The Business Case for Managed Security

Prepared by:
Benjamin Robson
Chief Technology Officer
IPSec Pty Ltd
Copyright & Confidentiality

All copyright, intellectual property rights and rights to the proprietary information contained in this document are owned by and remain with IPSec Pty Ltd (IPSec).

This document is provided by IPSec to the Client (as noted in Document Control) on condition that neither it nor any part of it shall be disclosed to any third party without the express written permission of IPSec.

Restrictions on this document do not extend to those details that have previously been published or otherwise provided to the public domain.

Document Control

Document Title: IPSec Whitepaper – The Business Case for Managed Security

Prepared by: Benjamin Robson
Chief Technology Officer
IPSec Pty. Ltd.
Building 10, Omnico Business Park
270 Ferntree Gully Road, Notting Hill VIC 3168

Ph: 1300 890 902
Fx: 1300 890 912
WWW: http://www.ipsec.com.au

Document Approval

<table>
<thead>
<tr>
<th>Version #</th>
<th>Date</th>
<th>Approval by:</th>
<th>Comment:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>09/06/17</td>
<td>BenR</td>
<td></td>
</tr>
</tbody>
</table>
# Table of Contents

Copyright & Confidentiality ................................................................. 2  
Document Control ........................................................................ 2  
Document Approval ......................................................................... 2  
Table of Contents ........................................................................... 3  
The business case for managed security .......................................... 4  
   The cyber security risk ................................................................ 4  
   The importance of people to cyber risk ...................................... 6  
   Why engage an advanced managed security service provider (AMSSP)? ...................................... 7  
IPSec vSOC ..................................................................................... 8  
About IPSec .................................................................................. 8
The business case for managed security

The cyber security risk

All organisations, whether public or private, are compelled to consider risk and whether an issue or event, foreseen or unforeseen may negatively impact on their operational condition or even their very existence. It is generally considered that there are five principal types of risk (strategic, compliance, operational, financial, and reputational) with each of these having many elements that can contribute to their influence over the organisation¹. A rapidly growing influence over any organisations’ risk is that presented by the data environment; cyber risks that have the capacity to impact the organisation’s strategic direction, regulatory compliance, operational function, financial performance, and reputational trust.

In a recent survey, conducted by the Australian Securities Exchange (ASX) of their index of top 100 companies (ASX100), questioning their board members and senior executives revealed:

- 80% of companies’ project increased cyber risk next year;
- 62% of companies experienced an increase in cyber-attacks last year;
- 92% of organisations have cyber security in their corporate risk register; and
- 88% of company boards are seeking knowledge of cyber security incidents that impact their organisation.²

The value of compromised data has, over the past few years, become well established and understood as a tradable commodity within the criminal community and we have consequently seen the rapid commercialization of hacking tools generating substantial revenues for underground organisations.

In 2016 IBM commissioned the Ponemon Institute to conduct research into the cost of data breaches. It was found that the total average cost per breach was $2.64 million, and the per record cost of breaches as $142. Whilst the report found that the per breach cost has seen a minor decline, it is still substantial.³

The Symantec 2017 Internet Security Threat Report revealed that globally $3 billion has been stolen via business email compromises over the past three years, and that one in every 131 emails sent were malicious (the highest rate in five years).⁴

As well as commercial motivations for accessing confidential information, cyber criminals increasingly attack data assets for political objectives, and seeking revenge or awareness for perceived injustices committed by the victim organisation.

Over the years, we have seen a number of hacking actions against government and commercial organisations motivated by political objectives, or social justice motives, rather than financial advantage.

In 2016, the Australian Bureau of Statistics (ABS) was unprepared for the distributed denial of service (DDoS) attack launched against them on census night which resulted in substantial damage to the reputation of the organisation and unprecedented interference with the census process.⁵

---

In May 2017, the world fell victim to the WannaCry ransomware attack, resulting in tens of thousands of computer systems around the world being encrypted and organisations losing access to their data. This included the national health service (NHS) of the United Kingdom suspending day surgeries due to their information systems being encrypted.

In January 2017, it was revealed that thousands (more than 3,000) of Australian government officials, including politicians, police, and judges had been compromised when Yahoo was the subject of a massive data breach. This breach resulted in over 1 billion victims having their Yahoo email account credentials stolen and sold to cyber criminals for US$300,000 each.

In September 2016, it was reported that H&L Australia had been hacked by Ukrainian cyber-criminals resulting in customer information from their customer relationship management (CRM) system being stolen. This information included details from Woolworths-owned Australian Leisure and Hospitality (ALH) Group. Whilst this did not include credit card data it was, none-the-less, a hit to the organisation’s reputation.

The Australian Bureau of Meteorology (BoM) was, in October 2016, the target of a massive malware attack. A “foreign power” was able to install malicious software on to BoM computer systems and stole sensitive documents and then compromised other government networks.

Lloyd’s insurance assessed the cyber-attack risk to Australia, in 2016, as being $16 billion. Lloyd’s global chief executive Inga Beale said, "It's not just for banks to worry about — it impacts retailers, travel and hospitality firms, education and healthcare providers, and any business with proprietary information worth protecting."

"Where a decade ago people would talk about preventing a cyber-attack, the reality is firms will be subjected to attacks."

"The issue is how you mitigate against that."

Over the past few years we have witnessed cyber-attacks against government departments, banks, utilities, media companies, healthcare providers, entertainment business, retail operations, and organisations from almost all industries and sectors.

This has compelled an increase in regulatory obligations towards cyber threats and, consequently, has compelled boards and senior executives of all organisations to put cyber risk firmly on their organisational agenda.

---

6 https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html?_r=0
7 https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20
11 https://www.lloyds.com/cityriskindex/
The importance of people to cyber risk

Technology solutions, designed to mitigate the threat posed by cyber risk, have become incredibly powerful. Modern enforcement and detection tools are capable of learning patterns of normal individual, group, system and application behavior enabling them to identify in real-time deviations from normal and flagging them as potential breaches of the information environment.

But, at the end of the day, all technology tools require humans to instruct them on how to behave and require humans to be available to take action when they flag a potential issue.

When asked “Could you name just one single most effective technology or security measure for enterprise protection from high profile attacks? What gives most bang for your buck?”, Eugene Kaspersky responded, “Today you have to do many things. There’s no silver bullet. But the best investment is in your information security team, in your people.”

Where Mr. Kaspersky could easily have recommended further investment in technology, even his company’s suite of solutions, his number one recommendation was to invest in the organisation’s information security team.

An effective cyber security team requires more than an individual within the organisation who has a passing interest in data protection. An effective cyber protection outcome within an organisation requires a suite of solutions beyond the capacity of an individual to know as an adjunct to their normal systems administration duties.

With almost all organisations having firewalls, intrusion prevention systems, anti-malware solutions, email security products, web security products, virtual private network appliances, multi-factor authentication capabilities, mobile device management tools, patch management solutions, and many other cyber protection tools it is very challenging for a single person to know how to effectively manage, maintain, monitor, and respond to all of these disparate outcomes, let alone on a 24x7 basis (including 3am on New Year's day).

<table>
<thead>
<tr>
<th>Security Program Requirements</th>
<th>In-house Minimum Security</th>
<th>In-house State-of-the-Art</th>
<th>Outsourced Security Service State-of-the-Art</th>
</tr>
</thead>
<tbody>
<tr>
<td>Staffing Requirement</td>
<td>1 Employee</td>
<td>5 Employees (24x7x365 coverage)</td>
<td>Outsourced Security Team</td>
</tr>
<tr>
<td>Staff Experience</td>
<td>Junior – Mid. Level</td>
<td>Mid. Level</td>
<td>Expert</td>
</tr>
<tr>
<td>Monitoring &amp; Response</td>
<td>9AM – 5PM</td>
<td>24x7x365</td>
<td>24x7x365</td>
</tr>
<tr>
<td>Administration</td>
<td>9AM – 5PM</td>
<td>24x7x365</td>
<td>24x7x365</td>
</tr>
<tr>
<td>Incident Response</td>
<td>Business Hours or Overtime</td>
<td>Immediate</td>
<td>Immediate</td>
</tr>
</tbody>
</table>

13

https://www.reddit.com/r/IAmA/comments/6ajstf/im_eugene_kaspersky_cybersecurity_guy_and_ceo_of/dhfd4lm/
To achieve an effective cyber risk mitigation outcome, this compels organisations to consider the need for a data security team with multiple individuals capable of operating around the clock. This causes the real cost of establishing an effective defense regime to rapidly climb.

<table>
<thead>
<tr>
<th>Security Program Requirements</th>
<th>In-house Minimum Security</th>
<th>In-house State-of-the-Art</th>
<th>Outsourced Security Service State-of-the-Art</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Staffing Salaries</strong></td>
<td>$80,000 + 20% Overhead + Overtime for incidents</td>
<td>$120,000 + 20% Overhead x 5 people</td>
<td>Not applicable</td>
</tr>
<tr>
<td><strong>IT Manager</strong></td>
<td>10% of Time @ $140,000</td>
<td>20% of Time @ $140,000</td>
<td>Not applicable</td>
</tr>
<tr>
<td><strong>Training</strong></td>
<td>$10,000</td>
<td>$10,000 x 5 people</td>
<td>Not applicable</td>
</tr>
<tr>
<td><strong>Total Annual Cost</strong></td>
<td>$120,000 + Overtime for incidents</td>
<td>$798,000</td>
<td>$40,000 – $200,000</td>
</tr>
</tbody>
</table>

Salary data is based on the 2016 Hays Salary Guide.¹⁴

Whilst it is very obvious that a single data security specialist within an organisation is an improvement over no specialist capabilities, it is equally obvious that the one individual will be quickly overwhelmed by the demands of the role without substantial additional support.

Even if the individual’s workload was such that they did not face a high demand the organisation would likely experience a security staff retention issue as the individuals they engage find themselves disconnected from the rapidly evolving cyber security space and would seek to establish themselves within a data security community, most likely within another, larger organisation.

Just as it can be easily determined that it is not sufficient to address the organisation’s data protection needs with an individual staff member, it can also be quickly identified that for most Australian organisations achieving an effective in-house cyber team is not achievable. Whilst the cyber threat posed to the organisation may be substantial, most organisations would struggle to justify a skilled team capable of operating 24 hours a day, 7 days a week, business days and non-business days.

**Why engage an advanced managed security service provider (AMSSP)?**

Advanced managed security service providers (AMSSPs) operate manned 24 x 7 security operations centres, staffed with trained and experienced cyber security specialists, designed to monitor, managed, maintain, and rapidly respond to the data protection outcomes of their customers.

Because AMSSPs are monitoring the data security of many organisations they are able to operate around the clock and have available experienced information security practitioners at all hours of the day.

To the customer organisation they offer a substantial cyber risk mitigation capability with powerful tools of breach detection and remediation, and are able to ensure that data security resources are continually trained and knowledgeable of emerging technologies, threats and remediation techniques.

Where an organisation may consider establishing an internal cyber team, taking on board the substantial annual costs associated with such an outcome, AMSSPs are able to offer significant data security outcomes for a fraction of the costs.

The cyber security realm is one of continual evolution and revolution, requiring substantial amounts of continuous training, so much so that it is almost impossible for any single individual to remain across all aspects of the changing information security world. This causes specialist security practitioners to seek communities of similar professionals to work with that may share the burden of maintaining continuous awareness of new and emerging threats and mitigation techniques.

Advanced managed security service providers act as hubs towards which cyber security professionals gravitate, so they are able to work with a team of similarly oriented professionals. This makes it easier for AMSSPs to attract and retain specialist information security personnel, and makes AMSSPs an attractive partner for most Australian organisations.

AMSSPs are able to provide to organisations significant cyber security capabilities and access to appropriately skilled, certified, and experienced resources at a fraction of the cost that might otherwise need to be incurred by the organisation.

---

**IPSec vSOC**

IPSec’s revolutionary suite of advanced managed security services provides your organisation with access to the expertise required to successfully protect information assets and to achieve the cyber security outcomes desired, 24 hours a day, 7 days a week, 365 days a year.

IPSec’s advanced managed security services provide for 24 x 7 security solution management, performance monitoring, and security monitoring. IPSec is ready to assist you to achieve your desired information security outcomes 24 x 7 x 365 with clear service levels and complete transparency.

The IPSec suite of advanced managed security services delivers the highest quality of security management outcomes within an achievable operational expense. Your IT resources are released from the burden of security management tasks, freeing up their time to focus on what is most important in the day to day information systems delivery.

---

**About IPSec**

IPSec are specialists in information asset security; technology experts who know how to mitigate risk to business by implementing end-to-end solutions that protect invaluable intelligence, data and information. From assessing vulnerabilities and threats, to designing and implementing customised security strategies, to managing execution and optimising results. IPSec are guardians of business confidence, providing high levels of protection and optimal assurance of an organisation’s security posture.

IPSec is about mitigating risk; enabling confidence and agility by ensuring a reliable IT environment that allows business to get on with business.