typically don't disclose them.

102 Https://www.surveymonkey.com

A list of all of the survey questions can be found in Appendix J.

ADVERSE IMPACTS OF CYBER SECURITY BREACHES

In this section of the survey, respondents were asked to indicate Yes, No, Not Sure or NA for various adverse impacts. The purpose of the “Not Sure” response was to capture data about “possible” adverse impacts. In the case of cyber security, the respondent may not be ‘certain’ that specific adverse impact was caused directly by a cyber security breach, or they may know institutional lore about an adverse impact that cannot be verified. In this part of the survey, we viewed “Not Sure” responses as indicating that a specific a - verse impact may have happened as a result of a cyber security breach.

Following are the key findings about the adverse impacts that missional organizations have experienced due to a breach of cyber security.

DEATH

4% reported the death of a local disciple / local worker / expat worker due to a breach of Cyber Security.

IMPRISONMENT

39% reported that local disciples / workers were imprisoned due to a breach of Cyber Security.

LOSS OF ORGANIZATIONAL REPUTATION

10% reported that there had been a loss of organizational reputation due to a breach of Cyber Security.

ARREST AND HARASSMENT

40% reported that local disciples / workers had been arrested or harassed due to a breach of Cyber Security.

EXPULSION

30% reported that an expat worker had been expelled from the country due to a breach of Cyber Security.

SHUT DOWN OF MINISTRY / PROGRAM

30% reported that they had a ministry or program shut down due to a breach of Cyber Security.

LOST TIME AND RESOURCES

47% reported that they had experienced a loss of time and resources due to a breach of Cyber Security.

ADVERSE IMPACT SCORE

To facilitate analysis of the overall impact of cyber security breaches, we have constructed a weighted scoring system based on the severity of adverse impacts that an organization has experienced. The purpose is to provide a single score that indicates how deeply an organization has been impacted due to a cyber security breach.

Weighted Scoring:

- Death of a worker or disciple is the most severe adverse impact and is scored as a 10, for both the impact on the family and colleagues of that worker, and the organization and ministry work as a whole.
- Imprisonment of a worker is scored as an 8, for the impact on the worker, their family, the organization and ministry work as a whole.
- Loss of organizational reputation is scored as an 8, for the broad impact on an organization in recruiting, fund raising and field operations
- Shut down of a ministry or program is scored as a 7, for the impact on the local ministry and the loss of resources invested in the work by the larger organization.
- Arrest and harassment of a worker is scored as a 5, for the impact on the worker, their family and the local ministry.
- Expulsion of an expat worker is scored as a 5, for the impact on the local work and the larger organization.
- Lost time and resources are scored as a 3, as it represents the least impact on the workers and the work of an organization.

Maximum Adverse Impact Score:

1. Death of national worker – 10 points
2. Death of expat worker – 10 points
3. Imprisonment of national worker – 8 points
4. Imprisonment of expat worker – 8 points
5. Loss of organizational reputation – 8 points
6. Shut down of ministry program – 7 points
7. Arrest or harassment of national worker – 5 points
8. Expulsion of expat worker – 5 points
9. Lost time and resources – 3 points

The total is 64 points for a maximum adverse impact score.

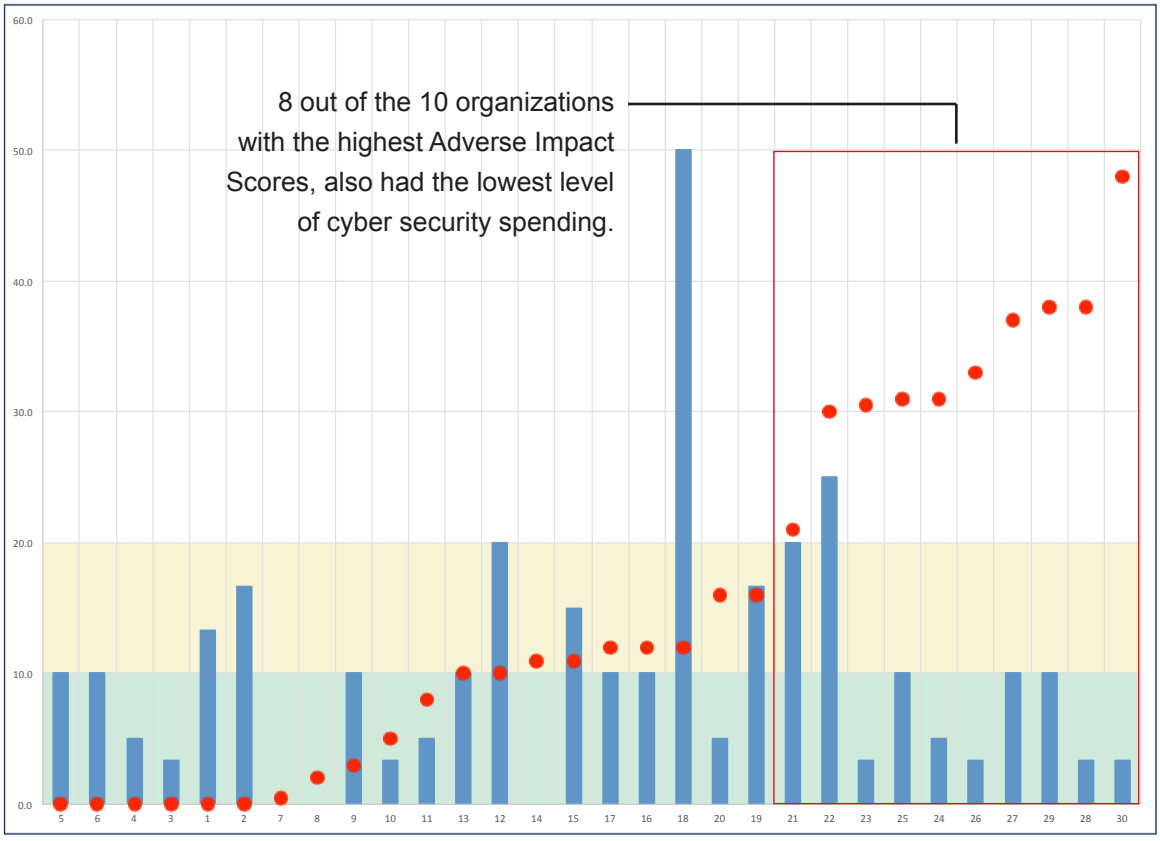
Because “not sure” responses represent possible impact, those were scored at 25% of the category score to capture the impact load for an organization.

After initial scoring, the data was reviewed to determine whether or not those organizations with low scores actually represented highly adverse impacts. For example, if an organization with a total score of 10 – which would be considered “low” over all – had reported a death due to a cyber security breach (a score of 10), this would indicate that the scoring system was actually down-grading the impact of that death. Review of the data showed that the scoring system was rational and was not downgrading or hiding highly adverse impacts.

The scored data fell into three main groupings:

Scores less than 10 – **low level** of adverse impact (9 respondents)
Scores of more than 10 but less than 20 – **medium level** of adverse impact (11 respondents)
Scores above 20 – **high levels** of adverse impact (10 respondents)

Adverse Cyber Impact vs. Relative Funding for Cyber Security



This graph represents the relationship between the Adverse Impact and the Cyber Security Funding Level. The vertical blue columns represent the amount of money spent on cyber security in proportion to the size of the organization. The red dots represent the Adverse Impact Score for the organization. The higher the Adverse Impact Score, the worse the result for the organization. The taller the vertical column, the more that was spent on cyber security. For data points with no column, the organization did not disclose Cyber Security Funding levels.

The horizontal lines represent both Relative Cyber Security Funding levels and Adverse Impact Score. A ranking of 10 or below is the lowest level of funding – where small organizations that spent $25K or less received a 10, medium-sized organizations with that level of spending received a 5, and large organizations with that level of spending received a 3. A ranking of 10 or below for Adverse Impact Score (shaded green) is a low level of adverse impact. A ranking between 10 and 20 (shaded yellow) is a moderate Adverse Impact Score. A ranking above 20 (not shaded) is a high Adverse Impact Score.

The most striking result from this graph is the following: 8 out of the 10 organizations with Adverse Impact Scores above 20 (see red box), also had the lowest level of relative cyber security spending.

Not all organizations with low cyber security spending had high levels of adverse impact, but **80% of those organizations with the highest levels of adverse impact had the lowest level of cyber security spending**.

CURRENT STATUS OF CYBER SECURITY PROGRAM

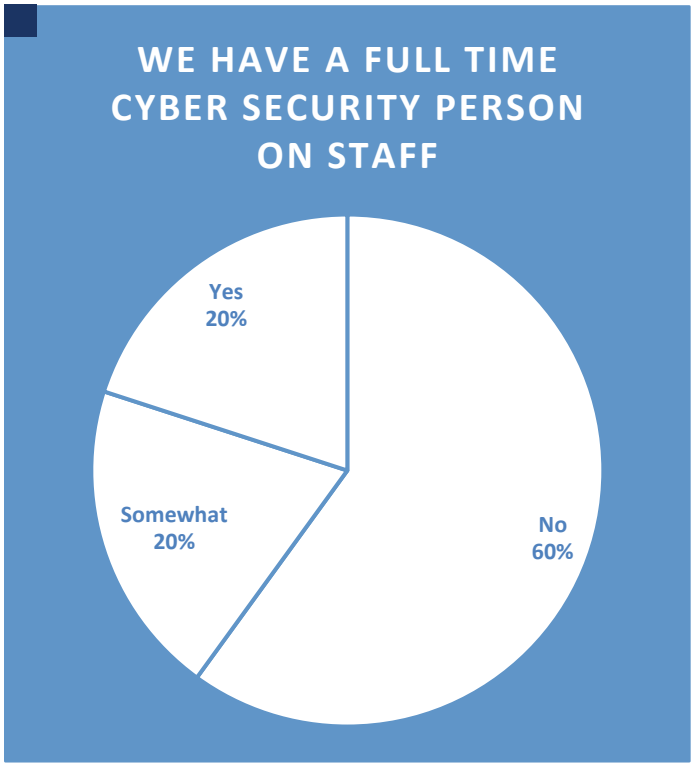
Five questions were asked to gain an understanding of the current cyber security programs utilized in the missional organizations:

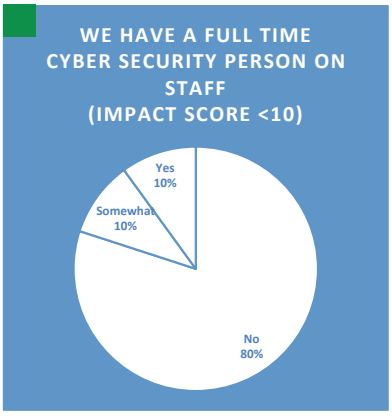
1. Do you have a full time cyber security person on staff?
2. Do you have a cyber security advisor or consultant?
3. Have you conducted a cyber security risk assessment?
4. Have you implemented a cyber security risk reduction plan?
5. Have you implemented a cyber security risk reduction training for staff?

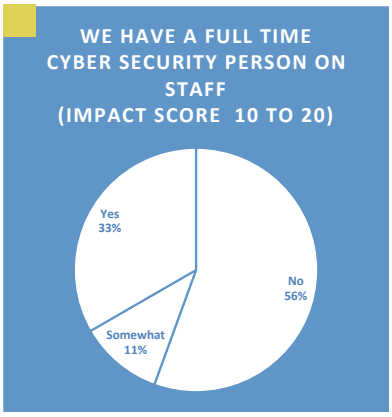
Responses were Yes, No and “Somewhat.” The “Somewhat” answer was allowed to capture partial efforts or informal relationships. For example, an organization may not have a full time cyber security professional on staff, but they may have someone part time in that role or at least have a staff member with cyber security as part of their job description.

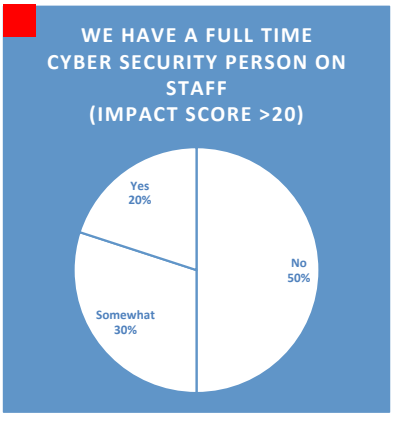
Following are the responses from the responding missional organizations.

CURRENT STATUS OF CYBER SECURITY PROGRAM: Question #1







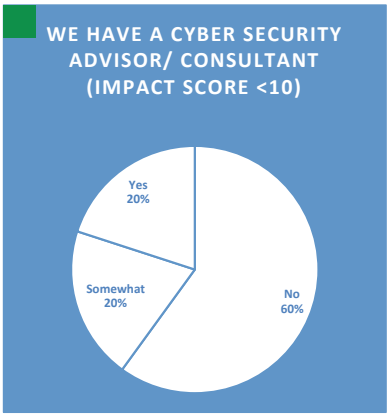


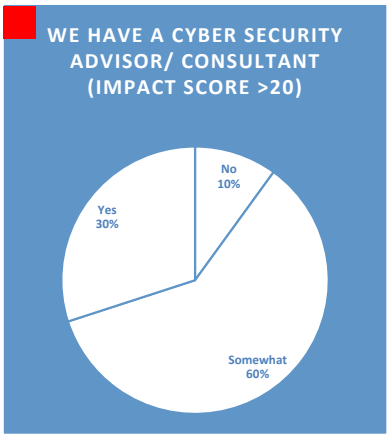
In response to the first question, 60% of all r - spondents reported that they did not have a full time cyber security professional on staff. Interest- ingly, large organizations (with more than 500 staff members) had only a slightly higher rate, with 50% reporting that they did not have a full time cyber security professional on staff.

When we break out the responses to this question based on the Adverse Impact Score, we find that those organizations with moderate scores (10 to 20), were more likely to report they had a full time cyber security professional on staff.

Low Impact Score
Medium Impact Score
High Impact Score

CURRENT STATUS OF CYBER SECURITY PROGRAM: Question #2

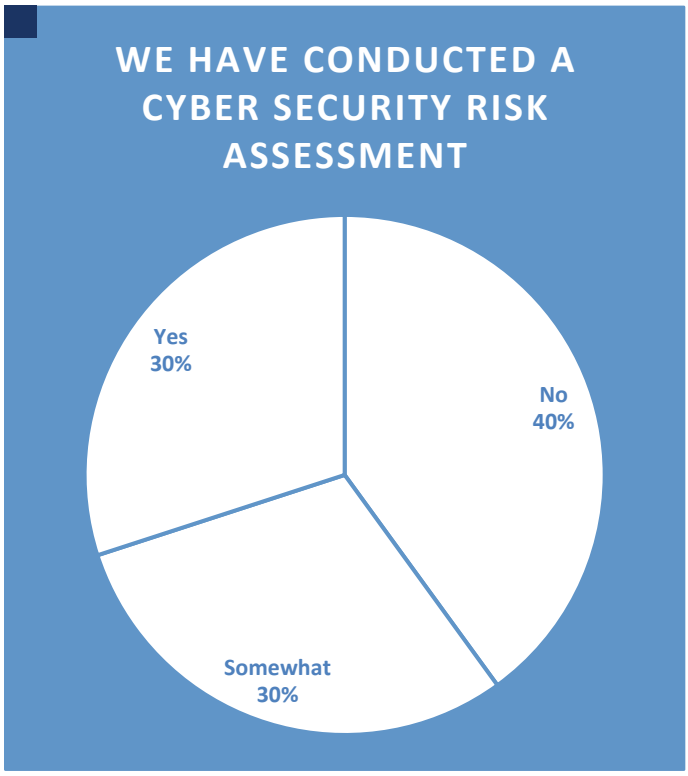


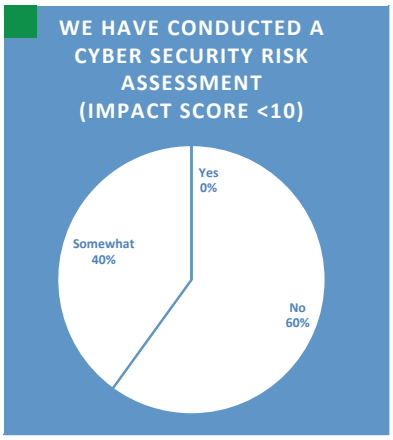


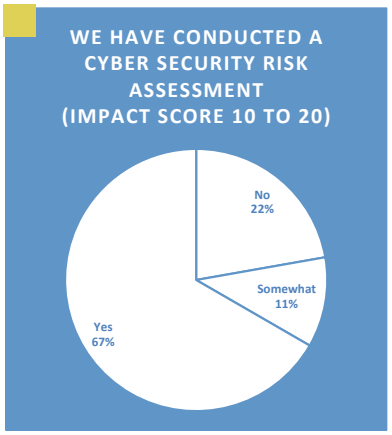
In response to the second question, 77% of all respondents said they had some type of cyber security advisor or consultant. However, when we break out the responses based on Adverse Impact Scores we get a very different picture. Among those organizations with moderate scores (10 to 20) almost 90% said that they definitely had a cyber security advisor or consultant. In contrast to this, among the organizations with the highest levels of Adverse Impact Scores, only 30% reported that they definitely had an adviso . Of those organizations with the lowest scores, 60% reported that they did not have an advisor. In the previous question about full time cyber security staff, 80% of these organizations reported that they did not have full time staff.

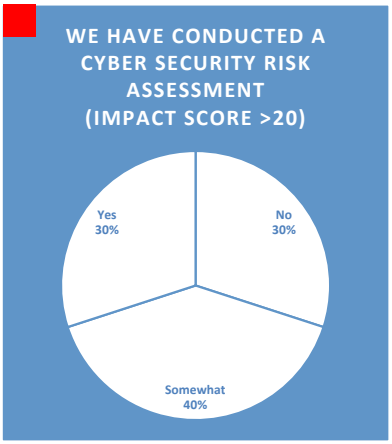
Low Impact Score
Medium Impact Score
High Impact Score

CURRENT STATUS OF CYBER SECURITY PROGRAM: Question #3







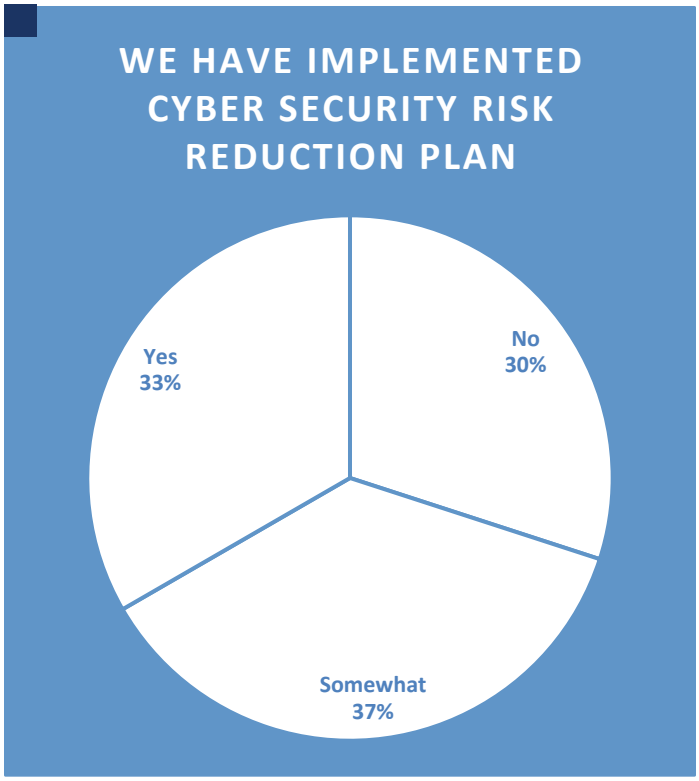


For the third question, 60% of all respondents indicated that they had done some type of cyber security risk assessment and 30% saying they had definitely conducted an assessment. Some 40% of organizations reported that they had not done any risk assessment at all.

Breaking out the results based on Adverse Impact Scores, those organizations with mid-level impact scores (10 to 20), 67% reported a definite cyber risk assessment rate, which is 37% higher than the average rate. Among those organizations with the highest Adverse Impact Scores, (>20), only 30% of entities reported that they had definitely done an assessment

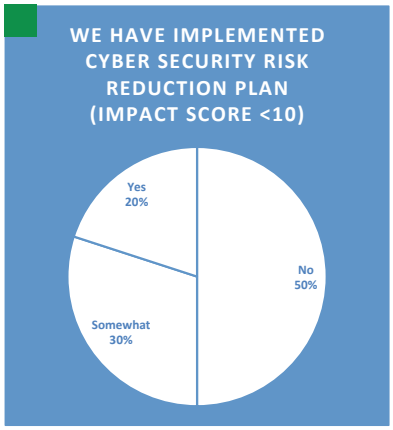
Low Impact Score
Medium Impact Score
High Impact Score

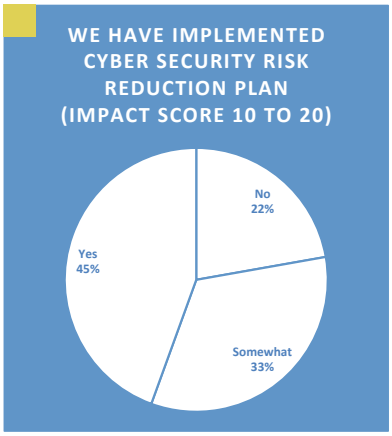
CURRENT STATUS OF CYBER SECURITY PROGRAM: Question #4

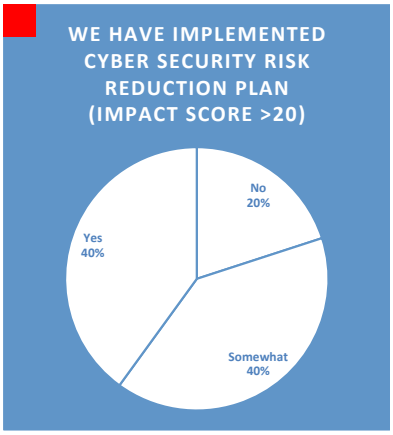


On question four, some 70% of respondents reported that they were implementing some type or cyber risk reduction plan. This was 10% more than those who reported having a cyber risk assessment.

When breaking the results out by Adverse Impact Scores, organizations with mid-level and high levels of adverse impact reported a nearly 80% rate for implementing some type of cyber risk reduction plan.





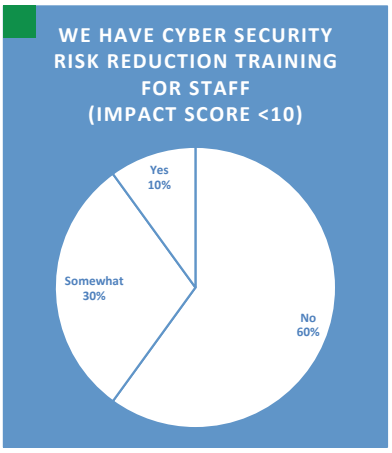


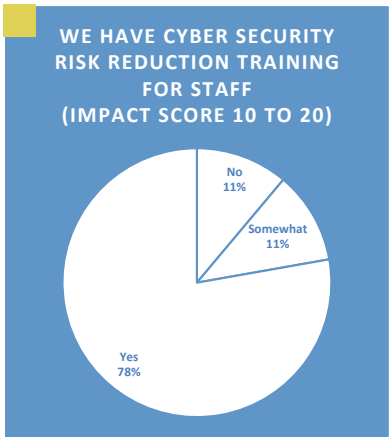
Low Impact Score
Medium Impact Score
High Impact Score

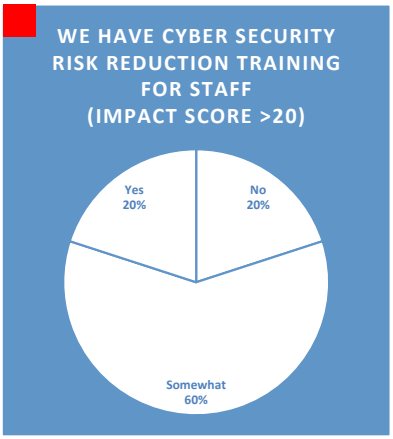
CURRENT STATUS OF CYBER SECURITY PROGRAM: Question #5

On question five, 70% of all respondents reported some type of cyber risk reduction training.

When we break out the results based on Adverse Impact Scores, we find that 78% of organizations with mid-level scores reported having definitely implemented cyber risk reduction training for staff. This is more than three times the level (20%) reported by those organizations with high adverse impact scores.







Low Impact Score
Medium Impact Score
High Impact Score

In analyzing the response to the five questions, it was important to break out the results by Adverse Impact Scores to get a more accurate picture of the importance the organizations place on cyber security.

For those organizations with low Adverse Impact Scores, it appears that cyber security is a low organizational priority as the majority did not have cyber risk assessments, cyber risk reduction plans or training. These organizations are therefore at risk of highly adverse cyber security breaches. It is also possible that these organizations have undetected cyber security breaches and unrecognized adverse impacts.

For organizations with mid-level Adverse Impact Scores, cyber security appears to be a high priority as almost 80% reported having cyber risk reduction training, almost 70% reported having a cyber risk assessment, and almost 90% reported having a cyber security advisor or consultant. The only gap in this reporting was in the development of a cyber risk reduction plan, with less than 50% reporting definite plans.

Overall, the data suggests that these organizations are aware of negative impacts, have invested in assessment and mitigation and are seeking to improve their risk profiles. In the case of organizations with high levels of Adverse Impact Scores, the profile is dominated by the response “somewhat.” This appears most strongly when comparing the results of organizations with mid-level Adverse Impact Scores and those with high Adverse Impact Scores.

Cyber Risk Mitigation	Mid-Level Score Response	High Level Score Response
Cyber Security Advisor	“Somewhat” 11%	“Somewhat” 60%
Cyber Risk Assessment	“Somewhat” 11%	“Somewhat” 40%
Cyber Risk Training	“Somewhat” 11%	“Somewhat” 60%

Because the “somewhat” answer indicates a partial or incomplete action as opposed to a “yes” response, it appears that those organizations with high Adverse Impact Scores are less engaged with cyber security issues than the organizations with Mid-Level Adverse Impact Scores. This might be explained in a couple of ways. The first would be that organizations with high Adverse Impact Scores are “playing catch up” in the face of multiple breaches. As this survey is a snapshot in time, these organizations might be much more focused on their cyber risk in a few months.

The second possibility is that the leadership of these organizations are not well informed – or do not take seriously – the adverse impacts that their organization is experiencing. The fact that 8 out of 8 of the organizations with high Adverse Impact Scores (in excess of 30) all have low relative cyber security spending levels, indicates that these organizations are not engaging with their cyber security breach issues in a focused and effective way.

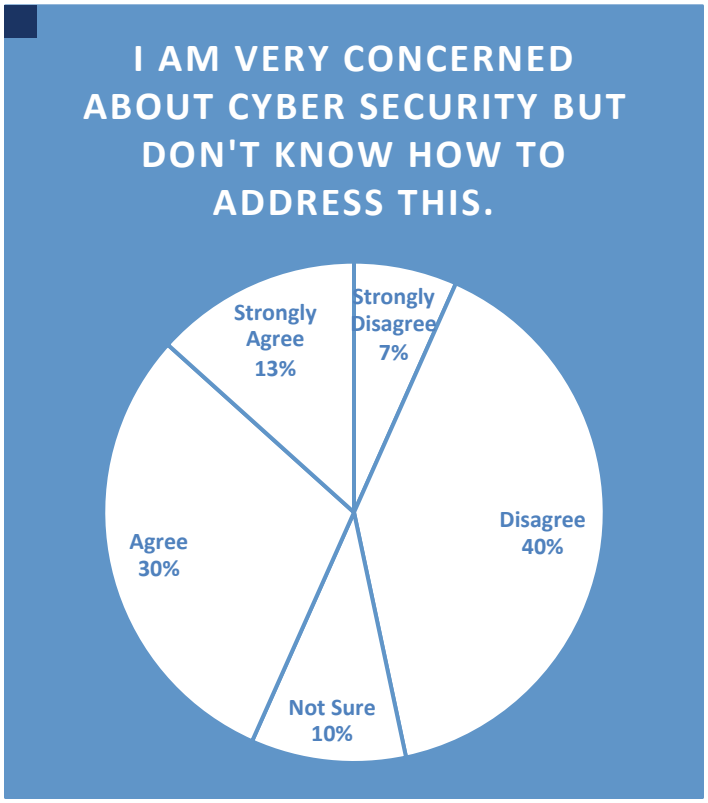
ATTITUDES ABOUT CYBER SECURITY

Six questions were asked that sought to measure organizational attitudes about cyber security risk. These were presented as statements with the response range of Strongly Agree, Agree, Not Sure, Disagree, Strongly Disagree:

1. I am very concerned about Cyber Security but don't know how to address this.
2. Cyber Security is important but not in our top ten list.
3. We lack personnel and specialty knowledge to address Cyber Security risk.
4. Our biggest hindrance to dealing with Cyber Security risk is lack of budget.
5. Cyber Security risk is the last thing I want to talk to a donor about.

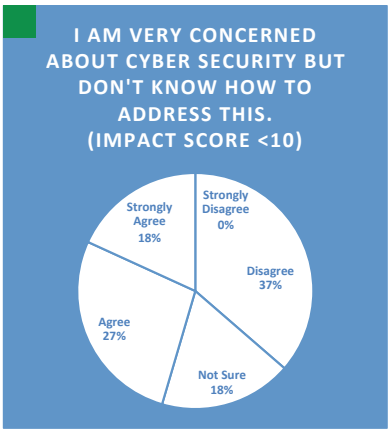
Following are the responses from the responding missional organizations.

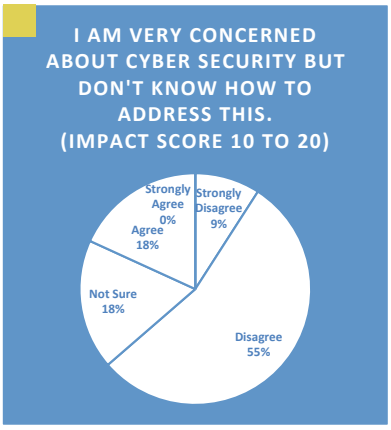
ATTITUDES ABOUT CYBER SECURITY: Question #1

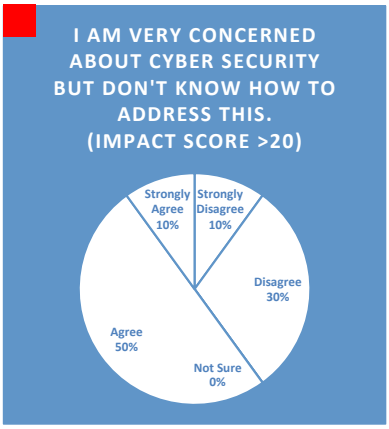


Of all respondents, 43% felt they did know how to address cyber security issues while 47% did not feel they knew how to address these issues.

When breaking responses out by Adverse Impact Scores we find some very important di ferences. Among those organizations with the highest Adverse Impact Scores, 60% felt they did not know how to address their cyber security issues. In contrast, 65% of those with mid-level Adverse Impact Scores (10 to 20) felt they did know how to address their issues. This fits with the trends we found in the last series of questions that appeared to show this group actively engaged in improving their cyber security profile

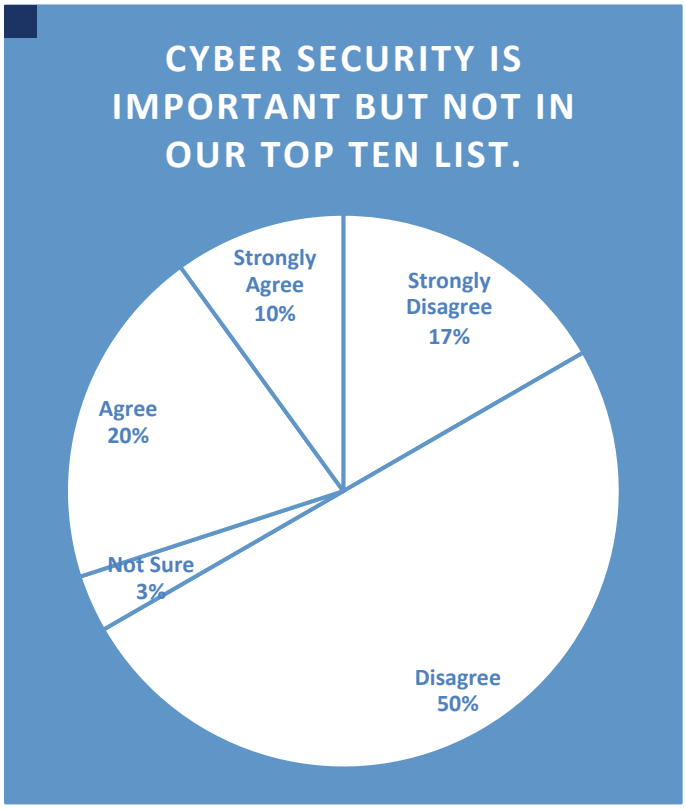






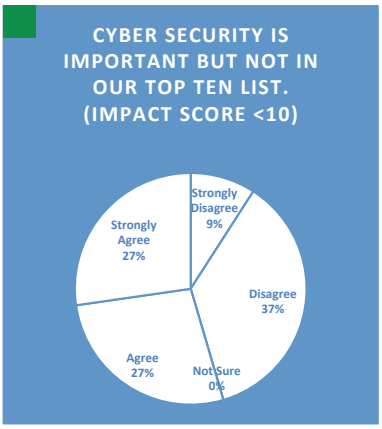
Low Impact Score
Medium Impact Score
High Impact Score

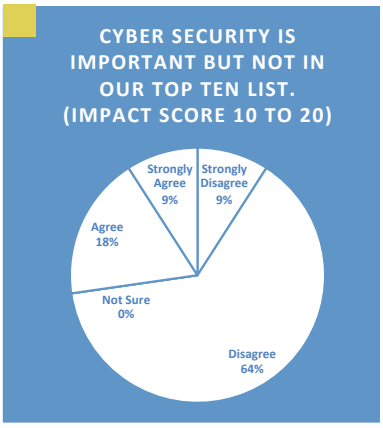
ATTITUDES ABOUT CYBER SECURITY: Question #2

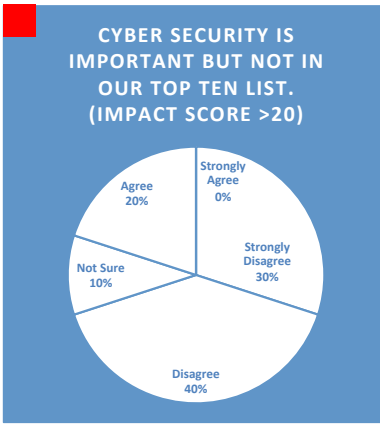


The goal of the second statement is to detect the level of urgency that an organization has about cyber security. Among all respondents, 30% indicated that cyber security was not a high priority.

When we break out results based on Adverse Impact Scores, we find that 54% of those org - nizations that currently experience a low level of adverse impact from breaches do not consider cyber security to be a high priority.

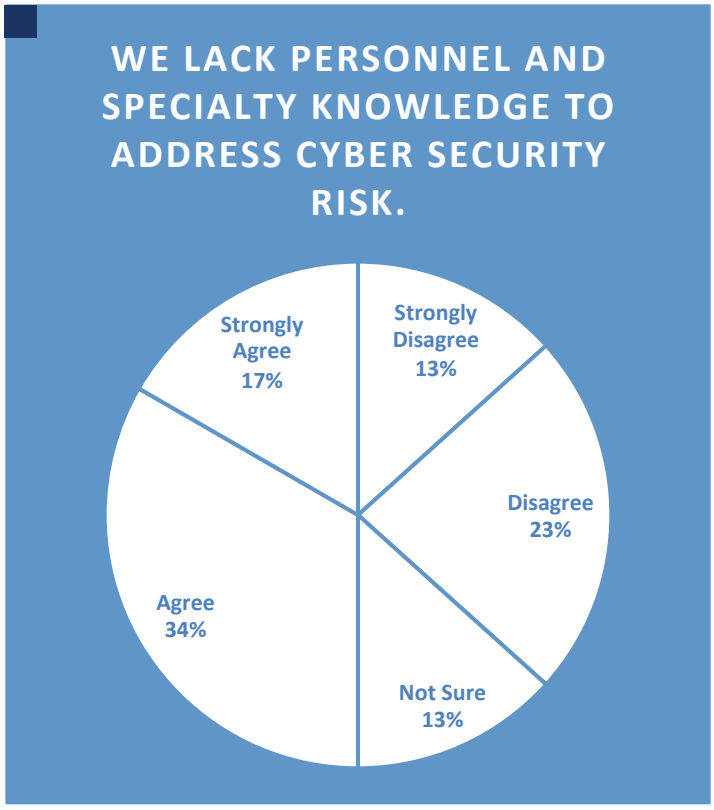






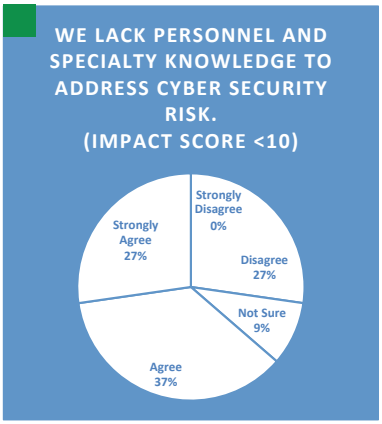
Low Impact Score
Medium Impact Score
High Impact Score

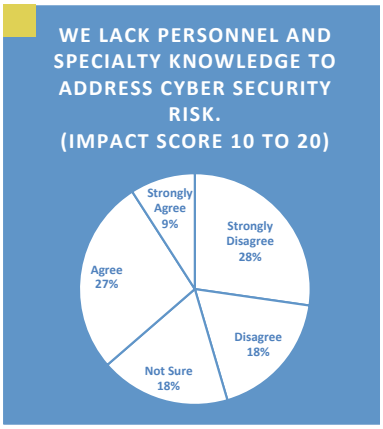
ATTITUDES ABOUT CYBER SECURITY: Question #3

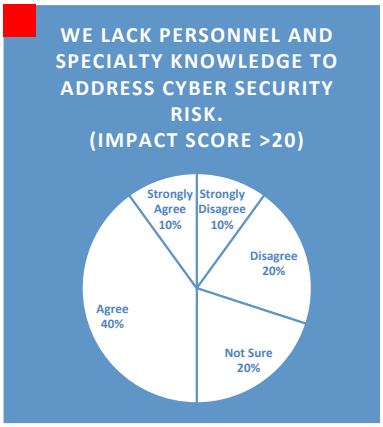


Among all respondents, over 50% felt they lacked the specialty personnel and knowledge to address their cyber security issues.

When breaking out the results based on Adverse Impact Scores, we find that only 36% of those with mid-level scores felt they lacked the specialty personnel and knowledge to address their cyber security issues. This appears to affirm the general finding that these entities are investing in and engaging to address cyber security risk.

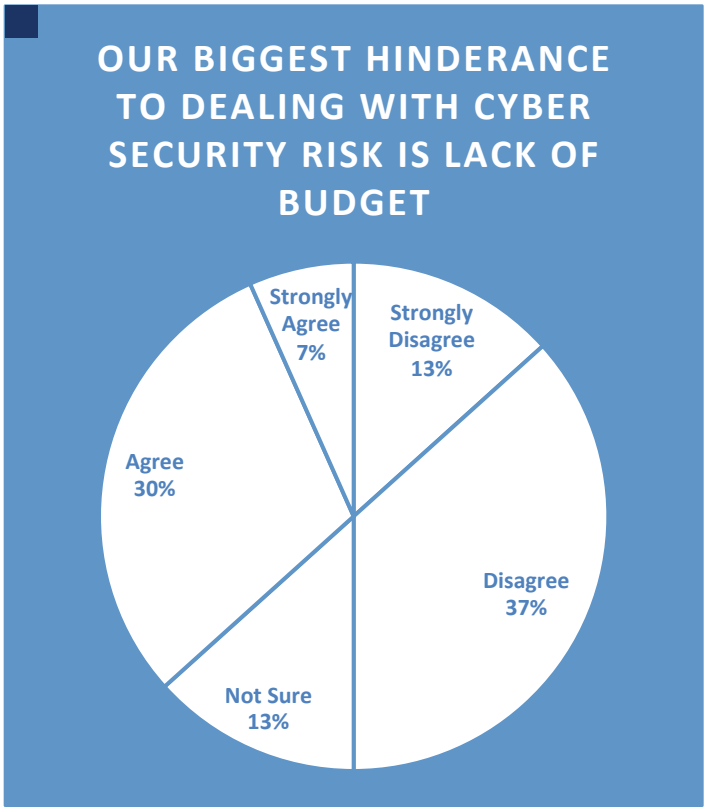






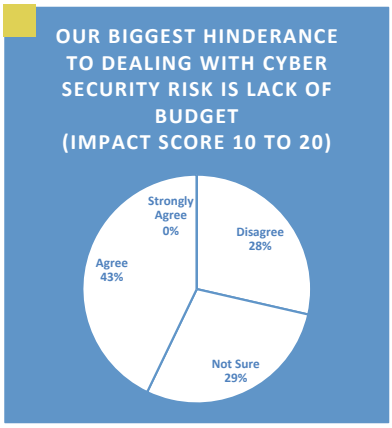
Low Impact Score
Medium Impact Score
High Impact Score

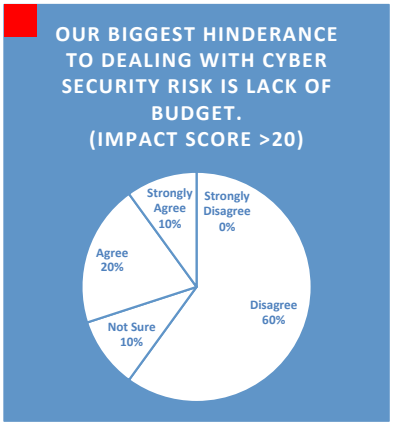
ATTITUDES ABOUT CYBER SECURITY: Question #4



Among all respondents, 50% felt that budget was not the greatest hindrance to dealing with their cyber security issues while 37% felt it was the single biggest challenge.

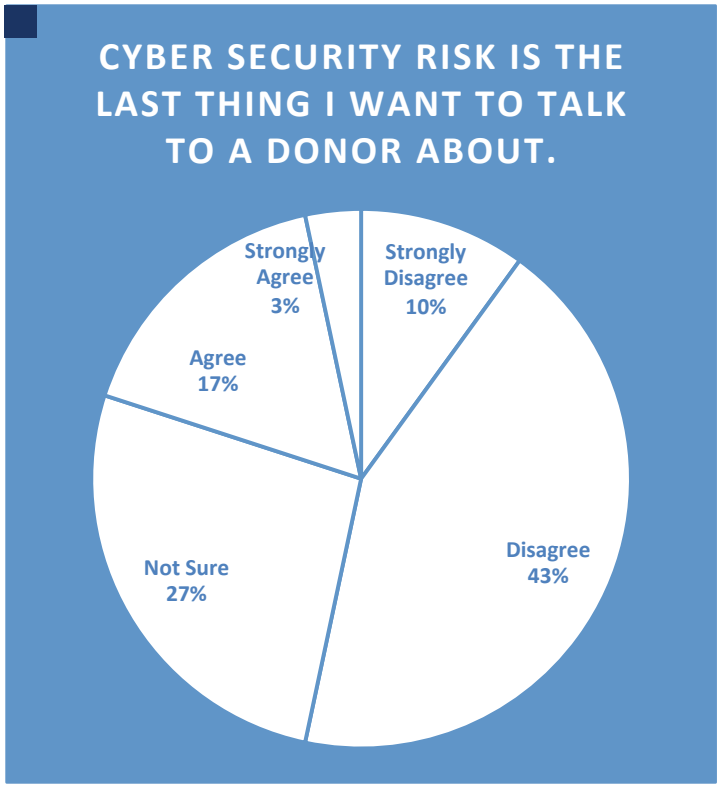
When breaking out the results based on Adverse Impact Scores, 60% of those with high scores (over 20) stated the budget was NOT their biggest hindrance. This group has some of the lowest levels of relative spending for cyber security. This appears to indicate that for these organizations, lack of funding does not control the level of expenditure for cyber security.

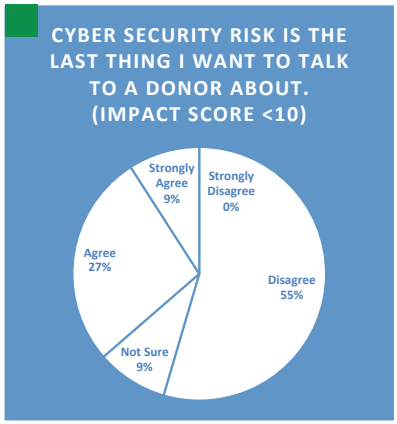


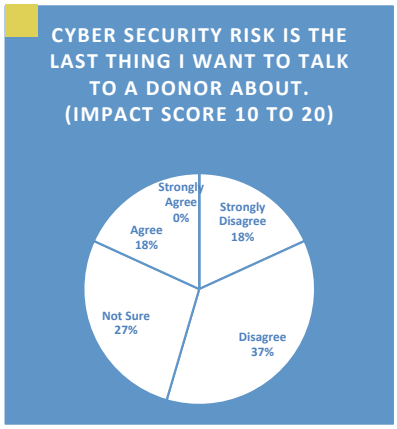


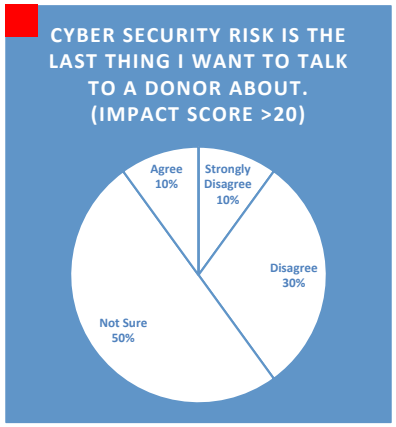
Low Impact Score
Medium Impact Score
High Impact Score

ATTITUDES ABOUT CYBER SECURITY: Question #5





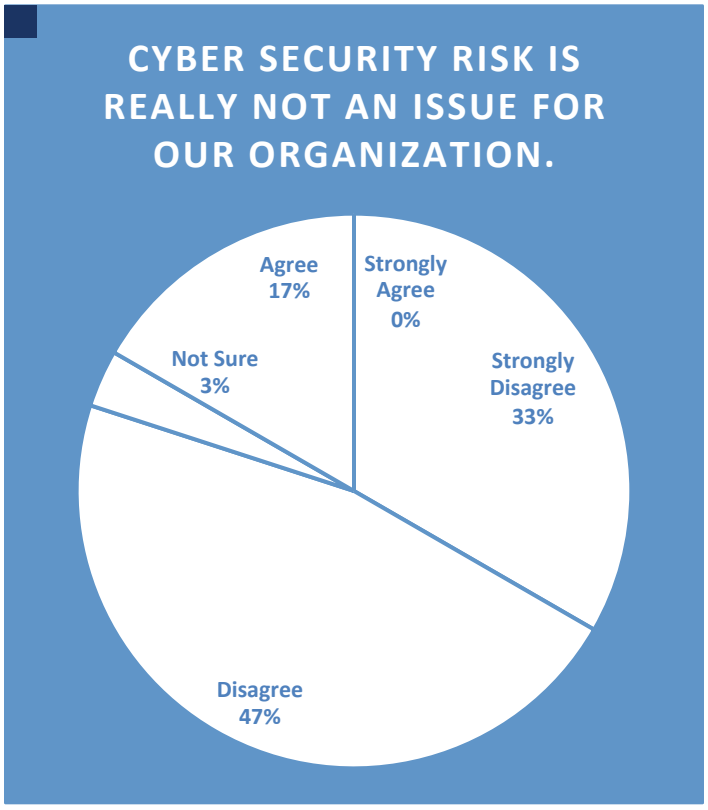




Among all respondents, 20% indicated they did not want to discuss these issues with donors (potentially cutting themselves off from funding for this very area). However, when taking into account "not sure" responses, 47% of all respondents were either unwilling or reluctant. When breaking out results based on Adverse Impact Scores, we found that entities with high scores were the most reluctant. It is worth noting that among those with high scores, they also indicated that budget was not the key factor holding back their response to cyber security needs. Additionally, 60% of this same group also responded that they "somewhat" had a cyber security advisor or consultant. There appears to be a correlation between the reluctance to discuss issues with donors and a reluctance to fully engage with a Cyber Security advisor or consultant.

Low Impact Score
Medium Impact Score
High Impact Score

ATTITUDES ABOUT CYBER SECURITY: Question #6



This statement attempts to capture attitudes about cyber security in general. Among all respondents, only 17% state that cyber security is not an issue for their organization.

When we break out the responses based on Adverse Impact Scores, only 8% of the Mid-level group indicate that cyber security is not an issue for their organization.

Low Impact Score
Medium Impact Score
High Impact Score

CYBER SECURITY ASPIRATIONS

The next set of statements are intended to capture the aspirations of organizations toward Cyber Security. Respondents were asked “Would any of these things help you in dealing with Cyber Security Risk?” The items were:

1. Cyber security risk assessment
2. Cyber security risk reduction plan
3. Cyber security training for technical staff
4. Cyber security training for field sta f
5. Trusted vendors that can help them
6. Funding for cyber security expertise, equipment and software
7. Cyber security network which shares threats and information

Following are the key findings about their cyber security aspirations:

RISK ASSESSMENT

Over 80% of all respondents felt that a Cyber Security Risk Assessment would improve their cyber risk profile

RISK REDUCTION PLAN

Over 80% of all respondents felt that a Cyber Risk Reduction Plan would improve their cyber risk profile

CYBER SECURITY TRAINING

Cyber Security Training for technical staff *and* field sta f was desired by over 70% of all respondents.

TRUSTED VENDORS

63% reported that utilizing Trusted Vendors that could help them would improve their cyber security profile

FUNDING

69% indicated that Funding for Cyber Security Expertise, Equipment and Software would be helpful in improving their cyber security profile

CYBER SECURITY NETWORK

The perceived usefulness of a Cyber Security Network (which shares threats and information) was overall positive with 81% of all respondents indicating this would help them improve their cyber security profile

Overall Findings

The respondents to the survey came from a nearly equal number of small, medium and large organizations. The most important result from the survey was the reporting of adverse impacts due to a cyber security breach. Currently there is no clearinghouse for such reports and typically missional organizations don't publicize these breaches. By computing an Adverse Impact Score for each entity, it was possible to filter the survey results in ways which revealed important insights into current cyber security programs, attitudes about cyber security, and cyber security aspirations of missional organizations – especially those with active work in the MENA region.

Overall, organizations aspire to have good cyber security, yet the clear majority do not currently have good practices in place and about half of the entities appear to feel they lack the personnel, knowledge, budget and strategy to address cyber security. Additionally, about half of the organizations that responded to the survey are unwilling or reluctant to talk to donors about cyber security needs.

When breaking out the data by Adverse Impact Scores, a much more nuanced picture is formed. Each Adverse Impact Score group has a profile that can be helpful in identifying key needs and attitudes.

Low Adverse Impact Group

This group has experienced very few or no known adverse impacts from cyber security breaches. One respondent in this group wrote that they have never suffered a cyber security breach. This group has generally low levels of spending on cyber security and has the lowest level of readiness. Even the bright spot of implementing a cyber risk reduction plan is brought into question when there were no entities that had conducted a full cyber risk assessment.

Organizations in this group aspire to have a good cyber security profile and recognize it as an important issue. They would welcome funding and outside expertise to assist them in improving their cyber security program, and more than half are willing to talk to donors about their needs in this area.

It is not clear if the organizations in this group are aware of the cyber security breaches which may have occurred, as they likely lack the capacity to monitor and report such incidents.

Mid-Level Adverse Impact Group

This group has experienced significant adverse impacts and is actively engaged in i - proving their cyber security profile. They are investing resources in cyber security and do not see outside funding as the key to their success in this area. They appear to have the best level of readiness of any of the Adverse Impact Groups. Most of this group feels it has a strategy, personnel and technical resources to improve their current cyber security status.

High Adverse Impact Group

This group is experiencing the more extreme adverse impacts – deaths, imprisonment, expulsion and shutting down programs. Yet the eight entities with Adverse Impact Scores of 30 or above have the lowest reported level of spending on cyber security. This group also exhibits low levels of cyber security readiness.

Just as with the low Adverse Impact Score group, they report that 40% of the organizations have implemented a cyber risk reduction plan, yet only 30% report having done a full assessment, which brings this response into question.

Most of this group feels that it does not know how to address their cyber security issues, and only 40% feel they have the needed knowledge and personnel to deal with this risk. Most of this group are unwilling or reluctant to discuss their cyber security issues with donors.

Taken together it appears that organizations in this group could benefit from

1. An experienced cyber security advisor.
2. A cyber risk assessment.
3. Cyber risk training.

Due to the extreme level of the Adverse Impacts experienced, it appears there is need for leadership in these organizations to have regular cyber breach and adverse impact reports to assist in prioritizing a response to this critical problem.

CYBER RISK ASSESSMENT

One of the key steps in the process of improving an organization's cyber risk profile i performing a Cyber Risk Assessment. Traditionally, this assessment was focused around a *Vulnerability Assessment.*[103] This type of assessment identifies areas where an organiz - tion *might* be attacked.[104] This results in mitigation efforts that produce best practices that can appear to be disconnected from the core mission of the organization. This can also produce mitigations that don't closely match the actual threats that an organization faces.[105]

An alternative to vulnerability assessment is *Threat Assessment,*[106] which comprises strategies or pathways used to determine the credibility and seriousness of a potential threat, as well as the likelihood that it will be carried out in the future. Performing a Threat Assessment allows an organization to clearly identify threat sources and the risk that each presents to the organization. This makes it possible for the organization to assess which risks are acceptable and where to focus limited resources to gain the best improvement for their cyber security profile [107] Additionally, threat assessments can be granular – having different levels of mitigation depending on the context – even if in the same organization.

A Cyber Threat Assessment as envisioned in this report entails three major components:

1. THREAT PROFILES

Threat Profiles seek to identify who the Threat Actors are and what Actions they will take. These Actors and Actions are not theoretical, but based on the specific work of the org - nization and the Actors who are likely to engage with the organization and what Actions those Actors would take.

2. MITIGATIONS

Technical solutions and behavioral changes that are implemented to mitigate the risk presented in the threat profiles.

3. DIGITAL SAFETY PROFILES

These are contextual and practical profiles that match up specifi Threat Actors and their most likely Actions with the appropriate technical solutions and behavioral changes needed. Digital Safety Profiles are clearly tied to the work processes of the organization. Thus, compliance with the safety profile "makes sense" to sta f members as they can understand the rationale for the mitigations and the importance of the protection offered. These profiles are also tailored for each context within an organization

103 https://en.wikipedia.org/wiki/Vulnerability_assessment
104 https://en.wikipedia.org/wiki/Vulnerability_(computing)
105 Expat Digital Resources, Threat Centric Digital Security, Presentation 2015, p3
106 https://en.wikipedia.org/wiki/Threat_assessment
107 https://www.sans.org/reading-room/whitepapers/auditing/overview-threat-risk-assessment-76

Developing Threat Profiles

Threat Profiles are made up of two components: Threat Actors, and Actions that those Actors may take. The identification of Threat Actors is specific to the work and context of each organization. However, for missional entities working in the MENA region, there are six Threat Actors[108] which can be identified as a starting pl ce for organizations. In the table below, each Actor is matched with potential risk Actions:

Threat Actors	Actions
Opportunistic Criminals	• Opportunistic theft of devices • Opportunistic theft of information • Malicious Software (Malware) • Password Guessing • Social Engineering • Collecting Public Information
Organizational Staff	• Poor Passwords • Use of apps which steal data • Clicking on links on suspect sites and emails • Opening suspect attachments • Careless handling of equipment • Careless handling of sensitive information • Inappropriate use of Social Media • Failure to follow good security practices • Failure to secure servers
The Curious *This is in the field context: Neighbors, Friends, Local Co-Workers, Host Government*	• Overhearing conversations • Passive monitoring of unencrypted email • Passive monitoring of Social Media • Passive monitoring of calls and SMS • Passive monitoring of web usage • Notice use of finances • Notice attitude toward local government and religion
The Suspicious *This is in the field context: Neighbors, Friends, Local Co-Workers, Host Government*	• Eavesdropping on conversations • Active monitoring of unencrypted email • Active monitoring of Social Media • Active monitoring of calls and SMS • Active monitoring of web usage • Scrutinize use of finances • Scrutinize attitude toward local government and religion • Attempts to access accounts
Militant Groups	• Watch for activity that looks like spying • Watch for activity that appears threatening • Watch for activity that is oppositional
State Actors	• Targeted Monitoring • Active Surveillance • Targeted Interventions

108 Expat Digital Resources, Digital Threat Profiles, Presentation, Rev 2016.0

Developing Mitigations

Mitigations to the Actions of Threat Actors are of two types – Behavioral and Technical. Behavioral mitigations are very important, as at least 25% of all cyber breaches are due to human error or negligence.[109] However, in the case of the Threat Profiles for missional organizations in the MENA region, **almost 70%** of the Threat Actions can be eliminated or greatly reduced by behavioral changes.

BEHAVIORAL MITIGATIONS

Behavioral mitigations are focused on organizational staff. Properly training staff, along with compliance and successful implementation, are critical. This will be the single most important factor in cyber risk reduction.

There are two core behavioral areas or mindsets that need development. The first is a SIR Mindset and the second is a Security Mindset. The SIR Mindset involves awareness of context, identity and reputation. The SIR Mindset is of critical importance for field workers. The Security Mindset involves awareness of secure and insecure actions and the impact of those actions.

1. SIR Mindset

SIR stands for Strategic Intercultural Relations.[110] A SIR Mindset involves three key elements:

- **Legitimacy** – Cultivating an appropriate identity
- **Awareness** – Understanding yourself and those around you
- **Respect** – Behavior that leads to an honorable reputation

Two quick negative examples can help:

> Suppose an expat Christian worker is in a country of focus with a local identity as a small business owner. However, this worker seldom seems to attend to their business and seems to have a disposable income several multiples greater than other owners of similar businesses. This worker casually makes jokes about the local religion and political leadership on social media. This worker also seems to have few local relationships.
>
> Suppose a local Christian worker has a local identity as a school teacher. Yet they have a laptop and mobile phone far more expensive than their peers. Somehow they seem to have more money than their peers and they travel internationally once or twice a year for personal reasons in a context where that would be rare. They also have multiple international phone calls and texts to their mobile phone from non-relatives.

109 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute Research Report, p 11
110 Expat Digital Resources, Threat Centric Digital Security, Presentation 2015, p6

When we place these behaviors in our Threat Profile we find that it would incite hig levels of scrutiny and suspicion by The Curious, The Suspicious, Militant Groups and State actors.

A SIR Mindset is not about deception, but rather actions and attitudes that are consistent with an identity within a culture. If there are communications or actions that are part of a Christian worker's purpose – yet would be incompatible with their cultural identity – those should be considered "sensitive information" and handled with a Security Mindset.

2. Security Mindset

A Security Mindset as used in this report consists of two key elements:

- Appropriate actions in response to known threats
- Using an RPD strategy to reduce the risk of "sensitive information"

Appropriate actions in response to known risks involves practices like: not sharing passwords, not clicking on suspect links and attachments, appropriate use of social media, safeguarding equipment, and other baseline behavioral practices.

RPD Strategy

Using an RPD strategy to reduce the risk of "sensitive information" involves three core concepts:

1. **Reduce** – Reduce the amount of "Sensitive Information" you create.
    - Communication Guidelines for how to communicate in this context.
    - Educate partners and constituents about what to communicate to you and about you – drawing from principles of the Communication Guidelines.
    - Know yourself and how you tend to communicate, choose wisely the form of communication and content.
    - Trim Down by reviewing sensitive communication and content and see what you can reduce or eliminate.
2. **Protect** – Protect the Information that you store and share using C3 Method (see Appendix K, L and M for C3 guidelines on VPN's, email, messaging)
    - COVER – to obscure the fact that there is anything to hide. When it is known that there is something of value hidden, scrutiny increases and it becomes much more difficult to keep that information concealed. Cover is tied closely with the SIR principle of Legitimacy – the cover should enable consistent legitimacy, not hinder it. The goal of cover, just like Legitimacy, is to avoid closer scrutiny.

RPD Strategy (continued)

- CONCEAL – If Cover has been compromised, concealment attempts to disguise and encrypt the sensitive information and communication. Concealment, while necessary, is less ideal than cover, because operating under scrutiny is an order of magnitude more difficult.
- COMPARTMENTALIZE - This is the concept that information and communication should be divided such that if it is compromised, it does not expose the entire life of a worker, team and other teams working in the host country or region. When all else fails, compartmentalization helps to limit the fallout.

3. **Detect** – Online Situational Awareness. This attempts to monitor – as close to real time as possible – any information which can compromise personnel or operations. One tool used for this is Google Alerts.

TECHNICAL MITIGATIONS

Technical Mitigations involve a wide range of technical actions – like having a firewall to protect a network and individual machines, using Anti-Virus and Anti-Malware software, hardened network configurations, keeping software and firmware patched and man other interventions.

The following table shows the most important behavioral mitigations, along with whether or not a technical mitigation is possible. It is important to note that in some threat profiles there are no technical mitigations. This table also illustrates that typically *both* behavioral and technical mitigations are needed.

It is critically important to understand that technical mitigations without behavioral mitigations will fail to improve cyber security. As the threat actors become more capable and threatening, behavioral mitigations become more critical for maintaining security.

THREAT PROFILE		MITIGATIONS	
Threat Actors	**Actions**	**Behavioral**	**Technical**
Opportunistic Criminals	• Opportunistic theft of devices	Appr. Actions	Yes
	• Opportunistic theft of information	Appr. Actions	Yes
	• Malicious Software (Malware)	Appr. Actions	Yes
	• Password Guessing	Appr. Actions	Yes
	• Social Engineering	Appr. Actions	No
	• Collecting Public Information	Appr. Actions	Yes
Organizational Staff	• Poor Passwords	Appr. Actions	Yes
	• Use of apps which steal data	Appr. Actions	Yes
	• Clicking on links on suspect sites and emails	Appr. Actions	Yes
	• Opening suspect attachments	Appr. Actions	Yes
	• Careless handling of equipment	Appr. Actions	Yes
	• Careless handling of sensitive information	Appr. Actions	Yes
	• Inappropriate use of Social Media	Appr. Actions	Yes
	• Failure to follow good security practices	Appr. Actions	No
	• Failure to secure servers	Appr. Actions	Yes
The Curious	• Overhearing conversations	SIR+RPD	No
	• Passive monitoring of unencrypted email	SIR+RPD	Yes
	• Passive monitoring of Social Media	SIR+RPD	Yes
	• Passive monitoring of calls and SMS	SIR+RPD	Yes
	• Passive monitoring of web usage	SIR+RPD	Yes
	• Notice use of finances	SIR+RPD	No
	• Notice attitude toward local gov. and religion	SIR+RPD	No
The Suspicious	• Eavesdropping on conversations	SIR+RPD	No
	• Active monitoring of unencrypted email	SIR+RPD	Yes
	• Active monitoring of Social Media	SIR+RPD	Yes
	• Active monitoring of calls and SMS	SIR+RPD	Yes
	• Active monitoring of web usage	SIR+RPD	Yes
	• Scrutinize use of finances	SIR+RPD	No
	• Scrutinize attitude toward local gov. and religion	SIR+RPD	No
	• Attempts to access accounts	SIR+RPD	Yes
Militant Groups	• Watch for activity that looks like spying	SIR+RPD	Yes
	• Watch for activity that appears threatening	SIR+RPD	Yes
	• Watch for activity that is oppositional	SIR+RPD	Yes
State Actors	• Targeted Monitoring	SIR+RPD	Yes
	• Active Surveillance	SIR+RPD	Yes
	• Targeted Interventions	SIR+RPD	Yes

SIR – Strategic International Relations; RPD – Reduce, Protect, Detect

Now that we have a Threat Profile and Mitigations we can build a Digital Safety Profil and develop a scoring system to help us to monitor progress in improving cyber security. Each Digital Safety Profile in this paper builds on the one before. Because of that, the first profile is actually the most critical to put in place as all the others – the more ch - lenging profiles – build upon it

DIGITAL SAFETY PROFILE – BASELINE	
Threat Profile **Opportunistic Criminals & Organizational Staff**	**Mitigations**
Opportunistic theft of devices Careless handling of equipment	Security Cable for laptops – lock down and remote wipe of devices; Full disk encryption of laptops
Opportunistic theft of information Careless handling of sensitive information Collecting Public Information	Sensitive Information – Reduce, know yourself, trim down; Encrypted communication
Malicious Software (Malware)	Anti-Malware; Patch software and firmware
Password Guessing / Poor Passwords	Password Policy; 2 Factor Authentication; Password Manager
Social Engineering	Training
Use of Apps which steal data	Training; Device level App approval
Clicking on links on suspect sites and emails	Training
Opening suspect attachments	Suspect link blocker
Inappropriate use of Social Media	Communication policy; Training
Failure to follow good security practices	Training
Failure to secure servers	Secure Servers, or move to secure cloud services

Once each mitigation(s) has been identified, they should then be listed and scored as to how much progress has been made in each area. This should be updated on a quarterly basis to help staff see the progress being made against goals.

CYBER RISK MITIGATION

One of the greatest challenges faced in implementing a cyber risk mitigation program is the question of where to start.

In our survey we found that respondents fell into 3 categories:

- **Small** – Organizations of less than 50 people (usually highly distributed and without a central computer network)
- **Medium** – Organizations of 50 to 500 people (often has a central computer network – at least in the main office
- **Large** – Organizations over 500 people (usually has a central IT infrastructure)

Clearly there is no “one size fits all” solution for cyber risk mitigation. Howeve , we will present possible approaches for each category of organization. For each one, the goal is to provide a starting place that is sound and as low cost as possible. In the previous section, we developed a Baseline – Digital Safety Profile – that identified base level threat and mitigations. The baseline profile is central to all other profiles Therefore, effort and resources invested in this profile will improve the cyber risk level of any organization.

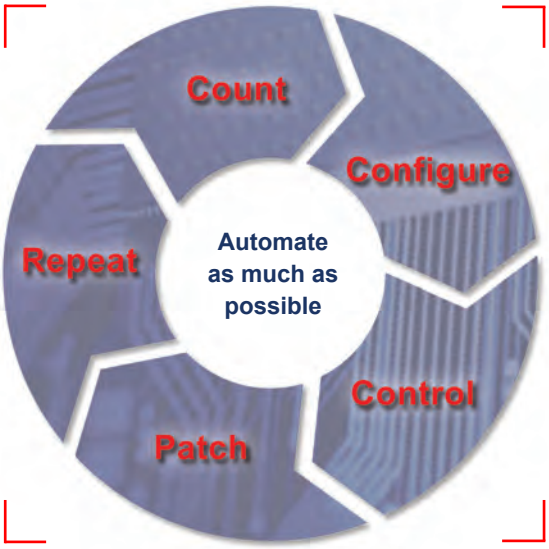
The SANS Institute has produced a guide for cyber risk mitigation that is called Center for Internet Security Critical Security Controls (CSC). However the full CSC[111] can be overwhelming for an organization just starting a cyber risk mitigation program. To focus on early “wins” that any organization can benefit from, the Center for Internet Security has launched a National Campaign for Cyber Hygiene[112] that focuses on the first five Critica Security Controls as the starting point.

NATIONAL CAMPAIGN FOR CYBER HYGIENE

Five core questions that all organizations should be able to answer:

1. Do we know what is connected to our systems and networks? (CSC 1)
2. Do we know what software is running (or trying to run) on our systems and networks? (CSC 2)
3. Are we continuously managing our systems using “known good” configur - tions? (CSC 3)
4. Are we continuously looking for and managing “known bad” software? (CSC 4)
5. Do we limit and track the people who have the administrative privileges to change, bypass, or over-ride our security settings? (CSC 5)

111 See Appendix C
112 https://www.cisecurity.org/cyber-pledge/



These questions can be further summarized by five key words that identify the main actions that need to take place (and to automate this process as much as possible):

- **Count**
- **Configure**
- **Control**
- **Patch**
- **Repeat**[113]

While these five Critical Security Controls are the most common ones that are recommended, to achieve the Baseline Digital Safety Profile these will need to be supplemented with the following

1. Security cable for laptops
2. Full disk encryption for laptops
3. Password manager software (see Appendix E for recommended products)
4. Security policies
    - Password policy (see model policy in Appendix G)
    - Communication policy (see model policy in Appendix F)
    - Sensitive information reduction (see model in Appendix I)

While the above actions are certainly more helpful than the full list of 20 core CIS Critical Security Controls, the actual implementation of mitigations can present a bewildering array of technologies that need to be evaluated, cost compared and then implemented. Also, cyber security staff can cost between $75,000 - $175,000[114] a year. To reduce cost and complexity, there are suggested paths forward (starting on page 60) for small, medium and large organizations to reduce cyber risk.

MOBILE DEVICES

Mobile devices dominate most organizations and present a prevailing security risk. In the recommendations that follow in this section of the report, the focus is on tools that lock down phones and prevent the installation of unapproved apps. They also allow leadership to remotely wipe the device of someone who is arrested or their device is stolen. We also recommend services that proxy all web browsing, allowing an organization to set content

113 https://www.sans.org/security-resources/posters/special/20-critical-security-controls-55
114 https://gooroo.io/analytics/skill/CISSP/#

access policies as well as block the activation of malware links that may be inadvertently clicked on by users.[115]

There is one recommendation that we can make to entities of any size regarding mobile, and that is migrating to iOS devices for greater security. In 2015, it was widely reported that 97% of malware for phones was targeted at the Android platform / apps.[116] In 2016, there were some well reported exploits for iOS, but these were mitigated quickly.[117] iOS phones don't provide perfect security, but they are much more secure than stock Android phones.

INTRUSION MONITORING

The widely reported penetration of the U.S. Office of Personal Management shows that having a well-funded cyber security program – with full-time cyber security professionals – does not assure cyber safety.[118] Continuous monitoring for intrusion is required to give assurance that systems are indeed safe. This type of monitoring is called Network Security Monitoring (NSM). NSM requires specialized software and specific technical skills to set up and monitor. One of the vetted vendors in Appendix E provides this service for missional organizations. However, this expense is often outside the budget of small organizations. To meet this need, a new low-cost service is in development by Expat Digital. This new service is expected in Q4, 2017. Inquiries can be sent to info@expatdigital.com.

SECURE SOCIAL CHAT

There is an abundance of social chat apps that claim to be secure. This often presents a confusing landscape for missional organizations, as the consequences of insecure communications can be imprisonment or even death. At this time, there are only two social chat apps that were recognized by the Electronic Frontier Foundation as reliably secure – Signal and WhatsApp.[119] However, the Signal app is generally associated with social change advocates[120] and it not widely used. Therefore, as of the date of this report, the pervasive WhatsApp would be our single recommendation for secure social chat.

SECURE CLOUD STORAGE

A number of organizations now share team resources on group cloud storage. However, this storage is often not encrypted – and even if it is – there can be other issues that put the information at risk, or the identity of those using it at risk. There are two services we recommend for secure cloud storage: https://spideroak.com, an audited and certified supplier, and https://tresorit.com, a very promising competitor.

115 http://info.publicintelligence.net/DHS-FBI-AndroidThreats.pdf
116 https://www.scmagazineuk.com/updated-97-of-malicious-mobile-malware-targets-android/article/535410/
117 http://www.zdnet.com/article/the-state-of-mobile-device-security-android-vs-ios/
118 https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/
119 https://www.eff.org/secure-messaging-scorecard
120 https://www.wired.com/2016/10/signal-cypherpunk-app-choice-adds-disappearing-messages/

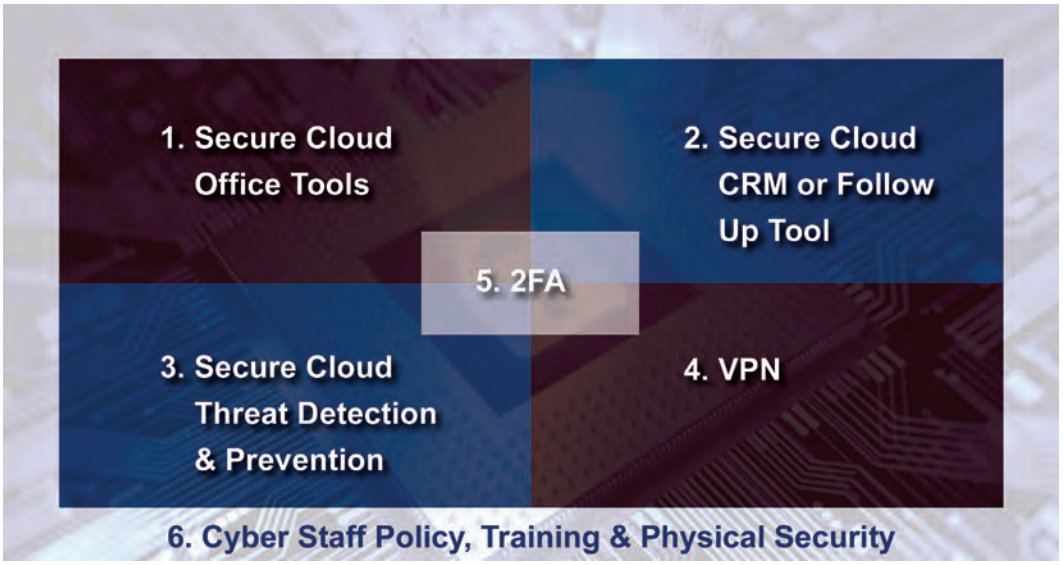
Cyber Risk Mitigation for Small and Highly Distributed Groups

About one-third of the organizations that participated in our survey had less than 50 staff members. Such organizations typically have tight budgets and seldom have dedicated IT staff. They are often highly distributed and do not have a central server infrastructure. They also tend toward BYOD (Bring Your Own Device) for most endpoints (laptops, tablets and phones) in their organization.

This profile presents five core problems for developing a cyber risk mitigation strateg

- Resource constraints
- Low level of IT support
- No centralized infrastructure to leverage for automating controls
- Securing one endpoint does not scale across the organization
- Lack of training for staff members on security processes and procedures.

To address these problems, we propose that small and highly distributed entities implement a secure cloud-based workflow and cloud-based security tools, along with physical security changes and policy implementations. This approach has six main elements:



1. SECURE CLOUD OFFICE TOOLS

The two main options are Google G-Suite and Microsoft Office 36 Live.[121] Both of these systems have SSL protected access to online resources and data, and have granular group policies that allow control over how access is used and how data is shared. In using these tools, the vast majority of documents created reside on the secure cloud, yet allow

121 Amazon WorkSpace is another potential solution, however at the time of this report there was not enough independent information to add it to our recommendations.

local work without access to the internet. This moves the concentration of sensitive data away from endpoints (laptops, tablets and phones) and concentrates them in the secure cloud.

G-Suite Option

G-Suite or Google Suite is a cloud-based service offered by Google for businesses. The suite includes email, calendar, internal communication tools (both audio and video), documents, spreadsheets, custom forms, presentations, internal websites and file storage. These services differ from the consumer apps, in that Google provides privacy and security guarantees for G-Suite clients.[122] G-Suite also allows users to benefit from Google security research and professionals. G-suite was designed to work with the low-cost Chromebook[123] computer, which has a custom operating system (Chrome OS) that is constantly updated against virus and malware attacks. G-Suite also provides a Mobile Management[124] app that allows protection of all mobile devices in an organization (including BYOD), and incorporates a centrally-managed remote wipe. For organizations with full or part time IT staff, G-Suite offers an organizational control panel. For those without IT staff, a registered service provider can supply needed support remotely and very cost effectively.

Standard Chromebooks can be purchased for $200 - $300 each, and present a lower risk of theft than standard laptops. The Business Suite of G-Suite is $10 a month per user,[125] and provides the needed security controls for in-house IT staff. If an organization lacks IT staff, a registered service provider or reseller can provide the support required remotely.

For a small and distributed organization the G-suite with a Chromebook – and using the Mobile management app – would cover the core issues addressed in the CIS five core requirements, and is an affordable and scalable solution.

122 https://support.google.com/work/answer/6056693?hl=en&ref_topic=6055719
123 https://www.google.com/chromebook/9 https://www.google.com/intl/en_uk/chromebook/about/
124 https://gsuite.google.com/products/admin/mobile/
125 https://gsuite.google.com/pricing.html

Office 365 Option

Microsoft Office 365 o fers a comprehensive set of tools for any size office – inclu - ing MS Word, Excel, Power Point, Skype for Business, SharePoint, Voice and Video calling, file storage and many other office tools The Enterprise Level 5 Package comes with the control panels needed to have admin and central security control for all users. Microsoft also offers Enterprise Mobility + Security that provides for mobile security and control.

MS Office 365 works on normal PCs and laptops that are more expensive than the average Chromebook. Also, normal PCs and laptops are subject to a range of intrusions that are much less common on the Chromebook. However, MS Office 365 Services can be used in a mixed environment with existing Microsoft Server networks. This allows organizations that already have a network – which is critical to their central office operations – to continue to use that, while flexibly increasing thei security profile. They can utilize Office 365 for those areas that do not need to access the central office network

MS Office 365 is more expensive than G-suite. The Enterprise Grade E5 service is $35 per user per month, plus $8.75 a month for Enterprise Grade E3 for Mobility + Security, for a total of $43.75 per month per user. For a staff or 50 people, this would be $2,187.50 a month. This is much less than the cost of a full time IT person, and certainly less than a staff security person.

However, Microsoft offers a discounted license to religious organizations that are not churches, but are registered 501c3 entities. This make it possible to acquire the license for Office 365 Enterprise E5 for $10 per user per mont [126] and the Microsoft Mobility + Security E3 is available for $1.65 per month per user[127] at the time of this report. This takes the price to $11.65 per month per user – which is quite close to the G-suite pricing. An organization can apply for religious[128] and non-profit pricing through Techsoup,[129] a non-profit organization that helps on-profits get free and discounted software.

126 https://products.office.com/en-us/nonprofit/office-365-nonprofit-plans-and-pri
127 https://www.microsoft.com/en-us/philanthropies/product-donations/products/enterprise-mobility
128 Microsoft has a non-discrimination policy that must be adhered to in order to qualify for reduced price and free software. However, currently Microsoft recognizes that religious entities are exempt from non-discrimination policy. This means that an organization that holds to a Biblical view of gender expression, for example, would be eligible for discounted and free software.
129 http://www.techsoup.org

2. SECURE CLOUD CRM OR FOLLOW-UP TOOL

Most mission organizations in this study are engaged in evangelism, discipleship and church planting. To support this focus, they need some way to keep track of personal details about people they are engaging. Many organizations will use Salesforce or some product built upon Salesforce. For end users, Salesforce can be accessed through a browser. Therefore, it can be accessed on a Chromebook running Chrome OS as well as on a PC or a Mac. This makes it possible for a small and distributed team to utilize a core technology in a secure cloud-based approach.

For organizations that need a distributed secure cloud-based solution for follow-up, ECHO[130] is designed to be browser-based and works very well on a Chromebook. It allows follow-up volunteers to engage those responding to ministry, without giving the volunteers access to the organization's internal network.

3. SECURE CLOUD THREAT DETECTION & PREVENTION

For small and distributed groups, it is difficult to have central antivirus and malware protection. However, new cloud-based services like Webroot[131] make it possible to have key security tools across a distributed organization that are centralized. Webroot provides three core offerings that would be very useful for small and distributed organizations:

WEBROOT® Smarter Cybersecurity

- **Endpoint Protection** – this is for computers and it protects against virus, malware and emerging threats to your computer.
- **Mobile Security** – this provides security similar to the Endpoint security but for mobile devices.
- **Secure Web Gateway** – this is a service that allows an organization to have all web browser usage done through the Webroot cloud-based system, providing for the deployment of web use policies, and monitoring usage. Additionally, the secure web gateway protects users who click on emails that take them to cyber-attack sites (and offer cyber-attack downloads), which are a major cause of security breaches.

  Webroot Endpoint Protection is not compatible with Chromebooks running Chrome OS, and is seen as unnecessary by the security model of Chrome OS. However, Webroot Endpoint Protection would be compatible with Office 365

130 https://www.echoglobal.org
131 https://www.webroot.com/us/en/business

Webroot Mobile protection would have overlap with both G-suite Mobile and Office 365 Mobility + Security, but it would function without conflicts. Testing would need to be conducted to see if there is any security gain from "doubling up" Webroot Mobile Security and the mobile security offerings by Office 365 and G-suite.

Webroot Secure Web Gateway is compatible with Chromebooks running Chrome OS as well as PC and Mac platforms. This would be a good tool to implement organizational web usage controls and a critical layer of protection from phishing attacks.

Webroot Endpoint Protection costs $25 per user per year. Non-profit pricing is avai - able, but has to be negotiated directly with Webroot sales. Webroot Mobile Protection is $15 per device per year, and this is much more expensive than the G-suite Mobile Security and Office 365 Mobility + Securit , which are licensed by user rather than device. Again, non-profit pricing is available but has to be negotiated directly with Webroot sales. Webroot Secure Web Gateway is $33 a year and also has non-profit pricing.

4. VPN – VIRTUAL PRIVATE NETWORK

Virtual Private Network (VPN) software can provide an encrypted path from an endpoint machine (computer, tablet or mobile phone) to another endpoint. That second endpoint can be a private server owned by the ministry – in which case it would be a closed private connection – or it can be to a server owned by a third party that provides access to the Internet. This second use is now a very common way to protect mobile endpoints (laptops, tablets and mobile phones) from having their web traffic monitored or hijacked when using public Internet access. VPNs can also allow users to bypass firewalls of countries that seek to limit access to online resources, and it protects the user from having their Internet usage monitored. However, not all VPNs are secure. This is especially true for third-party VPNs used to access the Internet. Third-party VPNs can log your Internet usage, sell your personal details (and browsing history), or push ads to you while using the system. Some third-party VPNs are free to use to the end-user, while others charge monthly or yearly fees. For the purpose of this study, we are primarily focused on the use of VPNs to avoid having Internet access monitored or hijacked.

There are a large number of third-party VPN services and it can be very difficult to dec - pher the sales jargon to compare vendors. A good resource for an independent evaluation of VPNs is: thatoneprivacysite.net[132] Once a VPN has been chosen for an organization, it should be installed on all mobile endpoints (laptops, tablets and mobile phones).

132 https://thatoneprivacysite.net/choosing-the-best-vpn-for-you/

It should be noted that Chromebooks with Chrome OS do allow VPN usage, but they only work with a limited number of VPN products. Therefore, is it important for those using Chromebooks with Chrome OS to confirm that their VPN of choice will work with that platform.

5. 2FA TWO FACTOR AUTHENTICATION

Two Factor Authentication or Multifactor Authentication uses more than a single password to access an Internet resource. The second factor is often a security code that is generated by a stand-alone device[133] or special mobile app.[134] The web resource requires that you provide the correct password and a time-limited secure token to gain access.

Some implementations of 2FA have used SMS to the phone of the user to provide the time limited token, however this has proven to be subject to attack by countries that control the national telecom.[135] Therefore, it is wise to avoid SMS-based 2FA.

G-Suite, Office 365, and many other secure cloud services support 2 A. It provides a significant layer of protection and helps to assure that only the authorized user is acces - ing a resource.

6. CYBER STAFF POLICY, TRAINING & PHYSICAL SECURITY

For the purpose of this study, we will be handling baseline policies, training and physical security under this heading. Core model policies for passwords and communication are provided in Appendix F and G. Cyber security training has typically been expensive and not very well focused on the needs of ministries. It has also been difficult to deliver the training to a distributed workforce. However, a new online cyber security training service for religious non-profits, Expatdigital.com [136] is offering an introductory rate of $25 a year per household, with volume pricing for organizations (see Appendix E). This cloud-based service can provide the ongoing training needed to mitigate the human risk factor that untrained staff present. To round out the baseline profile, the most critical physical security component is a laptop cable lock.

By implementing all six of the above components, a small and distributed organization can greatly improve their cyber risk profile and establish a cost-e fective foundation on which to build future improvements.

133 https://www.rsa.com/en-us/products-services/identity-access-management/securid/hardware-tokens
134 https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2
135 https://citizenlab.org/2015/08/iran_two_factor_phishing/
136 https://expatdigital.com

COST ESTIMATE FOR IMPLEMENTATION

G-Suite Option

- G-suite for 50 staff @ $10.00 per month or $500 a month and $6,000 a year.
- Chromebooks for 50 staff @ $300 each is $15,000, one time cost.
- The ECHO CRM/Follow-Up solution is $475 a month for 5 concurrent users with a $1,995 set up fee, for a first year cost $5,700 + $1,995 = $7,695
- Webroot Gateway for 50 staff is $1,650 a year. Multi-year discounts available.
- Computer lock for 50 staff @ $20 each is $1,000.
- High quality VPN for 50 staff @ $132 a year each is $6,600 (assumes totally distributed staff).
- Cyber Security Training with Expat Resources for 50 staff @ $25 a year is $1,250 for the first year and $500 a year thereafte .

Labor

- Once implemented the system must be monitored. It is estimated that this would take a staff network admin about 5 hours a week on average (or 1/8 of a network admin's time) at an average salary of $77,000 a year. This would come to $9,235 a year of admin time.

Total cost for 50 Staff: $38,595 first year cost
Total cost for 50 Staff: $19,850 each year afterward

Office 365 Option

This option assumes the use of existing computers.

- Office 365 E5 + Mobile Security (non-profit pricing) for 50 st f @ $11.65 a month or $139.80 each a year ($6,990 for all 50 staff).
- The ECHO CRM/Follow-Up solution is $475 a month for 5 concurrent users with a $1,995 set up fee, for a first year cost $5,700 + $1,995 = $7,695
- Webroot Endpoint protection (for computers) for 50 is $1,380 a year for the group.
- Webroot Gateway for 50 staff is $1,650 a year.
- Computer lock for 50 staff @ $20 each is $1,000.
- High quality VPN for 50 staff @ $132 a year each is $6,600 (assumes totally distributed staff)
- Cyber Security Training with Expat Resources for 50 staff @ $25 a year is $1,250 for the first year and $500 a year thereafte .

Office 365 Option (continued)

Labor

- Once implemented the system must be monitored. It is estimated that this would take a staff network admin about 5 hours a week on average or 1/8 of a network admin's time at an average salary of $77,000 a year. This would come to $9,235 a year of admin time.

First Year Cost: $35,800
Second Year Cost: $32,055

Cyber Risk Mitigation for Medium-Sized Groups

In our survey, about one-third of the respondents were from medium-sized organizations (50 - 499 people). In this group, one organization that reported the highest level of negative consequences due to cyber breach, spends more than $250,000 a year on cyber security. The organization that reported the second-highest level of negative consequences spends less than $25,000 a year. While it was outside the scope of this study to determine what type of attacks each organization was experiencing, it would be likely that the first organization has good basic cyber risk mitigation practices in place and is subject to targeted attacks, while the second organization likely has few cyber risk mitigation practices in place.

The best starting place is implementing the first 5 CIS Critical Security Controls and adding Cyber Staff Policy, Security Training and Baseline Physical Security (see Appendix F, G, H and I for model policies). For an organization that does not have a lot of key resources for their members on an internal network, moving towards G-suite with mobile security or Office 365 with Mobility + Security could greatly improve their security profile However, if an organization already has a central server configuration, then securing that server infrastructure and all the end points (computers, tablets and phones) that access those servers would be the most important next step.

A practical – yet very helpful – approach is proposed in a study[137] that identified the same key elements as the National Campaign for Cyber Hygiene, but in the context of a small business implementation. This study weighs various technologies with an eye to cost control and ease of implementation / maintenance and provides a "cookbook" (SBI Cookbook) for implementation.[138]

The SBI Cookbook assumes that most small to medium-sized businesses will have a Microsoft Windows Network. If that is not the case, the SBI Cookbook will still be of use, but it will need to be supplemented with other tools and skilled advice. A recommended vendor list can be found in Appendix E.

For organizations that are MS Windows Network centric, the following tools were used in the SBI Cookbook to implement the five Critical Security Controls that are the foundation of every cyber risk mitigation program. These tools are not the most sophisticated but were selected for their low cost and ease of use, while providing solid performance.

- **Spiceworks**[139] – Inventory tool to perform an automated inventory of a network including the software installed on each machine. This can also be set up to monitor all the mobile devices and installed software on those devices as well when used in conjunction with the MaaS360 app. Cost: Free – ad supported
- **OpenSSH**[140] – (for accessing Linux-based systems) – provides remote login with the SSH protocol. Cost: Free (open source)
- **MaaS360 app**[141, 142] – provides security control for mobile devices, both Android and iOS. Cost: $18 a year per device.
- **Microsoft Security Compliance Manager (SCM)**[143] – provides centralized security baseline management, a baseline portfolio and has customization capabilities. Cost: Free
- **Windows Deployment Services (WDS)**[144] – enables remote deployment of Windows operating system and also supports custom images. Cost: Free
- **Microsoft Deployment Toolkit (MDT)**[145] – provides a unified collection of tools, processes and guidance for automating desktop and server deployments. Also offers improved security and configuration management. Cost: Fre

137 Small Business Implementation of the Critical Security Controls – Cookbook Style.
138 See Appendix A and B
139 http://www.spiceworks.com/free-pc-network-inventory-software/
140 http://www.openssh.com
141 https://play.google.com/store/apps/details?id=com.fiberlink.maas360.android.contro
142 https://itunes.apple.com/us/app/maas360-for-ios/id459732007?mt=8
143 https://technet.microsoft.com/en-us/library/cc677002.aspx
144 https://technet.microsoft.com/en-us/library/cc771670(v=ws.10).aspx
145 https://technet.microsoft.com/en-us/windows/dn475741.aspx

- **Group Policy (GP)**[146] – feature built into the Active Directory Domain Services (AD DS) and allows centralized configuration control across all Windows PCs that are a - tached to the AD DS. Cost: Free
- **Enhanced Mitigation Experience Toolkit (EMET)** – EMET helps protect against new and undiscovered threats even before they are formally addressed through security updates or anti-malware software. Cost: Free
- **Windows Server** – Cost: $882 standard price[147] (non-profit pricing available through TechSoup,[148] $66)
- **Kaspersky Endpoint Security for Business (Select)**[149] – $21.99 per user for one year for 200 licenses (non-profit pricing available through negotiation with sales)

While these tools are low cost, they are not all free and there is also the cost of the hours needed to set up and manage the system once in place. Organizations that have a staff IT person should be able to put this cyber risk mitigation plan in place with mostly internal resources. However, it is a good idea to contract with an outside cyber security professional for review and advice (see Appendix E for recommended vendor list). By far, the largest cost involved will be the hours of skilled labor to install and configure the tools recommended in the SBI Cookbook.

A key concern of organizational leaders is how much time will it take to implement the cyber risk mitigation plan? That really depends on several factors:

- Size and complexity of the network
- The number of devices that have to be configure
- Whether or not the organization is currently using active directory
- How experienced the IT staff or consultant is with these tools
- How much troubleshooting is required to get the system in place.

Any Cyber Risk Mitigation project will have at least three main phases:

- Phase I – Implementing the CSC1 – CSC5 Controls
- Phase II – Monitoring, updating and tweaking the system
- Phase III – Cyber security training for staff.

While it is nearly impossible to predict the full cost involved – due to the number of factors that are unique to each entity – an estimate has been calculated for an organization with

146 https://technet.microsoft.com/en-us/library/hh147307(v=ws.10).aspx
147 https://www.microsoft.com/en/server-cloud/products/windows-server-2016/default.aspx
148 http://www.techsoup.org/search/products/microsoft%20server/
149 https://www.cdw.com/shop/products/Kaspersky-Endpoint-Security-for-Business-Select-subscription-license-re/2938515.aspx?

200 people that each have one mobile device. This organization would have a central IT center and have its own network server running MS Windows Server.

COSTS PHASE I:

Software

- Kaspersky Endpoint Select – 200 licenses - $4,400 per year
- MaaS360 – 200 licenses - $4,000 per year
- Spiceworks – Free
- MS Windows Server - $890 (but non-profit pricing is lower) per yea .
- MS network tools (EMET, GP,MDT, WDS and SCM) – Free
- Open SSH – Free

Total Minimum Estimated Software Cost Phase I: $9,290

Labor

- For internal IT staff, estimates range from 700 to 1000 hours to implement the Cyber Risk Mitigation plan (SBI Cookbook). This would be 1/3 to 1/2 of a full time IT person for a year. Assuming a network admin salary of $77,000[150] this would come to $25,000 to $39,000 of admin time.
- If an experienced external consultant were engaged it could take 320 hours @ a median cost of $125.00 per hour or approximately $40,000.

Total Minimum Estimated Labor Cost Phase I: $40,000

Total Minimum Estimated Cost for Phase I: $49,300

COSTS PHASE II:

Software

- Renewal - Kaspersky Endpoint Select – 25 licenses - $4,400 per year
- Renewal - MaaS360 – 25 licenses - $4,000 per year
- Renewal - Spiceworks – Free
- Renewal MS Windows Server - $890 (non-profit pricing is lower) per yea .
- MS network tools (EMET, GP,MDT, WDS and SCM) – Free
- Open SSH – Free

Total Minimum Estimated Software Cost Phase II: $9,300

150 https://gooroo.io/analytics/skill/Network_administrator/united-states#

COSTS PHASE II (continued):

Labor

- Once implemented, the system must be monitored, updated and patched to maintain viability. It is estimated that this would take a staff network admin about 5 hours a week on average or 1/8 of a network admin's time at an average salary of $77,000 a year. This would come to $9,235 a year of admin time.
- If an experienced external consultant were engaged it could take 10 hours a month at a median cost of $125.00 per hour or approximately $15,000.

Total Minimum Estimated Labor Cost Phase II: $12,000[151]

Total Minimum Estimated Cost Phase II: $23,300

While it is possible that the cyber risk mitigation plan could be implemented and maintained for less than this, it would certainly be possible for it to cost a great deal more. These estimates are provided as a starting place for planning and budgeting.

The third phase is training and it has typically been expensive and not very well focused on ministry's needs. However, a new online cyber security training service for religious non-profits, Expatdigital.com, is o fering an introductory rate of $25 a year per household, along with volume pricing for organizations.

COSTS PHASE III:

Training

- 250 member licenses for Expat Resources @ $1,500 for the first year and $500 each year after.

Labor

- 1 hour a week to manage the process at ~$2,000 a year

Total Minimum Estimated Cost Phase III: $3,500 a year

151 Average of staff admin cost and consultant cost

Cyber Risk Mitigation for Large-Sized Groups

In our survey, about one-third of the respondents were from large-sized organizations (greater than 500 people). Of these large organizations, 55% reported spending less than $25,000 a year on cyber security. Additionally, all of the large organizations that reported they had a project shut down due to a breach in cyber security, also spend less than $25,000 a year. And, 80% of the large organizations that reported arrests, imprisonment and possible deaths of workers, spent less than $25,000 a year on cyber security.

> ***Organizations that were poorly funded and staffed reported almost all of the negative outcomes.***

Our study, with one exception, shows a dichotomy between the poorly funded and staffed cyber security efforts, and the well funded and staffed cyber security efforts. The organizations that were well funded and staffed, reported almost no negative outcomes for cyber security breaches. Those that were poorly funded and staffed, reported almost all of the negative outcomes for their size category.

There was one area where both groups had negative outcomes, and that was with the expulsion of expat workers. It is likely that these situations may be due more to operational security – like inappropriate social media postings – rather than a cyber security breach of a server or endpoint. This will be addressed in Cyber Security Training.

For those organizations that are well funded and staffed, the additional training of personnel – like that provided by expatdigital.com – could improve already solid cyber risk mitigation programs. For those organizations that are poorly funded and staffed, it appears there is a need to educate organizational leaders about the high monetary, program and human costs that their organizations are experiencing.

While large organizations are more complex to secure – and tend to have a mixed cyber risk profile – the basics are still the same as those for small to medium-sized ones. A focus on the top five Critical Security Controls (along with polic , baseline physical security and cyber security training), are excellent places to start. Even a large enterprise could implement the guidance for small and highly distributed organizations in their remote and field locations, and implement the guidance for medium-sized organizations at their central offices. Certain large organizations will need a cyber security specialist, but that is beyond the scope of this study.

Overall, for organizations that are experiencing significant negative outcomes due to cyber security breaches, even moderate first steps can greatly improve the e fectiveness of the whole organization, and the safety of their staff and partners.

COST ESTIMATE FOR IMPLEMENTATION

Office 365 Option

This option assumes the use of existing computers. At this volume, additional discounts can usually be negotiated.

- Office 365 E5 + Mobile Security (non-profit pricing) for 1,000 st f @ $11.65 a month or $139.80 each a year and $139,800 for all 1,000 staff (ask for volume discounts –there are significant discounts when asked for individually)
- The ECHO CRM/Follow-Up solution is $900 a month for 9 concurrent users with a $1,995 set up fee, for a first year cost $10,800+ $1,995 = $12,795
- Webroot Endpoint protection (for computers) for 1,000 is less than $25,096 (ask for volume discount for lower price).
- Webroot Gateway for 1,000 staff is less then $28,884 a year (ask for volume discount for lower price).
- Computer lock for 1,000 staff @ $20[152] each is $20,000.
- High quality VPN for 1,000 staff @ $132[153] a year with hubs and individual users, 200 licenses @ $132, for a total of $26,400.
- The cost of training with Expat Resources for 1000 people is $5,000 the first year and $1,500 a year thereafter. Labor: 4 hours a week to manage the process at ~$8,000 a year in labor cost. Total Estimated Training Cost: $13,000.

Labor

- Once implemented the system must be monitored. It is estimated that this would take a staff network admin about 30 hours a week on average or 3/4 of a network admin's time, at an average salary of $77,000 a year. This would come to $57,750 a year of admin time.

Total First Year Cost: $ 323,725 a year
Total Second Year Cost: $298,235 a year

This breakout does not cover servers and services for a large organization.

152 https://www.amazon.com/Kensington-64068F-MicroSaver-Laptop-Business/dp/B00000K4KH
153 http://www.jungl.me/#pricing

Conclusion

Overall, it is clear that Cyber Security is a serious issue for missional organizations. The adverse impacts that are currently being experienced require organizations to raise cyber risk from a technical issue for the IT department, to the leadership of each organization that needs to put in place cyber risk mitigation strategies.

Please note that this is a “point in time” report and the whole area of cyber security is changing rapidly – both in terms of the data, types of risks, and the potential solutions to mitigate this challenge. And while technical interventions are important, they alone will not solve cyber security issues. Appropriate policies and strong cyber security training are crucial to a successful cyber risk reduction program, as addressing staff behavior is the single most important factor to reduce cyber risk.

This report has focused on how to simplify the cyber security process and reduce the cost for missional organizations, no matter the size. Additional resources and more complex solutions and recommendations are located in the Appendix. Media Impact International is also available to provide direction and referrals to address this important area, so that . . .

. . . more people in unreached areas are brought into God’s Kingdom and growing in their faith, through the effective utilization of media.

APPENDIX

A – Small Business Implementation of the CSCS Part 1

B – Small Business Implementation of the CSCS Part 2

C – Critical Controls Poster 2016

D – IBM MaaS360 Bundles

E – Vetted Service Providers

F – Models of Social Media / Communication Policies

G – Model of Password Policy

H – Phishing Training Model

I – Sensitive Information Reduction

J – Survey Questions

K – C3 Guidelines for Email

L – C3 Guidelines for VPN

M – C3 Guidelines for Messaging

N – Additional Country Profiles

APPENDIX A

Small Business Implementation of the CSCS Part 1

Small Business Implementation of the Critical Security Controls - Cookbook Style

November 2013, revised January 2014

Authors:

Josh Brower, Josh@DefensiveDepth.com

Courtney Imbert, courtneyimbert@gmail.com

Carrie Roberts, clr2of8@gmail.com

Abstract

With ever increasing compromises, what can businesses do to protect themselves and their employees? The 20 Critical Security Controls are an industry-recognized list of controls that help businesses better manage their digital risk. Does the priority of these controls change when considering the small business? We explored this question via research and by conducting a survey of security professionals. The top 5 Critical Security Controls for small business are chosen in order to provide the largest risk reductions with the smallest amount of effort. Tools that meet the low cost, low maintenance needs of small businesses are reviewed. The companion document to this paper is a cookbook of specific actions (recipes) that small businesses can take to protect their critical information and assets, based on the 20 Critical Security Controls, including descriptions of low-cost, low-maintenance solutions that address those high-priority controls.

Introduction

According to the Small Business Administration, small businesses employ half of all US private-sector workers (Frequently Asked Questions about Small Business, 2012). More than half of these businesses have had multiple data breaches involving electronic records (Survey Shows Small Businesses Have Big Data Breach Exposure, 2013). The private sector plays the primary role in cyber conflicts, and history has shown that nearly every significant incident has been resolved by the private sector (Healey, 2013). The importance of small business security is clear when we see that the private sector, comprised largely of small businesses, are playing a critical role in cyber security.

What can small businesses do to protect themselves? The 20 Critical Security Controls (CSC) are an industry-recognized list of controls that help businesses better manage their digital risk (20 Critical Security Controls, 2013). They focus on repeatable, automated processes for monitoring, mitigating and updating systems. The National Security Agency (NSA) has prioritized these controls by importance, but are these priorities applicable to small businesses as well as large businesses?

This paper compares and contrasts small and large businesses and the relative importance of the CSCs. The top 5 CSCs for small business are identified through research and a survey of security experts. Included are specific actions (recipes) that small businesses can take to protect their critical information and assets, based on the 20 Critical Security Controls. The focus is on "Quick Wins" that provide the largest risk reductions with the smallest amount of effort. Low-cost, low-maintenance solutions that address those high-priority controls were evaluated, tested, and documented. The result is a "cookbook" to aid small businesses (11-100 employees) in implementing the most effective solutions for the most common information security problems they may face.

Small Business Profile

As defined here, "small businesses" have 11-100 users. "Small business" includes non-profits, but excludes micro- and home-based businesses. Unless stated otherwise, the research referenced in this paper uses this definition of 11-100 users as a "small business" when surveying IT usage. For the sake of creating specific recommendations and recipes, the small business profile we used has a single primary location where most employees work, with at least several employees primarily working remotely some or nearly all of the time with mobile technology solutions.

The authors of this cookbook recognize that small businesses are highly diverse. In order to create a reasonable scope for our illustration of the top 5 Critical Security Controls, we needed to research and create a profile of small businesses. We did this by researching common IT implementations and policies small businesses already have, with a focus on ways small business IT differs from large business. Though we focused on small businesses in the USA, our findings should apply to any small business with a similar profile.

How do small business owners manage IT and information security?

Most SMBs are middle adopters of new IT technology (59%), with the remaining pie split between early and late adopters. The smaller the firm, the more likely it is to be a late adopter (CompTIA, 2011).

At the time of this paper, statistics indicate SMBs may be wary of outsourcing their IT tasks. 70% believe outsourcing IT will increase the chances of a data breach (CompTIA, 2011), which may explain why only 15% outsource their IT (Symantec, JZ Analytics, 2012). 57% have internal non-IT staff handling their support. 23% have internal formal IT staff. 2-6% have IT support handled by a building manager! Once the staff count increases to 100+ people, about 60% of businesses have dedicated, formal IT staff (Symantec, JZ Analytics, 2012).

This means the majority of small businesses have one or more associates that split their attention between two roles, such as IT and accounting. This creates a unique challenge for small businesses, since these employees may not have the time or education to specialize in IT.

What kinds of devices and networking do small businesses use?

66% of small business workplaces have polices that allow employees that use personally-owned laptops for business purposes, and 60% have employees that use personally-owned smartphones for business purposes. 43% have videoconferencing equipment (CompTIA, 2011). Most (67%) of small businesses have employees that use tablet computers, up from 57% one year ago. 85% use smartphones for some component of operations, which is more than double the usage 5 years ago. (AT&T, 2012)

63% of small businesses use locally-housed servers. Only 28% have implemented VoIP hardware (CompTIA, 2011). Nearly all (96%) of small businesses use wireless technology in their operations, with 63% of small business owners indicating it would be a major challenge to survive without it (AT&T, 2012).

How are small businesses similar to larger businesses?

Surprisingly, we found that the security priorities for large businesses and small businesses are the same, and our process for that finding is discussed in section entitled “Top 5 CSCs for Small Business”.

How are small businesses different from medium and larger businesses?

The primary difference between large and small businesses is that small businesses have severely constricted resources to implement information security solutions in three areas: time, money/budget, and expertise. Most large businesses have a dedicated, formal IT staff. Small businesses are much more likely to have an employee in one department, like Finance, with an additional responsibility to manage IT (Symantec, JZ Analytics, 2012). Given that IT management time is often restricted to less than one full-time employee, specialized training or work focus on information security is often limited.

If small businesses can overcome their resource restrictions, they have an advantage in flexibility because of the potential to operate like a “small ship”. Though it is still important to have change management and solid IT policies, changes can often be decided upon, implemented, and controlled through a single level of management and communication, while larger businesses may need more time, people, and formalized processes to implement the same change across the entire organization (Han, 2001).

Small businesses are not as likely to use centralized infrastructure as large businesses, like file servers (CompTIA, 2011). They are less likely to have a website that allows for user interaction by way of

payments or web-based applications, but if they do have a website, it is likely managed in-house. They are also more likely to use email and external sites like Facebook for marketing (Symantec, JZ Analytics, 2012).

Small business owners are less likely than large businesses to list IT security spending as a priority (AT&T, 2012), but counter intuitively, IT security is rated as a top concern (SMB Group, 2012).

Which current trends affect small businesses?

Mobile usage is a major trend that impacts small businesses. Increasingly, there is a demand to use personal devices to access corporate data or work remotely. Wireless networking is almost universally available. A mobile, BYOD, remote workforce may appear tempting for small businesses with low IT budgets, but can become an administration nightmare. (SMB Group, 2012)

Cloud data storage and applications are not widely used among small businesses, but appear poised to grow are likely to grow in popularity. As a result, small businesses may face pressure to integrate legacy apps with the cloud (SMB Group, 2012).

Top 5 CSCs for Small Businesses

The CSCs have been ordered according to their ability to mitigate attacks, but most of the implementation discussions have focused on the challenges faced by large businesses. With this in mind, one of the major questions that we asked about the CSCs is whether smaller businesses prioritize the CSCs the same way larger businesses do. We conducted a short survey that would help shed light on this issue, then focused our cookbook on the highest priority ones.

The primary two questions we asked were:

1. Please select the top 5 Critical Controls you feel would mitigate the most information security risk if they were implemented by a large business (2000+ computers).
   <List of all 20 Critical Security Controls>
2. Please select the top 5 Critical Controls you feel would mitigate the most information security risk if implemented by a small organization (11-100 computers).
   <List of all 20 Critical Security Controls>

We also asked which sized organizations respondents had worked for in the past, and requested open-ended comments on how small business security concerns differ from large organizations.

We sent the survey to the GIAC Advisory Board mailing list which is “made up of GIAC certified professionals who wish to give back to the security community by taking an active role in the GIAC program.” (Certified Professionals: Advisory Board)

We received 19 responses, with the following results for our two key questions:

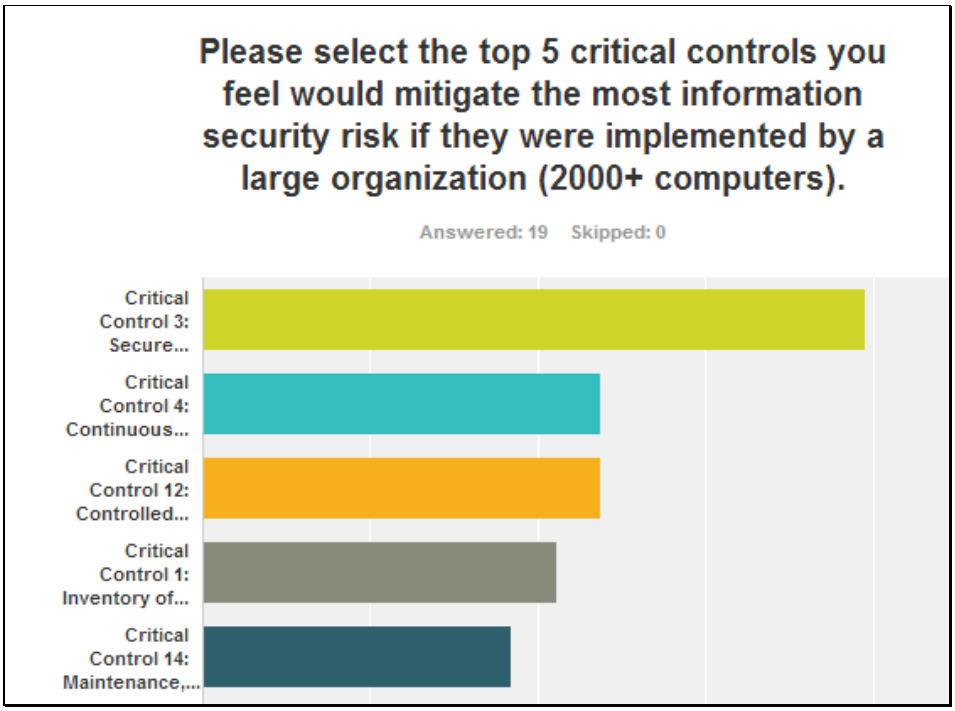


Figure 1 Survey Results for Large Businesses

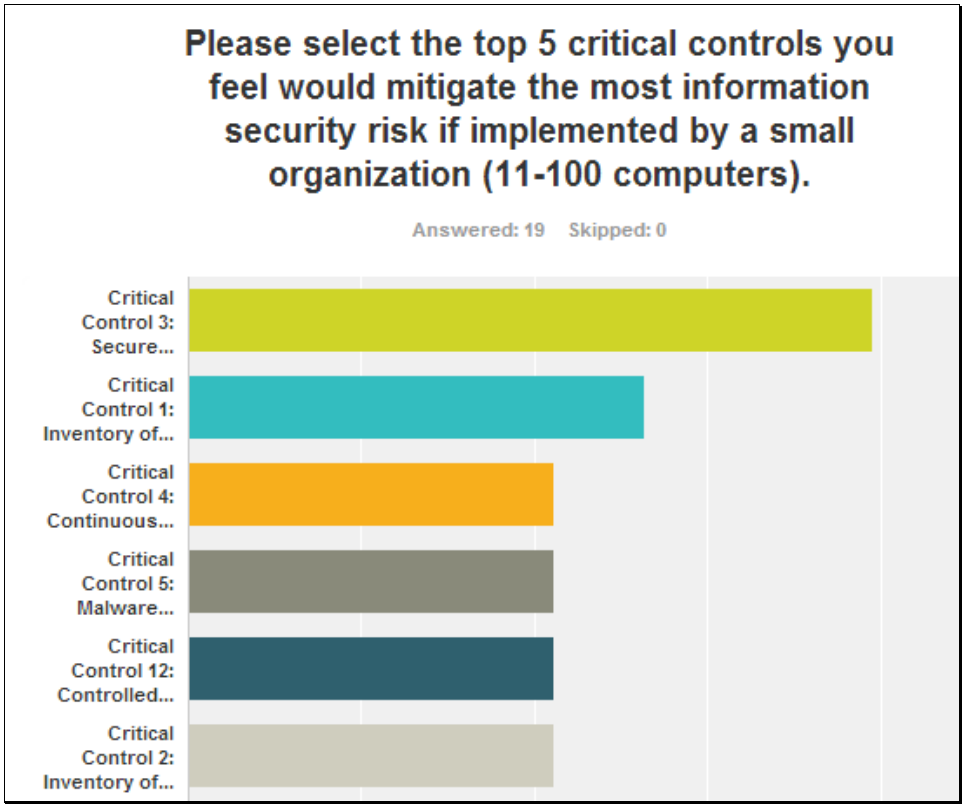


Figure 2 Survey Results for Small Businesses

As shown, the two were very close. The only major difference was that for larger organizations, CSC 14 (*Maintenance, Monitoring, and Analysis of Audit Logs*) landed in the top five, while CSC 2 (*Inventory of Authorized and Unauthorized Software*) was ranked highly for small businesses. We can see how larger organizations would have the personnel resources to implement CSC 14, whereas smaller organizations typically would not have the needed resources to implement it.

With the above results taken into consideration, for the purpose of a small business-focused cookbook, we decided to focus our efforts on the first 5 CSCs; specifically, the Quick Win sub-controls for each CSC.

The Cook Book

This paper is accompanied by a cookbook for implementing the 5 most important CSCs for small businesses, as identified in our survey. Each control has a set of sub-controls, defined as a "Quick Win" in the CSC documentation. Quick wins are considered the most effective means to stop the greatest damage to many businesses (20 Critical Security Controls, 2013). For each sub-control, the cookbook includes a "recipe". The recipes are relevant to small businesses that are primarily using Microsoft Windows for their servers, desktop and laptops, since this is representative of a majority of small businesses. Several sub-controls are extended to include a variety of mobile devices, not limited to a particular operating system. Some recipes include information for Linux servers and laptops as well, but this is not the focus.

A toolset for automating the first 5 CSCs was chosen based on the following criteria. We chose criteria that would make the toolset useful for the majority of small businesses that fit the profile we defined:

1) Low budget for tools
2) Minimal staffing for IT support
3) Primarily using a Microsoft Windows Domain and devices.

The low budget constraint gives heightened consideration for free and open source software or software already included as part of the Windows operating system. In consideration of the minimal staffing constraint, we placed an emphasis on choosing a few tools that can perform a variety of tasks so that learning overhead is reduced. These criteria led to the selection of three primary tools for implementing the first 5 CSCs for small businesses.

The first tool selected was Kaspersky, because it covers many of the quick wins and is low cost in comparison. Figures 3-7 show the comprehensive coverage that Kaspersky gives in implementing many of the quick wins. This is complemented by many of the Microsoft tools which include Security Compliance Manager (SCM), Windows Deployment Services (WDS), Microsoft Deployment Toolkit (MDT), Group Policy (GP) and the Enhanced Mitigation Experience Toolkit (EMET). This set of Microsoft software is our second tool choice, working hand in hand with Kaspersky to automate controls 2-5. Spiceworks was chosen as the third tool. It is an automated network scanner as well as a purchasing and ticketing system. It helps to automate quick wins for inventorying authorized and unauthorized devices.

The tool coverage of the "Quick Wins" is shown in the figures below. The description of each quick win can be found on the 20 Critical Security Controls website (20 Critical Security Controls, 2013).

CSC 1: Inventory of Authorized & Unauthorized Devices	
Quick Win	**Tool(s) Used in Recipe**
1.1	Spiceworks
1.3	Spiceworks

Figure 3 CSC 1 Recipe Tools

CSC 2: Inventory of Authorized & Unauthorized Software	
Quick Win	**Tool(s) Used in Recipe**
2.1	Kaspersky
2.2	Kaspersky + Policy
2.3	Kaspersky + Policy

Figure 4 CSC 2 Recipe Tools

CSC 3: Secure Device Configurations for H/W & S/W	
Quick Win	**Tool(s) Used in Recipe**
3.1	WDS + MDT + SCM + GPO+ EMET
3.2	Kaspersky
3.3	GP + Policy
3.4	WDS + MDT + Policy
3.5	Windows File Auditing + Policy

Figure 5 CSC 3 Recipe Tools

CSC 4: Continuous Vuln. Assessment & Remediation	
Quick Win	**Tool(s) Used in Recipe**
4.1	Kaspersky (Windows Only)
4.2	Kaspersky
4.3	GP + Kaspersky + Policy
4.4	Policy + Kaspersky

Figure 6 CSC 4 Recipe Tools

CSC 5: Malware Defenses	
Quick Win	**Tool(s) Used in Recipe**
5.1	Kaspersky
5.2	Kaspersky
5.3	Kaspersky
5.4	Kaspersky
5.5	Kaspersky
5.6	Kaspersky
5.7	MDT + GP + EMET
5.8	Policy

Figure 7 CSC 5 Recipe Tools

To simulate a small business environment, we created a small virtual lab and installed or implemented each of the tools and sub-controls within the lab. After the first draft of the cookbook was completed, it was reviewed and opened to comments from a panel of information security practitioners who have experience working with small businesses.

With this understanding of small business needs and a prioritized list of security controls, practitioners can work to implement the Critical Security Controls. Detailed implementation recipes are included in the accompanying Cookbook document. A summary of the controls and the selected tools are discussed below.

Critical Control 1: Inventory of Authorized and Unauthorized Devices

The processes and tools used to track/control/prevent/correct network access by devices (computers, network components, printers, anything with IP addresses) based on an asset inventory of which devices are allowed to connect to the network.

(Critical Control 1: Inventory of Authorized and Unauthorized Devices, 2013)

Spiceworks is an IT system management solution providing network inventory and monitoring including mobile devices, help desk ticketing and procurement tracking. It is an integrated solution that automates several aspects of the 20 Critical Security Controls, particularly the first control: inventory of authorized and unauthorized devices. For this control, it automates 2 of the 3 "Quick Wins" as well as additional sub-controls related to building an inventory of network equipment, printers, etc. The Spiceworks system scan also inventories software, showing version, installation and licensing information, which automates parts of Critical Control 2: Inventory of authorized and unauthorized software.

Critical Control 2: Inventory of Authorized and Unauthorized Software

The processes and tools organizations use to track/control/prevent/correct installation and execution of software on computers based on an asset inventory of approved software.

(Critical Control 2: Inventory of Authorized and Unauthorized Software, 2013)

You can't protect assets you don't know about. Paired with Critical Control 1 (Inventory of devices), this control grants a business total or near-total visibility over their information assets.

The practice of inventorying authorized and unauthorized software requires decisions that may be less concrete than determining which physical assets belong to the business. *Which* software is authorized? Are all versions authorized, or only versions tested by IT? Are modules or plug-ins of approved software (like browser add-ons) automatically approved? Is the purpose of controlling software simply to avoid malware on systems, or is it part of a Data Loss Prevention (DLP) program? What steps does a user need to take to install software – do they have to go through a change management or software request process, or do they have the autonomy to make their own decisions about their device? Furthermore, new challenges are presented by software on personal devices, which introduce a mostly uncontrolled

environment. There are no right or wrong answers to these questions; it all dependent on the business needs and acceptance of risk. It is critical to have a decision-maker with an understanding of business requirements, and incorporate technical and information security expertise to determine the acceptable risk of these policies.

Another critical component to software control is organizational policy. Policies should be clearly defined, communicated, and have the flexibility to change as needed. Throughout the sub-controls of this CSC, change control plays an important role. A change control process doesn't need to be complex, and it doesn't require expensive software. All that's needed is a way to request, communicate, and log changes for future auditing. Implementing a change control program may seem unnecessary for a small business with one or two IT associates, but it is necessary in order for this CSC to succeed over time. In fact, change control is critical to small businesses with a small IT team, because if one associate is unavailable for communication when an untracked or unauthorized change fails, it can throw a business into chaos and waste valuable resources.

CSC 1 is a prerequisite to completing this task, since you must know what computers and devices to scan prior to inventorying their software. In fact, it makes sense to pair them and complete both at the same time before implementing the other controls in this cookbook. Careful execution of CSCs 1 and 2 can create a solid foundation upon which to build your information security program.

Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers Critical

The processes and tools organizations use to track/control/prevent/correct security weaknesses in the configurations of the hardware and software of mobile devices, laptops, workstations, and servers based on a formal configuration management and change control process.

(Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers, 2013)

Configuration management is the next logical step once a hardware and software inventory has been done. Executing configuration management correctly is an extremely hard thing to do in today's environment because of issues such as BYOD and the continuing need for cross-platform applications. Because of the scope of this cookbook, this set of recipes will be focused on Microsoft Windows configuration management.

The majority of the Quick Win sub-controls in Critical Security Control 3 revolve around a set of tools that Microsoft provides for businesses that primarily use Microsoft Windows for their servers and workstations. This set of tools is as follows:

Microsoft Windows Deployment Services 2012 (WDS)

Windows Deployment Services (WDS) enables you to deploy Windows operating systems over the network, which means that you do not have to install each operating system directly from a CD or DVD (Windows Deployment Services Overview).

Microsoft Deployment Toolkit 2013 (MDT)

The Microsoft Deployment Toolkit provides a unified collection of tools, processes, and guidance for automating desktop and server deployments. In addition to reducing deployment time and standardizing desktop and server images, MDT offers improved security and ongoing configuration management (Microsoft Deployment Toolkit).

Microsoft Security Compliance Manager 3.0 (SCM)

SCM provides ready-to-deploy policies and DCM configuration packs based on Microsoft security guide recommendations and industry best practices, allowing you to easily manage configuration drift and address compliance requirements for Windows operating systems, Office applications, and other Microsoft applications (Microsoft Security Compliance Manager, 2013).

Microsoft Group Policy (GP and/or GPO)

Group Policy is an infrastructure that allows you to implement specific configurations for users and computers. Group Policy settings are contained in Group Policy objects (GPOs), which are linked to the following Active Directory directory service containers: sites, domains, or organizational units (OUs). The settings within GPOs are then evaluated by the affected targets, using the hierarchical nature of Active Directory (Group Policy).

Enhanced Mitigation Experience Toolkit 4.0 (EMET)

The Enhanced Mitigation Experience Toolkit (EMET) is a utility that helps prevent vulnerabilities in software from being successfully exploited. EMET achieves this goal by using security mitigation technologies. These technologies function as special protections and obstacles that an exploit author must defeat to exploit software vulnerabilities. These security mitigation technologies do not guarantee that vulnerabilities cannot be exploited. However, they work to make exploitation as difficult as possible to perform (The Enhanced Mitigation Experience Toolkit).

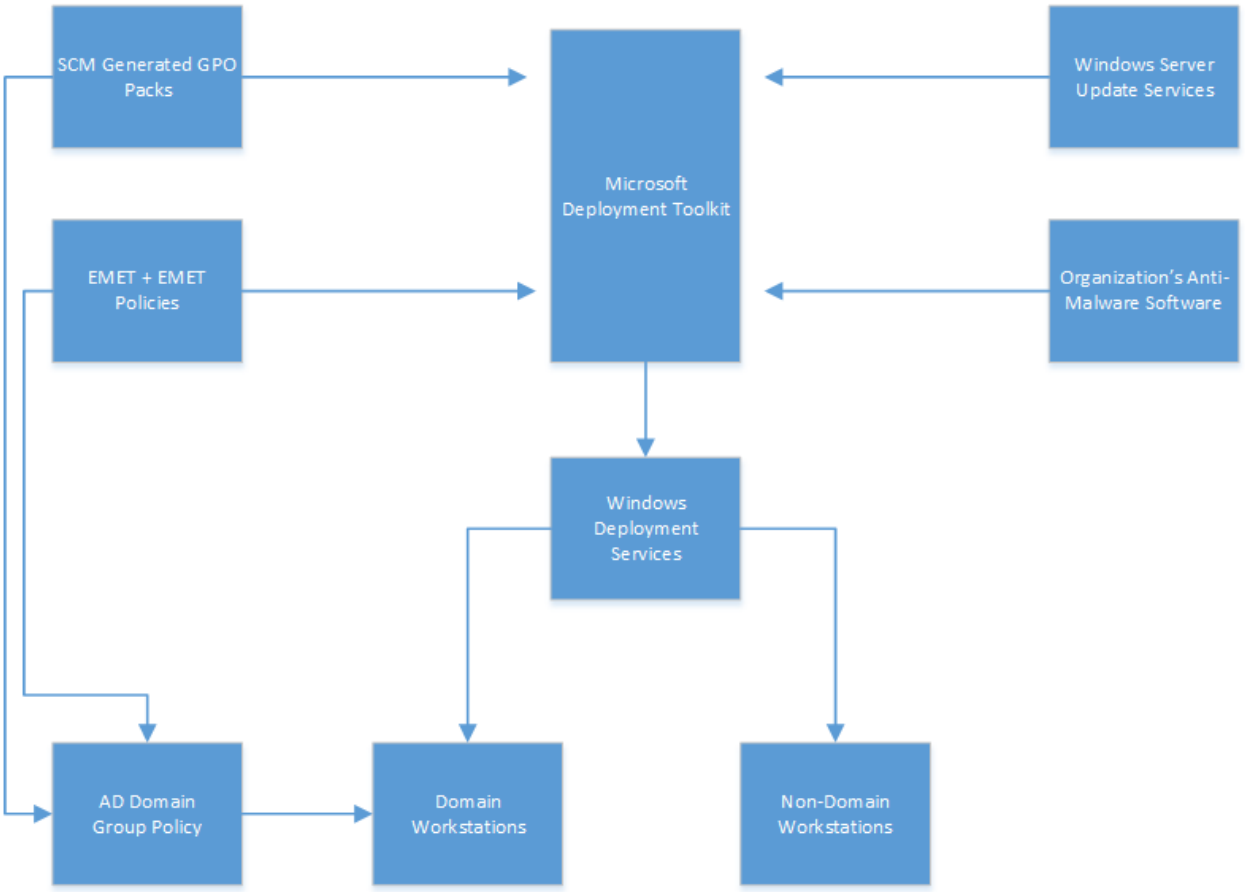


Figure 8 Microsoft Deployment Toolkit

As can be seen in Figure 8, the way it all works together is that MDT is used to configure a standard set of operating system images for workstations and servers. SCM will generate GPOs that will be used to harden the underlying operating system and applications installed on the system. EMET will be used as another layer of hardening for the images. WDS will then be used to deploy these images to the appropriate machines. For domain workstations and servers, GP will be used to continually refresh the state of the machine, so as to mitigate configuration drift.

Critical Control 4: Continuous Vulnerability Assessment and Remediation

The processes and tools used to detect/prevent/correct security vulnerabilities in the configurations of devices that are listed and approved in the asset inventory database.

(Critical Control 4: Continuous Vulnerability Assessment and Remediation , 2013)

In order for vulnerability assessments to be effective, a business must have confidence in the results of CSCs 1 (inventory of devices) and 2 (inventory of software).

Vulnerabilities are flaws in systems, software, hardware, policies, or configuration that could be exploited as part of an attack. Nearly every vulnerability assessment produces some results that must be remediated. But with the limited resources available to a small business, it may seem impossible to address all of them.

Vulnerability assessment and remediation plays into the overall discipline of risk management. There is ongoing and passionate debate in the information security community about the relationship between vulnerabilities, threats, business impact, probability, and risk. But for a small business making decisions on remediation, the key to addressing vulnerabilities is to prioritize the ones that present the highest probability of the highest impact to the business. ISO Guide 13335 defines risk as "The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization." (ISO/IEC 13335-1:2004, 2008)

Risk management is a discipline that is outside the scope of this paper. For a small business deciding which vulnerabilities to remediate first, this decision may be as simple as categorizing each vulnerability into a matrix such as the one found in Figure 9, combining the expertise of a business manager with the information security knowledge of an IT associate:

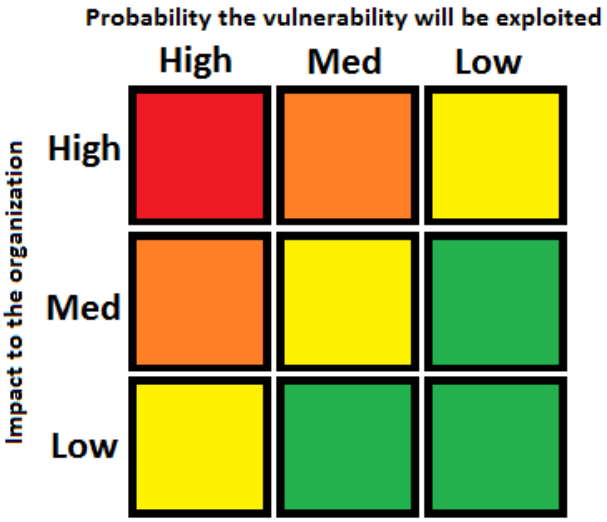


Figure 9 Vulnerability Categorization

The Common Vulnerability Scoring System (CVSS) framework provides a more detailed method of determining the priority of vulnerability remediation. It incorporates the CIA (Confidentiality, Integrity, Availability) triangle, as well as temporal and environmental factors. (National Institute of Standards and Technology, 2007)

Vulnerability remediation for personal devices can be more complex. Vulnerability assessment and remediation does not normally include personal devices in scope. However, this is where sub-control 4.4 (security intelligence) may help. If a savvy information security practitioner becomes aware of an

important vulnerability in a popular piece of software, she can remind her users to download the update, and this may lead to remediation of software on personal devices as well as corporate ones.

Critical Control 5: Malware Defenses

The processes and tools used to detect/prevent/correct installation and execution of malicious software on all devices. (Critical Control 5: Malware Defenses , 2013)

Malware ranks as the top concern of small business owners (Symantec, JZ Analytics, 2012), possibly because it is such a visible and persistent threat. At best, removing malware from a system takes up valuable time and monetary resources; at worst, it can severely impact information confidentiality, integrity, or availability (CIA triangle).

Though malware is the primary concern of executives, it is the last priority in this cookbook. That may seem counterintuitive. However, antivirus or anti-malware software on user computers should be the final threshold in a defense-in-depth focused security strategy. If the other Critical Security Controls in this cookbook are implemented correctly, malware should rarely require a defense at the endpoint. Application whitelists prevent executables from being loaded or run on a system. Vulnerability scans, remediation, and security intelligence can prevent malware from taking advantages of known exploits. Secure configuration prevents malware from being able to run and from spreading to other computers. In fact, if CSCs 1-4 are strictly enforced, anti-malware software should play only a minor role in a business's malware defense plan.

As with other CSCs, a solid catalog of procedures is critical to success, and procedures should be developed prior to implementing the tools listed in the cookbook. Though implementing the top 5 CSCs will go a long way toward preventing malware from infecting systems, incidents must be considered inevitable. Having a change management policy and incident handling policy can help a single IT associate plan and remediate malware incidents as they occur.

Due to the constraints to IT resources in most small businesses, we decided on several features that were critical to us when reviewing an anti-malware solution. The software we picked must:

- Fulfill the maximum number of controls specified in the 20 CSCs at a competitive (or free) cost
- Be centrally managed with an intuitive interface
- Have highly automated tasks and updates
- Effectively remove malware
- A good history of support and stability
- Available support in the event of zero-day malware incidents

Most of this section focuses on Kaspersky as a malware defense tool. At first, in an attempt to keep cost down, we researched and evaluated a number of free anti-malware solutions. However, none permitted the central management that is so critical to maximizing efficiency, none provided an acceptable level of support, and all of them lacked features that covered the top-rated 20 CSCs. We expanded our search to include competitively-priced malware solutions.

Kaspersky won out with competitive pricing (between $16-50, depending on licensing requirements), a solid stance in the anti-malware market, and features like application whitelisting, centralized application patch management, scheduled task management, and vulnerability scanning.

We should note here that Kaspersky is far from the only option for anti-malware. When simplifying the tools an IT resource is expected to learn and manage, we found Kaspersky to be the best choice to illustrate the sub-controls presented here. There are many options out there, and the market changes quickly!

If your small business opts to implement software from a different malware defense vendor, we recommend adhering to the criteria listed above. Businesses should evaluate whether the software is capable of implementing the sub-controls listed in this CSC.

Conclusion

The 20 Critical Security Controls are an industry-recognized list of controls that help businesses better manage their digital risk. Small businesses account for more the half of private sector workers. They are often the target of cyber-attacks and many have been compromised multiple times. Small businesses have unique constraints compared to their enterprise counterparts including limited financial and staffing resources. The recipes provided in the companion cookbook document provide specific actions (recipes) that small businesses can take to protect their critical information and assets, based on the 20 Critical Security Controls. The focus is on “Quick Wins” that provide the largest risk reductions with the smallest amount of effort. The hands-on recipes aid small businesses in implementing the most effective solutions for the most common information security problems. Following these steps will set a small business on a solid foundation of sound security principles.

References

20 Critical Security Controls. (2013). Retrieved October 15, 2013, from sans.org: http://www.sans.org/critical-security-controls/guidelines.php

AT&T. (2012). *AT&T Small Business Tech Poll 2012.* Retrieved from att.com: http://www.att.com/Common/about_us/files/pdf/national_findings_fact_sheet_wireless.pdf

Certified Professionals: Advisory Board. (n.d.). Retrieved November 4, 2013, from giac.org: http://www.giac.org/certified-professionals/advisory-board

CompTIA. (2011). *Small and Medium Business Technology Adoption Trends.* CompTIA Member Services.

Critical Control 1: Inventory of Authorized and Unauthorized Devices. (2013). Retrieved October 22, 2013, from sans.org: http://www.sans.org/critical-security-controls/control.php?id=1

Critical Control 2: Inventory of Authorized and Unauthorized Software. (2013). Retrieved October 22, 2013, from sans.org: http://www.sans.org/critical-security-controls/control.php?id=2

Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers. (2013). Retrieved October 22, 2013, from sans.org: http://www.sans.org/critical-security-controls/control.php?id=3

Critical Control 4: Continuous Vulnerability Assessment and Remediation . (2013). Retrieved October 22, 2013, from sans.org: http://www.sans.org/critical-security-controls/control.php?id=4

Critical Control 5: Malware Defenses . (2013). Retrieved October 22, 2013, from sans.org: http://www.sans.org/critical-security-controls/control.php?id=5

Frequently Asked Questions about Small Business. (2012, September). Retrieved November 2, 2013, from sba.gov: http://www.sba.gov/sites/default/files/FAQ_Sept_2012.pdf

Group Policy. (n.d.). Retrieved November 2, 2013, from TechNet: http://technet.microsoft.com/en-us/windowsserver/bb310732.aspx

Han, C. C. (2001). *Organizational Size, Flexibility, and Performance: A System Dynamics Approach.* Taipei: Tamkang University.

Healey, J. (2013). *A Fierce Domain: Conflict in Cyberspace, 1986-2012.* Cyber Conflict Studies Association.

ISO/IEC 13335-1:2004. (2008). Retrieved from iso.org: http://www.iso.org/iso/catalogue_detail.htm?csnumber=39066

Microsoft Deployment Toolkit. (n.d.). Retrieved November 2, 2013, from Technet: http://technet.microsoft.com/en-us/windows/dn475741.aspx

Microsoft Security Compliance Manager. (2013, January 28). Retrieved November 2013, 2013, from TechNet: http://technet.microsoft.com/en-us/library/cc677002.aspx

National Institute of Standards and Technology. (2007, June). *CVSS: A Complete Guide to the Common Vulnerability Scoring System.* Retrieved from first.org: http://www.first.org/cvss/cvss-guide.pdf

SMB Group. (2012). *SMB Group's 2013 Top 10 SMB Technology Market Predictions.* Retrieved from smb-gr.com: http://www.smb-gr.com/wp-content/uploads/2012/pdfs/2013_SMB_Predictions.pdf

Survey Shows Small Businesses Have Big Data Breach Exposure. (2013, March 6). Retrieved November 2, 2013, from http://www.hsb.com/HSBGroup/Subpage.aspx?id=579

Symantec, JZ Analytics. (2012). *2012 NCSA / Symantec National Small Business Study.* National Cyber Security Alliance.

Symantec, JZ Analytics. (2012). *2012 NCSA / Symantec National Small Business Study.* National Cyber Security Alliance.

The Enhanced Mitigation Experience Toolkit. (n.d.). Retrieved November 2, 2013, from Support.Microsoft.com: http://support.microsoft.com/kb/2458544/en-us

Windows Deployment Services Overview. (n.d.). Retrieved November 2, 2013, from TechNet: http://technet.microsoft.com/en-us/library/hh831764.aspx

APPENDIX B

Small Business Implementation of the CSCS Part 12

Critical Control 1: Inventory of Authorized and Unauthorized Devices

> The processes and tools used to track/control/prevent/correct network access by devices (computers, network components, printers, anything with IP addresses) based on an asset inventory of which devices are allowed to connect to the network.
>
> (Critical Control 1: Inventory of Authorized and Unauthorized Devices, 2013)

Spiceworks is an IT system management solution providing network inventory and monitoring including mobile devices, help desk ticketing and procurement tracking. It is an integrated solution that automates several aspects of the 20 critical security controls, particular the first control: inventory of authorized and unauthorized devices. For this control it automates 2 of the 3 "Quick wins" as well as additional sub-controls related to building an inventory of network equipment, printers, etc. The Spiceworks system scan also inventories software, showing version, installation and licensing information which automates parts of critical control 2: Inventory of authorized and unauthorized software. Spiceworks is able to scan Windows workstations and servers through Windows Management Instrumentation (WMI). It can scan Linux like systems through SSH and network device through SNMP. It can manage both iOS and Andriod phones and tablets through the use of the MaaS360 mobile device management app installed on those devices.

Sub-Control 1.1

> Deploy an automated asset inventory discovery tool and use it to build a preliminary asset inventory of systems connected to an organization's public and private network(s). Both active tools that scan through network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed. (Critical Control 1: Inventory of Authorized and Unauthorized Devices, 2013)

Introduction

Spiceworks uses Windows Management Instrumentation (WMI) to scan Windows devices. It uses SSH, SNMP and a variety of other mechanisms for scanning Linux, routers, modems and other network devices. For mobile devices such as phones and tablets the MaaS360 app by Fiberlink is used. Each of these must be properly configured to allow Spiceworks to fully inventory all network devices. Following this recipe will automate the first "Quick win" sub-control 1.1 listed above but utilizes only active scanning (versus active and passive).

Tools Used in this Recipe

- Spiceworks
- Windows Management Instrumentation (for Windows)
- OpenSSH (for Linux)
- Maas360 (for Mobile Devices)

Other Options

There are several other IT Asset management solutions including enterprise grade Nessus, Security Center by Tenable and BSA Visibility by insight. These provide passive scanning of systems which Spiceworks does not but Spiceworks is considered here due to its cost (free) and simplicity.

Getting Ready

The free Spiceworks application should be installed on a Windows workstation or server. It can be downloaded and installed from www.spiceworks.com. At least one user account must be created in order to login to the application.

How to do it…

Windows, Linux and mobile devices must be configured in order for Spiceworks to provide full system scan details. The following steps cover how to configure each of these. This is followed by instructions for performing the scan both manually and on a schedule within Spiceworks.

Enable WMI on Windows Servers and Workstations

Spiceworks uses Windows Management Instrumentation (WMI) to scan Windows devices. WMI must be properly configured to allow Spiceworks to fully inventory the system.

Paul Luciano has shared detailed instructions for setting up WMI; see *Configure Computers For WMI Access Using Spiceworks* (Luciano, 2012). The steps include creating an admin user whose credentials will be used by Spiceworks to login and inventory the system. Additional steps include enabling group policy, linking admin ID to WMI control and modifying the security policy. One of the steps listed is to disable UAC which is undesirable from a security perspective and is only required by systems that are not part of an active directory domain (Description of User Account Control and Remote Restrictions in Windows Vista, 2011). The referenced Microsoft Knowledge bulletin provides a solution for non-domain devices to allow remote administration without disabling UAC. This is done by setting the LocalAccountTokenFilterPolicy registry to a value of 1. A summary of the steps is included below:

1) Follow the "*Configure Computers for WMI Access Using Spiceworks*" (Luciano, 2012) instructions except for the step to disable UAC.
2) If the Windows system to be scanned is not part of a domain (e.g. WORKGROUP) set the *LocalAccountTokenFilterPolicy* registry to a value of 1 as described in the Microsoft Knowledge bulletin (Description of User Account Control and Remote Restrictions in Windows Vista, 2011).

With WMI properly enabled, Windows workstations and servers can be inventoried by the Spiceworks scan. Figure 1 shows the Spiceworks device details view for a Windows workstation. On the software tab there is a listing of all installed hotfixes but the drop down menu displayed on the right can switch the view to installed applications and services.

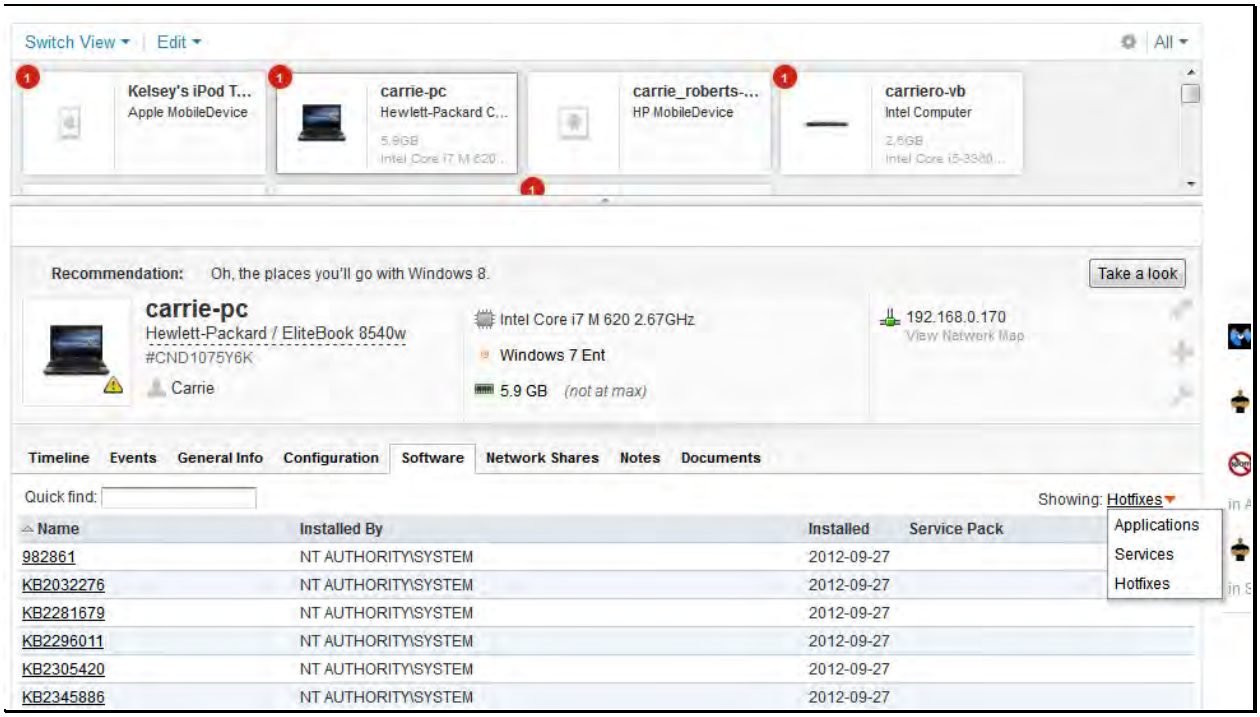


Figure 1 Spiceworks Device Software Inventory View (Windows)

Enable SSH access on Linux Servers and Workstations

SSH credentials can be used to enable scanning of Linux servers and workstations. A SSH server must be installed on the system to be scanned in order for the Spiceworks client to connect to it. OpenSSH is a common solution used to enable SSH. Details on installing and using SSH on Ubuntu can be found on the Ubuntu help site (SSH, 2013). Instructions for installing OpenSSH server on Ubuntu are included here but instructions for other Linux based operating systems are readily available on the internet.

First, install the OpenSSH server by entering the following command in a terminal window:

sudo apt-get install openssh-server

By default this will allow any of the systems current users to SSH into the server. The remaining instructions describe how to create a new user for doing scans and to limit SSH connection to only that user.

1) Add a new user, "*swuser*" in this example, with the following command:
   sudo useradd swuser

2) Set a strong password for this user as prompted by this command:
   sudo passwd swuser

3) Edit the SSH configs file to restrict access to only this user by editing the sshd_config file.
   sudo gedit /etc/ssh/sshd_config

4) To allow only the swuser account, add the following line to the bottom of the sshd_config file:
   AllowUsers swuser

5) Restart the SSH service to make the new configuration file setting take effect:
   sudo restart ssh

With SSH properly enabled, Linux workstations and servers can be inventoried by the Spiceworks scan. Figure 4 shows the details view for a Linux device. Unlike the Windows software inventory which provides a listing running services and installed hotfixes, for Linux only installed software is listed. The *Configuration* tab shows OS information as well as memory and disk usage.

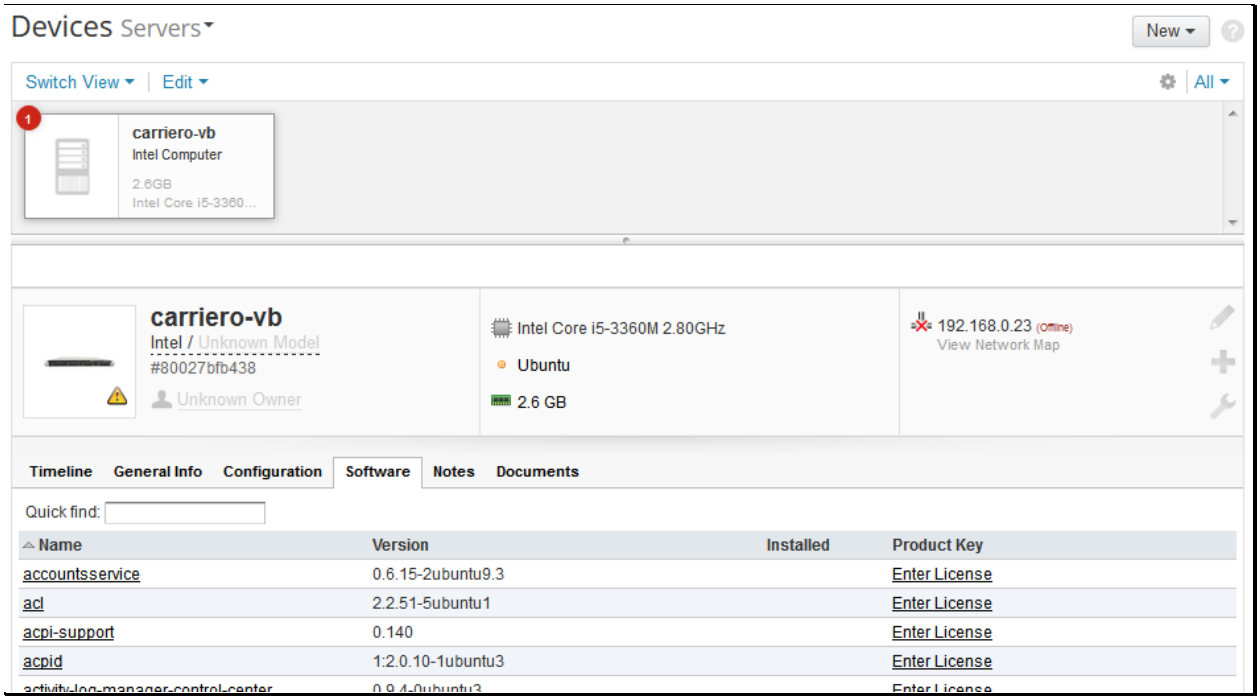


Figure 2 Spiceworks Device Software Inventory View (Linux)

Install Mobile Device Client app on each device to be monitored

Select *Inventory* → *Mobile Devices* from the main menu and click *Get Started*. Enter company name to create an account and click *Enroll your first device*. If iOS tablets or phones are to be monitored there is an additional one-time step required to create a certificate. The prompts will guide you through the process very clearly but the steps are summarized here for reference.

1) Authenticate with Apple ID
2) Create and save a Certificate Signing Request (CSR)
3) Upload the CSR to Apple
4) Import the signed Apple Certificate to Spiceworks

The MaaS360 app must be installed on each mobile device to be monitored. This process is started by selecting *Inventory* → *Mobile Devices* from the main menu, then clicking on *Enroll Device* near the top. Select an existing user or create a new one. Click *Send Request* to send a device enrollment request to the users email. Users must follow the instructions in the device enrollment request to download and install the MaaS360 app.

For iOS users

Prompts for each step will be given after clicking on the link in the email from the iOS. Be sure to open it in the Safari web browser. Each step is summarized below.

1) Authenticate by entering the passcode received in the device enrollment request.
2) Accept the terms of the end user license agreement.
3) Download and install profile.
4) Install the MaaS360 App.
5) Open the app and accept location and push notification prompts.

For Android users

Prompts for each step will be given after clicking on the link in the device enrollment request. Each step is summarized below.

1) Install the MaaS360 App from the Play store.
2) Open the MaaS360 and enter the corporate identifier and email address from the enrollment request.
3) Enter passcode and accept terms of use.
4) Click *Activate* to activate.

Similar procedures apply for Windows mobile devices.

Note that it can take 15-30 minutes after MaaS360 installation and activation before Spiceworks will successfully scan the device.

The free Maas360 app allows listing of software installed, jailbreak status, memory use, passcode status. Optionally, additional features such as remote device wipe, lock and locate services, passcode reset and application distribution can be accessed with a paid subscription. Figure 3 show the Mobile Devices dashboard within Spiceworks. The first thing shown is an alert for a device that does not have a passcode set. Next is a summary count of devices by type, pending enrollments and outstanding tickets. Additional summary report items follow including top 10 user installed apps.

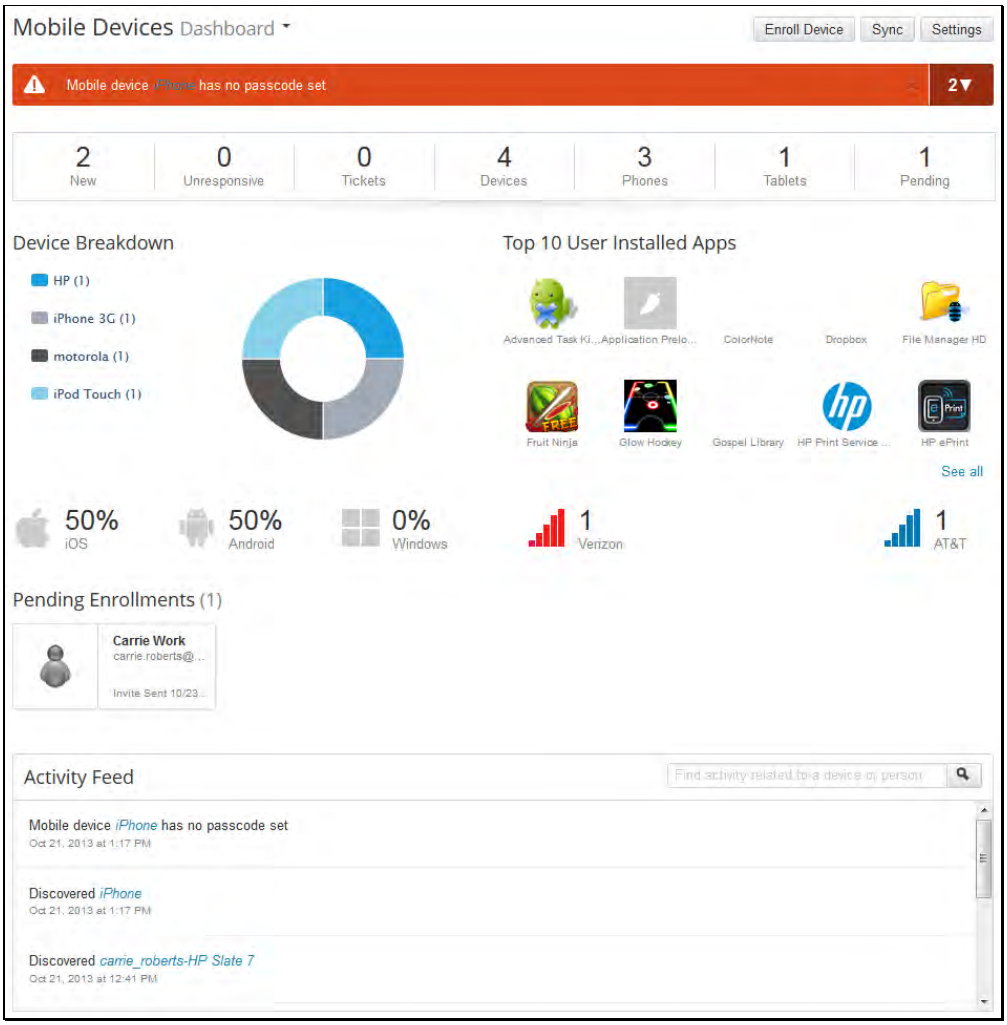


Figure 3 Spiceworks Mobile Devices Dashboard

Selecting the drop down menu next to Dashboard at the top will offer to switch to inventory view. Figure 4 shows the mobile device inventory view. Each mobile device is listed at top. Selecting one of the devices displays details for that device in the lower pane. The details include an inventory of all installed software and storage use.

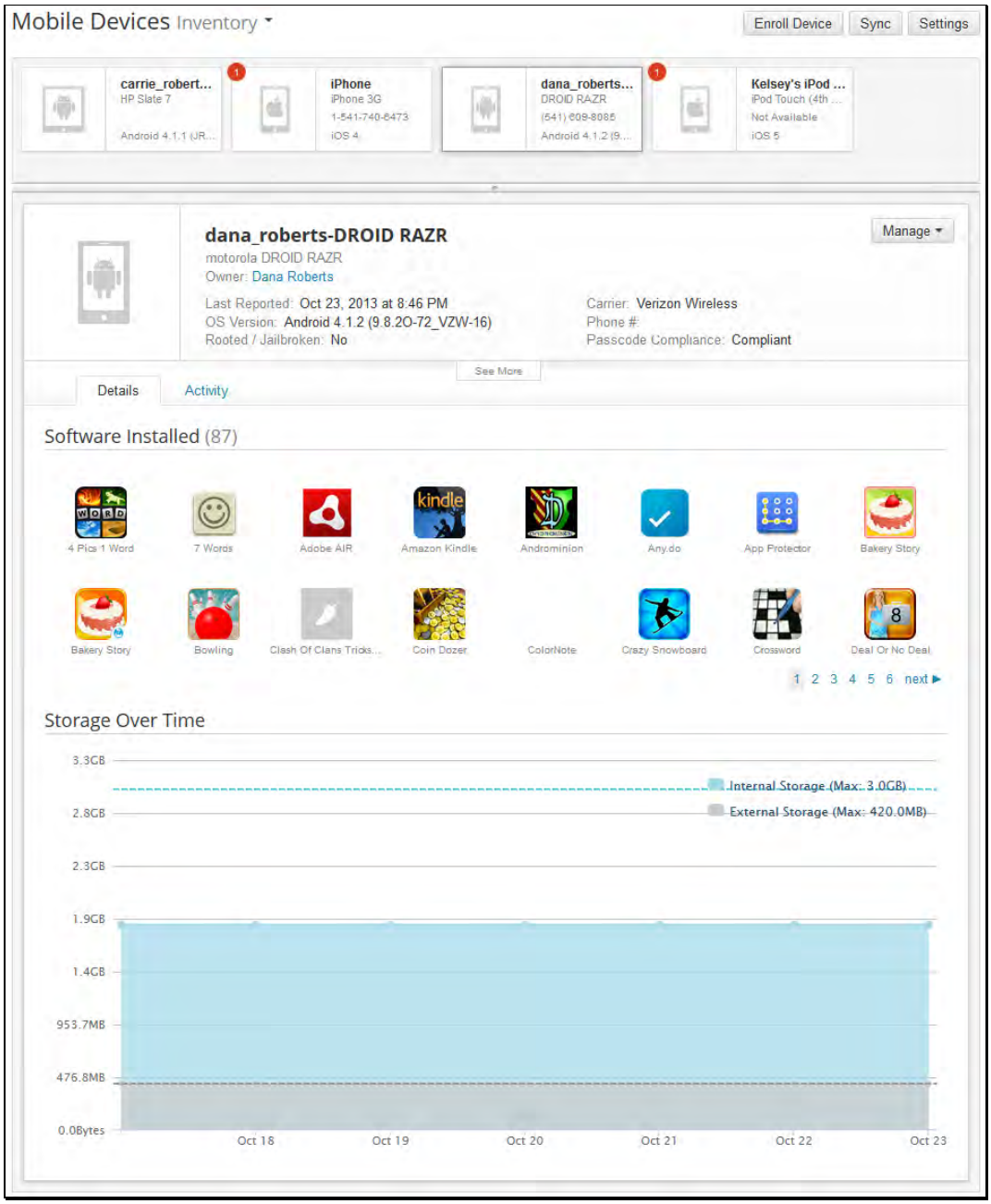


Figure 4 Spiceworks Mobile Device Inventory

Configure SNMP Access for Network Devices

Spiceworks can also inventory network devices such as routers and servers that use Simple Network Management Protocol (SNMP). Configure Spiceworks with this steps:

1) Navigate to *Inventory* → *Settings* → *Network Scan*.
2) In the *Stored Passwords* section (shown in Figure 5), add SNMP account credentials.
    a. Configure these settings, SNMP, SNMPv2c and/or SNMPv2c, as required by the devices on the network.

b. By default, Spiceworks will attempt to us the community string of "public" to access network devices unless otherwise configured.

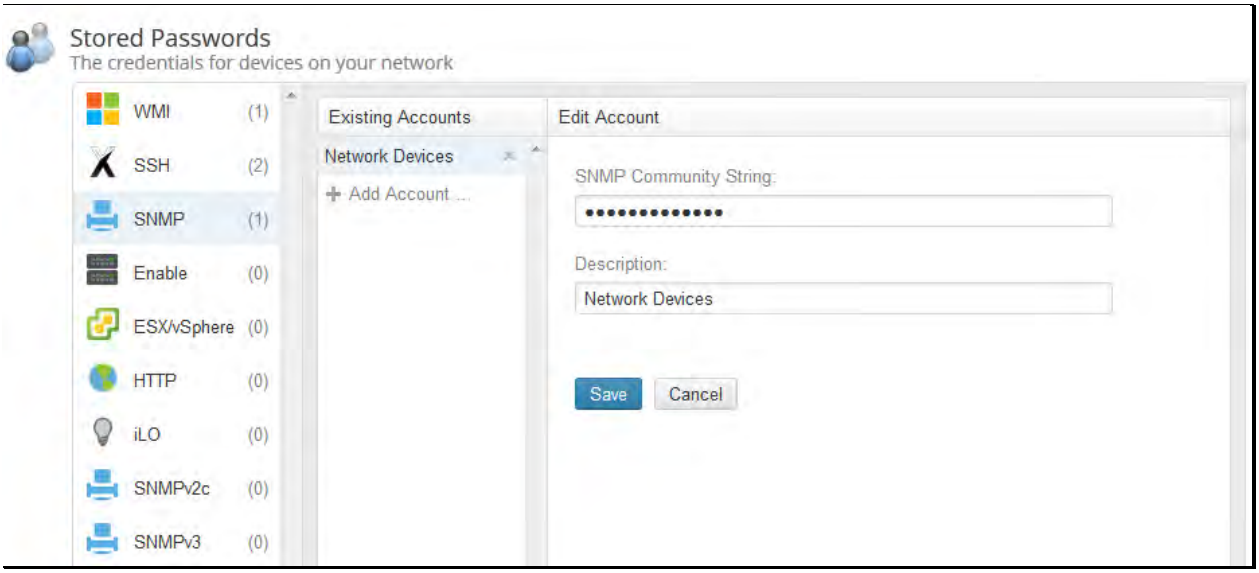


Figure 5 Spiceworks Authentication Settings for Network Scans

With SNMP properly enabled, network devices such as routers and servers can be inventoried by the Spiceworks scan. Figure 6 show the device details view for a modem that supports SNMP. The *General Info* tab includes the device serial number and mac address. The interface tab lists each interface on the device with links to bandwidth graphs where applicable.

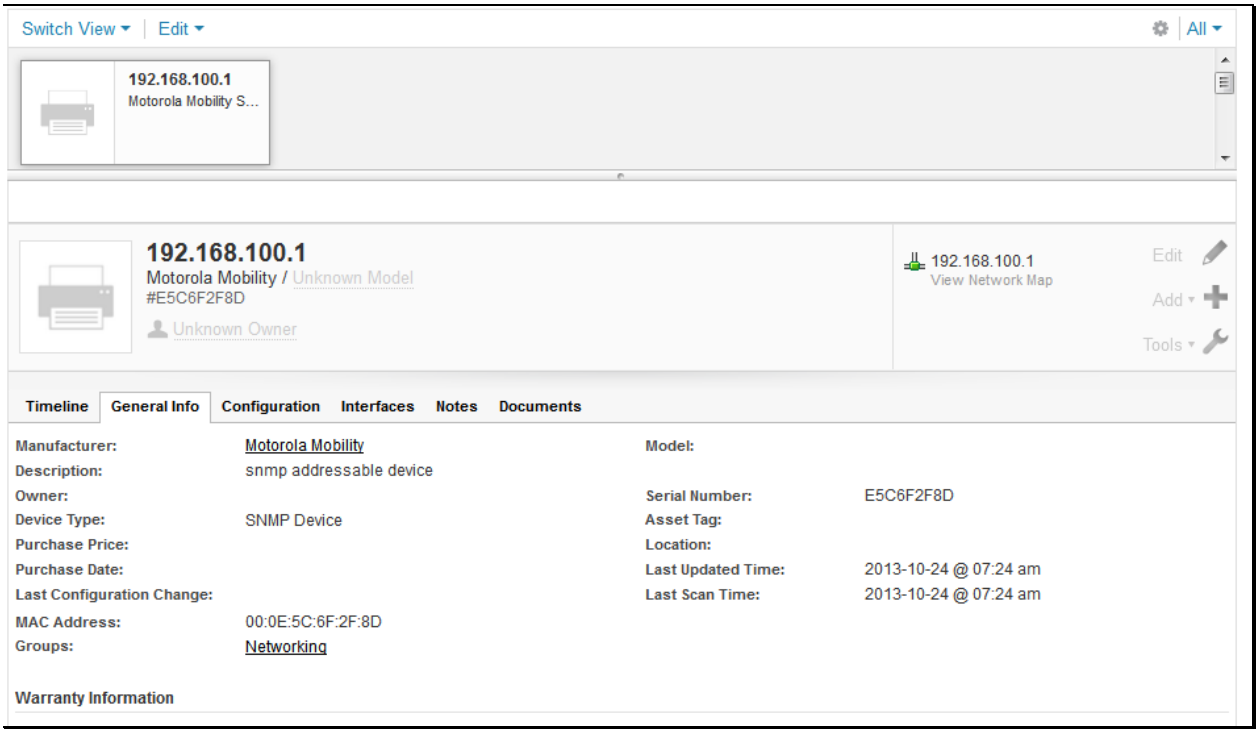


Figure 6 Spiceworks Network Device Details (Modem)

Scan Devices with Spiceworks

A variety of network devices are configured to allow scanning and Spiceworks is configured with the needed credentials to access those systems. Spiceworks can be configured to run scans on a custom schedule or scans can be invoked manually. Several scans are configured by default. Each of these can be edited or deleted. Instructions are included below for scheduling a new scan as well for manually invoking a scan.

Schedule a scan

1) Navigate to *Inventory* → *Settings* → *Network Scan*
2) In the *Schedules* section, select *Add Schedule* (see Figure 7)
3) Select a Scan Type (defined below):
    a. Resources: Configuration and capacities for disks, network adapters, mailboxes and switch ports.
    b. Utilization: Current system and network utilization
    c. Events: Windows events
    d. Up/Down: Ping for current network connectivity
    e. All: encompasses all the scan types
4) Enter a Device Group to be scanned. The default groups are (All devices, Not scanned in 30 days, Workstations, Servers, Printers, Networking, UPS, Others and User defined)
5) Enter a frequency at which to run the scan.

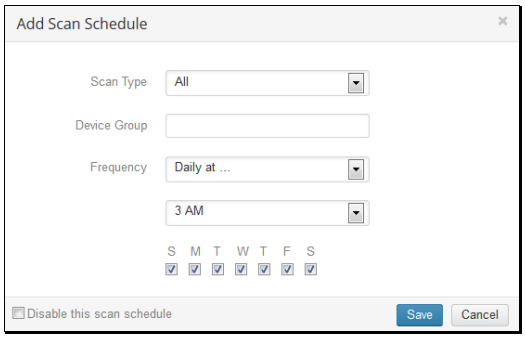


Figure 7 Spiceworks Add Scan Schedule Dialog Box

Manually invoke a scan

1) Navigate to *Inventory* → *Settings* → *Network Scan*
2) From the *Your Networks* section select the IP range(s) to scan or create a new range by selecting *Add IP Range* (see Figure 8)
3) Select *Start Scan* to start an immediate scan over the select IP address ranges.

Figure 8 Spiceworks Scan IP Address Range Selector

View Device Inventory in Spiceworks

Review the results of the scan by clicking on the *Inventory* link on the main menu. This view provides links to groups of devices and an environment summary as shown in Figure 9. The Environment Summary includes alerts, events, applications and more. Click on a group to select an individual device for review. Three examples of individual device details are shown in Figure 1 Spiceworks Device Software Inventory View (Windows), Figure 2 Spiceworks Device Software Inventory View (Linux) and Figure 4 Spiceworks Mobile Device Inventory.

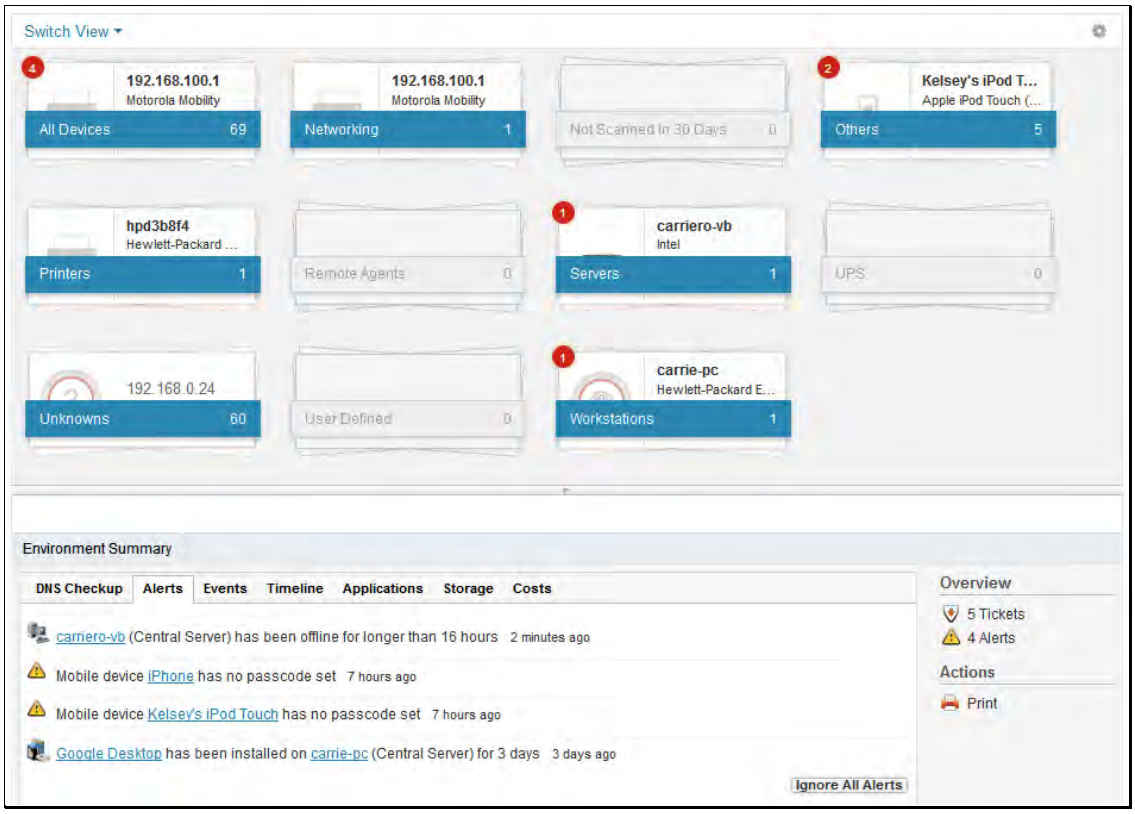


Figure 9 Spiceworks Inventory Summary View

The scan detail view for a network printer is shown in Figure 10. It includes printer ink levels and a link to the admin interface for the printer if applicable.

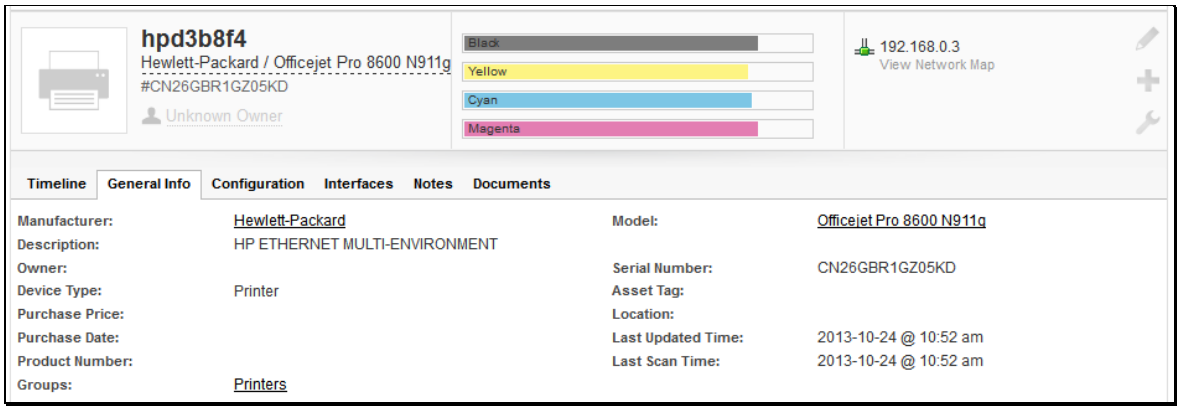


Figure 10 Network Printer Details in Spiceworks

For Linux systems, Spiceworks does not inventory installed software by default. This must be manually enabled.

Enable Linux Software Discovery

1) Navigate to *Inventory* → *Settings* → *Network Scan*

2) Click the *Show Additional Settings* link at the bottom of the page.
3) Set *Scan Linux software* to true as shown in Figure 11.

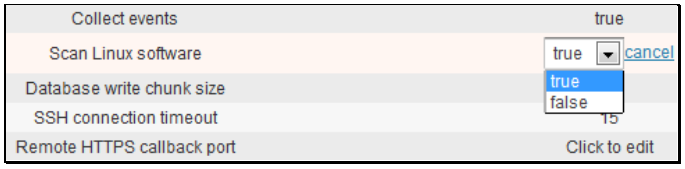


Figure 11 Enable Scanning of Linux Software in Spiceworks

These examples show how Spiceworks can be used to build a complete network inventory including installed software. Using Spiceworks in this way automates a significant portion of the first critical security control to inventory devices.

See Also

Spiceworks Online Help and Documentation (Help and Documentation - Spiceworks, 2013)
Spiceworks Inventory Feature Documentation (Getting Started - Spiceworks, 2013)
Spiceworks Adding New Devices Documentation (Adding New Devices - Spiceworks, 2013)

Sub-Control 1.2

Deploy dynamic host configuration protocol (DHCP) server logging, and utilize a system to improve the asset inventory and help detect unknown systems through this DHCP information. (Critical Control 1: Inventory of Authorized and Unauthorized Devices, 2013)

Introduction

DCHP is used to assign IP addresses to devices on the network. Windows server is commonly used as a DHCP server. The IP addresses that the server leases to devices is valuable information the can be correlated to the asset inventory for an organization. This recipe will describe how to enable DHCP server logging. The IP address and MAC address pairs can then be compared to the device inventory information collected through scanning as described in the previous recipe.

Tools Used in this Recipe

- Windows Server 2008

Other Options

Other versions of Windows Server and other DCHP services can provide this same functionality.

Getting Ready

A Windows Server used to administer DHCP to all devices on the network (Windows Server 2008 in this example).

How to do it…

On the Windows Server 2008 device that provides the DHCP service do the following steps to enable DHCP logging.

1) Start DHCP administration tool (*Start* → *Programs* → *Administrative Tools* → *DHCP*)
2) Click *Properties* on the *Action* menu
3) On the *General* tab, select *Enable DHCP audit logging*, and then click *OK*

DCHP logs are located at *%windir%\System32\Dhcp*. They are comma-delimited text files containing the following fields on each line:

1) A unique event ID
2) Date & Time of event
3) Description of event
4) IP address that has been leased out by the DHCP server
5) Host Name of DHCP client
6) MAC address of the client

Correlate the information in the logs with the inventory obtained through regular network scans to validate the results and potentially detect hidden devices.

See Also

Microsoft Technet Article on DHCP and Event Logging (More About DHCP Audit and Event Logging, 2013)

Sub-Control 1.3

Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network. A robust change control process can also be used to validate and approve all new devices. (Critical Control 1: Inventory of Authorized and Unauthorized Devices, 2013)

Introduction

Spiceworks is an IT system management solution providing network inventory, help desk and procurement. Although Spiceworks provides a purchasing module with many feature it falls short when it comes to linking purchases to devices found during the Spiceworks scan. It is possible to link a purchase to a device in the automated scan inventory. This can be a good indicator that the device belongs on the network, but there is no way to get a report showing which devices are linked to purchases. This limits the value of Spiceworks linking of acquisitions to device inventory. This recipe will provide instructions for creating a purchase and linking it to a device that was found through the automated device discovery scan in Spiceworks.

Tools Used in this Recipe

- Spiceworks

Getting Ready

The free Spiceworks application should be installed on a Windows workstation or server. It can be downloaded and installed from www.spiceworks.com. At least one user account must be created in order to login to the application. A device inventory through a Spiceworks scan should already exist. A recipe for doing this is included in this paper.

How to do it…

1) Navigate to *Purchasing* → *Purchase List* → *New Purchase*
2) Fill in Purchasing details (see Figure 12 for example)

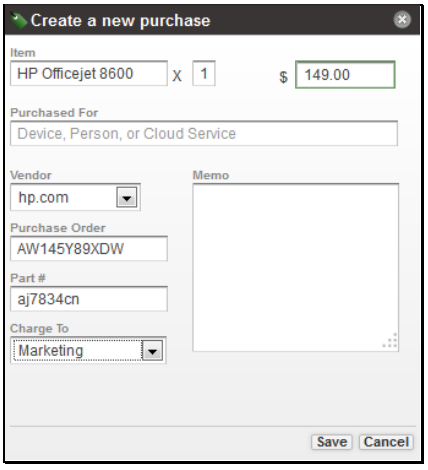


Figure 12 Spiceworks Create a New Purchase Dialog

3) Leave the P*urchased For* field blank. This will be used later to link this purchase to a device found during the inventory scan.
4) Click *Save* to create this item on the purchase list.
5) Select the row that was created on the purchase list and click on the *Edit Details* tab on the lower side of the highlighted row near the middle as shown in Figure 13.

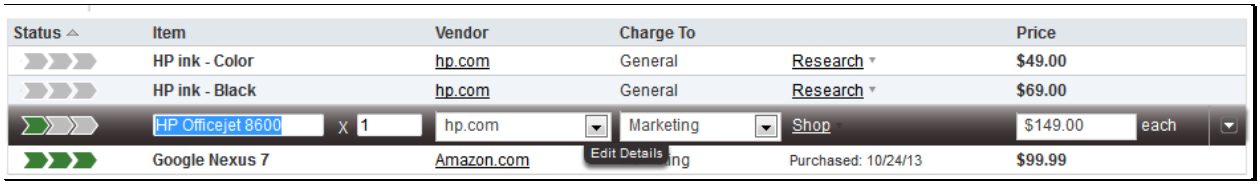


Figure 13 Spiceworks Purchase List

6) Optionally mark the device as received by clicking on the third arrow/flag in the left hand corner of the row.
7) Enter a device name (as it appears in the device inventory) in the *Purchased For* field to link this purchase to a particular device as shown in Figure 14.

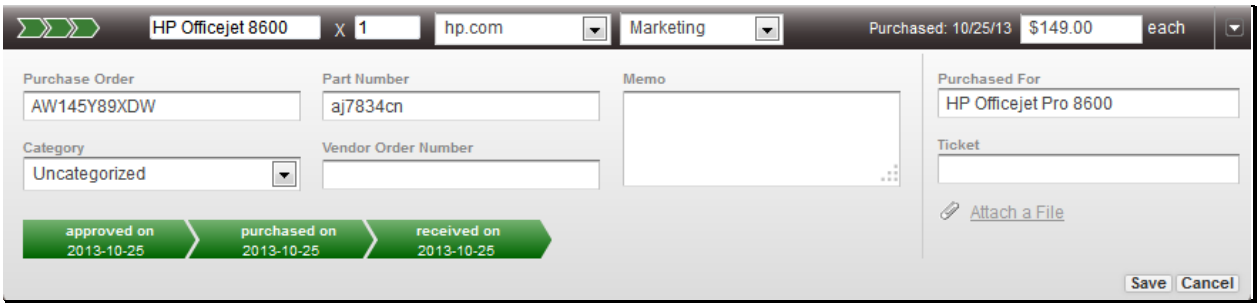


Figure 14 Spiceworks Edit Purchase Dialog

8) Click *Save* to save those changes.
9) Navigate to *Inventory* → *Devices* and select the device that was linked to the purchase (HP Officejet Pro 8600 in this example)
10) View the *General Info* tab for this device to see the purchase as shown in Figure 15.

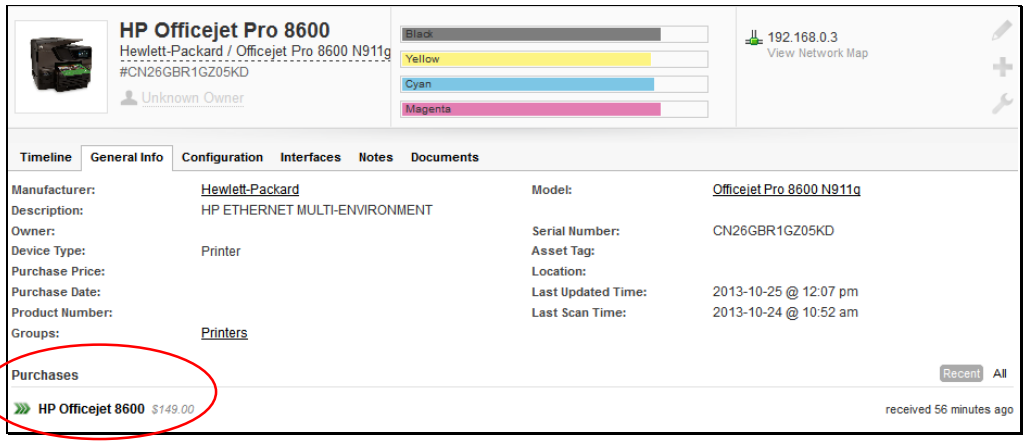


Figure 15 Purchase Linked to Inventory Item in Spiceworks

A purchase linked to a device on the network can be used as an indicator that the device is authorized to be connected. Unfortunately there is currently no mechanism to create a report or an alert of devices on the network that are not linked to purchases.

See Also

Spiceworks Online Help and Documentation (Help and Documentation - Spiceworks, 2013)
Spiceworks Purchasing Feature Documentation (Purchasing - Spiceworks, 2013)

Critical Control 2: Inventory of Authorized and Unauthorized Software

You can't protect assets you don't know about. Paired with Critical Control 1 (Inventory of devices), this control grants an organization total or near-total visibility over their information assets.

The practice of inventorying authorized and unauthorized software requires decisions that may be less concrete than determining which physical assets belong to the organization. *Which* software is authorized? Are all versions authorized, or only versions tested by IT? Are modules or plug-ins of approved software (like browser add-ons) automatically approved? Is the purpose of controlling software simply to avoid malware on systems, or is it part of a Data Loss Prevention (DLP) program? What steps does a user need to take to install software – do they have to go through a change management or software request process, or do they have the autonomy to make their own decisions about their device? Furthermore, new challenges are presented by software on personal devices, which introduce a mostly uncontrolled environment. There are no right or wrong answers to these questions; it all dependent on the business needs and acceptance of risk. It is critical to have a decision-maker with an understanding of business requirements pair with someone with technical and information security expertise to determine the acceptable risk of these policies.

Another critical component to software control is organizational policy. Policies should be clearly defined, communicated, and have the flexibility to change as needed. Throughout the sub-controls of this CSC, change control plays an important role. A change control process doesn't need to be complex, and it doesn't require expensive software. All that's needed is a way to request, communicate, and log changes for future auditing. Implementing a change control program may seem unnecessary for a small business with one or two IT associates, but it is necessary in order for this CSC to succeed over time. In fact, change control is critical to small businesses with a small IT team, because if one associate is unavailable for communication when an untracked or unauthorized change fails, it can throw an organization into chaos and waste valuable resources.

CSC 1 is a prerequisite to completing this task, since you must know what computers and devices to scan prior to inventorying their software. In fact, it makes sense to pair them and complete both at the same time before implementing the other controls in this cookbook. Careful execution of CSCs 1 and 2 can create a solid foundation upon which to build your information security program.

Sub-Control 2.1

Deploy application whitelisting technology that allows systems to run software only if it is included on the white list and prevents execution of all other software on the system. The white list may be very extensive (as is available from commercial white list vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the white list may be quite narrow. When protecting systems with customized software that may be seen as difficult to white list, isolate the custom software in a virtual operating system that does not retain infections. (Critical Control 2: Inventory of Authorized and Unauthorized Software, 2013)

Introduction

Traditionally, anti-malware software has operated using *blacklists* – a database of software signatures known to be malicious, and that should be denied access to the system. Unfortunately, this approach is ineffective against new (zero-day) threats and malware designed to change its signature, and over time, blacklists have grown to unmanageable sizes. More recently, anti-malware technology has trended toward *whitelisting* – gathering trusted and authorized software signatures.

Kaspersky gathers hashes of executable files from common Windows directories, like C:\Program Files. Kaspersky implements application whitelisting using the Bit9 database for file signatures. It compares gathered MD5 hashes with the Bit9 database to categorize applications as trusted, untrusted, unknown, and by software category (for example, “Games” or “Graphic Design”).

When comparing an executable to a white or blacklist, Kaspersky takes a hash of the file and compares it to the administrator-created policy to determine what action to take.

Tools Used in this Recipe

- Kaspersky Endpoint Security for Business, version 10

Other Options

Microsoft Applocker is an application control capability included as part of Windows 7 Ultimate/Enterprise and Server 2008 R2, and enhanced in Windows 8 Pro / Server 2012. It allows a user to set permissions for users to run specific applications and types of applications. However, we selected Kaspersky because many small businesses have a broad range of computers, which may not be attached to a central domain as is necessary for Applocker. Kaspersky requires only that managed computers have the Network Agent application installed. However, if a small business has most computers connected to a common domain, Applocker may be a good option.

Other third-party whitelisting management software includes Savant Protection, Faronics Anti-Executable, Lumension Application Control, and McAfee Application Control. Since whitelisting is an increasingly popular method of preventing malware, the vendor space is changing quickly.

Getting Ready

This recipe assumes you have Kaspersky Endpoint Security for Business Select installed, and that all of the computers and devices you need to manage in your whitelisting program are included in the console as managed devices.

How to do it…

The process for *deploying* whitelisting technology, when using Kaspersky, consists of installing the management server and endpoints, which is well-documented. Instead, here we lay the groundwork for creating an initial inventory of files related to existing applications to use in sub-control 2.2 to develop a whitelist.

Inventorying currently installed applications

Kaspersky inventories currently installed applications on Windows by searching common application directories (like C:\Program Files) for executable files like .bin and .exe.

A summary of the steps is included below:

3) Click *Tasks for Specific Computers* and select *Action* → *New* → *Task*. Enter a task name, like "Initial Application List".
4) Under *Kaspersky Endpoint Security for Windows*, select *Inventory*. This will create an inventory across endpoints.
5) Select the directories to inventory for installed applications. Generally, the defaults should be fine.
6) Select *Managed Computers* as the scope of your scan – this will perform an inventory across all computers currently managed by your server.
7) Since this is a onetime initial inventory, select *Once* or *Manually* for a scheduled start.
8) If you're ready to complete the inventory now, check the *Run task after Wizard Completes* box and click *Finish*. Otherwise, click *Finish* and run the task whenever you're ready.

While the task is running, you can view progress as shown below in Figure 16. This task may take a long time, depending on the number of applications installed and the number of computers being scanned.

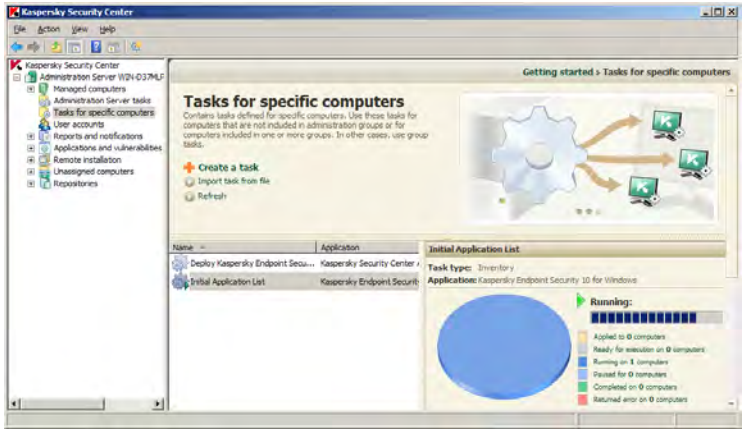


Figure 16

Once the run is complete, you have an inventory of currently-installed applications you can use to build a whitelist in sub-control 2.2, as shown below in Figure 17.

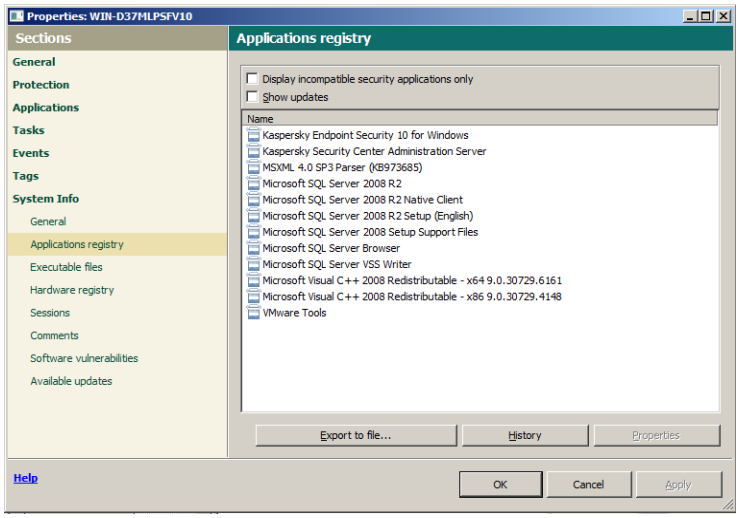


Figure 17

Managing custom or developing software

For customized software or software under development that is unmanageable to whitelist, the best option may be to whitelist virtual machine applications like VMWare Workstation, and run the custom software in virtual machine on a controlled network. This process should be documented in security policies.

See Also

Application Whitelisting: Panacea or Propaganda (Beechey, 2010)

Sub-Control 2.2

> Devise a list of authorized software that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified. (Critical Control 2: Inventory of Authorized and Unauthorized Software, 2013)

Introduction

Application whitelists inherently require some decision-making and attention. For low maintenance, application whitelisting can focus only on preventing malicious code from infecting a computer, and this type of whitelisting can be automated by using Kaspersky's Bit9 database as the whitelist. However, a small business may also opt to use application whitelisting to block legitimate applications that are not required for business and that increase security exposure (for example, a computer game that opens a listening port on a workstation). Whitelisting doesn't happen in a vacuum, and though systems with stable software (like SCADA systems) can be simple to manage, whitelists for user systems tend to be more dynamic and challenging to maintain. Small businesses that choose to implement application whitelisting should ensure:

- Users and business managers have a way to find out which applications are on the whitelist
- Users can request the evaluation of new applications as their jobs and needs change
- IT must have a change management process in place to initiate, manage, and audit changes to the whitelist
- The IT support team or person should be included in a panel responsible for evaluating new applications against business needs, security risk, and the organization's acceptable use policy.

It is worth noting that application whitelisting is impractical and not well enforceable for personal devices, so a separate policy (both technical and written) should be developed for these.

Tools Used in this Recipe

- Kaspersky Endpoint Security for Business, version 10

Other Options

The applications listed for SubControl 2.1 (Applocker, Faronics, Lumension, McAfee etc.) can be used to enforce whitelisting for this control.

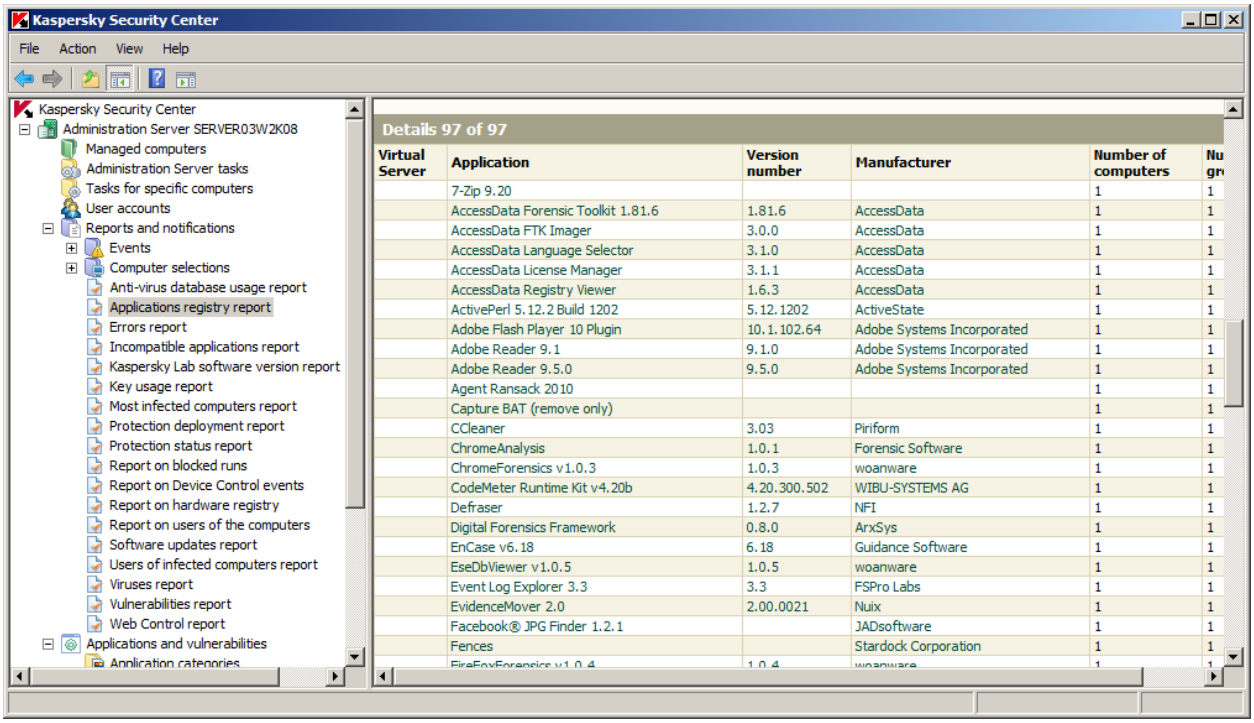
Getting Ready

This recipe assumes you have Kaspersky Endpoint Security for Business Select installed, and that all of the computers and devices you want to manage in your whitelisting program are included in the console as managed devices. You need to have gathered an automatic inventory of the pre-installed applications that exist on your network, using the process outlined in sub-control 2.1.

In addition, you must have access to a business authority or committee in your organization to assist in making decisions about which categories of software should be whitelisted.

How to do it…

After running the application inventory task specified in Quick Win 2.1, you can view a report of all the applications installed on computers on your network, as shown below in Figure 18. In the Kaspersky management console, open "Reports and Notifications" and select "Applications Registry Report". It will provide a list of the applications installed that you can export as HTML or TXT.



Virtual Server	Application	Version number	Manufacturer	Number of computers	Nu gr
	7-Zip 9.20			1	1
	AccessData Forensic Toolkit 1.81.6	1.81.6	AccessData	1	1
	AccessData FTK Imager	3.0.0	AccessData	1	1
	AccessData Language Selector	3.1.0	AccessData	1	1
	AccessData License Manager	3.1.1	AccessData	1	1
	AccessData Registry Viewer	1.6.3	AccessData	1	1
	ActivePerl 5.12.2 Build 1202	5.12.1202	ActiveState	1	1
	Adobe Flash Player 10 Plugin	10.1.102.64	Adobe Systems Incorporated	1	1
	Adobe Reader 9.1	9.1.0	Adobe Systems Incorporated	1	1
	Adobe Reader 9.5.0	9.5.0	Adobe Systems Incorporated	1	1
	Agent Ransack 2010			1	1
	Capture BAT (remove only)			1	1
	CCleaner	3.03	Piriform	1	1
	ChromeAnalysis	1.0.1	Forensic Software	1	1
	ChromeForensics v1.0.3	1.0.3	woanware	1	1
	CodeMeter Runtime Kit v4.20b	4.20.300.502	WIBU-SYSTEMS AG	1	1
	Defraser	1.2.7	NFI	1	1
	Digital Forensics Framework	0.8.0	ArxSys	1	1
	EnCase v6.18	6.18	Guidance Software	1	1
	EseDbViewer v1.0.5	1.0.5	woanware	1	1
	Event Log Explorer 3.3	3.3	FSPro Labs	1	1
	EvidenceMover 2.0	2.00.0021	Nuix	1	1
	Facebook® JPG Finder 1.2.1		JADsoftware	1	1
	Fences		Stardock Corporation	1	1
	FireFoxForensics v1.0.4	1.0.4	woanware	1	1

Figure 18

For this process, you need to determine which applications, or categories of applications, are appropriate for your small business. This is not a simple task! It should be accomplished by combining IT expertise with business and risk management knowledge to make research and make decisions. This may be best achieved with a committee or panel, reviewing a list of applications that has been grouped together or optimized by an IT associate.

When an application is selected for whitelisting, you can add it to a whitelist or blacklist category by selecting it in the *Applications and Vulnerabilities → Applications Registry* window, and clicking *Add to category*.

As you can see in Figure 19, Kaspersky whitelists applications by taking the MD5 hash value of executable files associated with the application, protecting the integrity of whitelisted applications. If an executable is corrupted by malware, the hash will change, and the application will no longer run in an environment that enforces a strict whitelisting policy.

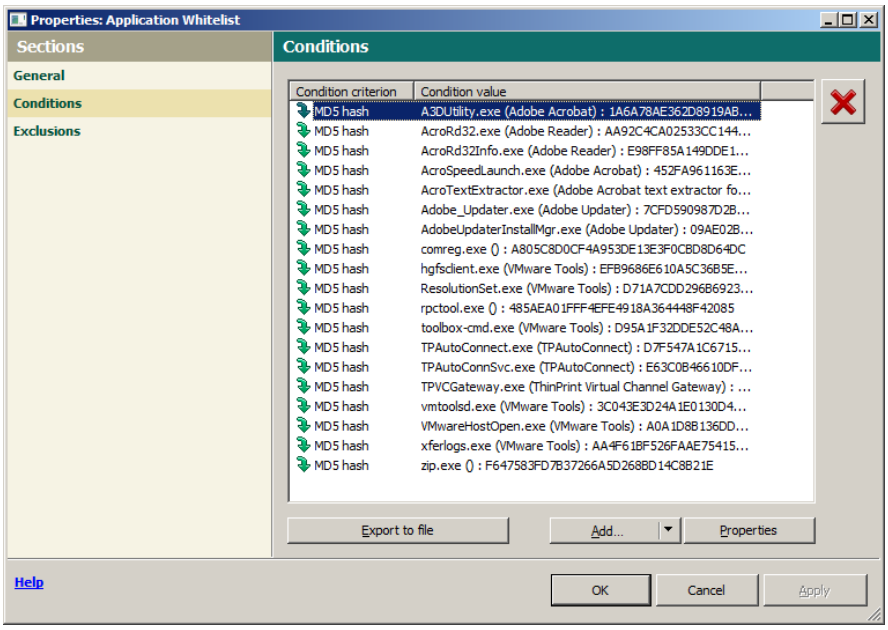


Figure 19

To automatically whitelist an entire category of software, like word processing applications, you can click *Add*, click *Add KL Category*, and select the appropriate checkboxes. It is also possible to restrict applications by user, which may be helpful for different roles within the same organization.

Bear in mind that whitelisting applications by inventorying pre-existing software on your network presents a potential problem. Existing applications (especially if unknown to the whitelisting application) may already be corrupted with undetected malware. If that's true, you've unknowingly whitelisted malicious software! To prevent this, you can decide on acceptable applications, gather files for whitelisted software from a clean, trusted source, then add those files to the whitelist.

See Also

Kaspersky Application Control and Default Deny Using Whitelisting Comparative Report (Andre Hall, 2012)

Sub-Control 2.3

Perform regular scanning for unauthorized software and generate alerts when it is discovered on a system. A strict change-control process should also be implemented to control any changes or installation of software to any systems on the network. (Critical Control 2: Inventory of Authorized and Unauthorized Software, 2013)

Introduction

If strict whitelisting is configured, and users have appropriate administrative rights, unauthorized installation of applications should be rare. However, regularly scheduled scans for new applications provide additional control and oversight.

Change Control is a critical part of information security, and part of the broader discipline of configuration and change management. When implemented in IT, it is a formal process to ensure changes to systems are authorized and coordinated appropriately. It provides accountability, communication, and historical data that reduces the time to respond to and resolve incidents.

There are many ways to implement change control. In a small organization, it may be as simple as creating a service ticket for each requested system change, requesting approval from data owners, communicating the change to affected parties, implementing the change as planned, and closing the ticket. There should also be a procedure in place for emergency changes that still allows for approval and communication. ITIL is a widely adopted approach for IT Service Management that includes guidance for the implementation of change management.

Change control should be audited occasionally, by comparing event logs and configuration changes with the corresponding change requests.

Tools Used in this Recipe

- Kaspersky Endpoint Security for Business, version 10

Getting Ready

This recipe assumes you have Kaspersky Endpoint Security for Business Select installed, and that all of the computers and devices you want to manage in your whitelisting program are included in the console as managed devices.

The recipe assumes that you have already inventoried your installed applications, and created a whitelist.

How to do it…

Automatically updating the Application Registry

1) Create a new task and select a descriptive name, like “Scheduled Application Inventory”.
2) Under *Kaspersky Endpoint Security for Windows*, select *Inventory*.
3) Click *Additional* and select *Scan only new and changed files*.
4) Select *Managed Computers* for the scope of the application scan.

5) Run the task on a recurring basis; depending on performance, you may want to run the task when Kaspersky starts, or on a schedule, like once per week or month.

This process will update the application registry with new applications.

Using Application Privilege Control

Application privilege control adds more granularity to whitelisting.

1) To access Application Privilege Control, select *Managed Computers* on the sidebar, then the *Policies* tab. Double-click the policy that applies to the computers you want to restrict.
2) For unknown applications, select *Low Restricted* or *High Restricted* if strict whitelisting is not important to you. If you want to enforce strict whitelisting, select *Untrusted* from the drop-down menu, as shown below in Figure 20

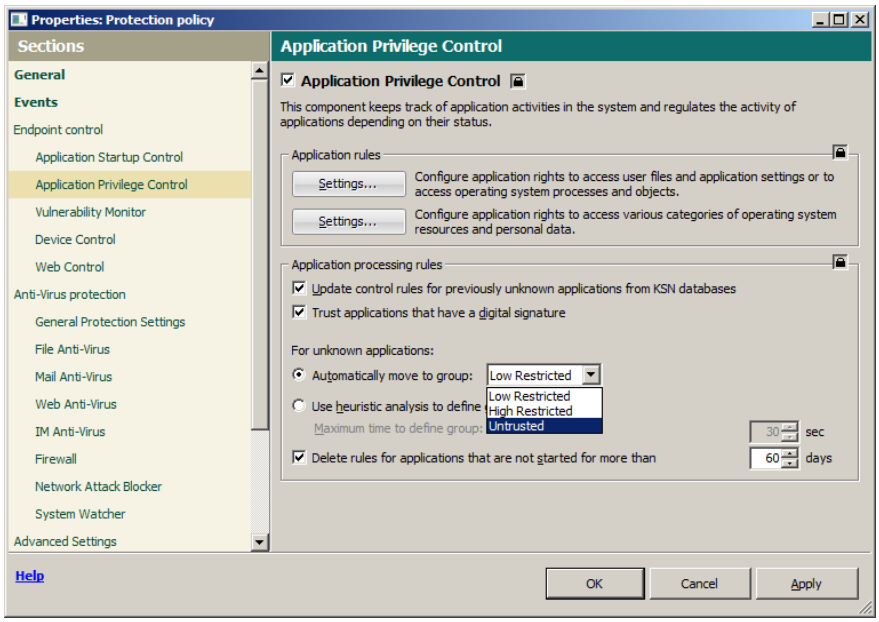


Figure 20

See Also

ITIL (ITIL Home, 2013)

Sub-Control 2.4

> Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops. The software inventory system should track the version of the underlying operating system as well as the applications installed on it. Furthermore, the tool should record not only the type of software installed on each system, but also its version number and patch level. The software inventory should be tied to vulnerability reporting/threat intelligence services to fix vulnerable software proactively. (Critical Control 2: Inventory of Authorized and Unauthorized Software, 2013)

Introduction

Fortunately, this control is somewhat automatic when other controls are in place. Using Kaspersky, the steps within this CSC, CSC 4 (Vulnerability Management) and sub-control 3.2 (patch management) combine to tie the software inventory in to vulnerable software management and reporting.

Tools Used in this Recipe

- Kaspersky Endpoint Security for Business, version 10

Other Options

There are many different options for software inventory available, including Spiceworks (covered elsewhere in this cookbook) and Lansweeper. Microsoft's SCCM also provides built-in capability to inventory software.

Getting Ready

This recipe assumes you have Kaspersky Endpoint Security for Business Select installed, and that all of the computers and devices you want to manage in your whitelisting program are included in the console as managed devices.

How to do it…

If sub-control 2.1 is implemented, the information required for this sub-control is already available.

In Kaspersky, OS versions (including service pack and update levels) can be viewed by selecting *Managed Computers*. Applications and version levels can be viewed *Reports and Notifications* → *Application Registry Report*.

If vulnerability scanning and system management is enabled in Kaspersky, the OS and application registry is integrated into vulnerability reporting and remediation.

Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers Critical

> The processes and tools organizations use to track/control/prevent/correct security weaknesses in the configurations of the hardware and software of mobile devices, laptops, workstations, and servers based on a formal configuration management and change control process.
>
> (Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers, 2013)

The majority of the Quick Win sub-controls in critical security control 3 revolve around a set of tools that Microsoft provides for organizations that primarily use Microsoft Windows for their servers and workstations. This set of tools is as follows:

Microsoft Windows Deployment Services 2012 (WDS)

> Windows Deployment Services (WDS) enables you to deploy Windows operating systems over the network, which means that you do not have to install each operating system directly from a CD or DVD. (Windows Deployment Services Overview)

Microsoft Deployment Toolkit 2013 (MDT)

> The Microsoft Deployment Toolkit provides a unified collection of tools, processes, and guidance for automating desktop and server deployments. In addition to reducing deployment time and standardizing desktop and server images, MDT offers improved security and ongoing configuration management. (Microsoft Deployment Toolkit)

Microsoft Security Compliance Manager 3.0 (SCM)

> SCM provides ready-to-deploy policies and DCM configuration packs based on Microsoft security guide recommendations and industry best practices, allowing you to easily manage configuration drift and address compliance requirements for Windows operating systems, Office applications, and other Microsoft applications. (Microsoft Security Compliance Manager, 2013)

Microsoft Group Policy (GP and/or GPO)

> Group Policy is an infrastructure that allows you to implement specific configurations for users and computers. Group Policy settings are contained in Group Policy objects (GPOs), which are linked to the following Active Directory directory service containers: sites, domains, or organizational units (OUs). The settings within GPOs are then evaluated by the affected targets, using the hierarchical nature of Active Directory. (Group Policy)

Enhanced Mitigation Experience Toolkit 4.0 (EMET)

> The Enhanced Mitigation Experience Toolkit (EMET) is a utility that helps prevent vulnerabilities in software from being successfully exploited. EMET achieves this goal by using security mitigation technologies. These technologies function as special protections and obstacles that an exploit author must defeat to exploit software vulnerabilities. These security mitigation technologies do not guarantee that vulnerabilities cannot be exploited. However, they work to make exploitation as difficult as possible to perform. (The Enhanced Mitigation Experience Toolkit)

The way it all works together is that MDT is used to configure a standard set of operating system images for workstations and servers. SCM will generate GPOs that will be used to harden the underlying operating system and applications installed on the system. EMET will be used as another layer of hardening for the images. WDS will then be used to deploy these images to the appropriate machines. For domain workstations and servers, GP will be used to continually refresh the state of the machine, so as to mitigate configuration drift.

Sub-Control 3.1

Establish and ensure the use of standard secure configurations of your operating systems. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system, such as those published by the vendor for high security situations and those released by the NSA, Defense Information Systems Agency (DISA), and the Center for Internet Security (CIS). This hardening would typically include removal of unnecessary accounts, disabling or removal of unnecessary services, and configuring non-executable stacks and heaps. Such hardening also involves, among other measures, applying patches, closing open and unused network ports, implementing intrusion detection systems and/or intrusion prevention systems, and erecting host-based firewalls. Running only standard, secure configurations will allow you to install all new security patches within 24-48 hours. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors. (Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers, 2013)

Introduction

This sub-control is by far the broadest of this critical security control. The key components of it are standardized, hardened images and configurations. It will be broken down into smaller sub-recipes as follows:

Setup & Initial Configuration of WDS, SCM, & MDT
Using SCM to Generate Baseline Security GPOs
Limiting Administrative Privileges
Setup & Configure EMET
Setup & Configure Anti-Malware application
Application Installs - Reference Image vs. Deployment
Setup & Configure other Applications for Deployment
Final Thoughts

Tools Used in this Recipe

- Microsoft Windows Deployment Services 2012 (WDS)
- Microsoft Deployment Toolkit 2013 (MDT)
- Microsoft Security Compliance Manager 3.0 (SCM)
- Microsoft Group Policy (GP or GPO for Group Policy Object)
- Enhanced Mitigation Experience Toolkit 4.0 (EMET)

Getting Ready

This recipe assumes that there is a working Windows domain, and clients that are joined to that domain. If there is not a working Windows domain, these tools can all be stood up and used in a standalone mode, but that configuration is outside the scope of this recipe.

How to do it…

To start off, we will get the main set of tools setup and initially configured.

Setup & Initial Configuration of WDS, SCM, & MDT

It is recommended that there is a dedicated server (virtual or physical) that can host the three primary tools (WDS, MDT & SCM). If there is not, they can be installed separately on different computers, but for long-term sustainability and efficient maintainability, it is recommend that they are installed all on one computer. There are many quality guides on how to install and do the initial configuration for most of these tools, so this sub-recipe will not go over those details. Instead, please find How To documents for the install and initial configuration for these tools below:

- Setting up and configuring WDS 2012 (Windows Deployment Services Getting Started Guide for Windows Server 2012, 2013)
- Setting up and configuring MDT 2013 (Microsoft Deployment Toolkit)
- Setting up and configuring SCM 3.0 (Microsoft Security Compliance Manager (SCM) - Getting Started, 2013)

Using SCM to Generate Baseline Security GPOs

The first step of hardening is to work with SCM to generate baseline security GPOs for each of the primary classes of devices that are present in the organization. Typically, that would include:

-Domain workstations
-Non-domain (standalone) Windows workstations
-Domain servers

We will start out with domain and standalone workstations.

1) Launch SCM, and under the left pane open *Microsoft Baselines*, navigate to the *Windows 8* section, and click on *Win8 Computer Security Compliance 1.0*
2) On the far right pane, under *Baseline*, click *Duplicate*
3) Change the Baseline Name to "Workstation-Win8-Baseline" and click *Save*
4) Customize the baseline according to your business requirements. The baseline can be exported as a spreadsheet for easier perusal. (Far right pane, Export Menu → Excel) A good rule of thumb is that if the Severity rating is Critical, then leave the default setting as is—Microsoft states "Settings with the severity level *critical* have a high degree of impact on the security of the computer or the data stored on it. We recommend nearly any organization to consider broadly implementing critical settings." (Microsoft Security Compliance Manager) Also remember that the baseline will need to be extensively tested before being applied to production systems.
5) Once the baseline has been customized, navigate to the *Export* menu on the far right column, and click *on GPO Backup (folder),* and select a place to locate the backup. Once it finishes the backup, rename the folder to something more coherent, such as "Windows8-Workstation-Baseline."

6) Repeat this process for domain servers, using *Windows Server 2012 Member Server Security Compliance 1.0* as a baseline.
7) The other SCM baseline that needs to be configured is *Windows 8 - Domain Security Compliance 1.0.* This baseline will be applied at the root of the domain. Repeat the above duplication, customization, and export process.
8) Each baseline now needs to be imported into its requisite location for deployment. Starting off with the workstation and server baselines, copy them to the MDT Deployment Share under the *Templates**GPOPacks* folder.
9) From the *<Deployment Share>**Templates**GPOPacks* folder, copy the following files to the two new folders that you just moved over
   GPOPack.wsf
   LocalPol.exe
   LocalSecurityDB.sdb
10) MDT 2013 applies a default GPO pack already during a standard deployment. To replace this default GPO pack with the customized GPO pack, configure the *GPOPackPath* property in the customsettings.ini file to point to the new folder—for instance:
   GPOPackPath = Windows8-WS-BL
11) Now the domain-level GPO should be applied at the root of the domain—Make sure to specify any exclusions if necessary.
12) Repeat the previous step for the server-specific GPO baseline and workstation-specific GPO baselines, targeting the relevant OUs.

Limiting Administrative Privileges

Limiting administrative privileges to authorized personnel only is an important part of hardening configuration. This particular recipe will be covered under sub-control 3.

Setup & Configure EMET

One of the other major hardening steps that will need to be taken is installing and configuring the Enhanced Mitigation Experience Toolkit (EMET). This will be covered in Critical Security Control 5, sub-control 7.

Setup & Configure Anti-Malware application

The final hardening step is to setup Kaspersky (or the relevant Anti-Malware application) for deployment.

1) To setup Kaspersky, make sure that the needed Kaspersky files have been copied over to the MDT server (Typically both the Network Agent and the Endpoint Client itself)
2) Import both the Network Agent and the Endpoint Client into MDT as applications—The silent install switches can be found on their support site. (Installing Kaspersky Endpoint Security 10 for Windows via command line prompt. Silent installation., 2013)

Application Installs - Reference Image vs. Deployment

The final step in this set of recipes is to setup and configure the other applications that are needed for deployment. But just a note: when should an application be pushed out—the reference image or during the actual deployment to production clients? Industry best practices suggest that the reference image should be kept as basic as possible, and that applications should be pushed out during the actual deployment of the reference image. This is much easier to maintain—rather than having to update the entire reference image when a new version of an application is released, the updated application can just be imported into MDT.

Setup & Configure other Applications for Deployment

1) With the above philosophy in mind, finish setting up the needed applications for deployment, using the authorized software list developed in Critical Security Control 2, sub-control 2
2) With applications such as Adobe Reader, use the Adobe Customization Wizard which enables a simple way of creating a customized version of Adobe Reader to be deployed. There are a number of How To documents that give more specific guidance. (Parker, 2013)

Final Thoughts

As new/updated tools like SCM and EMET are released, MDT should be updated as soon as possible.

See Also

The Sometimes Confusing Relationship between WDS and MDT (Bauer , 2013)

Sub-Control 3.2

Implement automated patching tools and processes that ensure security patches are installed within 48 hours of their release for both applications and for operating system software. When outdated systems can no longer be patched, update to the latest version of application software. Remove outdated, older, and unused software from the system. (Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers, 2013)

Introduction

Patching is critical to maintaining the security of individual systems, as malware often takes advantage of new and unpatched vulnerabilities. IT administrators should automate checks for software updates and test and install updates quickly. They should gather event logs for computers that are not receiving updates, or that are throwing errors when the update is installed.

Maintaining a whitelist will go a long way toward managing unpatched or insecure applications. Security intelligence (Quick Win 4.4) will also assist IT administrators in identifying applications that are reaching the end of their life cycles, and when critical updates should be manually pushed out.

Tools Used in this Recipe

- Kaspersky Endpoint Security for Business version 10

Other Options

There are several patch management software packages in the vendor space, including Kaseya Patch Management, and Secunia CSI. Microsoft has some patch management capabilities built in or added on to Windows servers, including Windows Server Update Services (WSUS) and System Center Configuration Manager (SCCM). In addition, many third-party applications, like Java and Adobe, can be configured to check for updates and install them automatically.

Getting Ready

This recipe assumes you have Kaspersky Endpoint Security for Business Select installed, and that all of the computers and devices you want to manage in your whitelisting program are included in the console as managed devices.

The recipe assumes that you have already inventoried your installed applications and devices, as shown in CSC 1 & 2.

How to do it…

Implementing this control requires a two-step process: check for applications that require patches, and update the vulnerable software.

Checking for updates

In order to implement this control, vulnerable software must be checked at least once every 48 hours. This can be completed by creating a task that runs automatically every one or two days.

1) Go to *Tasks for specific computers*. Click *Action* → *Create new task*.

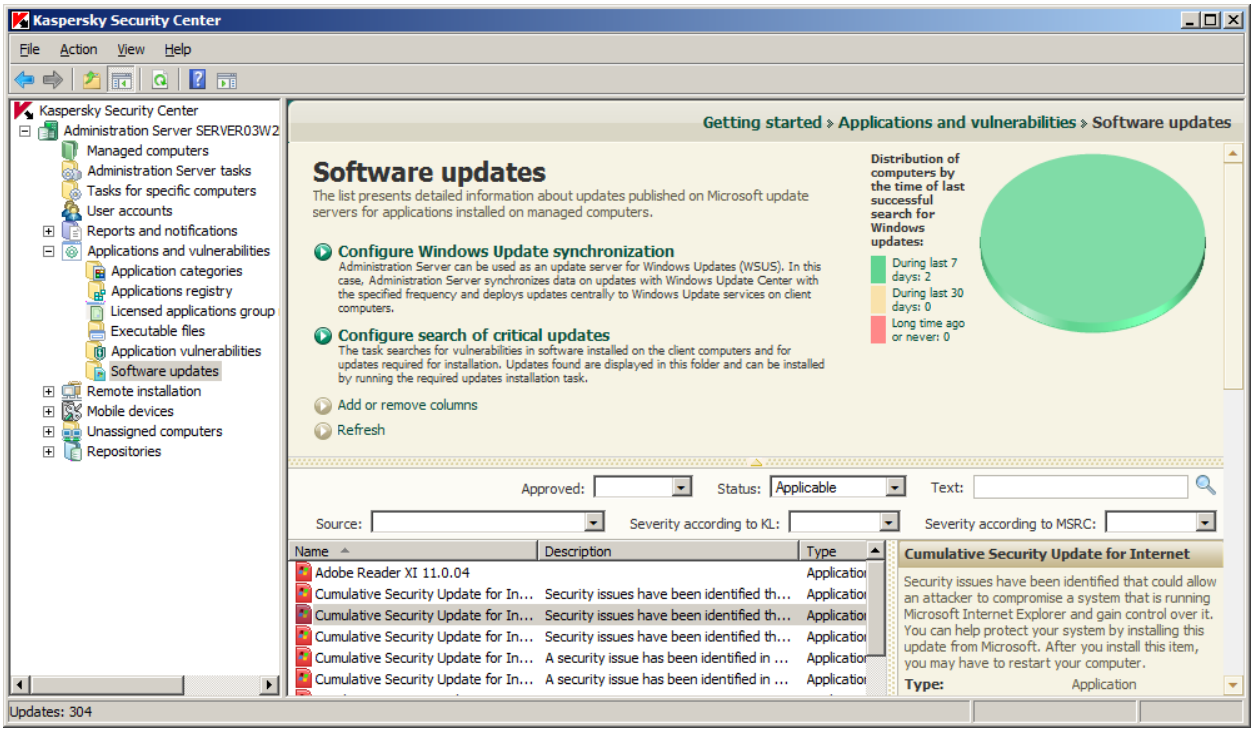
2) Name the task and click *Next*.
3) Select a task type of *Kaspersky Security Center Administration Server* → *Advanced* → *Find vulnerabilities and critical updates*. Click *Next*.
4) Check both *Use data from Windows Update Service* and *Use data from Kaspersky Lab*. This will check for patches documented by both sources. Click *Next*.
5) Select all *Managed Computers*. Click *Next*.
6) Schedule the start time of the task; if you want it to complete every two days, select *N hours* and specify 48. Otherwise, select *Daily.* Click *Next*. Click *Finish*.

All devices managed by Kaspersky will now check all installed applications for updates every 24 or 48 hours.

Viewing updates and installing them manually

Once the scan for updates is completed, you can view them in *Applications and vulnerabilities* → *Software updates*. As shown below, you can sort and filter updates by numerous criteria, including application and criticality. You can install patches manually by selecting the update and clicking *Fix Vulnerability (create new task)* in the right-hand pane.

From this view, you can also "ignore vulnerabilities" by double-clicking on one and checking *Ignore vulnerability*. Use this with caution – only if you have a specific, risk-justified reason to avoid an update!



Automating the installation of critical updates

An important note about update automation

Not all computers should be automatically updated and restarted, so think carefully about which group

you create an automated patch management rule for. In particular, servers should be updated on an agreed-upon schedule, with proper change management in place. Rebooting a business-critical server during business hours could be catastrophic. For servers, you may not want to create an automated patch installation rule; this should be done while an administrator is available to respond in case a problem occurs.

Patches and updates should be tested prior to deployment. If possible, patches should be deployed in waves, with the least-critical servers and workstations updated first. This can be managed granularly by creating a unique rule for each wave.

For updates and patches, a fallback plan should be in place in case the patches fail. This may be as simple as uninstalling the patch, or it could be as dramatic as restoring a server from a backup.

1) Go to *Tasks for specific computers*. Click *Action* → *Create new task*.
2) Name the task and click *Next*.
3) Select a task type of *Kaspersky Security Center Administration Server* → *Advanced* → *Install critical updates and fix vulnerabilities*. Click *Next*.
4) Customize any rules as necessary for third-party and Windows updates. Generally, the defaults should be fine.
5) Select an action to restart the computer or prompt the user. Since many operating system updates do not complete until a user reboots the computer, it is important to activate this capability in order to complete an update within 48 hours. It is highly recommended to reboot automatically after a specified time, since users may leave computers on for a long period of time, or a computer may be unattended when it updates.
6) Select the computers you want to automatically update.
7) Select a scheduled time. It should match the update/patch scan specified in the process above.
8) After the updates are installed, check the front page of the Security Center to ensure the patches were installed successfully.

Sub-Control 3.3

Limit administrative privileges to very few users who have both the knowledge necessary to administer the operating system and a business need to modify the configuration of the underlying operating system. This will help prevent installation of unauthorized software and other abuses of administrator privileges. (Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers, 2013)

Introduction

The implementation of this sub-control has the following sub-recipes:

Administrative Privileges Policy
Managing Domain Workstations & Servers: AD Group for Local Administrators
Managing Domain Workstations & Servers: Edge Cases
Managing Domain Workstations & Servers: Setting up Alerting for Relevant Events
Managing Non-domain Computers

Tools Used in this Recipe

- Microsoft Group Policy (GP)
- Kaspersky Endpoint Security for Business (Kaspersky)

Policies Used in this recipe

- Administrative Privileges Policy

Getting Ready

This recipe assumes that there is a working Windows domain, and clients that are joined to the domain, as well as standalone Windows clients.

How to do it…

Administrative Privileges Policy

The key part of this sub-control is that there is a policy developed and implemented that clearly defines who should have administrative privileges and why. At a minimum, this policy should outline the following:

-Define levels of Administrator Privileges (for example, domain administrators, workstation administrators, etc.)
-Dependent on business needs, which positions have which level of administrator privileges
-A Request and Appeal process that will cover edge cases

A couple quality reference policies can be found in the references section of this document. (Fisher College of Business Information Security, 2010) (Administrative/Special Access Policy, 2011)

Managing Domain Workstations & Servers: AD Group for Local Administrators

For users that need local administrator access to all domain workstations and servers, please follow one of these How To documents to setup a centrally managed AD group that will contain users that have local administrator rights for workstations and servers:

- *Add an Active Directory group to the local administrator group of workstation(s)* (Add an Active Directory group to the local administrator group of workstation(s))
- *How to Make a Domain User the Local Administrator for all PCs* (How to Make a Domain User the Local Administrator for all PCs, 2013)

Managing Domain Workstations & Servers: Edge Cases

There will be times when a user needs to be a local administrator for a particular device, but not for any others. This can be handled in one of two ways: either just add the user to the local administrator's group of the device, or setup a specific AD group and add it to the local administrator's group for that one device, and then add the user into the AD group. Neither option is ideal, which is why this scenario should be an edge case and not normal operations. Either option needs to be documented and monitored.

Managing Domain Workstations & Servers: Setting up Alerting for Relevant Events

A major part of this Critical Security Control is monitoring for changes to critical configurations. With this in mind, email alerts should be setup to monitor changes that are made to the security groups that were created in the previous sub-recipes (2 and 3). To do this, set up a scheduled task to send an email when a specific Event has been generated. Follow the referenced guide to accomplish this, using Event IDs 4764 and 4728 as a starting point. (OttoHelweg2, 2011) Remember that these events will only be generated on domain controllers, so that is where the tasks will need to reside.

Managing Non-domain computers

There will be times when standalone Windows computers will need to be deployed and maintained. Since they are not joined to the domain, the above methods of controlling local administrator access are not possible. To be able to achieve the required control, if Kaspersky is being used, (as it is in the rest of this cookbook), then its remote installation feature can be utilized.

1) Using the referenced documentation, create a batch file that implements the needed user change. (Delete/remove local user from local admin gro [Solved], 2009) (How to Add Local Users and Groups with a Batch File Distribution Package, 2008)
   For example:
   Net user Jim /delete
   This will delete the user "Jim" from the local computer.
2) Next, open up the Kaspersky Security Center and create a new package with the "…specified executable file" option
3) Name the package, select the batch file, and confirm the creation of the package.
4) The new install package can now be deployed to the managed non-domain workstations.
5) Though this method is more time-consuming than the group policy recipes above, it is still more efficient than having to touch each standalone workstation individually.

See Also

How to restrict developers' admin rights (Grimes, 2012)

Limiting admin rights chokes most Microsoft vulnerabilities (Ragan, 2011)

Sub-Control 3.4

Follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise. Any existing system that becomes compromised should be re-imaged with the secure build. Regular updates to this image should be integrated into the organization's change management processes. Images should be created for workstations, servers, and other system types used by the organization. (Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers, 2013)

Introduction

This sub-control builds on sub-control 1, which outlined the use of an imaging solution to standardize and harden system images—beyond that, there needs to be continuous refinement and updates to the images, deploying not only when new systems are brought online, but also when an in-production system has been compromised.

Tools Used in this Recipe

- Windows Deployment Services (WDS)
- Microsoft Deployment Toolkit (MDT)

Getting Ready

This recipe assumes that an imaging system has been deployed, such as Windows Deployment Services, which was laid out in sub-control 1.

How to do it…

First off, it is clear that a standardized image must be maintained for workstations and servers, as well as other types of systems that may exist in the environment. For example, there may be a business case to build a specific image for standalone field laptops versus domain desktops that usually do not move out of one location.

These images must be kept up to date. Industry best practices suggest that these images should be sparse, with only the absolute minimum of applications installed on them—rather, schedule the application install during deployment, through a tool like Microsoft Deployment Toolkit. This translates into less operational overheard of having to keep the images updated every time a new version of Adobe Reader is released--just replace one file on the MDT server. Windows Updates can also be pushed automatically to the system while it is being imaged. With this in mind, a good rule of thumb is to update system images once a quarter.

Updating the system images should entail at least the following:

1. Windows Updates
2. Application Updates
3. GPO Pack Updates, if needed
4. Any other configuration changes that need to be made

If a system is compromised, it must be re-imaged. To make this less of a burden to I.T. and the end user, make sure to either keep good backups of their files that reside on their system, or use some other technique such as Roaming Profiles and Folder Redirection, so that the user doesn't have any business data saved locally on the system itself. (Deploy Folder Redirection, Offline Files, and Roaming User Profiles, 2013) (Folder Redirection Overview)

See Also

How do you explain the necessity of "nuke it from orbit" to management and users? (Polynomial, KDEx, Taylor, & Schroeder, 2012)

Sub-Control 3.5

Store the master images on securely configured servers, with integrity checking tools and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network. Images should be tested at the hot or warm disaster recovery site if one is available. (Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers, 2013)

Introduction

This recipe describes how to implement sub-control five. A small script will be written to backup, setup auditing, and hash the current reference image. Though you can purchase other file integrity monitoring tools, or take the time to setup FOSS tools like OSSEC, for this sub-control, the built in windows auditing tools will work. If you do have OSSEC or other file integrity monitoring tools setup in your environment, substitute those in this sub-control.

Tools Used in this Recipe

- Windows File Auditing

Getting Ready

This recipe assumes that you have already implemented WDS (or another imaging solution), and have at least one reference image for your devices.

How to do it…

1. The server that will store the reference image must be a standardized, hardened install itself.
2. Write a script that will do the following:
    a. Confirm that only the following users have write access to the reference image
        i. SYSTEM
        ii. Local Administrators Group
    b. Turn on Windows Auditing for the reference image folder and its accompanying files
    c. Hash the reference images and its accompanying files
3. Setup email alerts for when the reference image has been modified. This can be accomplished by setting up a scheduled task to send an email when a specific Event has been generated. Follow the referenced guide to accomplish this, using Event ID 4656 as a starting point. (OttoHelweg2, 2011)
4. When it is time to update the reference image, update the image and execute the script written in step 2 to re-setup the appropriate settings for the updated reference image.

See Also

Download Free PowerShell Quick Reference Guides from Microsoft (Iwaya, 2013)

Critical Control 4: Continuous Vulnerability Assessment and Remediation

In order for vulnerability assessments to be effective, an organization must have confidence in the results of CSCs 1 (inventory of devices) and 2 (inventory of software).

Vulnerabilities are flaws in systems, software, hardware, policies, or configuration that could be exploited as part of an attack. Nearly every vulnerability assessment produces some results that must be remediated. But with the limited resources available to a small business, it may seem impossible to address all of them.

Vulnerability assessment and remediation plays into the overall discipline of risk management. There is ongoing and passionate debate in the information security community about the relationship between vulnerabilities, threats, business impact, probability, and risk. But for a small business making decisions on remediation, the key to addressing vulnerabilities is to prioritize the ones that present the highest probability of the highest impact to the organization. ISO Guide 13335 defines risk a "The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization." (ISO/IEC 13335-1:2004, 2008)

Risk management is a discipline that is outside the scope of this paper. For a small business deciding which vulnerabilities to remediate first, this decision may be as simple as categorizing each vulnerability into a matrix like this, combining the expertise of a business manager with the information security knowledge of an IT associate:

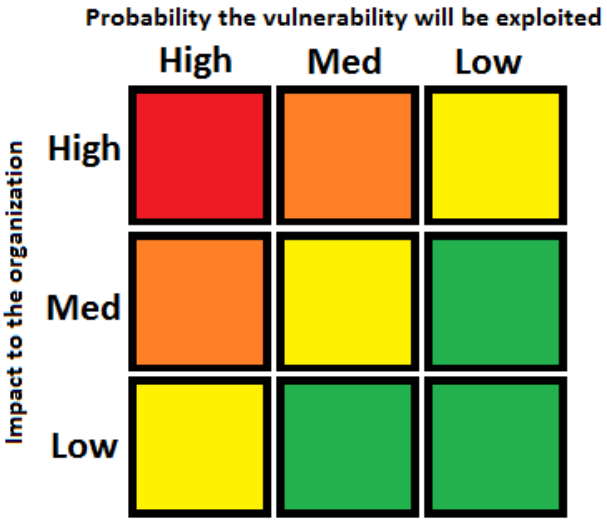


Figure 21

Vulnerability remediation for personal devices can be more complex. Vulnerability assessment and remediation does not normally include personal devices in scope. However, this is where sub-control 4.4

(security intelligence) may help. If a savvy information security practitioner becomes aware of an important vulnerability in a popular piece of software, she can remind her users to download the update, and this may lead to remediation of software on personal devices as well as corporate ones.

Sub-Control 4.1

Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project). Where feasible, vulnerability scanning should occur on a daily basis using an up-to-date vulnerability-scanning tool. Any vulnerability identified should be remediated in a timely manner, with critical vulnerabilities fixed within 48 hours. (Critical Control 4: Continuous Vulnerability Assessment and Remediation, 2013)

Introduction

Scheduling, updating, and running a vulnerability scan is the simple part! The challenge for many small organizations lies in addressing the vulnerability report in a systematic way.

Though the vulnerability scanner runs automatically, vulnerability scans require judgment and decision making. Vulnerabilities marked “critical” should be resolved as quickly as possible, but lower-priority vulnerabilities should be fixed at the organization’s discretion. In some cases, the return on risk may justify the vulnerability, or the vulnerability may be mitigated by another control. Whether the vulnerabilities are fixed or accepted, all vulnerabilities should be addressed and routed appropriately.

Tools Used in this Recipe

- Kaspersky Endpoint Security for Business Select

Other Options

There are several high-quality, widely-used vulnerability scanners, including Nessus and OpenVas. There are also proprietary, paid solutions, like BeyondTrust’s Retina, Secunia Corporate Security Inspector (CSI) and the Rapid7 Vulnerability Scanner.

For the best results, it helps to use more than one vulnerability scanner, because the methods of scanning (and, therefore, results) may vary across different products. Because Kaspersky scans for application vulnerabilities and not necessarily configuration problems, it is important to regularly schedule and run another vulnerability scan, like Nessus or OpenVAS, to confirm findings and catch additional vulnerabilities.

Getting Ready

This recipe assumes you have Kaspersky Endpoint Security for Business Select installed, and that all of the computers and devices you want to include in your vulnerability scan are included in the console as managed devices.

How to do it…

Setting up a scheduled vulnerability scan with Kaspersky

Kaspersky allows for some simple application vulnerability scanning, as shown below in Figure 22.

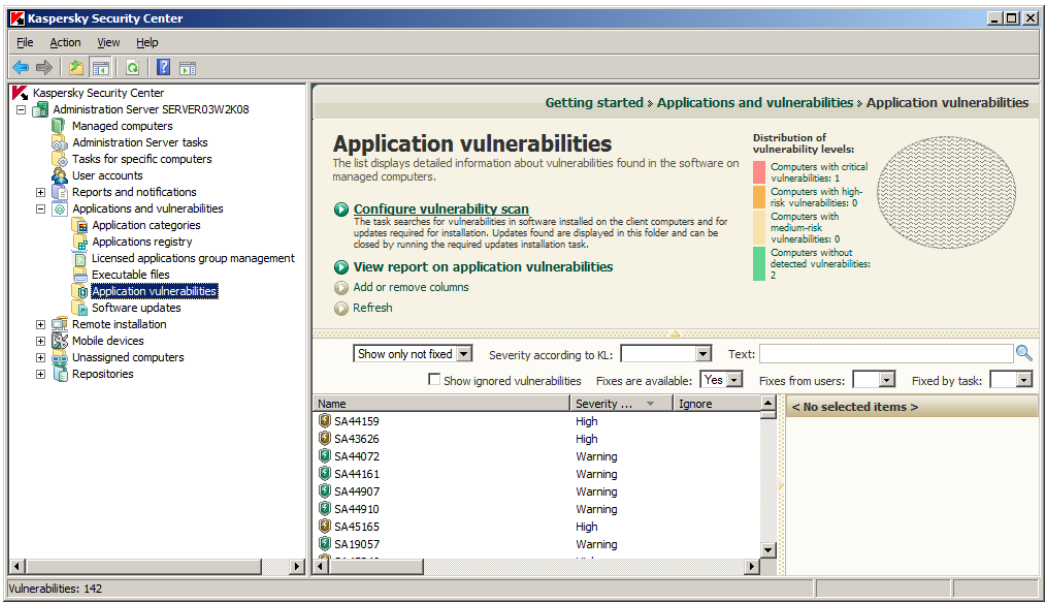


Figure 22

To configure the vulnerability scan task, click “Configure Vulnerability Scan” and double-click on the task.

To schedule a regular (weekly) vulnerability scan, select the “Schedule” section, shown below in Figure 23.

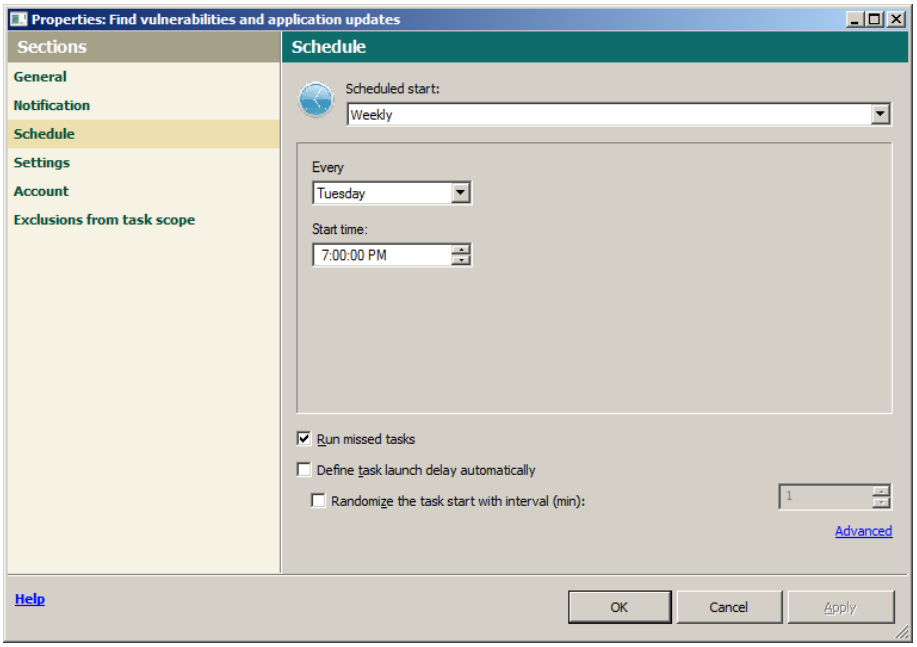


Figure 23

Reviewing vulnerability reports, communicating critical vulnerabilities to the right people, and fixing them quickly is a matter of having the correct communication channels in place, and a solid issue resolution process. Using Spiceworks' service ticket capability, combined with documentation and training, may be the most efficient way to implement this.

Resolving vulnerabilities via software updates with Kaspersky

Once Kaspersky has successfully run a vulnerability report, you can view it through the Security Center. Browse to *Reports and notifications* and click on *Vulnerabilities Report*, as shown below in Figure 24.

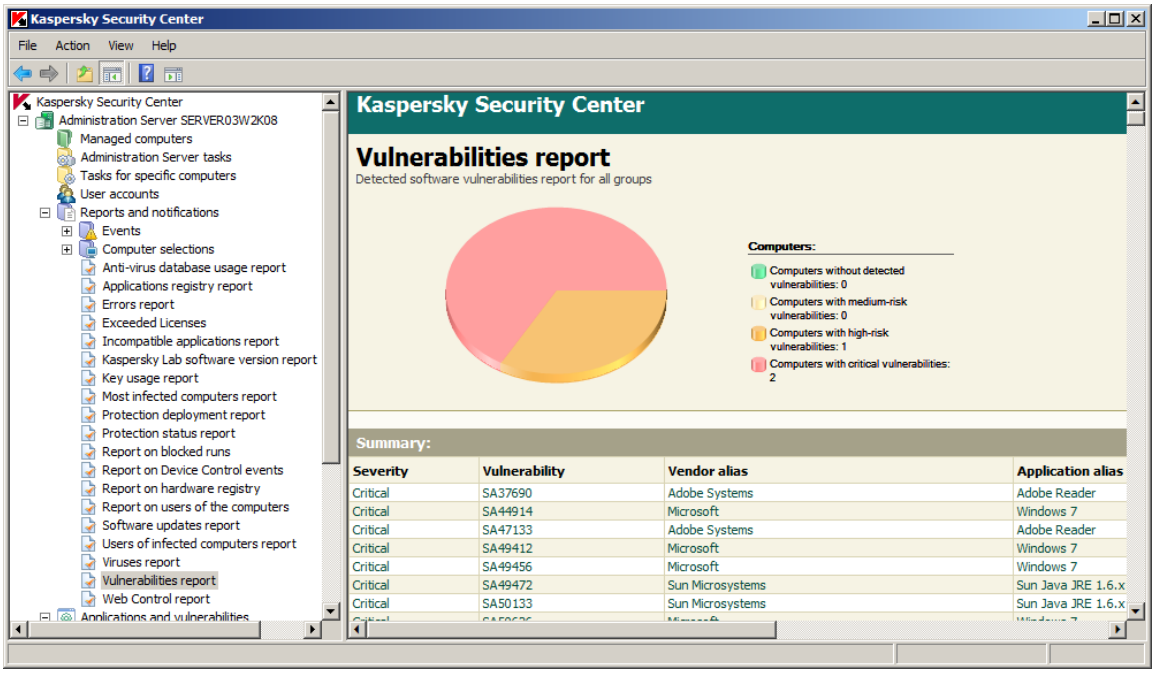


Figure 24

You can get details on each discovered vulnerability by browsing to *Applications and vulnerabilities*, then *Application vulnerabilities*. Double-clicking on any vulnerability will provide you with more detail, as well as the CVEs associated with the vulnerability and additional documentation.

The actions you need to take to remediate vulnerabilities depends on your organizational policy; it is possible that sending updates workstations don't require a change request, but sending an update to a server should result in a scheduled change request so the appropriate parties are notified. Using the tools in this cookbook, a change management notification can be done through the Spiceworks service ticket function.

Some vulnerabilities can be automatically addressed by creating a task in Kaspersky. The steps to create automatic installation of patches and updates are outlined in sub-control 3.2.

See Also

List of SCAPP-Approved Vulnerability Scanning Products (SCAPP-Approved Vulnerability Scanning Products, 2012)

Sub-Control 4.2

Correlate event logs with information from vulnerability scans to fulfill two goals. First, personnel should verify that the activity of the regular vulnerability scanning tools themselves is logged. Second, personnel should be able to correlate attack detection events with earlier vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable. (Critical Control 4: Continuous Vulnerability Assessment and Remediation, 2013)

Introduction

Implementing this sub-control in its entirety is unfortunately beyond the scope of this cookbook—it would require an Intrusion Detection System, Vulnerability Scanner, and a Log Aggregator to all be working together—essentially Security Information and Event Management (SIEM). Instead, this recipe will describe how to automatically generate regular vulnerability event reports from Kaspersky and save them to a local drive, so that they can be referenced and/or correlated as needed.

Tools Used in this Recipe

- Kaspersky Endpoint Protection 10 (Kaspersky)

Getting Ready

This recipe assumes that you have already implemented Kaspersky and the Kaspersky Security Center.

How to do it…

1) Launch the Kaspersky Security Center and navigate to *Reports and notifications.*
2) Right-click on *Vulnerabilities Report*, and select *Send Reports.*
3) Name the Delivery Task to something of your choosing (Daily Vulnerabilities Report, for example) and click *Next.*
4) Change the *Format* to your desired format: HTML, XML, or PDF.
5) Select *Save report to folder,* browse to the location it should be saved to, and then click *Next.*
6) Select the desired schedule that the report should be generated. It is recommended that the schedule be synced to the Kaspersky task that checks/fixes new vulnerabilities—If that task is run daily at 8am, then this report should be run daily at 1pm or thereabouts, to make sure that the previous task has time to complete.
7) Select *Next* and then *Finish.*
8) Run the task now and confirm that the report was generated and saved to the location specified.

See Also

The Open Source SIEM (www.alienvault.com)

Sub-Control 4.3

Use a dedicated account for authenticated vulnerability scans. The scanning account should not be used for any other administrative activities and tied to specific machines at specific IP addresses. Ensure that only authorized employees have access to the vulnerability management user interface and that roles are applied to each user. (Critical Control 4: Continuous Vulnerability Assessment and Remediation, 2013)

Introduction

Vulnerability scan results can be valuable information to an attacker, so it's important to keep the results secure and confidential. In addition to limiting user accounts, it's a good idea to have the traffic resulting from the vulnerability scan encrypted via SSL.

If the account is shared, ensure that you have a process to document which employees have access to the account, and restrict access in whatever way necessary as employees leave (by changing the password or removing access to the account). Better yet, create an administrative vulnerability scanning account for each person who may run it to allow for accountability.

Tools Used in this Recipe

- Kaspersky Endpoint Security for Business, version 10
- Active Directory

Other Options

All that's necessary to implement this control is whatever interface is used to create user and administrative accounts.

Getting Ready

For the sake of our cookbook recipe, we created a new user in Active Directory. However, you may also create a unique internal user within Kaspersky and many other vulnerability scanning applications.

How to do it…

1) In Kaspersky Security Center, select your administration server in the left menu.
2) Click *Action* → *Properties*.
3) Select *Security*, and click *Add* to create a new user for vulnerability scanning.
4) If you choose to use the AD user you created, select *From Windows*. Find the user, as shown below in Figure 25, and click *OK*.

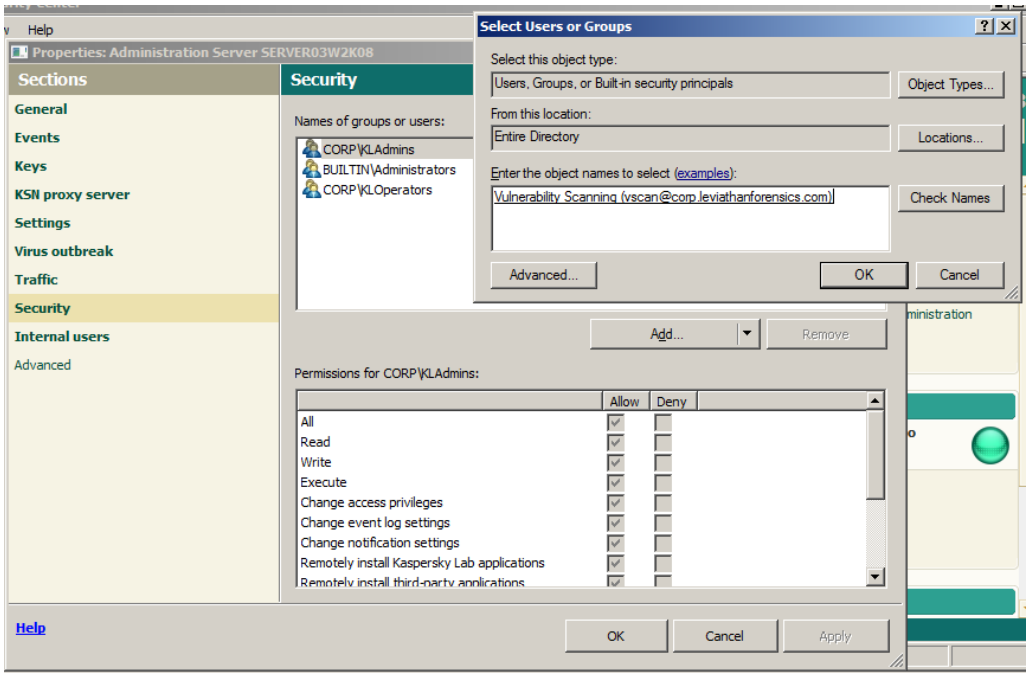


Figure 25

5) It is important to limit the capabilities of the user to completing vulnerability scans. At minimum, the user should have access to *Read* and *Execute* to complete a pre-defined vulnerability scanning task.

Sub-Control 4.4

> Subscribe to vulnerability intelligence services in order to stay aware of emerging exposures, and use the information gained from this subscription to update the organization's vulnerability scanning activities on at least a monthly basis. Alternatively, ensure that the vulnerability scanning tools you use are regularly updated with all relevant important security vulnerabilities. (Critical Control 4: Continuous Vulnerability Assessment and Remediation, 2013)

Introduction

This sub-control presents two options: to parse and analyze security intelligence subscriptions, and to rely on automated updates to vulnerability scanning tools. For a small business with highly limited resources, it is likely more effective to keep scanning tools updated. Email lists are no good if no one reads them. If your time is highly limited and you find yourself ignoring vulnerability alerts or missing them for several days at a time, it may be a better use of time to rely on the automated updates to your vulnerability scan and focus on the results or regular scans. The most critical factor in vulnerability management is whether found vulnerabilities are remediated in a timely manner.

However, if you have the time, security advisories and intelligence can alert you to urgent vulnerabilities, keep you connected with the security community, and provide insight on security trends and threats.

Tools Used in this Recipe

- Kaspersky Endpoint Security for Business Select

Other Options

More proactive administrators may wish to subscribe to vulnerability alerts as time allows, since these can give them the ability to respond to vulnerabilities quickly, or even put protective measures in place for vulnerabilities with as-yet-unavailable patches. It may be time-effective to subscribe to vulnerability alerts from only those vendors from whom you've purchased software, and consolidate them all using an RSS list or dedicated email address. You can also subscribe to a consolidated email list or RSS feed, like the ones in the "Resources" section below.

Getting Ready

This recipe assumes you have deployed Kaspersky's security administration console and endpoints, and that you are using it to scan for vulnerabilities and

How to do it…

By default, Kaspersky checks for updates once every hour and downloads them if they're immediately available. Generally, vulnerability scanners should be updated with the latest signatures prior to running a scan. For a part-time IT resource with limited experience in remediating vulnerabilities, this may be enough.

To check or edit the update task in Kaspersky:

1) Click *Administration Server Tasks*.

2) Double-click *Download Updates to the Repository*.
3) To edit the scheduled time updates are refreshed, click *Schedule* and edit as desired.

See Also

Common Vulnerabilities and Exposures (CVE, 2013)
ICS-Cert Advisories (Information Products, 2013)
CVE Details to create a custom RSS feed containing specific criteria (CVE Details, 2013)

Critical Control 5: Malware Defenses

Malware ranks as the top concern of small business owners (Symantec, JZ Analytics, 2012), possibly because it is such a visible and persistent threat. At best, removing malware from a system takes up valuable time and monetary resources; at worst, it can severely impact information confidentiality, integrity, or availability (CIA triangle).

Though malware is the primary concern of executives, it is the last priority in this cookbook. That may seem counterintuitive. However, Antivirus or anti-malware software on user computers should be the final threshold in a defense-in-depth focused security strategy. If the other Critical Security Controls in this cookbook are implemented correctly, malware should rarely require a defense at the endpoint. Application whitelists prevent executables from being loaded or run on a system. Vulnerability scans, remediation, and security intelligence can prevent malware from taking advantages of known exploits. Secure configuration prevents malware from being able to run and from spreading to other computers. In fact, if CSCs 1-4 are strictly enforced, antivirus software should play only a minor role in an organization's malware defense plan.

As with other CSCs, a solid catalog of procedures is critical to success. Though implementing the top 5 CSCs will go a long way toward preventing malware from infecting systems, incidents must be considered inevitable. Having a change management policy and incident handling policy can help a single IT associate plan and remediate malware incidents as they occur.

Due to the constraints to IT resources in most small businesses, we decided on several features that were critical to us when reviewing an anti-malware solution. The software we picked must:

- Fulfill the maximum number of controls specified in the 20 CSCs at a competitive (or free) cost
- Be centrally managed with an intuitive interface
- Have highly automated tasks and updates
- Effectively remove malware
- A good history of support and stability
- Available support in the event of zero-day malware incidents

Most of this section focuses on Kaspersky as a malware defense tool. At first, in an attempt to keep cost down, we researched and evaluated a number of free anti-malware solutions. However, none permitted the central management that is so critical to maximizing efficiency, none provided an acceptable level of support, and all of them lacked features that covered the top-rated 20 CSCs. We expanded our search to include competitively-priced malware solutions.

Kaspersky won out with competitive pricing (between $16-50, depending on licensing requirements), a solid stance in the anti-malware market, and features like application whitelisting, centralized application patch management, scheduled task management, and vulnerability scanning.

We should note here that Kaspersky is far from the only option for anti-malware. When simplifying the tools an IT resource is expected to learn and manage, we found Kaspersky to be the best choice to illustrate the sub-controls presented here. There are many options out there, and the market changes quickly!

If your small business opts to implement software from a different malware defense vendor, we recommend adhering to the criteria listed above. Organizations should evaluate whether the software is capable of implementing the sub-controls listed in this CSC.

Sub-Control 5.1

Employ automated tools to continuously monitor workstations, servers, and mobile devices for active, up-to-date anti-malware protection with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers. The endpoint security solution should include zero-day protection such as network behavioral heuristics. (Critical Control 5: Malware Defenses, 2013)

Introduction

Typically on the enterprise level, anti-malware software runs on each computer or device, while reporting in to a central administration console. The administration console gathers data and logs, generates alerts, provides notification of updates, and allows for configuration on a larger scale. A centralized console can also correlate events, like multiple computers being infected with the same virus.

Though it may be tempting to save money by using standalone "free" antivirus software, managing configuration and incident response centrally is critical to securing a small business. Saving money on anti-malware deployment may well cost more in administration and incident-related costs in the long run.

Tools Used in this Recipe

- Kaspersky Endpoint Security for Business, version 10

Other Options

The anti-malware vendor space is broad, with more options than it's possible to cover here. More popular vendors of anti-malware capabilities include Trend Micro**,** Sophos**,** McAfee, and Norton. Free anti-malware tools (as of the writing of this paper in 2013) generally do not fit the criteria required for this sub-control, since they have limited licensing and do not allow for centralized administration.

Getting Ready

In order to protect all the devices and computers on your network, you need to be aware of them. Therefore, it's vital to complete work on CSC 1, Inventory of Authorized and Unauthorized Devices, prior to implementing this control. Once you have an accurate inventory of devices, you can create a plan for installing and managing anti-malware software across devices.

How to do it…

The majority of anti-malware tools currently available scan, update, and report on results automatically, and Kaspersky is no exception.

Kaspersky allows for centralized management, logging, and administration of client computers, as shown below in Figure 26.

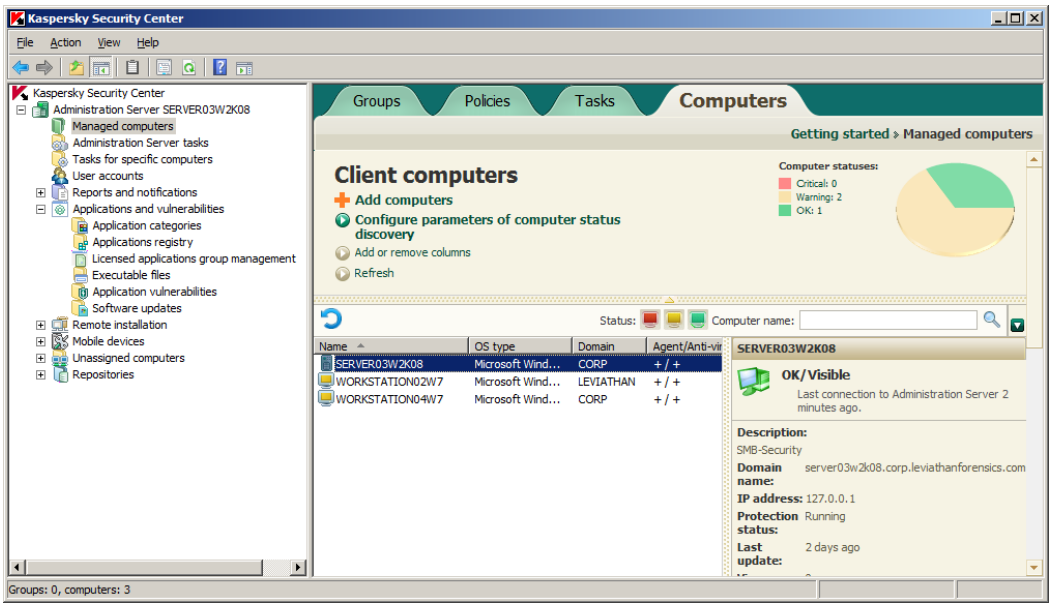


Figure 26

Many anti-malware packages include features that can ensure computers on your network continue being protected over time. These include:

- The ability to set a password to prevent antivirus software from being disabled or uninstalled, either by the user or by malware itself
- Automatic and frequent updates of the anti-malware software engine, administrator-set configuration, and malware or whitelist signatures
- Automatic polling of your network to detect unprotected computers
- Alerting administrators via SMS or email when events occur, or when events reach a threshold that indicates an ongoing incident
- Customizable reporting

Sub-Control 5.2

Employ anti-malware software and signature auto-update features or have administrators manually push updates to all machines on a daily basis. After applying an update, automated systems should verify that each system has received its signature update. (Critical Control 5: Malware Defenses, 2013)

Introduction

Tools Used in this Recipe

- Kaspersky Endpoint Security for Business, version 10

Other Options

Generally, all centrally-managed anti-malware software includes the ability to update endpoints.

Getting Ready

This recipe requires that you have deployed Kaspersky to endpoints, and that they are managed centrally by the Security Center.

How to do it…

Generally, updates and resulting reports are configured automatically for modern anti-malware software, and no further configuration is needed. However, you may want to configure notification when updates fail, because it may indicate a problem with the client.

By default in Kaspersky, updates are installed whenever updates are downloaded to the repository, and are then distributed to all managed clients. Updates can be configured and validated by selecting *Managed Computers*, and clicking the *Tasks* tab.

As you can see here in Figure 27, the *Download update* task is highlighted in red, because at least one of the managed computers did not complete an update successfully.

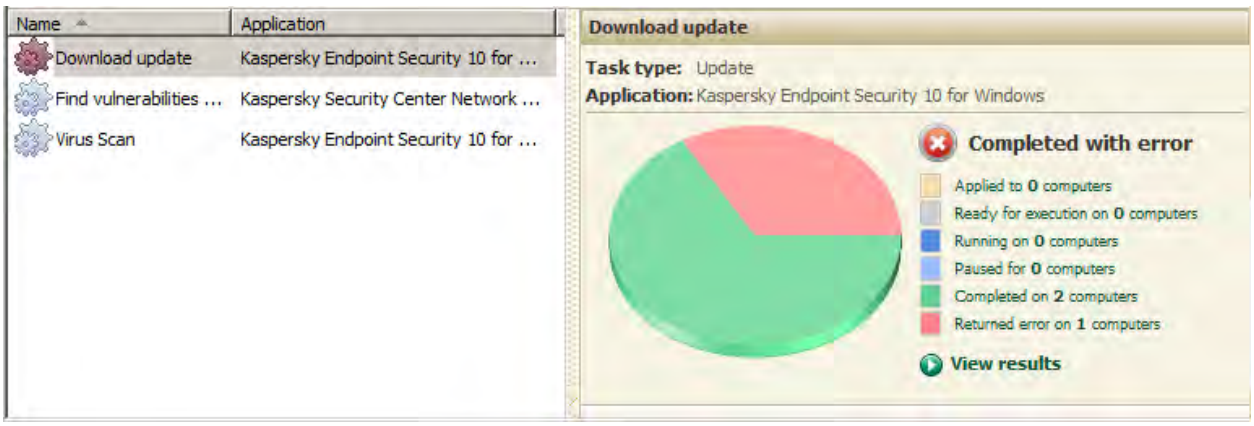


Figure 27

You can further configure updates by double-clicking the *Download update* task. If you are interested in computers that fail to receive updates, you can configure the update task to notify you of any errors, so

you can re-attempt the update or fix the problem. This is done by double-clicking the task and selecting *Notification*, as shown in Figure 28.

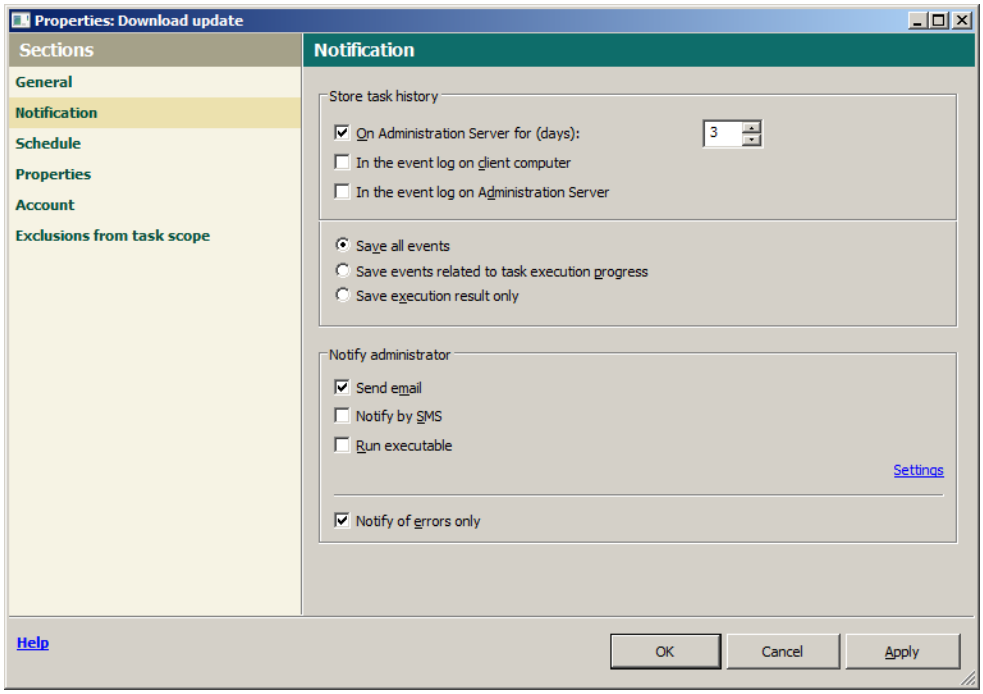


Figure 28

Sub-Control 5.3

Configure laptops, workstations, and servers so that they will not auto-run content from USB tokens (i.e., "thumb drives"), USB hard drives, CDs/DVDs, Firewire devices, external serial advanced technology attachment devices, mounted network shares, or other removable media. If the devices are not required for business use, they should be disabled. (Critical Control 5: Malware Defenses, 2013)

Introduction

Malware distributed through removable media dates all the way back to floppy drives, but it continues to be a highly effective way to spread viruses. Disabling autorun can stop a virus from spreading through a department via shared drives, or from spreading to an entire organization through a network share.

Tools Used in this Recipe

- Kaspersky Endpoint Security for Business Select

Other Options

Autorun can be disabled in modern distributions of Windows by editing the registry or through GPO. For the steps to disable Autorun in different versions of Windows, follow the links in the “See Also” section of this sub-control.

Getting Ready

This recipe assumes that you have Kaspersky deployed at endpoints and controlled by an administrative server. In Kaspersky, autorun on removable media is disabled by default, since this is a common method for malware to spread.

In order to have access to device control, you must enable the Advanced Anti-Malware interface in Kaspersky. Select your administration server, and click *View* → *Configure Interface*. Select *Display Advanced Anti-Malware* as shown below in Figure 29.

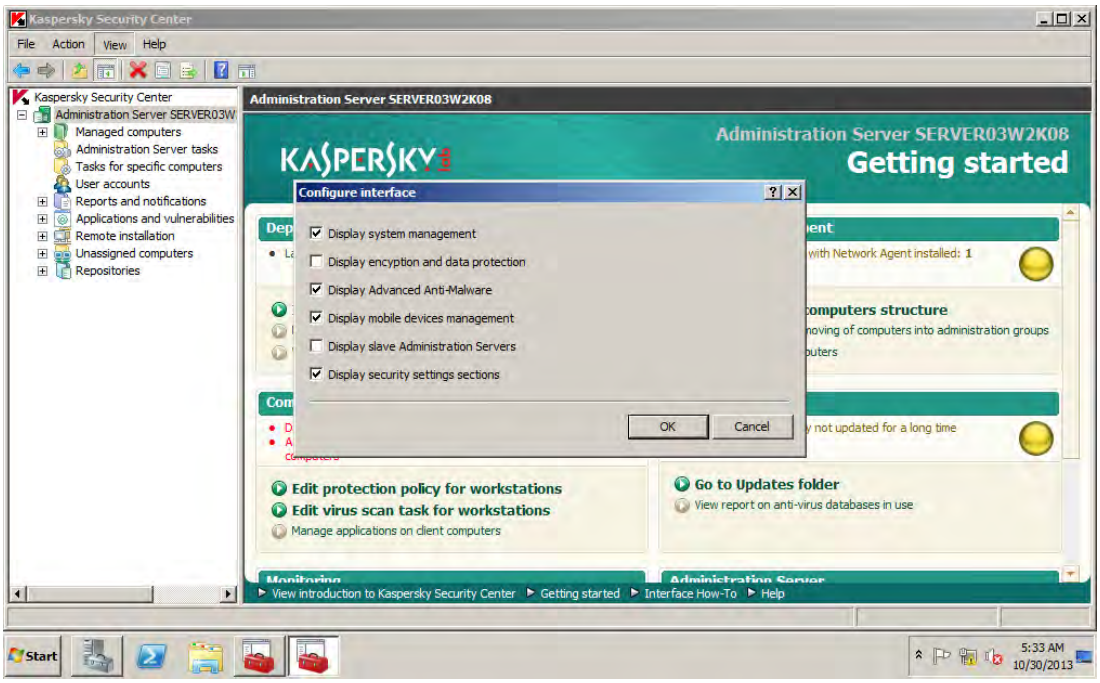


Figure 29

How to do it…

Creating an anti-autorun policy

Once again, application white and blacklisting come in handy here. Other anti-malware or security management products may simply have an option or checkbox to disable autorun.

1) Go to *Applications and vulnerabilities*, then *Application Categories*. Click *Create a category*, as shown below in Figure 30.

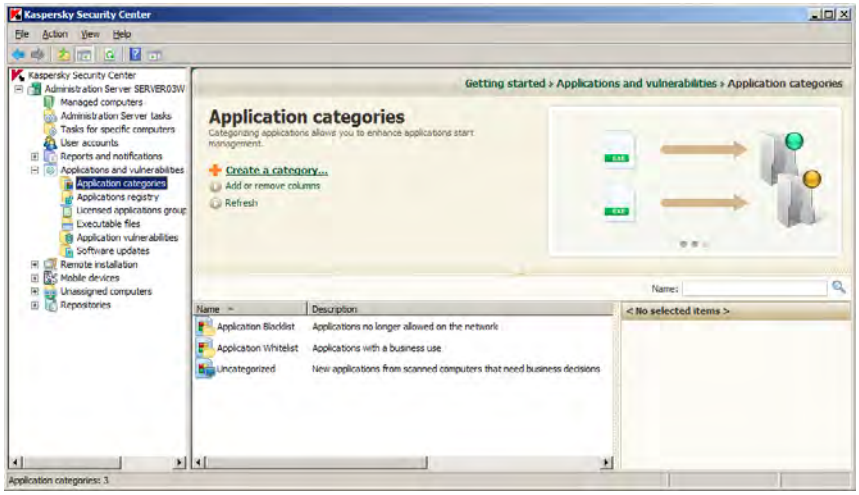


Figure 30

2) Select *Category with content added manually*.

3) Select a name for the category, like “Anti-autorun”.
4) Click *Add*, and select *From file properties*.
5) Under *File name*, type “autorun.inf”, as shown below in Figure 31. This is the filename recognized by Windows to automatically run the executables listed within that script. Blacklisting the file this way will prevent it from running from any source, including network shares and removable media.

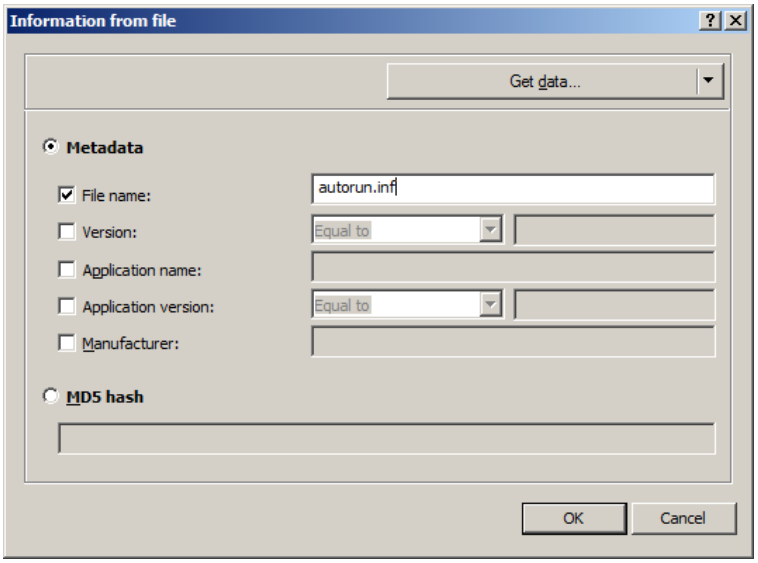


Figure 31

6) Click *OK*, *Next*, and *Finish* to complete the creation of the category.
7) To apply the category, on the sidebar, click *Managed Computers*, select the *Policies* tab, and double-click the policy that applies to your computers. Select *Application Startup Control*, as shown below in Figure 32.

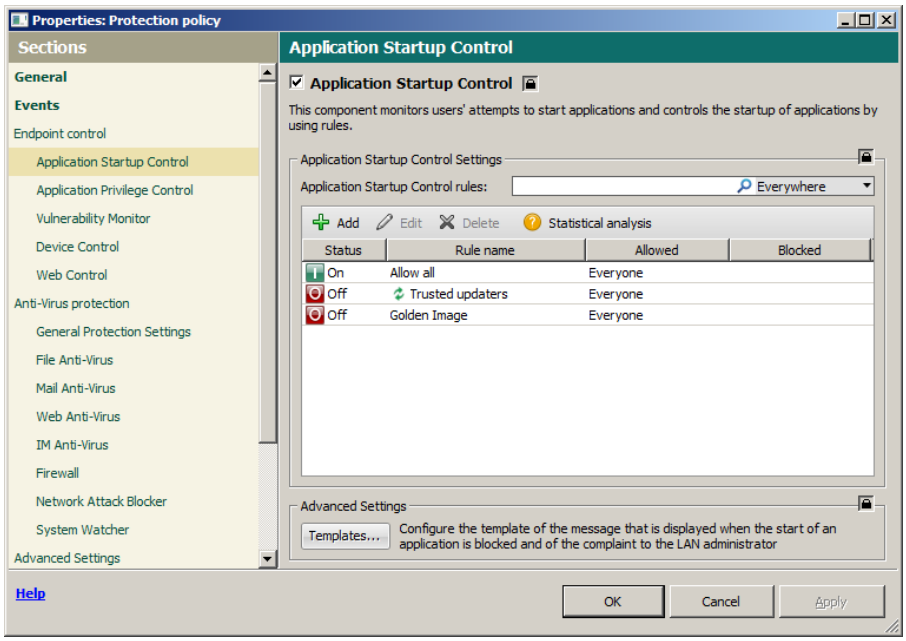


Figure 32

8) Click *Add*. Under *Category*, select the anti-autorun category you just created, as shown in Figure 33.

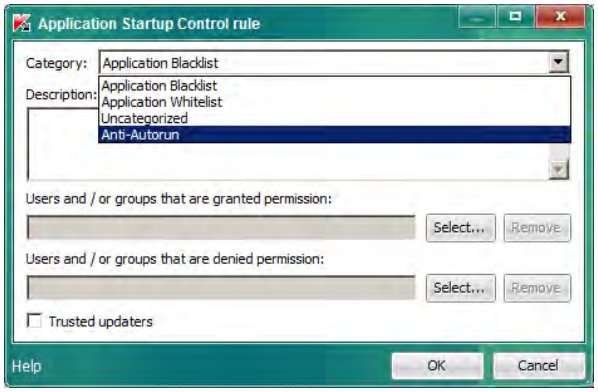


Figure 33

9) Click *OK*. You will receive a warning dialog box telling you all users will be prohibited from starting applications corresponding to the rule. Click *Yes*.

You have now prohibited autorun.inf from running.

Disabling Devices

If devices are not required for business use, they should be disabled. To disable device types in Kaspersky, follow the following steps.

1) Select *Managed Computers*, then click on the *Policies* tab. Double-click the policy you want to change.

2) Within the *Device Control* section of the policy, you can disable specific types of devices. The device control policy also allows for notifying users that the device has been blocked, and provides a way for users to notify the administrator to request an exception (which would be added under "Trusted Devices").

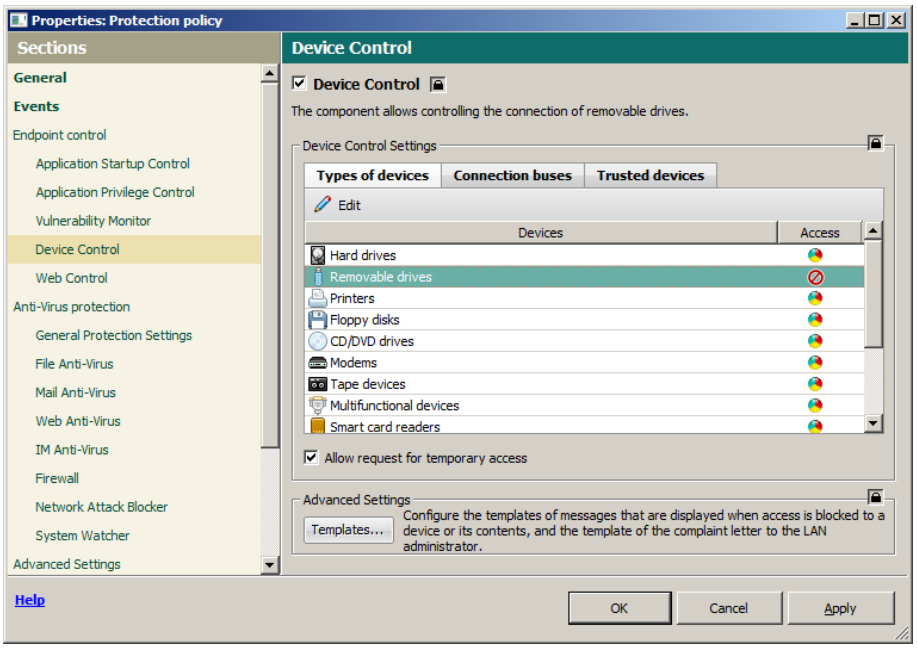


Figure 34

See Also

How to disable the Autorun function in Windows (Disable the Autorun Function in Windows, 2013)

Sub-Control 5.4

Configure systems so that they conduct an automated anti-malware scan of removable media when it is inserted. (Critical Control 5: Malware Defenses, 2013)

Introduction

When combined with sub-control 5.3, this control effectively prevents the spread of malware through removable media and shared network resources.

Tools Used in this Recipe

- Kaspersky Endpoint Security for Business, version 10

Other Options

Other anti-malware software packages can also scan removable media when it is inserted; in fact, this is a highly common functionality.

Getting Ready

This recipe requires that you have deployed Kaspersky to endpoints, and that they are managed centrally by the Security Center.

How to do it…

1) Go to your managed computers and click on the *Tasks* tab. Right-click the policy that applies to your workstations and select *Properties*. Go to *Advanced Settings* → *Application Settings*.

2) Under Action on *Removable Drive Connection*, select *Full Scan*, as shown below in Figure 35. If users connect large drives to their computers frequently, it may be better to select *Quick Scan* to optimize performance.

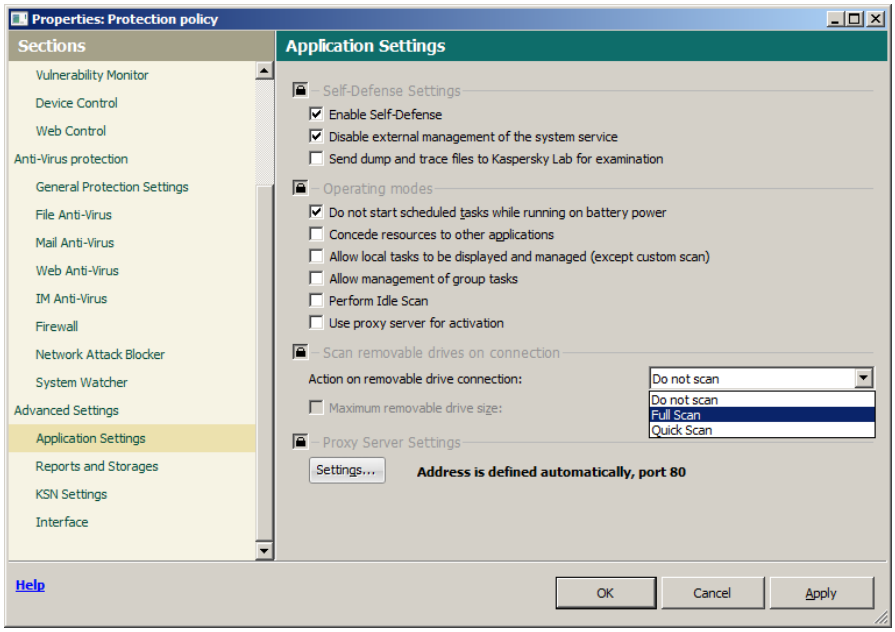


Figure 35

Obviously, this takes effect only on drives that are not disabled by Device Control.

Sub-Control 5.5

Scan and block all e-mail attachments entering the organization's e-mail gateway if they contain malicious code or file types unneeded for the organization's business. This scanning should be done before the e-mail is placed in the user's inbox. This includes e-mail content filtering and web content filtering. (Critical Control 5: Malware Defenses, 2013)

Introduction

Email spam and malware are inextricably linked with each other. Often, email is generated from pre-infected computers or botnets, and sent on to infect further computers. Though this is an older method of infection, it's still easy and highly effective for attackers.

It is worthwhile to scan for both incoming and outgoing malware within email at the gateway. However, due to the volume of incoming malware, you may want to set alerts only for outgoing infected email.

Tools Used in this Recipe

- Kaspersky Endpoint Security for Business Select

Other Options

Most anti-malware vendors, including Kaspersky, include scanning products specifically for mail gateways as part of their offering. MailScanner and ClamAV are two popular free scanning solutions for email gateways.

Getting Ready

This recipe requires that you have deployed Kaspersky to endpoints, and that they are managed centrally by the Security Center.

How to do it…

This control can be implemented at at least two points in a network: at the mail server, and as the mail is sent to the user (but before it is accessible). For the sake of defense-in-depth, it is a good idea to scan email at both points.

Scanning at the Gateway

Due to the need for high performance, email gateway antivirus products are typically developed and sold separately from endpoint security. Given this paper's focus on implementing a minimum of tools within a small business, this is out of the scope of the paper.

Scanning at endpoints

In Kaspersky, email scanning is managed as part of a general antivirus policy.

1) To view options, select your managed computers in the sidebar, select the *Policies* tab, and double-click the policy that applies to the computers you want to protect. Select the *Mail Anti-Virus* section, as shown below in Figure 36.

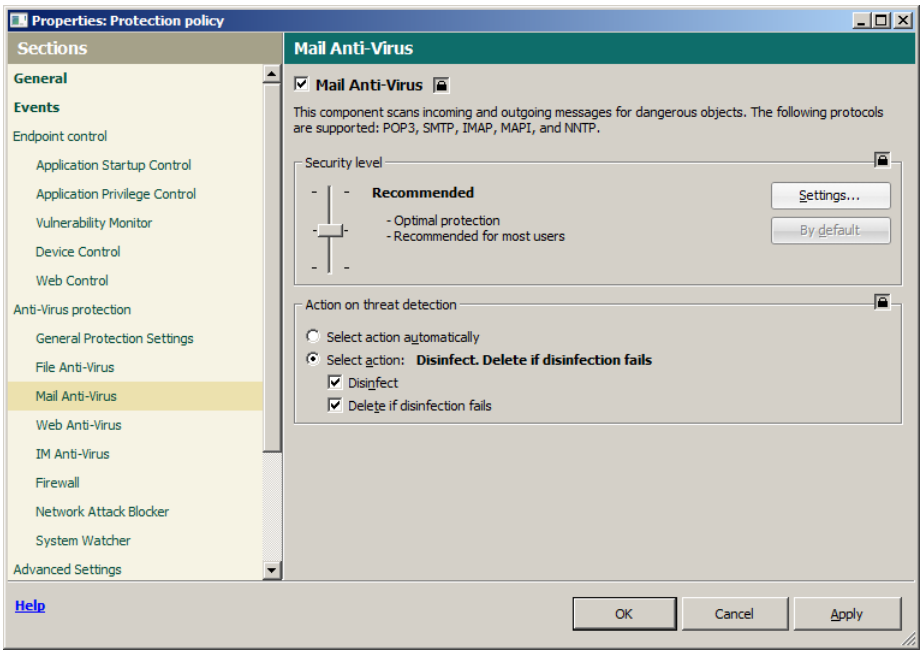


Figure 36

2) To manage additional settings, including blocking specific types of attachments, click the *Settings* button, which presents the options shown below in Figure 37.. One of the more useful features is to block specific high-risk attachments, like .cmd and .exe files, which are executables that could include malware.

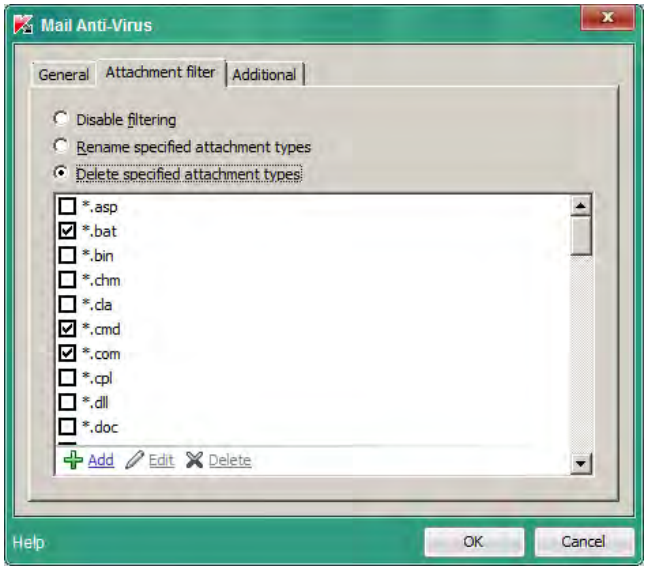


Figure 37

See Also

Clam AV (Clam AV, 2013)

Mailscanner (MailScanner, 2013)

Sub-Control 5.6

Apply anti-virus scanning at the Web Proxy gateway. Content filtering for file-types should be applied at the perimeter. (Critical Control 5: Malware Defenses, 2013)

Introduction

The web continues to be a primary source of malware. Browser vulnerabilities and unaware users both contribute to the proliferation of malware via web surfing. The advantage of adding web-specific protection to endpoints is that the endpoints are secured regardless of which network the endpoint connects to, making it ideal for laptops and mobile devices.

Tools Used in this Recipe

- Kaspersky Endpoint Security for Business, version 10

Other Options

Similarly to email gateway scanning, web proxy scanning has special performance and protocol considerations that make the application work differently from endpoint protection. Therefore, it is typically sold separately or as a part of a bundle by the same anti-malware vendors that provide endpoint protection.

Given this paper's focus on implementing a minimum of tools to manage within a small business, evaluating web proxy gateway scanning is out of the scope of the paper. However, there are several low-cost and low-maintenance web proxy antivirus scanners out there, including SquidClamav.

Getting Ready

This recipe requires that you have deployed Kaspersky to endpoints, and that they are managed centrally by the Security Center.

How to do it…

1) In Kaspersky, select *Managed Computers* in the sidebar. Select the *Policies* tab and double-click the policy that protects your computers. Click the *Web Control* section, as shown below in Figure 38.

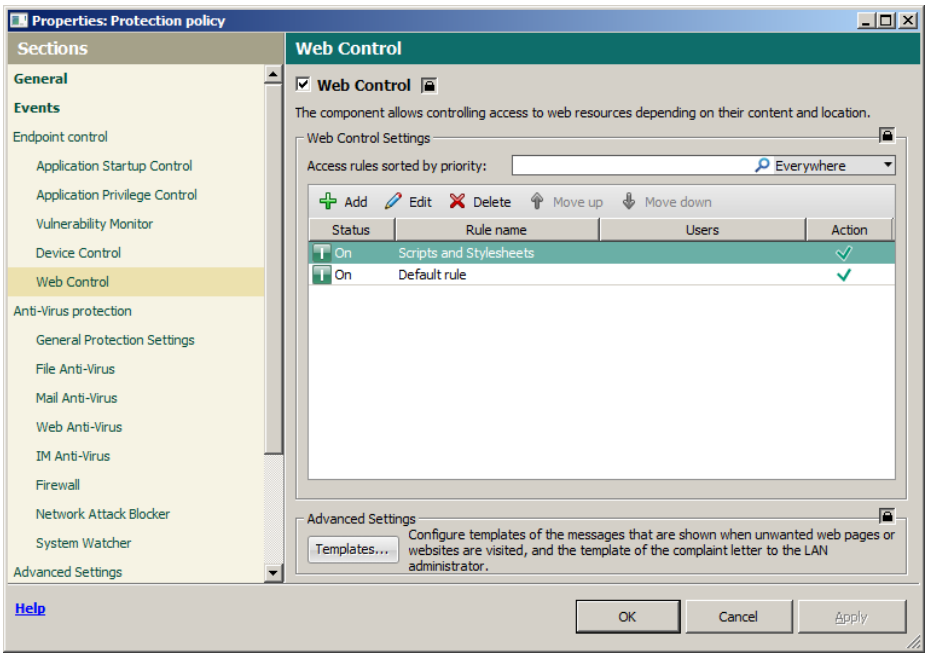


Figure 38

2) As shown in Figure 39, you can add policies to protect against risky content by clicking the "Add" button:

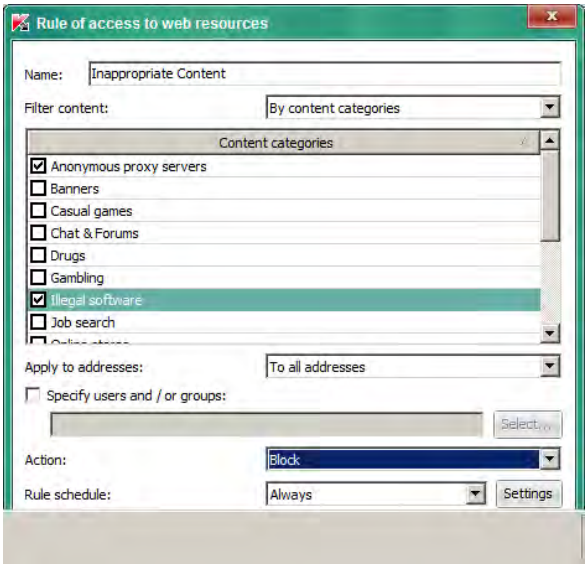


Figure 39

3) You can also filter by type of data (like streaming video), or specify websites to white/blacklist with wildcards, as shown below in Figure 40.

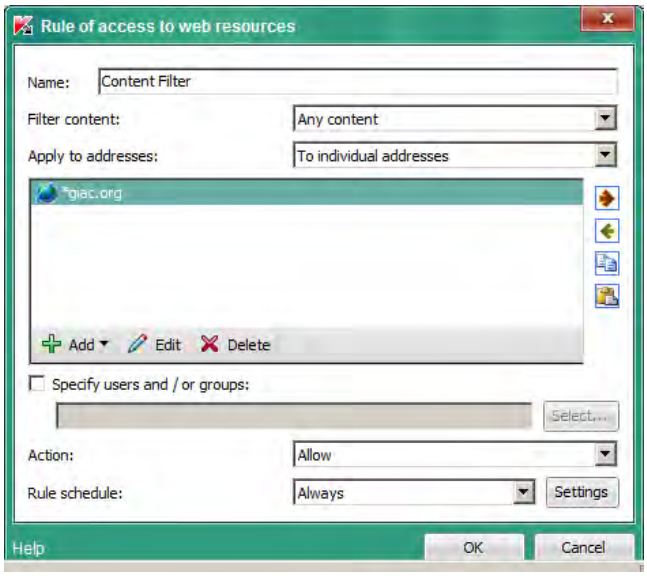


Figure 40

See Also

SquidClamav (SquidClamAV, 2013)

Sub-Control 5.7

Deploy features and toolkits such as Data Execution Prevention (DEP) and Enhanced Mitigation Experience Toolkit (EMET), products that provide sandboxing (e.g., run browsers in a Virtual Machine), and other techniques that prevent malware exploitation. (Critical Control 5: Malware Defenses, 2013)

Introduction

This recipe describes how to implement sub-control seven. EMET, which includes DEP and a number of other hardening features, will be one of the very few applications installed in the reference images created in CSC 1. These reference images can then be deployed to both domain and standalone Windows computers.

Tools Used in this Recipe

- Microsoft Deployment Toolkit 2013 (MDT)
- Microsoft Group Policy (GP or GPO)
- Enhanced Mitigation Experience Toolkit 4.0 (EMET)

Getting Ready

This recipe assumes that you have already implemented WDS and MDT (or another imaging solution), and have at least one reference image for your devices.

How to do it…

1) First, EMET needs to be downloaded and saved to a location that will be accessible by the MDT server. [ref1]
2) Open up the MDT Deployment Workbench, and import the EMET MSI. The silent install command is as follows:

   "msiexec /i "EMET Setup.msi" /qn /norestart"
3) Deploy the reference image to the reference computer and select the option to install EMET. Confirm that it installed correctly.
4) Once EMET is installed, it needs to be configured. For domain workstations and servers, this can be done through a GPO. From the EMET User's Guide: [ref]

When EMET is installed, EMET.admx and EMET.adml files are also installed to the "Deployment\Group Policy Files" folder. These files must then be copied onto \Windows\PolicyDefinitions and \Windows\PolicyDefinitions\en-US folders respectively. Once this is done, EMET system and application mitigation settings can be configured via Group Policy.

5) Once the EMET settings can be configured via Group Policy, create a new GPO targeting the computer objects, and go through the seven sets of policies available, which are listed below, from the EMET User's Guide: [ref1]
6) System Mitigations: Named System ASLR, System DEP and System SEHOP, these policies are used to configure system mitigations. Please note that modifying system mitigation settings may require a reboot to be effective.

7) Default Protection: There are three: Internet Explorer, Recommended Software, and Popular Software. Protection Profiles are pre-configured EMET settings that cover common home and enterprise software. Apply these policies to enable them.
8) Application Configuration: This leads to a freeform editor where additional applications not part of the default protection profiles can be configured. The syntax is application executable name followed by an optional list of mitigations that does not need to be enabled. If no mitigation is specified, all EMET application mitigations will be enabled.
9) Default Action and Mitigation Settings: These settings are related to the advanced settings for the ROP mitigations, described in section 1.2.9, and for the default action when an exploit is detected (Audit only or Stop).
10) EMET Agent Visibility: This setting allows to automatically hide the EMET Agent icon in the tray area of the taskbar.
11) EMET Agent Custom Message: This entry allows to define a customized message that will be displayed in the alert that is shown when EMET detects an attack. The Tray Icon reporting setting must be turned on to display this message.
    a. *Reporting*: This entry allows to toggle the reporting configuration for the Windows Event Log, the Tray Icon, and the Early Warning Program.
12) For standalone workstations, use the previously referenced Group Policy templates to import into the Local Group Policy Editor (To automate it, this step could actually be done on the reference image for both domain and standalone workstations—domain workstation's local Group Policy will be overridden by the Domain Group Policy)
13) For both domain and standalone workstations, once EMET has been configured with Group Policy, the following command must be run to make them effective: (just run it via another GPO, or every time the system restarts)

    "EMET_Conf --refresh"
14) The last thing to keep in mind is that as new and updated tools like EMET are released, they should be integrated into the business environment as soon as possible, as another defensive layer against Malware.

See Also

EMET v4 review & extensive tutorial (Ljubuncic, 2013)

Sub-Control 5.8

Limit use of external devices to those that have a business need. Monitor for use and attempted use of external devices. (Critical Control 5: Malware Defenses, 2013)

Introduction

This sub-control ties into several other parts of the Critical Security Controls, especially CSC 1 (Inventory of Authorized and Unauthorized Devices). Any device with storage capability can be used to house and distribute malware, including smartphones, digital cameras, music players, and even digital photo frames.

The usage of personal and external devices should be specified in the organization's Acceptable Use Policy, but it can be controlled or limited with software policies.

Tools Used in this Recipe

- Kaspersky Endpoint Security for Business Select

Other Options

Microsoft has some capabilities built in to Group Policy that allows for disabling the installation of new device drivers, as documented in the URL in the "See Also" section. The Data Loss Prevention (DLP) vendor space, which includes Lumension, GFI, McAfee, and Bitdefender, also provides many options for granular device control and monitoring.

Getting Ready

This recipe requires that you have deployed Kaspersky to endpoints, and that they are managed centrally by the Security Center.

How to do it…

Kaspersky allows control over external devices by way of the Device Control section of security policy. Attempted and successful use of devices can be viewed in the event logs of the Kaspersky Security Center, as shown below in Figure 41.

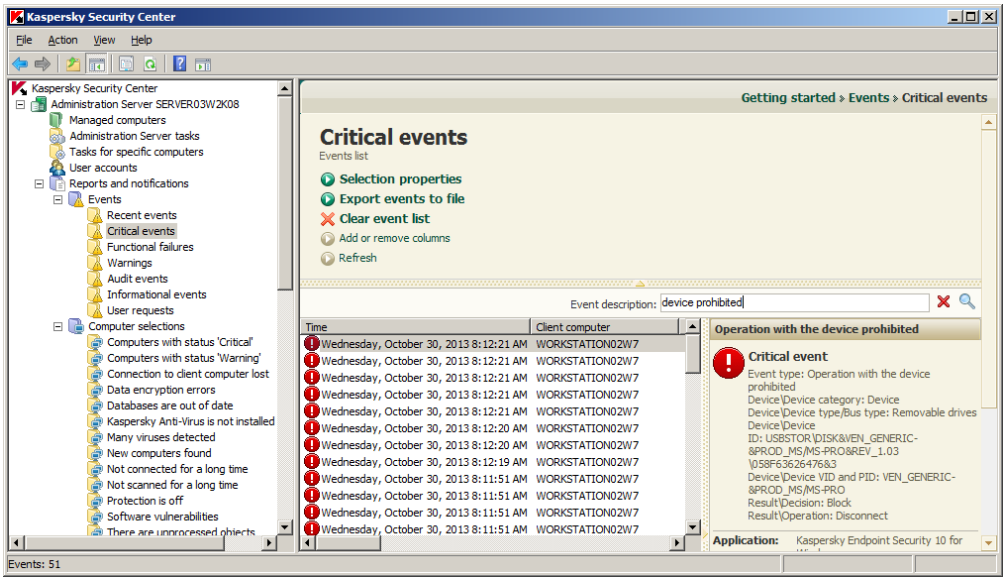


Figure 41

See Also

Step-by-step Guide to Controlling Device Installation Using Group Policy (Controlling Device Installation Using Group Policy, 2013)

Conclusion

The 20 Critical Security Controls are an industry-recognized list of controls that help organizations better manage their digital risk. Small businesses account for more the half of private sector workers. They are often the target of cyber-attacks and many have been compromised multiple times. Small businesses have unique constraints compared to their enterprise counterparts including limited financial and staffing resources. The recipes provided in this paper provide specific actions (recipes) that small businesses can take to protect their critical information and assets, based on the 20 Critical Security Controls. The focus is on "Quick Wins" that provide the largest risk reductions with the smallest amount of effort. The hands-on recipes aid small organizations in implementing the most effective solutions for the most common information security problems. Following these steps will set a small business on a solid foundation of sound security principles.

References

(n.d.). Retrieved November 2, 2013, from www.alienvault.com: http://www.alienvault.com/open-threat-exchange/projects

How to Add Local Users and Groups with a Batch File Distribution Package. (2008, January 26). Retrieved November 2, 2013, from LANDesk: http://community.landesk.com/support/docs/DOC-2413

ISO/IEC 13335-1:2004. (2008). Retrieved from iso.org: http://www.iso.org/iso/catalogue_detail.htm?csnumber=39066

Delete/remove local user from local admin gro [Solved]. (2009). Retrieved November 2, 2013, from Kioskea: http://en.kioskea.net/forum/affich-36226-delete-remove-local-user-from-local-admin-gro

(2010, January 31). Retrieved from Fisher College of Business Information Security: http://fisher.osu.edu/supplements/10/8803/FCOB-LAPS.pdf

Administrative/Special Access Policy. (2011). Retrieved November 2, 2013, from Larmar University: http://facultystaff.lamar.edu/it-services-and-support/policies/administrativespecial-access-policy.html

Description of User Account Control and Remote Restrictions in Windows Vista. (2011, September 23). Retrieved October 21, 2014, from support.microsoft.com: http://support.microsoft.com/kb/951016

Frequently Asked Questions about Small Business. (2012, September). Retrieved November 2, 2013, from sba.gov: http://www.sba.gov/sites/default/files/FAQ_Sept_2012.pdf

SCAPP-Approved Vulnerability Scanning Products. (2012, 11 01). Retrieved from nist.gov: http://nvd.nist.gov/scapproducts.cfm

20 Critical Security Controls. (2013). Retrieved October 15, 2013, from sans.org: http://www.sans.org/critical-security-controls/guidelines.php

Adding New Devices - Spiceworks. (2013). Retrieved October 20, 2013, from http://community.spiceworks.com/help/Adding_New_Devices

Clam AV. (2013, 11 1). Retrieved from clamav.net: http://www.clamav.net

Controlling Device Installation Using Group Policy. (2013, 11 1). Retrieved from microsoft.com: http://msdn.microsoft.com/en-us/library/bb530324.aspx

Critical Control 1: Inventory of Authorized and Unauthorized Devices. (2013). Retrieved October 22, 2013, from sans.org: http://www.sans.org/critical-security-controls/control.php?id=1

Critical Control 2: Inventory of Authorized and Unauthorized Software. (2013, 11 1). Retrieved from sans.org: http://www.sans.org/critical-security-controls/control.php?id=2

Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers. (2013). Retrieved October 22, 2013, from sans.org: http://www.sans.org/critical-security-controls/control.php?id=3

Critical Control 4: Continuous Vulnerability Assessment and Remediation. (2013, 11 1). Retrieved from sans.org: http://www.sans.org/critical-security-controls/control.php?id=4

Critical Control 5: Malware Defenses. (2013, 10 31). Retrieved from sans.org: http://www.sans.org/critical-security-controls/control.php?id=5

CVE. (2013, 11 1). Retrieved from mitre.org: http://cve.mitre.org/

CVE Details. (2013, 11 1). Retrieved from cvedetails.com: http://www.cvedetails.com/

Deploy Folder Redirection, Offline Files, and Roaming User Profiles. (2013, July 3). Retrieved November 2, 2013, from TechNet: http://technet.microsoft.com/en-us/library/jj649074.aspx

Disable the Autorun Function in Windows. (2013, 11 1). Retrieved from microsoft.com: http://support.microsoft.com/kb/967715

Getting Started - Spiceworks. (2013). Retrieved October 20, 2013, from http://community.spiceworks.com/help/Getting_Started#Inventory

Help and Documentation - Spiceworks. (2013). Retrieved October 20, 2013, from http://community.spiceworks.com/help/

How to Make a Domain User the Local Administrator for all PCs. (2013, October 29). Retrieved November 2, 2013, from TechNet: https://social.technet.microsoft.com/wiki/contents/articles/7833.how-to-make-a-domain-user-the-local-administrator-for-all-pcs.aspx

Information Products. (2013, 11 01). Retrieved from us-cert.gov: http://ics-cert.us-cert.gov/Information-Products

Installing Kaspersky Endpoint Security 10 for Windows via command line prompt. Silent installation. (2013, March 13). Retrieved November 2, 2013, from Kaspersky Support : http://support.kaspersky.com/us/9363

ITIL Home. (2013, 11 02). Retrieved from ITIL Home: http://www.itil-officialsite.com/

MailScanner. (2013, 11 1). Retrieved from mailscanner.info: http://www.mailscanner.info/

Microsoft Security Compliance Manager. (2013, January 28). Retrieved November 2013, 2013, from TechNet: http://technet.microsoft.com/en-us/library/cc677002.aspx

Microsoft Security Compliance Manager (SCM) - Getting Started. (2013, January 29). Retrieved November 2, 2013, from TechNet: http://social.technet.microsoft.com/wiki/contents/articles/1866.microsoft-security-compliance-manager-scm-getting-started.aspx

More About DHCP Audit and Event Logging. (2013). Retrieved October 20, 2013, from http://technet.microsoft.com/en-us/library/dd759178.aspx

Purchasing - Spiceworks. (2013). Retrieved October 20, 2013, from Help and Documentation - Spiceworks

SquidClamAV. (2013, 11 1). Retrieved from darold.net: http://squidclamav.darold.net/

SSH. (2013). Retrieved October 23, 2013, from https://help.ubuntu.com/community/SSH

Survey Shows Small Businesses Have Big Data Breach Exposure. (2013, March 6). Retrieved November 2, 2013, from http://www.hsb.com/HSBGroup/Subpage.aspx?id=579

Windows Deployment Services Getting Started Guide for Windows Server 2012. (2013, June 17). Retrieved November 2, 2013, from TechNet: http://technet.microsoft.com/en-us/library/jj648426.aspx

Add an Active Directory group to the local administrator group of workstation(s). (n.d.). Retrieved November 2, 2013, from Spiceworks: http://community.spiceworks.com/how_to/show/2123-add-an-active-directory-group-to-the-local-administrator-group-of-workstation-s

Andre Hall, R. P. (2012, February 20). *Kaspersky Application Control and Default Deny Using Whitelisting Comparative Report.* Retrieved from West Coast Labs: http://www.westcoastlabs.com/downloads/productTestReport_0076/Application_Control_and_Whitelisting.pdf

AT&T. (2012). *AT&T Small Business Tech Poll 2012.* Retrieved from att.com: http://www.att.com/Common/about_us/files/pdf/national_findings_fact_sheet_wireless.pdf

Bauer , N. (2013, July 17). *The Sometimes Confusing Relationship Between WDS and MDT*. Retrieved November 2, 2013, from uiu4you.com: http://www.uiu4you.com/Blog/tabid/169/PostID/131/Default.aspx

Beechey, J. (2010, December). *sans.org.* Retrieved from sans.org: http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599?show=application-whitelisting-panacea-propaganda-33599&cat=application

Certified Professionals: Advisory Board. (n.d.). Retrieved November 4, 2013, from giac.org: http://www.giac.org/certified-professionals/advisory-board

CompTIA. (2011). *Small and Medium Business Technology Adoption Trends.* CompTIA Member Services.

Folder Redirection Overview. (n.d.). Retrieved November 2, 2013, from TechNet: http://technet.microsoft.com/en-us/library/cc732275.aspx

Grimes, R. (2012, June 19). *How to restrict developers' admin rights*. Retrieved November 2, 2013, from infoworld.com: http://www.infoworld.com/d/security/how-restrict-developers-admin-rights-195856

Group Policy. (n.d.). Retrieved November 2, 2013, from TechNet: http://technet.microsoft.com/en-us/windowsserver/bb310732.aspx

Healey, J. (2013). *A Fierce Domain: Conflict in Cyberspace, 1986-2012.* Cyber Conflict Studies Association.

Iwaya, A. (2013, July 30). *Download Free PowerShell Quick Reference Guides from Microsoft*. Retrieved November 2, 2013, from howtogeek.com: http://www.howtogeek.com/169246/download-free-powershell-quick-reference-guides-from-microsoft/

Ljubuncic, I. (2013, September 20). *Microsoft EMET v4 review & extensive tutorial*. Retrieved November 2, 2013, from www.dedoimedo.com: http://www.dedoimedo.com/computers/windows-emet-v4.html

Luciano, P. (2012). *Configure Computers For WMI Access Using SpiceWorks*. Retrieved October 21, 2014, from http://community.spiceworks.com/how_to/show/2712-sbs-1220111045-configure-computers-for-wmi-access-using-spiceworks

Microsoft Deployment Toolkit. (n.d.). Retrieved November 2, 2013, from Technet: http://technet.microsoft.com/en-us/windows/dn475741.aspx

Microsoft Security Compliance Manager. (n.d.). Retrieved November 2, 2013, from Microsoft.com: http://technet.microsoft.com/en-us/solutionaccelerators/cc835245.aspx

OttoHelweg2. (2011, August 25). *Trigger a PowerShell Script from a Windows Event*. Retrieved November 2, 2013, from TechNet: http://blogs.technet.com/b/wincat/archive/2011/08/25/trigger-a-powershell-script-from-a-windows-event.aspx

Parker, C. (2013, August 27). *How To: Deploy Adobe Reader XI msi with MDT 2012.* Retrieved November 2, 2013, from MDTGuy: http://mdtguy.wordpress.com/2013/08/27/how-to-deploy-adobe-reader-xi-msi-with-mdt-2012/

Polynomial, KDEx, Taylor, A., & Schroeder. (2012). *How do you explain the necessity of "nuke it from orbit" to management and users?* Retrieved November 2, 2013, from http://security.stackexchange.com/: http://security.stackexchange.com/questions/24195/how-do-you-explain-the-necessity-of-nuke-it-from-orbit-to-management-and-users

Ragan, S. (2011, April 13). *Limiting admin rights chokes most Microsoft vulnerabilities*. Retrieved November 2, 2013, from thetechherald.com: http://www.thetechherald.com/articles/Limiting-admin-rights-chokes-most-Microsoft-vulnerabilities/13321/

SMB Group. (2012). *SMB Group's 2013 Top 10 SMB Technology Market Predictions.* Retrieved from smb-gr.com: http://www.smb-gr.com/wp-content/uploads/2012/pdfs/2013_SMB_Predictions.pdf

Symantec, JZ Analytics. (2012). *2012 NCSA / Symantec National Small Business Study.* National Cyber Security Alliance.

Symantec, JZ Analytics. (2012). *2012 NCSA / Symantec National Small Business Study.* National Cyber Security Alliance.

The Enhanced Mitigation Experience Toolkit. (n.d.). Retrieved November 2, 2013, from Support.Microsoft.com: http://support.microsoft.com/kb/2458544/en-us

Windows Deployment Services Overview. (n.d.). Retrieved November 2, 2013, from TechNet: http://technet.microsoft.com/en-us/library/hh831764.aspx

APPENDIX C

Critical Controls Poster 2016

CIS Critical Security Controls

CSC 1
Inventory of Authorized and Unauthorized Devices
Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

CSC 2
Inventory of Authorized and Unauthorized Software
Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and unauthorized and unmanaged software is found and prevented from installation or execution

CSC 3
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Establish, implement, and actively manage (track, report on, and correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

CSC 4
Continuous Vulnerability Assessment and Remediation
Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, and to remediate and minimize the window of opportunity for attackers.

CSC 5
Controlled Use of Administrative Privileges
Track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

CSC 6
Maintenance, Monitoring, and Analysis of Audit Logs
Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

CSC 7
Email and Web Browser Protections
Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and e-mail systems.

CSC 8
Malware Defenses
Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

CSC 9
Limitation and Control of Network Ports, Protocols, and Services
Manage (track, control, and correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

CSC 10
Data Recovery Capability
Properly back up critical information with a proven methodology for timely recovery.

CSC 11
Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
Establish, implement, and actively manage (track, report on, and correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

CSC 12
Boundary Defense
Detect, prevent, and correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

CSC 13
Data Protection
Prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

CSC 14
Controlled Access Based on the Need to Know
Track, control, prevent, correct, and secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

CSC 15
Wireless Access Control
Track, control, prevent, and correct the security use of wireless local area networks (LANS), access points, and wireless client systems.

CSC 16
Account Monitoring and Control
Actively manage the life-cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.

CSC 17
Security Skills Assessment and Appropriate Training to Fill Gaps
Identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify and remediate gaps, through policy, organizational planning, training, and awareness programs for all functional roles in the organization.

CSC 18
Application Software Security
Manage the security life-cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

CSC 19
Incident Response and Management
Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight).

CSC 20
Penetration Tests and Red Team Exercises
Test the overall strength of an organization's defenses (technology, processes, and people) by simulating the objectives and actions of an attacker.

SANS

PRESENTS

CIS Critical Security Controls

POSTER

The CIS Critical Security Controls for Effective Cyber Defense Now

The CIS Critical Security Controls are a recommended set of actions for cyber defense that provide **specific and actionable ways to stop today's most pervasive and dangerous attacks.** A principle benefit of the Controls is that they prioritize and focus a smaller number of actions with high pay-off results. The Controls are effective because they are derived from the most common attack patterns highlighted in the leading threat reports and vetted across a very broad community of government and industry practitioners. They were created by the people who know how attacks work – NSA Red and Blue teams, the US Department of Energy nuclear energy labs, law enforcement organizations and some of the nation's top forensics and incident response organizations – to answer the question, "what do we need to do to stop known attacks." That group of experts reached consensus and today we have the most current Controls. The key to the continued value is that the Controls are updated based on new attacks that are identified and analyzed by groups from Verizon to Symantec so the Controls can stop or mitigate those attacks.

In addition to being grounded in current attack data, the Controls align with numerous other frameworks, such as PCI-DSS, ISO 27001, US CERT recommendations, NIST SP 800-53, and the NIST Framework. The Controls don't try to replace these other frameworks, but they are frequently used by enterprises to make sense of other frameworks. The Controls are a highly practical approach to prioritize the overarching security strategy for an enterprise. Further, once a program for cyber security is in place and operational, the Controls can also be used with the Critical Security Controls Measurement Companion to assess the effectiveness of the organization's security efforts.

The Controls take the best-in-class threat data and transform it into actionable guidance to improve individual and collective security in cyberspace. Too often in cybersecurity, it seems the "bad guys" are better organized and collaborate more closely than the "good guys." The Controls provide a means to turn that around.

The CIS Critical Security Controls are the Core of the NIST Cybersecurity Framework

Since its release in February 2014, the NIST *Framework for Securing Critical Infrastructure Cybersecurity* has become a major part of the national conversation about cybersecurity for the critical infrastructure and beyond. (The Center for Internet Security was an active participant in the development of the Cybersecurity Framework, and the CIS Critical Security Controls are called out as one of the "Informative References" that can be used to drive specific implementation).

The Framework provides a way to organize, conduct, and drive planning on security goals and improvements, for individual enterprises and across communities of enterprises. But it does not include any specific risk management process, or specify any priority of action. Those decisions and judgments are left to the adopter to manage for their specific situation and context.

CIS believes that this task is beyond the ability or resources of most enterprises to do effectively and repeatedly. And this approach doesn't recognize the interdependency that every enterprise has with its many vendors, partners, suppliers, and customers. This is why the Controls take a community-first approach by considering attacks that we all face today, translating them into specific actions that are embodied in the Controls, and then creating a community to help enterprises remove barriers to positive action. This approach emphasizes the common threat that we all face, shares the labor and insight needed to identify solutions, and does so in a open way that can be explained and shared no matter the compliance framework, regulatory framework, or demands from the marketplace.

To the right is an example of the working aids that CIS maintains to help our community leverage the Framework. This chart shows the mapping from the CIS Critical Security Controls (Version 6.0) into the most relevant NIST CSF (Version 1.0) Core Functions and Categories.

CIS Critical Security Controls (V6.0)	Cybersecurity Framework (CSF) Core				
	Identify	Protect	Detect	Respond	Recover
1 Inventory of Authorized and Unauthorized Devices	AM				
2 Inventory of Authorized and Unauthorized Software	AM				
3 Secure Configuration of End-User Devices		IP			
4 Continuous Vulnerability Assessment & Remediation	RA		CM	MI	
5 Controlled Use of Administrative Privileges		AC			
6 Maintenance, Monitoring, and Analysis of Audit Logs			AE	AN	
7 Email and Web Browser Protections		PT			
8 Malware Defense		PT	CM		
9 Limitation & Control of Network Ports, Protocols, and Service		IP			
10 Data Recovery Capability					RP
11 Secure Configuration of Network Devices		IP			
12 Boundary Defense			DP		
13 Data Protection		DS			
14 Controlled Access Based on Need to Know		AC			
15 Wireless Access Control		AC			
16 Account Monitoring and Control		AC	CM		
17 Security Skills Assessment and Appropriate Training		AT			
18 Application Software Security		IP			
19 Incident Response and Management			AE	RP	
20 Penetration Tests and Red Team Exercises				IM	IM

A Case Study in Auditing the CIS Critical Controls at the U.S. Federal Reserve

The U.S. Federal Reserve audit community consists of individually chartered audit functions representing each of the 12 regional Reserve Banks. In recognizing the unique and pervasive nature of cybersecurity risk, the collective of Fed internal auditors uses a highly coordinated approach to audit coverage that leverages the CIS Critical Security Controls framework. The approach allows for the prioritization of audit coverage as well as the consideration of control effectiveness as demonstrated in previous audits, organized by the Controls, in business and IT areas across the Fed. The prioritized nature of the Controls is also useful to Fed management, informing cybersecurity and risk management activities.

Cybersecurity risk applies across all business and IT areas, and risks for individual Reserve Banks may vary. Since the Controls are set forth in priority order, they provide a strong starting point for prioritizing audit coverage. The varying levels of control effectiveness in business and IT areas are best known by the local chief audit executives and information security officers. This combination of prioritization and local risk knowledge supports an effective balance of cybersecurity audit coverage applied throughout the Reserve Banks.

As part of management's layered control framework, Fed management assigns an overall maturity score of Fed controls organized by the Controls. Lower assigned maturity scores drive stronger investment and management attention. This aligns the cybersecurity risk focus between management and the internal audit, and improves organizational conversations about relative control effectiveness. It is increasingly apparent that cybersecurity risk isn't just an IT risk – it is an enterprise-wide business risk that requires broad awareness and coordination. The Controls provide a useful framework for both management and auditors for the assessment and management of cybersecurity risk.

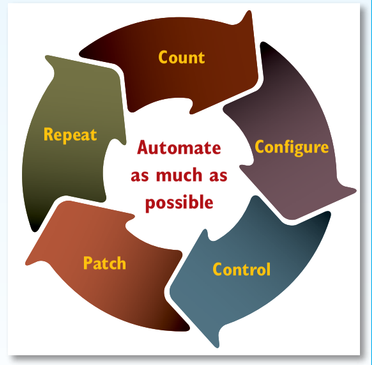
The National Campaign for Cyber Hygiene

The National Campaign for Cyber Hygiene was developed to provide a plain-language, accessible, and low-cost foundation for implementation of the CIS Critical Security Controls. Although the Controls already simplify the daunting challenges of cyber defense by creating community priorities and action, many enterprises are starting from a very basic level of security.

The Campaign starts with a few basic questions that every corporate and government leader ought to be able to answer:

- Do we know what is connected to our systems and networks? (CSC 1)
- Do we know what software is running (or trying to run) on our systems and networks? (CSC 2)
- Are we continuously managing our systems using "known good" configurations? (CSC 3)
- Are we continuously looking for and managing "known bad" software? (CSC 4)
- Do we limit and track the people who have the administrative privileges to change, bypass, or over-ride our security settings? (CSC 5)

These questions, and the actions required to answer them, are represented in plain language by the Top 5 Priorities of the Campaign: "**Count, Configure, Control, Patch, Repeat**." To support the Campaign, volunteers have created documentation and toolkits to guide implementation.



Although the language is simple and catchy, behind the scenes each of these questions is associated with a primary CIS Critical Security Control that provides an action plan. The Campaign is also designed to align with the first five of the CIS Critical Security Controls, the Australian Signals Directorate's Top Four Strategies to Mitigate Targeted Intrusions, and the DHS Continuous Diagnostic and Mitigation Program. This provides a strong and defendable basis for the Campaign Priorities, a growth path for maturity beyond these basic actions, and the benefits of a large community of experts, users, and vendors.

The National Campaign for Cyber Hygiene has been jointly adopted by the Center for Internet Security (home of the Multi-State Information Sharing and Analysis Center) and the National Governor's Association Homeland Security Advisory Council as a foundational cybersecurity program across many state, local, tribal, and territorial governments.

The CIS Critical Security Controls as the Basis for Cybersecurity Audits

Daily headlines of significant cyber intrusions with their associated effects on consumers and citizens have generated an outcry from the public and lawmakers to demand better performance in cybersecurity for enterprises in every sphere. Executives and board directors have become sensitized to the problem but are, for the most part, still largely unaware of how best to protect their IT and sensitive data.

Jane Holl Lute, Chief Executive Officer of the Center for Internet Security (CIS), frequently meets with CEOs and CIOs of major companies and government organizations who are grappling with the cybersecurity problem. As the former Deputy Secretary and Chief Operating Officer for the Department of Homeland Security, Jane understands the challenges facing leaders who must make tough choices about how to allocate resources to cybersecurity. The problem has shifted from a traditional technology and product view of security to also include the executive's view of the risk to the business. Therefore our solutions (both as individual enterprises and as communities) must bridge this gap in a manner that can be openly described, assessed, shared, and negotiated.

The CIS Critical Security Controls provide a highly practical and useful framework for every organization to use for both implementation and assessment. Because the Controls are developed by the community and based on actual threat data, they are an authoritative, industry-friendly, and vendor-neutral approach to assessment and auditing of security.

Getting Started: Ask and Answer Key Questions

- **What am I trying to protect?** Create a prioritized list of business- or mission-critical processes and inventory the computing assets that map to those processes. This information will be crucial for creating a baseline of your current capabilities against the CIS Critical Security Controls.
- **Where are my gaps?** For each business- or mission-critical asset, compare existing security controls against the CIS Critical Security Controls, indicating the sub-controls that the existing controls already meet and those they do not meet.
- **What are my priorities?** Based on your identified gaps and specific business risks and concerns, take immediate tactical steps to implement the Top 5 Controls and develop a strategic plan to implement the other Controls.
- **Where can I automate?** As you plan your implementation of the Controls, focus on opportunities to create security processes that can be integrated and automated using tools that relieve skilled security and administrative staff of grunt work. The Controls were specifically created to enable automation. The goal is to more rapidly and efficiently deliver accurate, timely, and actionable information to the system administrators and others who can take proactive steps to deter threats.
- **How can my vendor partners help?** Some vendor solutions significantly improve and automate implementation for the Critical Controls, especially in terms of continuous monitoring and mitigation. Contact your current vendors to see how they can support your implementation of the CIS Critical Security Controls and compare their capabilities with other vendor products.

The Configuration Benchmarks Community

The Center for Internet Security (CIS) develops and distributes secure configuration benchmarks and automated configuration assessment tools, and certifies security software products designed to help organizations improve their security posture. The internationally recognized benchmarks are developed through an open, consensus-based process and are aligned with the CIS Critical Security Controls. Cybersecurity and industry professionals from around the world volunteer to participate in CIS's open security benchmark development community. New and updated benchmark development efforts are continually launched for a wide array of system, network and device technologies. The CIS Configuration Assessment Tool (CIS-CAT) enables organizations to identify system vulnerabilities, assess configurations against the benchmarks, and monitor security improvement over time. For more information on CIS-CAT or CIS Benchmark membership, visit **cisecurity.org**.

Security through Collaboration

The Center for Internet Security (CIS) is a not-for-profit organization that is dedicated to enhancing the cybersecurity readiness and response among public and private sector entities. Utilizing its strong industry and government partnerships, CIS combats evolving cybersecurity challenges on a global scale and helps organizations adopt key best practices to achieve immediate and effective defenses against cyber attacks. CIS is home to the Multi-State Information Sharing and Analysis Center, CIS Benchmarks, and CIS Critical Security Controls. To learn more, please visit **cisecurity.org** or follow us at **@CISecurity**.

Where to Learn More

Here are some additional resources for effective planning and implementation of the CIS Critical Security Controls

1) SANS courses on planning and implementing the CIS Critical Security Controls include:

TWO-DAY COURSE

SEC440: Critical Security Controls: Planning, Implementing and Auditing

This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security.

SEC440 does not contain any labs. If the student is looking for hands-on labs involving the Critical Controls, they should take SEC566.

sans.org/course/critical-security-controls-planning-implementing-auditing

FIVE-DAY COURSE

SEC566: Implementing and Auditing the Critical Security Controls – In-Depth

The course shows security professionals how to implement the controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Controls are effectively implemented.

sans.org/course/implementing-auditing-critical-security-controls

2) The SANS Solution Directory posts case studies of organizations that have successfully implemented the Controls and seen immediate benefits.
sans.org/critical-security-controls/vendor-solutions

3) Summits where managers from user organizations and strategists from vendor companies share lessons learned and plan for future improvements.
sans.org/summit

4) The Center for Internet Security delivers world-class cybersecurity solutions and best practices in order to prevent and rapidly respond to cyber incidents to enable an environment of trust in cyberspace.
cisecurity.org

CSC-P-v1-2-16

MAPPINGS TO THE

CIS Critical Security Controls

CIS CRITICAL SECURITY CONTROL	NIST 800-53 rev4*	NIST Core Framework	DHS CDM Program	ISO 27002:2013	ISO 27002:2005	NSA MNP	Au Top 35	NSA Top 10	GCHQ 10 Steps	UK Cyber Essentials	UK ICO Protecting Data	PCI DSS 3.0	HIPAA	FFIEC Examiners Handbook	COBIT 5	NERC CIP v5	NERC CIP v4	NERC CIP v3	Cloud Security Alliance	FY15 FISMA Metrics	ITIL 2011 KPIs
1 Inventory of Authorized & Unauthorized Devices	CA-7 IA-3: SI-4 CM-8 SA-4 PM-5 SC-17	ID.AM-1 ID.AM-3 PR.DS-3	• HWAM: Hardware Asset Management	A.8.1.1 A.9.1.2 A.13.1.1	A.7.1.1 A.10.6.2 A.10.6.1 A.11.4.6	• Map Your Network • Baseline Management • Document Your Network • Personal Electronic Device Management • Network Access Control • Log Management					• Inappropriate Locations for Processing Data	2.4	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services • BAI09: Manage Assets	CIP-002-5 R1 CIP-002-5 R2	CIP-002-4 R1 CIP-004-4 R4 CIP-002-4 R2 CIP-005-4 R2 CIP-002-4 R3 CIP-006-4 R3 CIP-003-4 R5	CIP-002-3 R1 CIP-003-3 R5 CIP-002-3 R2 CIP-004-3 R4 CIP-002-3 R3 CIP-005-3 R2 CIP-002-3 R4 CIP-006-3 R3	DCS-01 MOS-09 MOS-15	1: System Inventory 2: Continuous Monitoring	Information Security Management
2 Inventory of Authorized & Unauthorized Software	CA-7 CM-8 SA-4 SI-4 CM-2 CM-10 SC-18 PM-5 CM-11 SC-34	ID.AM-2 PR.DS-6	• HWAM: Hardware Asset Managementt • SWAM: Software Asset Management	A.12.5.1 A.12.6.2		• Baseline Management • Executable Content Restrictions • Configuration and Change Management	1 14 17	• Application Whitelisting			• Decommissioning of Software or Services		• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services				CCC-04 MOS-3 MOS-04 MOS-15	1: System Inventory 2: Continuous Monitoring	Information Security Management
3 Secure Configurations for Hardware & Software	CA-7 CM-6 CM-11 SC-15 CM-2 CM-7 MA-4 SC-34 CM-3 CM-8 RA-5 SI-2 CM-5 CM-9 SA-4 SI-4	PR.IP-1	• CSM: Configuration Settings Management	A.14.2.4 A.14.2.8 A.18.2.3	A.15.2.2	• Patch Management • Baseline Management • Data-at-Rest Protection • Configuration and Change Management	2-5 21	• Control Administrative Privileges • Set a Secure Baseline Configuration • Take Advantage of Software Improvements	• Secure Configuration	• Secure Configuration • Patch Management		2.2 2.3 6.2 11.5	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services • BAI10: Manage Configuration	CIP-007-5 R2 CIP-010-5 R2	CIP-003-4 R6 CIP-007-4 R3	CIP-003-3 R6 CIP-007-3 R3	IVS-07 MOS-15 MOS-19 TVM-02	2: Continuous Monitoring	Information Security Management
4 Continuous Vulnerability Assessment & Remediation	CA-2 RA-5 SI-4 CA-7 SC-34 SI-7	ID.RA-1 DE.CM-8 ID.RA-2 RS.MI-3 PR.IP-12	• VUL: Vulnerability Management	A.12.6.1 A.14.2.8	A.12.6.1 A.13.1.2 A.15.2.2	• Patch Management • Log Management • Configuration and Change Management	2 3	• Take Advantage of Software Improvements		• Patch Management	• Software Updates	6.1 6.2 11.2	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R2 CIP-010-5 R3	CIP-005-4 R4 CIP-007-4 R3 CIP-007-4 R8	CIP-005-3 R4 CIP-007-3 R3 CIP-007-3 R8	IVS-05 MOS-15 MOS-19 TVM-02	2: Continuous Monitoring	Information Security Management
5 Controlled Use of Administrative Privileges	AC-2 AC-19 IA-5 AC-6 CA-7 SI-4 AC-17 IA-4	PR.AC-4 PR.MA-2 PR.AT-2 PR.PT-3		A.9.1.1 A.9.2.2 - A.9.2.6 A.9.3.1 A.9.4.1 - A.9.4.4	A.10.4.4 A.11.5.1 - A.11.5.3	• User Access • Baseline Management • Log Management	4 9 11 25	• Control Administrative Privileges	• Monitoring	• Access Control	• Configuration of SSL and TLS • Default Credentials	2.1 7.1 - 7.3 8.1 - 8.3 8.7	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• Authentication and Access Controls	• APO13: Manage Security • DSS05: Manage Security Services	CIP-004-5 R4 CIP-004-5 R5 CIP-007-5 R5	CIP-003-4 R5 CIP-005-4 R3 CIP-004-4 R4 CIP-006-4 R3 CIP-005-4 R2 CIP-007-4 R3	CIP-003-3 R5 CIP-005-3 R3 CIP-004-3 R4 CIP-006-3 R3 CIP-005-3 R2 CIP-007-3 R3	IAM-09 - IAM-13 MOS-16 MOS-20	3: Identity Credential & Access Management	Information Security Management
6 Maintenance, Monitoring, & Analysis of Audit Logs	AC-23 AU-6 AU-11 IA-10 AU-2 AU-7 AU-12 SI-4 AU-3 AU-8 AU-13 AU-4 AU-9 AU-14 AU-5 AU-10 CA-7	PR.PT-1 DE.DP-3 DE.AE-3 DE.DP-4 DE.DP-1 DE.DP-5 DE.DP-2	• Generic Audit Monitoring	A.12.4.1 - A.12.4.4 A.12.7.1	A.10.10.1 - A.10.10.3 A.10.10.6	• Log Management	15-16 35		• Monitoring			10.1 - 10.7	• 164.308(a)(1): Security Management Process - Information System Activity Review R • 164.308(a)(5): Security Awareness and Training - Log-in Monitoring A	• Security Monitoring	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R4	CIP-005-4 R3 CIP-007-4 R6	CIP-005-3 R3 CIP-007-3 R6	IVS-01 IVS-03		Information Security Management
7 Email & Web Browser Protections	CA-7 CM-6 CM-11 SC-15 CM-2 CM-7 MA-4 SC-34 CM-3 CM-8 RA-5 SI-2 CM-5 CM-9 SA-4 SI-4	PR.IP-1	• CSM: Configuration Settings Management	A.14.2.4 A.14.2.8 A.18.2.3	A.15.2.2	• Patch Management • Baseline Management • Data-at-Rest Protection • Configuration and Change Management	2-5 21	• Control Administrative Privileges • Set a Secure Baseline Configuration • Take Advantage of Software Improvements	• Secure Configuration	• Secure Configuration • Patch Management		2.2 2.3 6.2 11.5	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services • BAI10: Manage Configuration	CIP-007-5 R2 CIP-010-5 R2	CIP-003-4 R6 CIP-007-4 R3	CIP-003-3 R6 CIP-007-3 R3	IVS-07 MOS-15 MOS-19 TVM-02	2: Continuous Monitoring	Information Security Management
8 Malware Defenses	CA-7 SC-44 SI-4 SC-39 SI-3 SI-8	PR.PT-2 DE.CM-4 DE.CM-5		A.8.3.1 A.12.2.1 A.13.2.3	A.10.4.1 - A.10.4.2 A.10.7.1	• Device Accessibility • Virus Scanners & Host Intrusion Prevention Systems • Security Gateways, Proxies, & Firewalls • Network Security Monitoring • Log Management	7 26 17 30 22	• Use Anti-Virus File Reputation Services • Enable Anti-Exploitation Features	• Removable Media Controls • Malware Protection	• Malware Protection		5.1 - 5.4	• 164.308(a)(5): Security Awareness and Training - Protection from Malicious Software A • 164.310(d)(1): Device and Media Controls - Accountability A • 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R3	CIP-007-4 R4	CIP-007-3 R4	MOS-01 MOS-15 TVM-01 TVM-03	4: Anti-Phishing & Malware Defense	Information Security Management
9 Limitation & Control of Network Ports	AT-1 AT-4 PM-13 AT-2 SA-11 PM-14 AT-3 SA-16 PM-16	PR.AC-5 DE.AE-1	• Boundary Protection	A.9.1.2 A.13.1.1 A.13.1.2 A.14.1.2	A.10.6.1 - A.10.6.2 A.11.4.4	• Baseline Management • Configuration and Change Management	2 13 3 27 12	• Limit Workstation-to-Workstation Communication	• Network Security		• Decommissioning of Software or Services • Unnecessary Services	1.4	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• Network Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R1	CIP-007-4 R2	CIP-007-3 R2	DSI-02 IVS-06 IPT-04		Information Security Management
10 Data Recovery Capability	CP-9 CP-10 MP-4	PR.IP-4		A.10.1.1 A.12.3.1	A.10.5.1 A.10.8.3	• Backup Strategy						4.3 9.5 - 9.7	• 164.308(a)(7): Contingency Plan - Data Backup Plan R • 164.308(a)(7): Contingency Plan - Disaster Recovery Plan R • 164.308(a)(7): Contingency Plan - Testing & Revision Procedure A • 164.310(d)(1): Device & Media Controls - Data Backup & Storage A	• Encryption	• APO13: Manage Security • DSS05: Manage Security Services		CIP-009-4 R4 CIP-009-4 R5	CIP-009-3 R4 CIP-009-3 R5	MOS-11		Information Security Management
11 Secure Configurations for Network Devices	AC-4 CA-9 CM-5 MA-4 CA-3 CM-2 CM-6 SC-24 CA-7 CM-3 CM-8 SI-4	PR.AC-5 PR.IP-1 PR.PT-4	• CSM: Configuration Settings Management • Boundary Protection	A.9.1.2 A.13.1.1 A.13.1.3	A.10.6.1 - A.10.6.2 A.11.4.5 A.11.4.7 A.11.5.1 - A.11.5.3	• Map Your Network • Patch Management • Baseline Management • Document Your Network • Security Gateways, Proxies, and Firewalls • Configuration and Change Management	2 3 10	• Set a Secure Baseline Configuration • Segregate Networks and Functions	• Secure Configuration • Network Security	• Boundary Firewalls & Internet Gateways • Secure Configuration • Patch Management	• Software Updates • Inappropriate Locations for Processing Data	1.1 - 1.2 2.2 6.2		• Network Security	• APO13: Manage Security • DSS05: Manage Security Services • BAI10: Manage Configuration	CIP-005-5 R1 CIP-007-5 R2	CIP-003-4 R6 CIP-006-4 R3 CIP-004-4 R4 CIP-007-4 R3 CIP-005-4 R2	CIP-003-3 R6 CIP-006-3 R3 CIP-004-3 R4 CIP-007-3 R3 CIP-005-3 R2	DSI-02 IVS-09 IAM-03 MOS-19 IVS-06 TVM-02	3: Identity Credential & Access Management	Information Security Management
12 Boundary Defense	AC-4 CA-7 SC-7 AC-17 CA-9 SC-8 AC-20 CM-2 SI-4 CA-3 SA-9	PR.AC-3 PR.AC-5 PR.MA-2 DE.AE-1	• Boundary Protection	A.9.1.2 A.12.4.1 A.13.1.3 A.12.7.1 A.13.2.3 A.13.1.1	A.10.6.1 - A.10.6.2 A.11.5.1 - A.11.5.3 A.11.7.1 - A.11.7.2 A.10.10.2 A.11.4.2 A.11.4.5 A.11.4.7	• Map Your Network • Network Architecture • Baseline Management • Document Your Network • Personal Electronic Device Management • Security Gateways, Proxies, and Firewalls • Remote Access Security • Network Security Monitoring • Log Management	10-11 18-20 23 32-34	• Segregate Networks and Functions	• Home and Mobile Working • Monitoring • Network Security	• Boundary Firewalls & Internet Gateways	• Configuration of SSL and TLS • Inappropriate Locations for Processing Data	1.1 - 1.3 8.3 10.8 11.4		• Network Security • Security Monitoring	• APO13: Manage Security • DSS05: Manage Security Services	CIP-005-5 R1 CIP-005-5 R2 CIP-007-5 R4	CIP-005-4 R3 CIP-007-4 R6	CIP-005-3 R3 CIP-007-3 R6	DSI-02 IVS-01 IVS-06 IVS-09 MOS-16	3: Identity Credential & Access Management 6: Network Defense 7: Boundary Protection	Information Security Management
13 Data Protection	AC-3 CA-9 SC-8 SI-4 AC-4 IR-9 SC-28 AC-23 MP-5 SC-31 CA-7 SA-18 SC-41	PR.AC-5 PR.DS-2 PR.DS-5 PR.PT-2		A.8.3.1 A.10.1.1 - A.10.1.2 A.13.2.3 A.18.1.5	A.10.7.1 A.12.3.1 - A.12.3.2 A.12.5.4 A.15.1.6	• Network Architecture • Device Accessibility • Security Gateways, Proxies, and Firewalls • Network Security Monitoring	26		• Removable Media Controls			3.6 4.1 - 4.3	• 164.308(a)(4): Information Access Management - Isolating Health Care Clearinghouse Function R • 164.310(d)(1): Device and Media Controls - Accountability A • 164.312(a)(1): Access Control - Encryption and Decryption A • 164.312(e)(1): Transmission Security - Integrity Controls A • 164.312(e)(1): Transmission Security - Encryption A	• Encryption • Data Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-011-5 R1			DSI-02 DSI-05 EKM-01 - EKM-04 MOS-11	5: Data Protection	Information Security Management
14 Controlled Access Based on the Need to Know	AC-1: AC-6 RA-2 AC-2: AC-24 SC-16 AC-3 CA-7 SI-4 MP-3	PR.AC-4 PR.DS-2 PR.AC-5 PR.PT-2 PR.DS-1 PR.PT-3	• TRUST: Access Control Management • PRIV: Privileges	A.8.3.1 A.9.1.1 A.10.1.1	A.10.7.1 A.10.10.1 - A.10.10.3 A.11.4.5 A.11.4.7 A.11.6.1 - A.11.6.2 A.12.5.4	• Network Architecture • Device Accessibility • User Access • Data-at-Rest Protection • Log Management	26	• Segregate Networks and Functions	• Managing User Privileges • Network Security	• Access Control	• Inappropriate Locations for Processing Data	1.3 - 1.4 4.3 7.1 - 7.3 8.7	• 164.308(a)(1): Security Management Process - Information System Activity Review R • 164.308(a)(4): Information Access Management - Isolating Health Care Clearinghouse Function R • 164.308(a)(4): Information Access Management - Access Authorization A • 164.312(a)(1): Access Control - Encryption and Decryption A • 164.312(c)(1): Integrity - Mechanism to Authenticate Electronic Protected Health Information A • 164.312(e)(1): Access Control - Automatic Logoff A • 164.312(d): Person or Entity Authentication - R • 164.312(e)(1): Transmission Security - Integrity Controls A • 164.312(e)(1): Transmission Security - Encryption A	• Authentication and Access Controls • Encryption • Data Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-005-5 R1 CIP-005-5 R2 CIP-007-5 R4 CIP-011-5 R1	CIP-003-4 R5 CIP-004-4 R4 CIP-005-4 R2 CIP-006-4 R3	CIP-003-3 R5 CIP-004-3 R4 CIP-005-3 R2 CIP-006-3 R3	DSI-02 IVS-09 MOS-11		Information Security Management
15 Wireless Access Control	AC-18 CM-2 SC-40 AC-19 IA-3 SI-4 CA-3 SC-8 CA-7 SC-17			A.10.1.1 A.12.4.1 A.12.7.1		• Map Your Network • Baseline Management • Document Your Network • Personal Electronic Device Management • Network Access Control			• Monitoring • Network Security			4.3 11.1		• Network Security • Encryption • Security Monitoring	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R4	CIP-005-4 R3 CIP-007-4 R6	CIP-005-3 R3 CIP-007-3 R6	IVS-01 IVS-06 IVS-12 MOS-11		Information Security Management
16 Account Monitoring & Control	AC-2 CA-7 AC-3 IA-5 AC-7 IA-10 AC-11 SC-17 AC-12 SC-23	PR.AC-1 PR.AC-4 PR.PT-3	• CRED: Credentials and Authentication Management	A.9.1.1 A.9.2.1 - A.9.2.6 A.9.3.1 A.9.4.1 - A.9.4.3 A.11.2.8	A.8.3.3 A.11.2.1 A.11.2.3 - A.11.2.4 A.11.3.1 - A.11.3.3 A.11.5.1 - A.11.5.3	• User Access • Baseline Management • Log Management	25		• Managing User Privileges	• Access Control	• Configuration of SSL and TLS	7.1 - 7.3 8.7 - 8.8	• 164.308(a)(1): Security Management Process - Information System Activity Review R • 164.308(a)(4): Information Access Management - Access Authorization A • 164.308(a)(4): Information Access Management - Access Establishment and Modification A • 164.308(a)(5): Security Awareness and Training - Password Management A • 164.312(a)(1): Access Control - Unique User Identification A • 164.312(a)(1): Access Control - Automatic Logoff A • 164.312(d): Person or Entity Authentication - R • 164.312(e)(1): Transmission Security - Integrity Controls A • 164.312(e)(1): Transmission Security - Encryption A	• Authentication and Access Controls	• APO13: Manage Security • DSS05: Manage Security Services	CIP-005-5 R1 CIP-005-5 R2 CIP-007-5 R4	CIP-005-4 R3 CIP-007-4 R5 CIP-007-4 R6	CIP-005-3 R3 CIP-007-3 R5 CIP-007-3 R6	IAM-02 IAM-09 - IAM-12 MOS-14 MOS-16 MOS-20	3: Identity Credential & Access Management	Information Security Management
17 Security Skills Assessment and Appropriate Training to Fill Gaps	AT-1 AT-4 PM-13 AT-2 SA-11 PM-14 AT-3 SA-16 PM-16	PR.AT-1 PR.AT-4 PR.AT-2 PR.AT-5 PR.AT-3	• BEHV: Security-Related Behavior Management	A.7.2.2	A.8.2.2	• Training	28		• User Education & Awareness			12.6	• 164.308(a)(5): Security Awareness and Training - Security Reminders A • 164.308(a)(5): Security Awareness and Training - Protection from Malicious Software A • 164.308(a)(5): Security Awareness and Training - Log-in Monitoring A • 164.308(a)(5): Security Awareness and Training - Password Management A	• Personnel Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-004-5 R1 CIP-004-5 R2	CIP-004-4 R1 CIP-004-4 R2	CIP-004-3 R1 CIP-004-3 R2	HRS-10 MOS-05	8: Training and Education	Information Security Management
18 Application Software Security	SA-13 SA-20 SI-11 SA-15 SA-21 SI-15 SA-16 SC-39 SI-16 SA-17 SI-10	PR.DS-7	• VUL: Vulnerability Management	A.9.4.5 A.12.1.4 A.14.2.1 A.14.2.6 - A.14.2.8	A.10.1.4 A.12.5.2 A.12.2.1 A.12.5.5 A.12.2.4	• Training	24				• SQL Injection	6.3 6.5 - 6.7		• Application Security • Software Development & Acquisition	• APO13: Manage Security • DSS05: Manage Security Services				AIS-01 CCC-02 AIS-03 CCC-03 AIS-04 IVS-08 CCC-01		Information Security Management
19 Incident Response & Management	IR-1 IR-4 IR-7 IR-2 IR-5 IR-8 IR-3 IR-6 IR-10	PR.IP-10 RS.AN-1-4 DE.AE-2 RS.MI-1-2 DE.AE-4 RS.IM-1-2 DE.AE-5 RC.RP-1 DE.CM-1-7 RC.IM-1-2 RS.RP-1 RC.CO-1-3 RS.CO-1-5	• Plan for Events • Respond to Events	A.6.1.3 A.7.2.1 A.16.1.2 A.16.1.4 - A.16.1.7	A.6.1.6 A.8.2.1 A.13.1.1 A.13.2.1 - A.13.2.2	• Incident Response and Disaster Recovery Plans			• Incident Management			12.10	• 164.308(a)(6): Security Incident Procedures - Response and Reporting R		• APO13: Manage Security • DSS05: Manage Security Services • DSS02: Manage Service Requests and Incidents	CIP-008-5 R1 CIP-008-5 R2 CIP-008-5 R3	CIP-008-4 R1 CIP-008-4 R2	CIP-008-3 R1 CIP-008-3 R2	SEF-01 - SEF-05	9: Incident Response	Information Security Management
20 Penetration Tests & Red Team Exercises	CA-2 CA-8 PM-6 CA-5 RA-6 PM-14 CA-6 SI-6			A.14.2.8 A.18.2.1 A.18.2.3	A.6.1.8 A.15.2.2 A.15.3.1	• Audit Strategy						11.3			• APO13: Manage Security • DSS05: Manage Security Services • MEA02: Monitor, Evaluate and Assess the System of Internal Control						Information Security Management

***NIST 800-53 LISTINGS**

AC-1: Access Control Policy and Procedures
AC-2: Account Management
AC-3: Access Enforcement
AC-4: Information Flow Enforcement
AC-6: Least Privilege
AC-7: Unsuccessful Logon Attempts
AC-11: Session Lock
AC-12: Session Termination
AC-17: Remote Access
AC-18: Wireless Access
AC-19: Access Control for Mobile Devices
AC-20: Use of External Information Systems
AC-23: Data Mining Protection
AC-24: Access Control Decisions
AT-1: Security Awareness and Training Policy and Procedures
AT-2: Security Awareness Training
AT-3: Role-Based Security Training
AT-4: Security Training Records
AU-2: Audit Events
AU-3: Content of Audit Records
AU-4: Audit Storage Capacity
AU-5: Response to Audit Processing Failures
AU-6: Audit Review, Analysis, and Reporting
AU-7: Audit Reduction and Report Generation
AU-8: Time Stamps
AU-9: Protection of Audit Information
AU-10: Non-repudiation
AU-11: Audit Record Retention
AU-12: Audit Generation
AU-13: Monitoring for Information Disclosure
AU-14: Session Audit
CA-2: Security Assessments
CA-3: System Interconnections
CA-5: Plan of Action and Milestones
CA-6: Security Authorization
CA-7 Continuous Monitoring
CA-8: Penetration Testing
CA-9: Internal System Connections
CM-2: Baseline Configuration
CM-3: Configuration Change Control
CM-5: Access Restrictions for Change
CM-6: Configuration Settings
CM-7: Least Functionality
CM-8: Information System Component Inventory
CM-9: Configuration Management Plan
CM-10: Software Usage Restrictions
CM-11: User-Installed Software
CP-9: Information System Backup
CP-10: Information System Recovery and Reconstitution
IA-3: Device Identification and Authentication
IA-5: Authenticator Management
IA-10: Adaptive Identification and Authentication
IR-1: Incident Response Policy and Procedures
IR-2: Incident Response Training
IR-3: Incident Response Testing
IR-4: Incident Handling
IR-5: Incident Monitoring
IR-6: Incident Reporting
IR-7: Incident Response Assistance
IR-8: Incident Response Plan
IR-9: Information Spillage Response
IR-10: Integrated Information Security Analysis Team
MA-4: Nonlocal Maintenance
MP-3: Media Marking
MP-4: Media Storage
MP-5: Media Transport
PM-5: Information System Inventory
PM-6: Information Security Measures of Performance
PM-13: Information Security Workforce
PM-14: Testing, Training, & Monitoring
PM-16: Threat Awareness Program
RA-2: Security Categorization
RA-5: Vulnerability Scanning
RA-6: Technical Surveillance Countermeasures Survey
SA-4: Acquisition Process
SA-9: External Information System Services
SA-11: Developer Security Testing and Evaluation
SA-13: Trustworthiness
SA-15: Development Process, Standards, and Tools
SA-16: Developer-Provided Training
SA-17: Developer Security Architecture and Design
SA-18: Tamper Resistance and Detection
SA-20: Customized Development of Critical Components
SA-21: Developer Screening
SC-7: Boundary Protection
SC-8: Transmission Confidentiality and Integrity
SC-15: Collaborative Computing Devices
SC-16: Transmission of Security Attributes
SC-17: Public Key Infrastructure Certificates
SC-18: Mobile Code
SC-20: Secure Name/Address Resolution Service (Authoritative Source)
SC-21: Secure Name/Address Resolution Service (Recursive or Caching Resolver)
SC-22: Architecture and Provisioning for Name/Address Resolution Service
SC-23: Session Authenticity
SC-24: Fail in Known State
SC-28: Protection of Information at Rest
SC-31: Covert Channel Analysis
SC-34: Non-Modifiable Executable Programs
SC-39: Process Isolation
SC-40: Wireless Link Protection
SC-41: Port and I/O Device Access
SC-44: Detonation Chambers
SI-2: Flaw Remediation
SI-3: Malicious Code Protection
SI-4: Information System Monitoring
SI-6: Security Function Verification
SI-7: Software, Firmware, and Information Integrity
SI-8: Spam Protection
SI-10: Information Input Validation
SI-11: Error Handling
SI-15: Information Output Filtering
SI-16: Memory Protection

CIS Critical Security Controls

APPENDIX D

IBM MaaS360 Bundles

Total Enterprise Mobility

Presented by {Tavie Omele}

Your Name |tomele@fiberlink.com | www.maas360.com

Top Enterprise Mobility Initiatives

Embrace Bring Your Own Device (BYOD)

Migrate from BlackBerry to multi-OS

Deploy public and enterprise apps

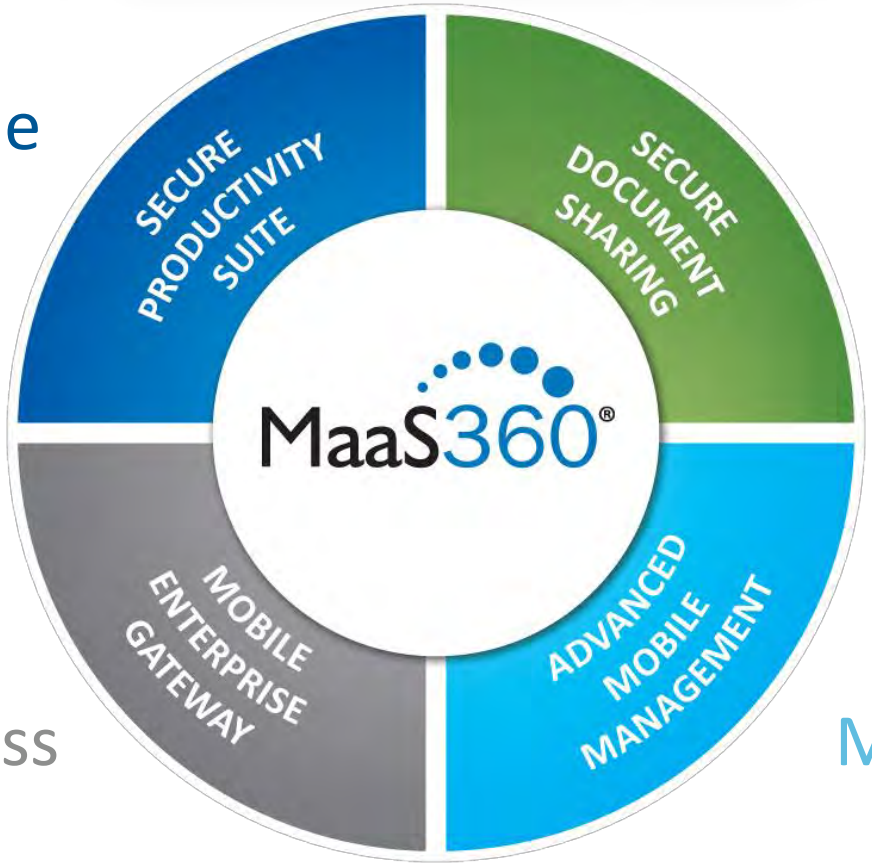
Provide access to work content

Protect sensitive corporate data

MaaS360 Delivers an Integrated Approach

Secure Mobile Containers

Secure Content Collaboration

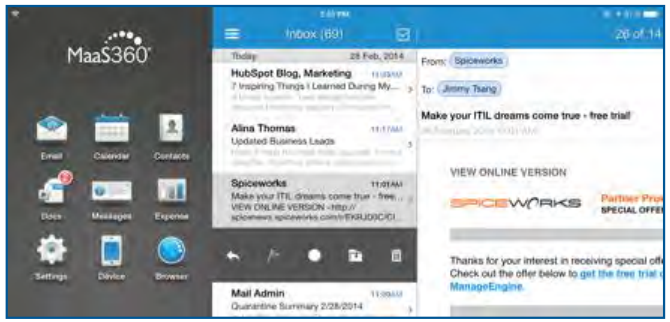


Seamless Enterprise Access

Comprehensive Mobile Management

One Platform for All Your Mobile Assets

MaaS360 Secure Productivity Suite

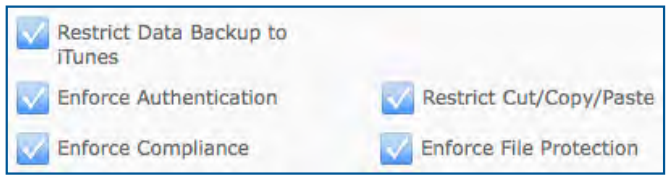


Secure Mail

- Contain email text & attachments to prevent data leakage
- Enforce authentication, copy/paste & forwarding restrictions
- FIPS 140-2 compliant, AES-256 bit encryption for data at rest

Secure Browser

- Enable secure access to intranet sites & web apps w/o VPN
- Define URL filters based on categories & whitelisted sites
- Restrict cookies, downloads, copy/paste & print features



Application Security

- Contain enterprise apps with a simple app wrapper or SDK
- Enforce authentication & copy/paste restrictions
- Prevent access from compromised devices

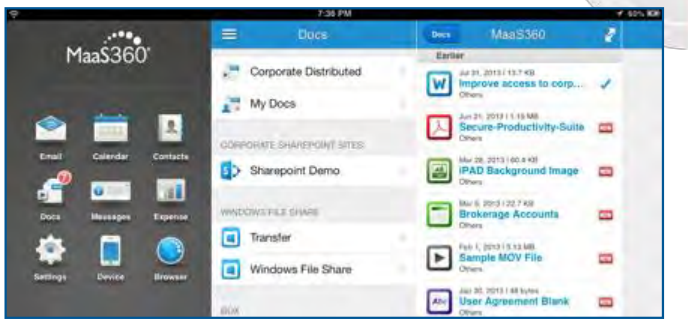
TruSaaS

MaaS360 by Fiberlink, an IBM company

MaaS360 Secure Document Sharing

Mobile Content Management

- Contain documents & files to prevent data leakage
- Enforce authentication, copy/paste & view-only restrictions
- Access MaaS360 distributed content & repositories such as SharePoint, IBM Connections, Box, Google Drive & CMIS



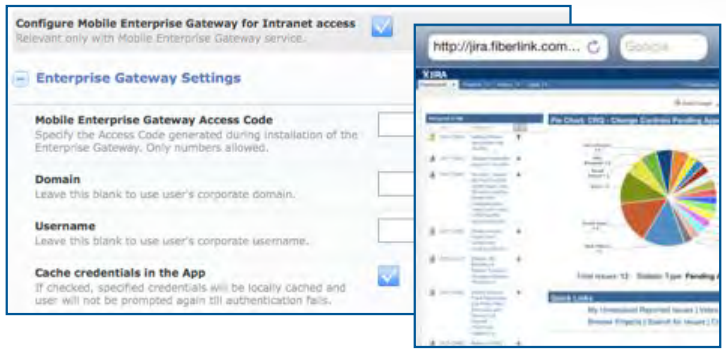
Secure Editor

- Create, edit & save content in a secure, encrypted container
- Collaborate on Word, Excel, PowerPoint & text files
- Change fonts & insert images, tables, shapes, links & more

Secure Document Sync

- Synchronize user content across managed devices
- Restrict copy/paste & opening in unmanaged apps
- Store content securely, both in the cloud & on devices

MaaS360 Mobile Enterprise Gateway

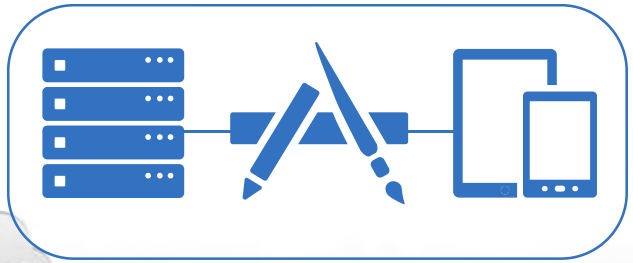


Mobile Enterprise Gateway for Browser

- Enable MaaS360 Secure Browser to access enterprise intranet sites, web apps & network resources
- Access seamlessly & securely without needing a VPN session on mobile device

Mobile Enterprise Gateway for Docs

- Enhance MaaS360 Mobile Content Management with secure access to internal files, e.g. SharePoint & Windows File Share
- Retrieve enterprise documents without a device VPN session



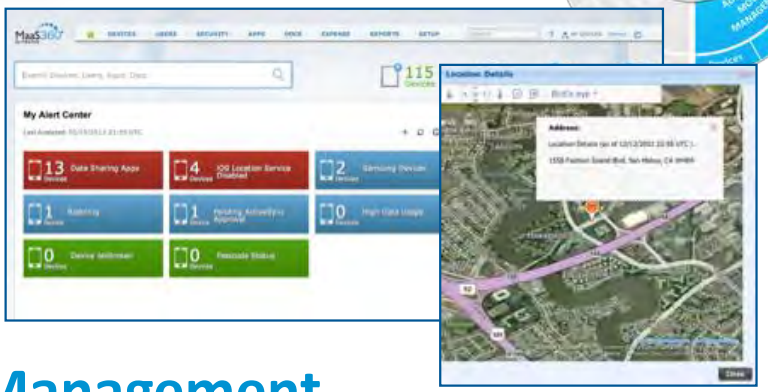
Mobile Enterprise Gateway for Apps

- Add in-app VPN to MaaS360 Application Security to integrate behind-the-firewall data in enterprise apps
- Incorporate enterprise data without a device VPN session

MaaS360 Advanced Mobile Management

Mobile Device Management

- Manage smartphones, tablets & laptops featuring iOS, Android, Windows Phone, BlackBerry, Windows PC & OS X
- Gain complete visibility of devices, security & network
- Enforce compliance with real-time & automated actions



Mobile Application Management

- Deploy custom enterprise app catalogs
- Blacklist, whitelist & require apps
- Administer app volume purchase programs

Mobile Expense Management

- Monitor mobile data usage with real-time alerts
- Set policies to restrict or limit data & voice roaming
- Review integrated reporting and analytics

APPENDIX E

Vetted Service Providers

Vetted Service Providers

ExpatDigital RESOURCES

2016.10 Edition, ExpatDigital.com

Vetted Service Providers
Email

ExpatDigital RESOURCES

SERVICE PROVIDER	COST	SIGN UP HERE	MISC NOTES
FastMail	Min. of $10/User a year	https://www.fastmail.com/signup/	—
Google	**Google Mail - Free**	https://accounts.google.com/SignUp?service=mail	Scanning of email for targeted ads-Can be partially disabled.
	Google Apps - Paid Min. of $60/User a year	https://apps.google.com/pricing.html	No scanning of email for targeted ads. Includes 1TB of Google Drive Storage
Outlook	**Outlook.com - Free**	http://www.microsoft.com/en-us/outlook-com/	—
	Office 365 - Paid Min. of $70/User a year	https://products.office.com/en-us/office-365-personal	Includes Office 2016 Desktop Applications and 1TB of OneDrive storage

Vetted Service Providers
Messaging

ExpatDigital RESOURCES

SERVICE PROVIDER	COST	ACCESS THROUGH	SIGN UP HERE	MISC NOTES
iMessage	Free	Apple Mobile Devices & Apple computers	Included as part of your Apple account signup.	Only usable with iOS & OS X devices. Not way to schedule automatic deletion of old messages.
Slack	**Slack - Free**	Mac, PC, iOS, Android	Slack.com	No way to schedule automatic deletion of old messages.
	Slack - Paid Min. of $80/User a year	Mac, PC, iOS, Android	Slack.com/pricing	Schedule automatic deletion of old messages. User Groups. Two Factor Authentication can be required.
Skype	**Free**	Mac, PC, iOS, Android	Skype.com	Do not download Skype or use Skype if in China. No way to schedule automatic deletion of old messages.
WhatsApp	**Free**	iOS, Android Limited Support for PC & Mac	Download and Open Mobile App	Mobile App only - no desktop software No way to schedule automatic deletion of old messages.

Vetted Service Providers
VPN

SERVICE PROVIDER	COST	DEVICE SUPPORT	SIGN UP HERE	MISC NOTES
BolehVPN	Yearly: $6.67/month	Mac, PC, iOS, Android, Linux	https://portal.bolehvpn.net	Have 30 / 60 / 180 day subscriptions in addition to yearly Includes support for integration into DD-WRT routers & more
IVPN	Yearly: $7.92/month	Mac, PC, iOS, Android, Linux	https://www.ivpn.net/pricing	Includes support for integration into DD-WRT routers & more.
Jungl	Yearly: $9.17/month up to $13.75/month	Mac, PC, iOS, Android, Linux	http://www.jungl.me/#pricing	Works especially well for users in East Asia
Proxy	Yearly: $3.33/month up to $16.66/month	Mac, PC, iOS, Android, Linux	https://proxy.sh/prices	Lots of advanced technical options Short Term VPN: $2 for 72 hours

Vetted Service Providers
Anti-Malware

ExpatDigital RESOURCES

SERVICE PROVIDER	COST	SIGN UP HERE	MISC NOTES
Avast	Free for Personal use	https://www.avast.com/en-us/index	—
ESET **Smart Security**	1 Device for 1 Year, $60	https://www.eset.com/int/home/smart-security/	—
F-Secure	**Internet Security** 1 Device for 1 Year, $50 **Advanced Workstation** 1 Device for 1 Year, $20	https://www.f-secure.com/en_US/web/home_us/internet-security http://gseaonline.com/contactus.aspx	—
Kaspersky **Internet Security**	3 Devices for 1 Year, $40	http://usa.kaspersky.com/products-services/home-computer-security/internet-security/	—
Sophos	Free for Personal Use	https://www.sophos.com/en-us/lp/sophos-home.aspx	—

Vetted Service Providers
Encrypted Backup

ExpatDigital RESOURCES

SERVICE PROVIDER	COST	DEVICE SUPPORT	SIGN UP HERE	MISC NOTES
BackBlaze	$50/Year for one device for Unlimited Data	Mac, Windows, Linux	https://www.backblaze.com/cloud-backup.html	—
CrashPlan+	$60/Year for one device for Unlimited Data	Mac, Windows, Linux	https://store.crashplan.com/store/	Pricing for more than one device available.
Mozy Home	Starts at $60/Year for one device with 50GB data	Mac, Windows, Linux	http://mozy.com/product/mozy/personal	Pricing for more than one device and more data available.
SpiderOak One	Starts at $79/Year with 30GB data	Mac, Windows, Linux	https://spideroak.com/solutions/spideroak-one	Pricing for more data available.

Vetted Service Providers
Full Disk Encryption

ExpatDigital RESOURCES

SERVICE PROVIDER	COST	DEVICE SUPPORT	SETUP INSTRUCTIONS
Apple FileVault	Included in OS X License	Mac OS X 10.7 “Lion” or newer	https://support.apple.com/en-us/HT204837
Jetico BestCrypt	$100 for one device (Inludes one year of support)	Mac, PC, Linux	https://www.jetico.com/web_help/bcve3/
McAfee Complete Date Protection	N/A	Mac, PC, iOS, Android, Linux	N/A
Microsoft Bitlocker	Included in Windows Pro or Enterprise License	Microsoft Windows Vista or newer	http://www.howtogeek.com/192894/how-to-set-up-bitlocker-encryption-on-windows/

Vetted Service Providers
Password Managers

ExpatDigital RESOURCES

SERVICE PROVIDER	COST	DEVICE SUPPORT	SIGN UP HERE	MISC NOTES
Dashlane	Free or $40/Year	Mac, PC, iOS, Android, Linux	https://www.dashlane.com	Cloud Service. Free accounts have limited features. See comparison here: https://www.dashlane.com/premium
KeePass	Free	Mac, PC, Linux	http://keepass.info	Not a cloud service. No built-in syncing across devices. (Plugins Available) Open Source.
1Password	$36/Year or $60/Year	Mac, PC, iOS, Android, Linux	https://1password.com/	Cloud Service. See comparison between plans here: https://1password.com/sign-up/

FAQ

ExpatDigital RESOURCES

How have these Service Providers been chosen?
To be added to this list, a Service Provider must meet the requirements found in the Service Provider Requirements document, which can be found here: https://expatdigital.com/download/347/

Though there are certainly other Service Providers that meet the outlined requirements, for simplicity and maintainability, we have kept this list short. Feel free to use the Service Provider Requirements to vet a service provider not on this list.

How often do you update this list?
We update this list a couple times a year. To find out the last time it was updated, look at the bottom of any page for the Edition date.

Can I send you a Service Provider that I think should be on this list?
Feel free to send us a suggested Service Provider, but please understand that we do not have the resources to individually vet every suggestion sent to us.

Do you have a list of Service Providers that you vetted but did not meet the requirements to be included on this list?
Yes, you can find that list here: https://expatdigital.com/download/688/

Changelog

VERSION	MAJOR CHANGES
2016.09	Added FAQ Page and Changelog
2016.10	Removed Yahoo! from Email listing

Vetted Service Providers: Addendum

Security Consulting

Kevin Branch, Consultant
Branch Network Consulting, LLC
kevin@branchnetconsulting.com
www.branchnetconsulting.com
765-251-7450 (US Eastern Time)

With a former background in overseas and US stateside missionary service, including advanced network engineering and information security, I am now soon to complete my 10th year as an independent consultant to a variety of Christian missionary organizations. I have served clients, colleagues, and partners in the USA, Latin America, Europe, and Asia, working with both small offices and moderately large enterprise networks.

While I offer a wide variety of network and security consulting services, my passion is network security monitoring (NSM), in which an organization's electronic devices and data assets are actively monitored for indicators of compromise based on a wide spectrum of data points collected and analyzed by an NSM system which is monitored by an NSM practitioner. No defenses are perfect. I want to help organizations become promptly aware when their electronic defenses have been breached so that damage can be promptly prevented or contained. For small to medium sized networks, I offer a standard NSM deployment package consisting of a one time $2,500 setup fee (client provides the NSM server hardware), plus a $600 monthly subscription for my daily monitoring and ongoing tuning of reports and alerts, routine NSM system maintenance, access to a commercial security intel feed, and access to my NSM cloud infrastructure.

I also offer general network and security consulting services at the rate of $110/hour on demand or $90/hour as part of a retainer agreement. Such services might include incident response, risk assessment, network problem diagnosis, network planning and design, IT vendor liaison service, vulnerability scans, firewall configuration assistance, VPN deployment, etc.

Security Training
Individual Pricing: $25 for the first year, $10/year after that

Organizational Pricing – 4 tiers based on organizational size (in units):
-A unit is either a husband & wife or a single person
-We have multiple ways to manage users (Import via CSV, API or unique discount code)
-To keep the costs down, we offer very limited tech support to end users -

Organizational Members	First Year Cost	Yearly Maintenance Fee
Up to 250 member units	$1,500	$500
Up to 500 member units	$3,000	$1,000
Up to 1000 member units	$5,000	$1,500
Up to 2000 member units	$7,500	$2,000

Hilton – Security Specialist
Organizations face the unique challenge of finding a balance between providing the right tools to workers while not allowing technology to become a burden. This is especially true in closed or creative access countries where an information breach can cause damage and put lives at risk. I can help organizations understand the nature of these risks and develop a security posture and program to meet these challenges. We have a proven track record operating information systems and providing access to people in hard to reach places and can provide technical security consulting as well as risk assessment of current or planned systems.
I charge $50 USD per hour for NGO work.

email is info@telenet.com.au or via Whatsapp on +61484081567

APPENDIX F

Models of Social Media / Communication Policies

Model Communication and Social Media Policy

This model policy is a place to start. It is not comprehensive. However, you may use it freely under the creative commons license.

1) Communicate with an SIR Mindset – Strategic Intercultural Relations.
    - **Legitimacy –** Cultivating an appropriate identity
    - **Awareness –** Understanding yourself & those around you
    - **Respect –** Behavior that leads to an honorable reputation & opens doors
2) Remember that all forms of digital communication can go places you never intended.
3) Do not mention people, places or activities of ministry without permission.
4) Do not disclose your location. This can tell thieves your house is empty or kidnappers were you can be found.
5) Don't post to social media if you are HALT – Hungry, Angry, Lonely or Tired
6) If you have a need to share ministry content via a digital channel – remove all meta data from that content.
7) Would a co-worker or leader be unhappy to see this posted? Talk it over first.

APPENDIX G

Model of Password Policy

Password Protection Policy

Free Use Disclaimer: *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.*

Things to Consider: *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.*

Last Update Status: *Updated June 2014*

1. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of <Company Name>'s resources. All users, including contractors and vendors with access to <Company Name> systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any <Company Name> facility, has access to the <Company Name> network, or stores any non-public <Company Name> information.

4. Policy

4.1 Password Creation

4.1.1 All user-level and system-level passwords must conform to the *Password Construction Guidelines*.

4.1.2 Users must not use the same password for <Company Name> accounts as for other non-<Company Name> access (for example, personal ISP account, option trading, benefits, and so on).

4.1.3 Where possible, users must not use the same password for various <Company Name> access needs.

4.1.4 User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges.

4.1.5 Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and

system and must be different from the passwords used to log in interactively. SNMP community strings must meet password construction guidelines.

4.2 Password Change

4.2.1 All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis.

4.2.2 All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every four months.

4.2.3 Password cracking or guessing may be performed on a periodic or random basis by the Infosec Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

4.3 Password Protection

4.3.1 Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential <Company Name> information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.

4.3.2 Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication.

4.3.3 Passwords must not be revealed over the phone to anyone.

4.3.4 Do not reveal a password on questionnaires or security forms.

4.3.5 Do not hint at the format of a password (for example, "my family name").

4.3.6 Do not share <Company Name> passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.

4.3.7 Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.

4.3.8 Do not use the "Remember Password" feature of applications (for example, web browsers).

4.3.9 Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

4.4 Application Development

Application developers must ensure that their programs contain the following security precautions:

4.4.1 Applications must support authentication of individual users, not groups.

4.4.2 Applications must not store passwords in clear text or in any easily reversible form.
4.4.3 Applications must not transmit passwords in clear text over the network.
4.4.4 Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

4.5 Use of Passwords and Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies and Processes

- Password Construction Guidelines

7 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

- Simple Network Management Protocol (SNMP)

8 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

APPENDIX H

Phishing Training Model

APWG

Unifying the Global Response to Cybercrime

Carnegie Mellon CyLab

Supporting Trust Decisions Project
cups.cs.cmu.edu/trust

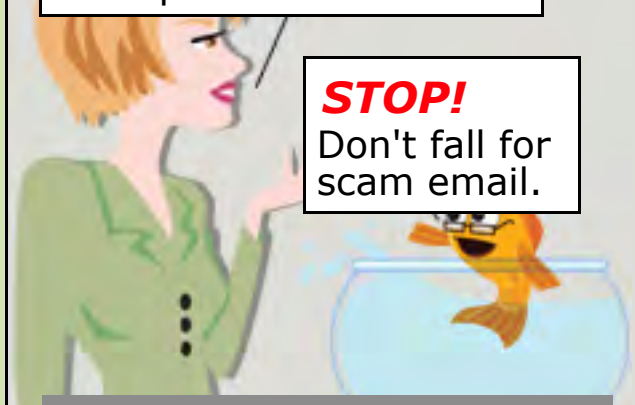
WARNING!

The web page you tried to visit might have been trying to steal your personal information. That page was removed after being identified as a "phishing" web page. A phishing web page tricks people out of bank account information, passwords and other confidential information.

How You Were Tricked

This email is from my bank. It asks me to update my information. I better click on the link and update it.

STOP! Don't fall for scam email.



My Inbox

From: service@Wombank.com

Dear Jane, Your account will be suspended if you do not update your information.

http://www.Wombank.com/update

How to Help Protect Yourself

1 Don't trust links in an email.

DANGER! http://www.amazon.com/update

2 Never give out personal information upon email request.

DANGER! Name: Jane Smith
Credit Card: 1234 5678 9101 1213

3 Look carefully at the web address.

4 Type in the real website address into a web browser.

5 Don't call company phone numbers in emails or instant messages. Check a reliable source such as a phone book or credit card statement.

Credit Card Statement

For Customer Service call:1-800 xxx-xxx

6 Don't open unexpected email attachments or instant message download links.

My Inbox

Here is the updated document.
attachment

How Phishers Trick You Into Giving Out Personal Information

My Inbox

From: service@Wombank.com

Dear Jane, Your account will be suspended if you do not update your information.

http://www.Wombank.com/update

- He forges email addresses to look genuine
- He provokes the computer user with an urgent request
- He adds links that appear to connect to a real bank but bring users to the phisher's counterfeit site - to take their information and money

How You Can Help

Should I report this suspicious email?

For additional information, please visit APWG's resources page at
https://apwg.org/resources/

Legal Disclaimer

PLEASE NOTE: The APWG, Carnegie Mellon University, and any cooperating service providers have provided this message as a public service, based upon information that the URL you were seeking has been involved in a phishing or malware exploit. There is no guarantee that you have not been phished or exposed to malware from this URL you were seeking, or previously. This is not a complete list of steps that may be taken to avoid harm from phishing, and we offer no warranty as to the completeness, accuracy or pertinence of this advisory with respect to the page you attempted to access. Please see https://www.apwg.org for more information. The PhishGuru goldfish character is a trademark of Wombat Security Technologies, Inc.

APPENDIX I

Sensitive Information Reduction

How to Guard Against Sensitive Information Compromise

Reduce

Assume everything you put on a computer is impossible to get rid of.
Ask yourself "Is there a Legitimate, Aware, and Respectful reason that I store / share / write this digitally?
If I still must store / share / write it, am I limiting the 'where' it goes as best as possible?"

Communication Guidelines: The foundation of reducing Sensitive Information is Communication Guidelines. If your organization has communication guidelines, make sure that you understand them, and how they apply in your specific cross-cultural context. This information will give you practical guidance on what you should and should not say in different situations.

Educate: Your friends, family and partners need to understand the risk that certain types of communication can have and how they should communicate both *to* you and *about* you. Drawing principles from your Communication Guidelines, educate your friends, family and partners.

Know Yourself: If you know that you struggle to communicate graciously and respectfully, especially in your digital communications, perhaps it would be wise to reduce your public communications to a minimum—at least until you have had the time to grow and mature in this area.

Trim Down: Looking through your sensitive communication and content, can you lessen the risk of exposure by reducing or even eliminating certain forms of communication or not storing certain types of digital content? If you don't store or communicate it, it can't be compromised.

Protect

Protect the information that you store & share.

Identify both tools and the processes to use the tools, so that you are implementing the C3 principles of Cover, Conceal and Compartmentation whenever you are handling Sensitive information. This would include using a C3 Container to store your sensitive information, and a C3 Communications strategy.

Detect

Online Situational Awareness

Set up an automated process whereby when your online identity is tied to Sensitive information, you are alerted—possibly even in near real-time. This is both proactive and reactive. It is proactive in the sense that we are hoping to be able to remove the information before it is seen by the wrong people, but it is reactive in the sense that the information is already out there. An example of this would be Google.com/alerts.

Sensitive Information

Sensitive information is information that no matter the context, will most likely always violate the Strategic Intercultural Relations (SIR) principles of Legitimacy, Awareness & Respect—yet, it is required for our work. Examples of this would include: culture notes, planning documents, our personal journal, etc. Sensitive information would also include the mistakes of our imperfect application of SIR principles, including others using our identity in a way inconsistent with SIR. Examples of this would include: cultural gaffes, making our travel details publically known, partners posting newsletters online, etc. We refer to all of this information as Sensitive as it is made up of known information that would have a major impact on relationships or personal security if it was seen by certain people.

C3 Strategies

Includes Storage & Communications

Cover: With Cover, we want to obscure the fact that we have anything to hide. When it is known that we have something of value hidden, scrutiny increases and it becomes much more difficult to keep that information concealed. Cover is tied closely with the SIR principle of Legitimacy - Our cover should *enable* consistent legitimacy, not *hinder* it. **The goal of cover, just like Legitimacy, is to avoid closer scrutiny.**

Conceal: Once Cover has been compromised, we must attempt to disguise and encrypt the sensitive information & communication—**Concealment, while necessary, is less ideal than cover, because operating under scrutiny is an order of magnitude more difficult.**

Compartmentation: This is the concept that you should divide your information and communication such that if it is compromised, it does not expose your entire life, team and other teams working in the host country or region. **When all else fails, compartmentation helps to limit the fallout.**

C3 Storage Example

Cover

Diversion safe (hair brush) to store microSD card.

Conceal

Encrypted microSD card. Small, cross-platform.

Compartmentation

Archive old information to safer storage.

APPENDIX J

Survey Questions

CyberSecurity Survey

Welcome to Cyber Security Survey

Thank you for participating in our Cyber Security survey. Your feedback is important. You will be asked 10 question and it should take less than 10 minutes. Your responses will be kept confidential.

1. How has a breach of Cyber Security Impacted Your Organization?

	Yes - this has happened	Not sure - may have happened	No - this has not happened	N/A
Death of a National Worker or Disciple.	○	○	○	○
Imprisonment of a National Worker or Disciple	○	○	○	○
Arrest or Harassment of a National Worker or Disciple	○	○	○	○
Death of a Expat Worker	○	○	○	○
Imprisonment of an Expat Worker	○	○	○	○
Expulsion of an Expat Worker	○	○	○	○
Shut down of a ministry or program	○	○	○	○
Lost time and resources due to cyber sabotage or cyber attack	○	○	○	○
Loss of organizational reputation	○	○	○	○

Other (please specify)

2. What is the highest level of accountability for Cyber Security in your organization?

- ◯ Board Level
- ◯ Senior Leader (CEO, COO, CIO,etc)
- ◯ Management
- ◯ IT Department
- ◯ No One Has Specific Accountability for this.
- ◯ Other (please specify)

3. Including Salary, Equipment, Software and Outside Services - what level of budget do you have for Cyber Security?

- ◯ More than $250,000 a year
- ◯ $151,000 to $250,000 a year
- ◯ $76,000 to $150,000 a year
- ◯ $26,000 to 75,000 a year
- ◯ less than $25,000 a year
- ◯ Other (please specify)

4. Please indicate if you agree or disagree with the following statements

	Yes	Somewhat	No
We have a full time cyber security person on staff	◯	◯	◯
We have a cyber security advisor/ consultant	◯	◯	◯
We have conducted a cyber security risk assessment	◯	◯	◯
We have implemented cyber security risk reduction plan	◯	◯	◯
We have cyber security risk reduction training for staff	◯	◯	◯

Other (please specify)

5. How much do you agree or disagree with these statements?

	Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
I am very concerned about Cyber Security but don't know how to address this.	○	○	○	○	○
Cyber Security is important but not in our top ten list.	○	○	○	○	○
We lack personnel and specialty knowledge to address Cyber Security risk.	○	○	○	○	○
Our biggest hinderance to dealing with Cyber Security risk is lack of budget	○	○	○	○	○
Cyber Security risk is the last thing I want to talk to a donor about.	○	○	○	○	○
Cyber Security risk is really not an issue for our organization.	○	○	○	○	○

6. Would any of these things help you with Cyber Security Risk?

	Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
Cyber Security Risk Assessment	○	○	○	○	○
Cyber Security Risk Reduction Plan	○	○	○	○	○
Cyber Security Training for technical staff	○	○	○	○	○
Cyber Security Training for field staff	○	○	○	○	○
Trusted vendors who can help us	○	○	○	○	○
Funding for Cyber Security expertise, equipment and software	○	○	○	○	○
Cyber Security Network which shares threats and information	○	○	○	○	○

Other (please specify)

7. How many people are in your organization?

- ◯ more than 500
- ◯ between 300 and 499
- ◯ between 150 and 299
- ◯ between 50 and 149
- ◯ less than 50

8. What is your organizational annual budget?

- ◯ More than $10,000,000
- ◯ between $5,000,000 and $10,000,000
- ◯ between $1,000,000 and $5,000,000
- ◯ Less than $1,000,000

9. What areas of the world is your ministry active (choose all that apply)

- ☐ MENA - Middle East and North Africa
- ☐ Europe
- ☐ Central Asia
- ☐ Asia
- ☐ Asia Pacific
- ☐ Global
- ☐ Other (please specify)

10. What would be the one thing that would be of most help to your organization in the area of Cyber Security?

APPENDIX K

C3 Guidelines for Email

C3 Email

v. 2016.02.04

Service Provider Requirements

Requirement	Technical Notes
Cover	The goal of cover is to avoid closer scrutiny.
1.1 Is the provider publicly associated with activism, extremism, religion or extreme paranoia?	Use tools such as SimilarWeb, Maltego and general search engine queries. Look for these type of connections with the email domain, mailserver, and service provider organization.
Concealment	Encryption of sensitive information & communication
2.1 Are encrypted connections the only way the user can send or receive email? Webmail, SMTP, IMAP	Protocols: TLS 1.0, 1.1 or 1.2 only. SSL3 can be enabled, but only if TLS_FALLBACK_SCSV is enabled at the same time to prevent protocol downgrade attacks. Certificate Private Keys: 2048-bit RSA or 256-bit ECDSA by Jan 2017 Certificate Signing/Hash: SHA2 by Jan 2017; Cipher Suites: Prioritize suites that provide authentication and encryption of 128 bits or stronger. RC4 and 3DES can be used, but should be the lowest priority*
2.2 Does the service support encryption in transit between their servers and other service providers?	Encryption in-transit between service providers is a key part of mitigating mass passive surveillance.
Compartmentation	When all else fails, compartmentation helps to limit the fallout.
3.1 Does the service provider support Two Factor Authentication for Webmail & Desktop clients?	2FA helps limit the damage if a user's password is compromised, as the perpetrator will not be able to login without the One-Time-Password or certificate.
3.2 Does the service provider offer webmail access?	Allows the user the option of not storing any email locally on their device, compartmentalizing their device from their sensitive email.
3.3 Does the service support Forward Secrecy for user webmail connections on modern browsers?	"A protocol feature that enables secure conversations that are not dependent on the server's private key. With cipher suites that do not support Forward Secrecy, someone who can recover a server's private key can decrypt all earlier encrypted conversations if they have them recorded. You need to support and prefer ECDHE suites in order to enable Forward Secrecy with modern web browsers. To support a wider range of clients, you should also use DHE suites as fallback after ECDHE" *
3.4 Is there a level of trust in the service provider; that	Is the provider operated by trusted personnel? At a minimum, do they have transparency

**SSL/TLS Deployment Best Practices: https://www.ssllabs.com/downloads/SSL_TLS_Deployment_Best_Practices.pdf*

they will not easily give up user data to threat actors?	reports that outline how they deal with information requests, where their datacenters are, etc?

APPENDIX L

C3 Guidelines for VPN

VPN

v. 2016.04

Service Provider Requirements

Requirement	Technical Notes
Cover	The goal of cover is to avoid closer scrutiny.
1.1 Is the provider publicly associated with activism, extremism, religion or extreme paranoia?	Use tools such as SimilarWeb, Maltego and general search engine queries. Look for these type of connections with the service provider organization.
Concealment	Encryption of sensitive information & communication
2.1 Are secure protocols offered?	Protocols: OpenVPN or "SSL" VPNs. L2TP/IPSEC. No PPTP. OpenVPN protocols: Handshake = RSA 2048 or higher Data = AES 128 or 256 "SSL" VPN protocols: TLS 1.0, 1.1 or 1.2 only Certificate Private Keys: 2048-bit RSA or 256-bit ECDSA by Jan 2017 Certificate Signing/Hash: SHA2 by Jan 2017; Cipher Suites: Prioritize suites that provide authentication and encryption of 128 bits or stronger. RC4 and 3DES can be used, but should be the lowest priority*
2.2 Auto-Reconnect (Recommended)	Does the service auto reconnect when the VPN drops? At a minimum, is the user alerted in some way?
Compartmentation	When all else fails, compartmentation helps to limit the fallout.
3.3 Does the service support Forward Secrecy? (This is a recommendation only)	"A protocol feature that enables secure conversations that are not dependent on the server's private key. With cipher suites that do not support Forward Secrecy, someone who can recover a server's private key can decrypt all earlier encrypted conversations if they have them recorded." *
3.4 Is there a level of trust in the service provider; that they will not easily give up user data to threat actors?	Is the provider operated by trusted personnel? Do they have transparency reports that outline how they deal with information requests, or a warrant canary?
3.5 Does the service provider allow the use of generic usernames?	If logs are ever leaked, they will typically show the associated username with browsing logs - utilizing an username not tied to the user's personal identity offers some protection from tieing logs to a specific person.

APPENDIX M

C3 Guidelines for Messaging

C3 Messaging

v. 2016.02.04

Service Provider Requirements

Requirement	Technical Notes
Cover	The goal of cover is to avoid closer scrutiny.
1.1 Is the provider publicly associated with activism, extremism, religion or extreme paranoia?	Use tools such as SimilarWeb, Maltego and general search engine queries. Look for these type of connections with the email domain, mailserver, and service provider organization.
Concealment	Encryption of sensitive information & communication
2.1 Are messages encrypted in-transit?	????
Compartmentation	When all else fails, compartmentation helps to limit the fallout.
3.1 Does the service provider support Two Factor Authentication for Webmail & Desktop clients? (Recommended Only)	2FA helps limit the damage if a user's password is compromised, as the perpetrator will not be able to login without the One-Time-Password or certificate.
3.2 Does the service provider offer a way to delete old messages?	
3.3 Does the service support Forward Secrecy?	"A protocol feature that enables secure conversations that are not dependent on the server's private key. With cipher suites that do not support Forward Secrecy, someone who can recover a server's private key can decrypt all earlier encrypted conversations if they have them recorded. You need to support and prefer ECDHE suites in order to enable Forward Secrecy with modern web browsers. To support a wider range of clients, you should also use DHE suites as fallback after ECDHE" *
3.4 Is there a level of trust in the service provider; that they will not easily give up user data to threat actors?	Is the provider operated by trusted personnel? At a minimum, do they have transparency reports that outline how they deal with information requests, where their datacenters are, etc?

**SSL/TLS Deployment Best Practices:* https://www.ssllabs.com/downloads/SSL_TLS_Deployment_Best_Practices.pdf

APPENDIX N

Additional Country Profiles

ADDITIONAL COUNTRY PROFILES

BAHRAIN

Bahrain is a small island nation with the highest level of Internet penetration in the Middle East.[1] Bahrain has a native Christian community that holds citizenship and makes up 10% of the total population.[2] The expansive banking and commerce economy has attracted cyber criminals.[3] Common risks reported were untargeted phishing[4] and cyber blackmail.[5] It is reported that "Cyber Crime as a Service" is easily accessible to the average web user in Bahrain, and that an open marketplace exists where identity information is for sale at bargain rates.[6]

Bahrain has a reputation for oppressing political and social dissidents.[7] Cyber intrusion and monitoring tools are reported[8] to be a significant elem nt of this repression.[9] There is public evidence that Bahrain has DPI, LIG, FinFisher surveillance software, remote access tools from The Hacking Team and over-the-air surveillance systems that allow for the tracking, interception and monitoring of cell phone calls in real time.[10]

Despite the formidable cyber capabilities of the state, political and social activists report that use of good cyber security practices and encrypted communication have been effective at reducing arrest and suppression.[11] There have been no reports of cyber attacks on missional organizations by Bahrain.

The most likely threats are:

1. Monitoring of unencrypted email, SMS, VOIP, and phone calls.
2. Monitoring of unencrypted web and social media usage.
3. Circumventing SSL and VPN to allow monitoring of communication.
4. Untargeted malware and phishing attacks – criminal.
5. Untargeted cyber blackmail attacks – criminal.

1 https://en.wikipedia.org/wiki/Bahrain
2 bid
3 http://www.dilmun-times.com/?p=22072
4 http://www.bizbahrain.com/cyber-security-a-grim-reality/
5 http://www.philstar.com/world/2015/02/22/1426473/bahrain-cracks-down-rampant-cyber-crime-cases
6 http://www.newsofbahrain.com/viewNews.php?ppId=5773&TYPE=Posts&pid=21&MNU=2&SUB=3
7 https://www.hrw.org/middle-east/n-africa/bahrain
8 http://www.bahrainrights.org/en/node/7001
9 https://giswatch.org/en/country-report/communications-surveillance/bahrain
10 https://sii.transparencytoolkit.org/search?utf8=□&utf8=□&q=bahrain
11 https://giswatch.org/en/country-report/communications-surveillance/bahrain

For those engaged in ministry directly in the country that raises concerns by the government:

1. Targeted cyber attack on personal devices.
2. Targeted network attacks.
3. Active monitoring of all communications – phone, SMS, VOIP, Chat, email, etc.
4. Remote entry to computers and mobile devices allowing access to encrypted files, webcams and microphones on those devices.

ISRAEL

Israel is engaged in a tit-for-tat with Palestine on many fronts and cyber intrusion is one of them. Israel is also engaged in monitoring and intervening on many fronts in the Middle East. Israel is a major "cyber power" internationally. In 2014, Israel had $6 billion in exports of cyber security and surveillance technology, about 10% of the global market. Israel is also one of the most cyber attacked nations in the world.[12]

In a constant struggle with a wide range of state and non-state actors that hack a range of websites and infrastructure, one tactic that is used against opponents is to expose their real world identity.[13] There are also at least 6 major hacker groups aligned with Israel, that engage in activates ranging from website defacement, DDOS attacks, and attacks on the national infrastructures of Arab states opposed to Israel.[14]

A major effort is placed on analysis of social media,[15] since this is often the precursor to violent action in the region. This analysis likely involves machine learning and artificial intelligence to evaluate intent and influence [16]

Israel has a military unit called 8200, which is seen as the Israeli version of the USA's NSA. Any attempt to catalog Israeli cyber capabilities would be a monumental task. There is public evidence that Israel has DPI, LIG, FinFisher surveillance software, remote access tools from The Hacking Team and over-the-air surveillance systems that allow for the tracking, interception and monitoring of cell phone calls in real time.[17] However, for missional organizations the core question is "what are the most likely risks that I will face?" There were no reports of cyber attacks against a missional organization by Israel. The government has a reputation of being generally tolerant of Christianity. Most incidents of persecution originate at the personal and family level.[18]

---

12 https://www.thecipherbrief.com/article/israel's-cyber-capabilities
13 http://www.israeltoday.co.il/NewsItem/tabid/178/nid/29032/Default.aspx?topic=article_title
14 http://www.bluekaizen.org/CSCAMP2012/CONFHpdfs/EbrahimHegazy/Cyber-Warfare-in-the-middle-east.pdf
15 http://www.al-monitor.com/pulse/originals/2016/07/israel-cyber-warfare-individual-intifada-technology-monitor.html
16 https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c
17 https://sii.transparencytoolkit.org/search?utf8=✓&utf8=✓&q=Israel
18 http://www.persecution.com/pdfs/Global_Report_2016.pdf

Currently the most likely threats are:

1. Monitoring of unencrypted email, SMS, VOIP, and phone calls.
2. Monitoring of unencrypted web and social media usage.

For those who are engaged in high profile activities, or have drawn the attention of the government the following are likely threats:

1. Targeted malware and phishing attacks.
2. Targeted malware and phishing attacks – which could result in exposure of a network of contacts.
3. Targeted cyber attacks on personal devices.
4. Targeted network attacks.
5. Active monitoring of all communications – phone, SMS, VOIP, Chat, email, social media accounts etc.
6. Circumvention of SSL and VPN to monitor encrypted communication.
7. Automated profiling and tracking

KUWAIT

Petty theft is an ongoing risk, especially in outdoor markets and shopping malls. Cyber crime examples include spear phishing, impersonating company executives to make funds transfers, and hijacking of social media accounts to gain personal information.[19] Malicious software known as Bladabindi and Jenxcus – which is said have been installed on more than 7 million PCs – was written and distributed by developers in Kuwait and Algeria.[20]

Considered to be a relatively liberal state toward other religions, Kuwait has a small indigenous population of Christians and a growing population of converts from Islam.[21] However, Kuwait has also been described as the “epicenter of funding for terrorist groups in Syria” and has been identified as a major funder of al-Qaeda [22] It is also considered to be deeply involved in human trafficking, some of which feeds into the domestic worker market in Kuwait.[23]

Kuwait filters web content and blocks access to circumvention tools and VOI services. Using VOIP in Kuwait is illegal.[24] There is public evidence that Kuwait has DPI, LIG and over-the-air surveillance systems that allow for the tracking, interception and monitoring of cell phone calls in real time.[25]

---

19 https://www.osac.gov/pages/ContentReportDetails.aspx?cid=19057
20 http://gulfnews.com/news/gulf/kuwait/major-cyber-crime-rings-in-kuwait-and-algeria-busted-1.1354372
21 https://www.vomcanada.com/kuwait.htm
22 https://www.washingtonpost.com/world/national-security/kuwait-top-ally-on-syria-is-also-the-leading-funder-of-extremist-rebels/2014/04/25/10142b9a-ca48-11e3-a75e-463587891b57_story.html?utm_term=.9699fb8531c4
23 https://en.wikipedia.org/wiki/Human_rights_in_Kuwait
24 https://en.wikipedia.org/wiki/Human_rights_in_Kuwait
25 https://sii.transparencytoolkit.org/search?utf8=✓&utf8=✓&q=kuwait

There have been no reports of cyber attacks on missional organizations by Kuwait. The most likely threats are:

1. Monitoring of unencrypted email, SMS, VOIP, and phone calls.
2. Monitoring of unencrypted web and social media usage.
3. Untargeted malware and phishing attacks – criminal.
4. Untargeted cyber blackmail attacks – criminal.
5. Petty theft.

For those engaged in ministry directly in the country that raises concerns by the government, *especially work with human trafficking:*

1. Targeted cyber attacks on personal devices.
2. Targeted network attacks.
3. Real time monitoring of mobile devices and real time physical tracking.
4. Active monitoring of all communications – phone, SMS, VOIP, Chat, email, etc.
5. Remote entry to computers and mobile devices allowing access to encrypted files, webcams and microphones on those devices.

OMAN

Oman is ranked as the most cyber-secure country in the Middle East, and the third most secure in the world.[26] Oman heavily filters and monitors all Internet traffic and prohibit the use of VOIP technology. VPN use is common and at the time of this report, still considered legal. Although there was a proposed law that would have fined users of VPNs, this law does not appear to have been implemented. Ransomware, – malware that encrypts the data on a computer and requires a ransom payment to recover the data – is an issue for users of the Internet in Oman.[27] Another malware-based issue has been cyber blackmail, malware that has captured some private information and threatens to expose the information publicly or to the police if a blackmail payment is not made. This threat appears to be a trend among children.[28]

While it is not illegal for a Muslin to change their religion in Oman,[29] the government blocks access to sites that question Islam.[30] Militant groups like ISIS and Al-Qeada in the Arabian Peninsula (AQAP) while active in Yemen, and to some extent in Saudi Arabia, are not publicly active in Oman.[31]

---

26 http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Oman-third-best-prepared-in-world-to-thwart-cyber-attacks.aspx
27 https://www.osac.gov/pages/ContentReportDetails.aspx?cid=19108
28 http://timesofoman.com/article/95256/Oman/Science-/Hackers-out-to-get-your-personal-secrets-warn-cyber-experts-in-Oman
29 https://www.state.gov/j/drl/rls/irf/2014/nea/238472.htm
30 https://en.wikipedia.org/wiki/Internet_censorship_and_surveillance_by_country#.C2.A0Oman
31 https://www.osac.gov/pages/ContentReportDetails.aspx?cid=19108

There are no reports of state sponsored or aligned hacking groups in Oman. Oman engages in pervasive surveillance of web usage and all forms of communication. They have purchased and use many highly advanced cyber surveillance tools. The central government of Oman has advance cyber attack and monitoring tools. There is public evidence that Oman has DPI, LIG and over-the-air surveillance systems that allow for the tracking, interception and monitoring of cell phone calls in real time.[32]

There have been no reports of cyber attacks on missional organizations by Oman. The most likely threats are:

1. Monitoring of unencrypted email, SMS, VOIP, and phone calls.
2. Monitoring of unencrypted web and social media usage.
3. Circumventing SSL and VPN to allow monitoring of communication.
4. Untargeted malware and phishing attacks – criminal.
5. Untargeted cyber blackmail attacks – criminal.

For those engaged in ministry directly in the country that raises concerns by the government:

1. Targeted cyber attacks on personal devices.
2. Targeted network attacks.
3. Active monitoring of all communications – phone, SMS, VOIP, Chat, email, etc.
4. Remote entry to computers and mobile devices allowing access to encrypted files, webcams and microphones on those devices.

PALESTINE

Palestine is engaged in a continuing tit-for-tat with Israel on many fronts and cyber intrusion is one of those. Palestine as state, or semi-state, has limited control over its infrastructure. However there are very capable hackers in Hezbollah,[33] ISIS,[34] and Hamas[35] that are aligned with the Palestinian cause or some aspects of it. Some of the hacking tools used are modifications of open source tools and "borrowed" tools from Iran [36] These include web server shells, Trojans – Extreme RAT & Poison Ivy,[37] USB malware,[38] spear phishing,[39] virus, and DDOS tools.[40]

---

32 https://sii.transparencytoolkit.org/search?utf8=✓&utf8=✓&q=oman
33 http://www.timesofisrael.com/hezbollah-we-hacked-into-israeli-security-ca eras/
34 http://europe.newsweek.com/isis-hackers-join-forces-pro-palestine-hackers-anonghost-413999?rm=eu
35 http://www.securityweek.com/gaza-cybergang-attacks-attributed-hamas
36 http://www.haaretz.com/israel-news/.premium-1.650860
37 http://pwc.blogs.com/cyber_security_updates/2015/04/attacks-against-israeli-palestinian-interests.html
38 http://www.haaretz.com/israel-news/.premium-1.650860
39 http://www.haaretz.com/israel-news/.premium-1.642800
40 https://www.researchgate.net/publication/229005501_Asymmetric_Cyber-warfare_between_Israel_and_

In addition to these focused attack tools, there are gangs of cyber criminals in Gaza that seek to hijack credit cards, telephone lines, and the websites of financial institutions. They also create false websites for businesses and seek to collect web credentials and credit card details.[41]

There is public record that Palestine has acquired DPI technology.[42] While there is no record of other advanced cyber tools, it is likely that Palestine is able to receive help with cyber attacks and surveillance from aligned state actors and militant groups. The most likely threats are:

1. Monitoring of unencrypted email, SMS, VOIP, and phone calls.
2. Monitoring of unencrypted web and social media usage.
3. Untargeted malware and phishing attacks – criminal.
4. Untargeted theft of credit cards – criminal.
5. Untargeted hijacking of phone lines – criminal.
6. Untargeted fake websites seeking to gain access to credentials and credit cards – criminal.

For those engaged in ministry directly in the country that raises concerns by the government:

1. Targeted cyber attacks on personal devices.
2. Targeted network attacks.
3. Targeted malware and phishing attacks to gather personal information to be used by militant groups.
4. Targeted malware and phishing attacks to gather contact information to be used by militant groups.

QATAR

Qatar has the highest per capita income in the world, and has used its buying power to become fully equipped in cyber Intrusion and monitoring tools. Qatar has been the victim of several high profile cyber attacks on government, media and energy industry sites. One high profile attack on the Qatar National Bank utilized an SQ injection technique which was an open source tool.[43] It now has a strong cyber incident response capability.[44] However, new cyber security law makes a provision about public release of information that is offensive or embarrassing. This has resulted in revocation of visas, and large fines for social media posts, blog posts – even factual news reports. This law could be used to stifle almost any form of expression.

41 http://www.usnews.com/news/articles/2016-03-14/a-glimpse-into-the-world-of-gazas-cyber-pirates
42 https://sii.transparencytoolkit.org/search?utf8=□&utf8=□&q=palestine
43 https://blog.cybelangel.com/bank-qatar-hacked-nearly-anonymous-data-leak/
44 https://www.osac.gov/pages/ContentReportDetails.aspx?cid=19398

There are no reports of hacker groups aligned with Qatar. However, there are reports of varying levels of cyber crime – untargeted phishing, malware, and identity theft.[45]

Qatar has a reputation as being weak on human rights and of mistreating expat laborers. A fake human rights charity (Voiceless Victims) emerged in Qatar that sought to network with other charities in human rights, and was soliciting stories from expat workers of human rights violations. This effort appears to have been a "false flag" operation – designed to gather as much information as possible about who was involved in human rights issues in Qatar, – and who among the expat worker community was reporting issues.[46]

There is public evidence that Qatar has DPI, LIG, FinFisher surveillance software, remote access tools from The Hacking Team and over-the-air surveillance systems that allow for the tracking, interception and monitoring of cell phone calls in real time.[47]

There have been no reports of cyber attacks on missional organizations by Qatar. The most likely threats are:

1. Monitoring of unencrypted email, SMS, VOIP, and phone calls.
2. Monitoring of unencrypted web and social media usage.
3. Untargeted malware and phishing attacks – criminal.
4. Untargeted cyber blackmail attacks – criminal.
5. Petty theft.
6.

For those engaged in ministry directly in the country that raises concerns by the government, *especially human rights work among expat workers*, or engaging in any form of digital speech that can be determined to be "offensive"[48] under the Qatar cyber security law:

1. Targeted cyber attacks on personal devices.
2. Targeted network attacks.
3. Active monitoring of all communications – phone, SMS, VOIP, Chat, email, etc.
4. Attempts to subvert SSL and VPN encryption to monitor all communications.
5. Remote entry to computers and mobile devices allowing access to encrypted files, webcams and microphones on those devices.

45 https://www.osac.gov/pages/ContentReportDetails.aspx?cid=19398
46 http://www.forbes.com/sites/thomasbrewster/2016/12/21/voiceless-victims-a-fake-charity-spying-qatar-activists/#100faf1417a4
47 https://sii.transparencytoolkit.org/search?utf8=✓&utf8=✓&q=qatar
48 https://www.washingtonpost.com/news/worldviews/wp/2014/09/19/say-what-you-want-about-qatar-just-be-careful-about-doing-it-on-the-web/?utm_term=.174f39091111

SUDAN

Named a state sponsor of terror in 1993, Sudan has been a safe haven and training ground for multiple terrorist groups.[49] However at the time of this report, Sudan had distanced itself from many terror groups and sought to strengthen ties with the U.S. and Europe.[50]

As of 2016, Sudan does not block news, political content, or social media sites, but does block pornography. It is not known how much Gospel content is blocked by the government. At the time of this report there was greater freedom of information and expression on the web than in printed works in the country. WhatsApp is a very popular social media app and there is no evidence that there is any attempt to interfere with it. Rather than use technical means to block content, Sudan appears to deploy it's Cyber Jihadist Unit to monitor, shape and deflect online discussion and information [51] The Cyber Jihadist Unit also is reported to engage in hacking social media accounts of activists, posting content to discredit the account owner, and surface activist contacts. One social engineering technique is to create a social media account with the picture of an activist and then send invitations to contacts saying this is a new account because the old one got hacked. This lures those contacts to connect and expose their network of contacts.[52] The Cyber Jihadist Unit is reported to have over 200 staff members.[53]

The information infrastructure of Sudan is generally poor.[54] This makes it ripe for exploitation and cyber crime. Though on international embargo lists, Sudan has been able to purchase advanced technical tools that allow it to monitor phone calls, web and social media usage. There is public evidence that Sudan has DPI, LIG and remote access tools from The Hacking Team.[55]

There have been no reports of missional organizations being hacked by Sudan or it's surrogates. Currently the most likely threats are:

1. Monitoring of unencrypted email, SMS, VOIP, and phone calls.
2. Monitoring of unencrypted web and social media usage.
3. Untargeted Malware and phishing attacks – criminal
4. Untargeted theft of credit cards – criminal.

---

49 https://en.wikipedia.org/wiki/Terrorism_in_Sudan
50 http://www.atlanticcouncil.org/blogs/africasource/sudan-still-a-state-sponsor-of-terrorism
51 https://www.justice.gov/eoir/page/file/9169 1/download
52 http://www.dc4mf.org/en/content/online-war-sudan
53 https://www.apc.org/en/blog/online-surveillance-and-censorship-sudan
54 https://www.osac.gov/pages/ContentReportDetails.aspx?cid=19746
55 https://sii.transparencytoolkit.org/search?utf8=□&utf8=□&q=sudan

For those engaged in ministry directly in the country that raises concerns by the government:

1. Targeted cyber attacks on personal devices.
2. Targeted network attacks.
3. Targeted malware and phishing attacks to gather personal information.
4. Targeted attacks on social media accounts.
5. Targeted action to subvert social media campaigns.
6. Targeted action to discredit recognized voices.

YEMEN

Yemen is engaged in a civil war that is a proxy battle between Saudi Arabia/UAE and Iran. Therefore, the cyber warfare tools that Iran and Saudi Arabia/UAE have are available for use in this conflict. Al-Qeada in the Arabian Peninsula (AQAP) is a third party not aligned with other combatants. Those aligned with ISIS have also sought to control some territory. The presence of AQAP has prompted the USA to commit Special Operations Forces to aid Saudi Arabia/UAE with operational and intelligence support.[56]

The Houthi rebels that are aligned with Iran have control of much of the infrastructure of the country – including YemenNet – the core ISP of Yemen. There is evidence that Netsweeper is being used to restrict access to sites on the Internet – generally political news and commentary – as well as the entire Israeli name space. The type of political content being blocked in Yemen is mirrored by the blocking systems in both Saudi Arabia and Iran.[57] However, it has been confirmed that the site http://answering-islam.or [58] is specifically blocked at the IS level for all of Yemen. The provision of the Internet has been unstable and completely broken at times.[59] Foreign and domestic electronic surveillance is widespread and has resulted in wiretapped telephone conversations, and tracking of the physical location of specific users on the mobile phone network, as well as monitoring of SMS traffic. Houthi leaders are said to use Thuraya satellite phones in an attempt to sidestep monitoring of the telecom.[60]

The Yemen Cyber Army (thought to be an Iranian hacking team) has conducted large-scale targeted cyber attacks on Saudi Arabian infrastructure.[61] These attacks have demonstrated surprising sophistication for a hacking group that is new on the scene.[62]

---

56 http://www.openbriefing.org/publications/intelligence-briefings/remote-co rol-warfare-briefing-16-june-2016 increasing-awareness-of-risks-of-cyber-conflict-saudi-led- oalition-forces-in-yemen-receive-us-special-forces-support-islamic-state-linked-group-urges/
57 https://citizenlab.org/2015/10/information-controls-military-operations-yemen/
58 Ibid
59 Ibid
60 Ibid
61 Ibid
62 http://motherboard.vice.com/read/theres-evidence-the-yemen-cyber-army-is-actually-iranian

No reports have been received of direct cyber attacks on missional organizations originating from Yemen. However, the most likely threats are the following.

For those physically present in Yemen:

1. Petty theft.
2. Monitoring of unencrypted email, SMS, VOIP, and phone calls.
3. Monitoring of unencrypted web and social media usage.
4. Untargeted malware and phishing attacks – criminal.

For those engaged in ministry in Yemen that are physically present:

1. Targeted theft.
2. Active monitoring of all communications – phone, SMS, VOIP, Chat, email, etc.
3. Exposure of personal information by radical Muslim hackers to hostile militant groups.
4. Possible torture and death of nationals in country that are exposed in a cyber breach.
5. Targeted malware and phishing attacks – which could lead to kidnapping in county.

For those engaged in ministry to those in Yemen, but not physically present:

1. Targeted cyber attacks on personal devices.
2. Targeted network attacks.
3. Active monitoring of all communications of those being contacted in Yemen – phone, SMS, VOIP, Chat, email, etc.
4. Exposure of personal information by radical Muslim hackers to hostile militant groups.
5. Possible torture and death of nationals in country who are exposed in a cyber breach.
6. Targeted malware and phishing attacks – which could lead to kidnapping in county.