Sinu. Your IT Department.

Oh, the humanity!

The role people play in data security

NYC: 212.380.1230 | DC: 202.800.7510
www.sinu.com

Sinu. Your IT Department.

Oh, the humanity! The role people play in data security

CONTENTS

INTRODUCTION

As the technology department for many nonprofits and small businesses, Sinu strives to add value in all aspects of each organization we work with, including helping structure polices and sharing best practices to protect your data. We hope this document is useful in helping to support a culture of data security that begins with the people in your organization. If you are interested in a more complete listing of security topics to consider when evaluating your technology, please refer to Addendum I of this document*: Security Priorities for Nonprofits.*

PEOPLE: THE FIRST AND LAST LINE OF DEFENSE IN DATA SECURITY

High-profile intrusions over the past few years, including iCloud, Sony, and JP Morgan, have brought to the forefront the importance of data security. While organizations may be more diligent about utilizing security hardware and software, people play a critical role in protecting against data security breaches. In fact, studies show that 95 percent of IT security breaches are attributed, in part, to human error (according to IBM's 2014 Cyber Security Intelligence Index report).

Large companies with big technology budgets are not immune to the human side of data security. One of the largest data breaches in recent history was with JP Morgan in 2014. That year alone, the company spent $250 million on computer security, yet it turned out that human error was, in part, to blame for the breach. The company's security team apparently forgot to upgrade an overlooked server in its vast network, leaving JP Morgan vulnerable to intrusion.

With the human factor so critical to preventing data breaches, it is important to put a clear, easy-to-adopt security protocol in place and clearly communicate expectations to employees in order to minimize your organization's risk. Even with a modest security budget, there are ways to create a culture of data security within your organization. This brief outlines several security best practices that most organizations can adopt with a little time, good internal communication, and without a large investment.

Note: *This brief was developed to provide sample IT policies, security guidelines, and other tools that your organization can use as a starting point when managing your data security. All policy information provided is of a general nature; you should work with your Human Resources and Legal Departments when creating your own policies.*

NYC: 212.380.1230 | DC: 202.800.7510
www.sinu.com

CONTENTS

DOCUMENT AND STREAMLINE YOUR TECHNOLOGY INFRASTRUCTURE

Most small businesses and nonprofits no longer need a large in-house technology infrastructure. It is often an unnecessary cost, takes a lot of time to manage and support, and can pose an unnecessary risk.

It is important to recognize today's accelerated replacement cycle and develop a plan to retire your solutions accordingly. We recommend developing a replacement plan that reflects a 3-year replacement cycle on desktops and laptops and a 2-year cycle for mobile devices. If you are running computers that are over 4 years old, they will not run the latest operating systems and may no longer be supported and will not receive anti-malware and security updates. Just one piece of obsolete technology can pose a threat to your entire infrastructure.

As part of developing a data security protocol, it is important to map out all your solutions and infrastructure, as well as the employees who have access to them. These are potential points of access to data and can therefore pose a data breach risk. Keep track of which systems require passwords and who has access to them. Review system security regularly and remove any unused accounts. Reset passwords at least twice a year and more often if you have high employee turnover.

LIMIT ACCESS TO SENSITIVE DATA AND KNOW THE RISK OF LOCAL ADMINISTRATOR RIGHTS

Limit access to sensitive data to only those who need it and try to integrate the authentication of as many of your systems as possible. Several systems now support 'Single Sign On' where one system will let you in if you have already authenticated to another one. This can help reduce the number of passwords you need to manage and allow you to more easily update them on a regular basis and/or when you have staff changes.

IT best practices dictate that employees not be given local administrator rights (LAR). LAR is the highest level of permission that is granted to a computer user; this level of permission normally allows the user to install software and change configuration settings. Auditors also frown upon the practice because of its inherent risk. There are a number of reasons employees may ask for LAR, arguing convenience and expediency. However, LAR give someone the ability to shut off the security controls used to protect an organization's systems, including password controls and anti-malware software. Unapproved software could also be installed, breaking critical applications and causing disruption and downtime. A company can also be exposed to malware, including a number of different phishing scams that can deliberately run code on systems with full permissions if someone inadvertently clicks on a malicious link or opens infected email content.

CONTENTS

CREATE AND MANAGE STRONG PASSWORDS

Passwords are often the last defense against hackers. However, the top 2 passwords over the past few years have been “123456” and “password.”

To protect your organization’s data, commit to automatically generating strong passwords that are changed every 3 to 6 months and use two-factor authentication whenever possible. Password generators can help produce hard-to-hack passwords and password managers can safely store and keep track of your passwords.

Whether or not you decide to use a password generator or manager, here are 5 tips for securing your passwords:

1. Generate a different password for each online account;
2. Change your passwords every 3 to 6 months and don’t reuse them;
3. When generating your own password, it should contain upper and lowercase letters, punctuation, a number, and be 7-14 characters long;
4. Do not store your password list in the cloud, such as on Google Docs or Dropbox; and
5. Use two-step verification on all cloud-based services that offer it by providing a mobile number and/or email address as well as a password. (While it may take an extra step to set up two-factor authentication, your data has a much better chance of remaining safe in the event of a password breach.)

When generating your own password, it should contain upper and lowercase letters, punctuation, a number, and be 7-14 characters long.

If you have not already done so, we recommend developing a simple, organization-wide password security policy. Even if your organization’s leadership has adopted best practices to generate and manage passwords, your employees need to follow suit; each person in an organization plays an important role in protecting against data security breaches.

Addendum II of this document provides a sample password security policy.

CONTENTS

RECOGNIZE MALICIOUS EMAILS

The greatest threats to our data security can come through email. We've all been repeatedly warned to check for suspicious downloads, but spoof emails and phishing scams are getting harder to detect, especially when they come with a logo from your local bank or another trusted company. According to the 2014 McAfee Labs Threats Report, 80% of business users failed to spot a malicious email. Understanding how to recognize and handle these types of threats, as well as sharing this information within your organization, could help mitigate the risk of a data breach.

One of the most common phishing techniques is email spoofing whereby hackers hide the true origin of an e-mail message to trick someone into clicking on a link or providing sensitive information. By changing certain properties of the e-mail, such as the From, Return-Path, and Reply-To fields (which can be found in the message header), ill-intentioned users can make the email appear to be from someone other than the actual sender. In fact, scammers "spoof" because they know you are more likely to take action on an email from a familiar party (family, friend, or vendors like PayPal, Amazon, and Quickbooks).

Example of a spoof email courtesy of Visa

Phishing is not executed using malware or a virus so software and hardware protections are not entirely effective in filtering out this kind of email.

There are a number of ways to identify a suspicious or malicious email:

1. Absence of company logos and letterheads;
2. Poor grammar and/or spelling;
3. The body of the message is an image rather than true text;
4. File attachments ending in: .exe, .zip, .bat, or any other container-type of file;
5. The origin web site of the email will often have the name of the familiar company in it, but it will have extraneous information in the web address;
6. Email requests with high urgency and quick action (if you are in doubt, double check the request with the sender either by phone or by composing a new email—never reply to the email itself; and
7. Unsolicited email – if you didn't prompt a password reset, for instance, don't click the link.

It is important to remember that email was never designed to be a secure communication medium and banks and other trusted companies will not use email to request sensitive information from you.

CONTENTS

BACK UP LAPTOPS

Most organizations regularly back up their servers, but do not have a system to back up data from the laptops that are increasingly being used in the workplace by employees. Because people using laptops often store data on the local drive rather than on the server, mobility poses a data security risk if not mitigated. We recommend an online file backup solution for each laptop.

Online backup services provide a simple, secure, and economical way to protect all the files on a laptop's hard drive. If the hard drive crashes, the laptop is stolen, information is accidentally erased, or access to important files is lost, online backup services give you the ability to quickly restore any lost information.

If you are currently backing up files to an external hard drive, switching to online backup can provide additional data security for several reasons listed below.

1. External hard drives have the same hardware failure issues that the internal hard drive of a computer does and puts the stored information at risk when a hard drive eventually fails.
2. If your external hard drive is misplaced or stolen, you immediately lose all the backup information that is stored there. Online backup services allow you to store your information remotely and securely on servers that are professionally maintained.
3. External hard drives have storage limitations, while top-rated online backup services offer unlimited storage capacity.
4. The cost of online backup is about 50% less than external hard drives for the same amount of storage.

Because people using laptops often store data on the local drive rather than on the server, mobility poses a data security risk if not mitigated. We recommend an online file backup solution for each laptop.

While there is some cost to online backup solutions for laptops, most organizations find it worth the investment because it not only protects data, but also allows for data recovery in the incidence of a crashed hard drive. Additionally, you can access the data from an employee's laptop should they leave the company.

CONTENTS

BE WARY OF PUBLIC WI-FI

There's nothing more frustrating than being unable to connect to the Internet when you could really use it. While coffee shops and airports often provide free public Wi-Fi, hackers are also capitalizing on people's desire for convenience.

Airports are particularly prime spots for hackers to target because there are many people disconnected from their traditional Wi-Fi networks. Below are several tips for protecting your identity and data while traveling or outside of your usual networks.

1. **Know Your Wi-Fi**
   Whenever possible, use Wi-Fi networks you know and that are secured with a password to ensure you are accessing a legitimate Wi-Fi connection.
2. **Turn Off File Sharing**
   Whether you're on a PC or an Apple computer, you can turn off access to your files from outside parties very quickly by turning off file and printer sharing.
3. **Forget the Network**
   To forget the network on a device, hold down on the network name until the option pops up. On a computer, go into your network preferences and remove the network from your computer's memory. This will prevent your computer or device from automatically connecting to that unsecured network in the future.
4. **Use a HotSpot**
   Most cell phone carriers are now offering the option for a personal hotspot, turning your cell phone into a mobile Wi-Fi. Be sure to secure the network with a password.
5. **Require Networks To Get Your Permission**
   When you're not using your device, you should get in the habit of turning off your Wi-Fi network, or configure your device to request your permission before connecting to a new Wi-Fi network.
6. **Buy A Data Plan**
   If you travel often with your device, it is worth investing in a data plan so you're using a secure network.
7. **Avoid Paying Bills on Public Wi-Fi**
   When paying bills or making purchases online, it's best to do it on a trusted network.

CONTENTS

ADDENDUM I: SECURITY PRIORITES FOR NONPROFITS

Sinu recommends that nonprofits approach security practices in order of priority. Listed below are several priorities for consideration in order to begin a conversation about security.

FIRST PRIORITY

- Perimeter (email) spam and virus protection
- Intrusion prevention (firewall)
- Wireless security
- Data protection policy (local and remote backup)
- Server and workstation antivirus protection (viruses)
- Inventory of hardware assets
- Annual risk assessment

SECOND PRIORITY

- Physical Network Security – locked, climate controlled space
- Web traffic filtering (for malware)
- Password policy
- Permission review
- Legal compliance review
- Business continuity management

THIRD PRIORITY

- Email encryption
- Email compliance policy and practice
- Laptop recovery software

INFORMATION SECURITY

Information security is the set of business processes and policies that protects information. Information security typically involves both physical and digital security measures to protect data from unauthorized access, use, replication or destruction, and often includes:

- Analysis of the organization's information security risks
- Security policy
- Asset management: inventory and classification of information assets
- Human resources security: security aspects for employees joining, moving, and leaving
- Physical and environmental security: protection of the computer facilities
- Access control: restriction of access rights to networks, systems, applications, functions, and data
- Information systems acquisition, development, and maintenance: building security into applications
- Information security incident management
- Business continuity management: protecting, maintaining, and recovering business-critical systems
- Compliance: ensuring conformance with information security policies, standards, and laws

CONTENTS

ADDENDUM II: SAMPLE PASSWORD SECURITY POLICY

Passwords are the first line of defense in the protection of information assets contained in the [ORGANIZATION's] systems. All individuals are responsible for taking appropriate steps to select and maintain the security of their passwords.

- Individuals must not disclose their passwords to anyone, whether inside or outside the [ORGANIZATION]. If, on occasion, individuals are required to share their password with other staff, they must change their password once the task is completed.

- Passwords must be constructed according to the [ORGANIZATION's] established complexity standards. Good passwords include a mixture of upper- and lower-case letters, numbers, and symbols. They should be at least seven characters long and should not include any English dictionary words.

- Passwords should be changed at least once every 90 days.

- It is recommended that individuals not select the same password to access [ORGANIZATION] systems that they have selected for accessing systems not hosted by the [ORGANIZATION] (including, but not limited to, personal on-line banking services, market data services, personal email accounts, etc.).

- Failure to comply may subject individuals to disciplinary action by the [ORGANIZATION] up to and including termination. In addition, conduct that is unlawful may subject individuals to civil, and in some cases criminal, liability.

Note: *All policy information provided is of a general nature; you should work with your Human Resources and Legal Departments when creating your own policies.*

CONTENTS

ABOUT SINU

Sinu is an IT company that was founded in 2000 on a simple premise: People matter, things don't. In other words, technology is just one more tool to help employee productivity and support the goals of your organization and it's our job to deliver reliable service for your employees.

We believe that our customers should have access to the competitive advantages delivered by proven technologies and best practices usually only accessible to big businesses with big IT budgets. So Sinu built enterprise best practices and network security into our small business IT solution and nonprofit IT services platform. The platform streamlines IT management and our customers experience superior network performance and employee productivity.

For an affordable all-inclusive fee, Sinu offers the technology, stability and performance usually accessible only to big businesses, without the significant investments in computer hardware and software or the time and expense to train employees on new systems.

Sinu's IT management service provides predictable costs for your organization because all essential technologies and support for your nonprofit are included in an all-inclusive fee that is based on the number of your employees that need the Sinu service. No need to budget for new hardware or to try to get by on technology that should be retired. It is all part of the service. Backups, updates and patches happen automatically and we are there to support your employees whenever they need us and as often as they need us – all for the same fee.

At Sinu, we are driven to provide a superior customer experience, not only through reliable technology but also with ongoing customer support. Each customer has a senior account manager that can provide CTO-level consulting to help your company navigate through the vast – and ever-changing – array of technology options and maximize the Sinu platform to best meet your organizational goals.

Ultimately, our customers turn to us because of our value proposition. From CTO-level consultation to a full-time help desk and friendly onsite service, we are dedicated to supporting your organization and employee productivity through proven, reliable technology and excellent customer service.

For more information about Sinu and our IT management services, contact David Owen, Principal & CSO, at dowen@sinu.com or call (212) 380-1230.