HR TOOLKIT

Cyber Security

Provided by: Troy Benefits Consulting

TROY
BENEFITS
CONSULTING

Table of Contents

Introduction

The majority of cyber criminals are indiscriminate when choosing their victims. The Department of Homeland Security (DHS) asserts that cyber criminals will target vulnerable computer systems regardless of whether the systems belong to a Fortune 500 company, a small business or a home user.

Cyber criminals look for weak spots and attack there, no matter how large or small the organization. Small businesses, for instance, are becoming a more attractive target as many larger companies tighten their cyber security.

Most small businesses can't afford the ramifications of a cyber attack, and as a result, nearly 60 percent of the small businesses victimized by a cyber attack close permanently within six months of the attack. Many of these businesses put off making necessary improvements to their cyber security protocols until it is too late because they fear the costs would be prohibitive.

Businesses both large and small need to be proactive in order to protect against growing cyber threats. This planning guide is designed to help employers protect their business, information and customers from cyber threats. This guide is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. It is generally recommended that businesses using sophisticated networks with dozens of computers consult a cyber security expert in addition to using this cyber security planning guide.

Privacy and Data Security

Data security is crucial for all businesses. Customer and client information, payment information, personal files, bank account details—this information is often impossible to replace if lost and is extremely dangerous in the hands of criminals. Data lost due to disasters such as a flood or fire is devastating, but losing data to hackers or a malware infection can have far greater consequences. How you handle and protect your data is central to the security of your business and the privacy expectations of customers, employees and partners.

Action Items

1 Conduct an Inventory

Conducting an inventory will help you answer the following questions:

- **What kind of data does your business have?**
  - A typical business will have all kinds of data, some of it more valuable and sensitive than others—but all data has value to someone. Your business data may include customer data such as account records, transaction accountability and financial information, contact and address information, purchasing history, and buying habits and preferences, as well as employee information such as payroll files, direct payroll account bank information, Social Security numbers, home addresses and phone numbers, and work and personal email addresses.
  - You may also have proprietary and sensitive business information such as financial records, marketing plans, product designs, and state, local and federal tax information.

- **How is that data handled?**
  - Security experts are fond of saying that data is most at risk when it's on the move. If all your business-related data resided on a single computer or server that was not connected to the internet, and never left that computer, it would probably be very easy to protect.
  - To be meaningful, data must be accessed and used by employees, analyzed and researched for marketing purposes, used to contact customers and even shared with key partners. Every time data moves, it can be exposed to different dangers.

- o As an HR professional, you should have a straightforward plan and policy—a set of guidelines, if you will—about how each type of data should be handled, validated and protected based on where it is traveling and who will be using it.

- **Who has access to that data and under what circumstances?**

  - o Not every employee needs access to all of your information. Your marketing staff shouldn't need or be allowed to view employee payroll data, and your administrative staff may not need access to all your customer information.

    Once you've done an inventory of your data and you know exactly what data you have and where it's kept, it is important to assign access rights to that data. Doing so means creating a list of the specific employees, partners or contractors who have access to specific data, under what circumstances they have access to it, and how those access privileges will be managed and tracked.

    Your business could have a large assortment of data of varying value, including the following:

    - Customer sales records
    - Customer credit card transactions

    - Customer mailing and email lists
    - Customer support information

    - Customer warranty information
    - Patient health or medical records

    - Employee payroll records
    - Employee email lists

    - Employee health and medical records
    - Business and personal financial records

    - Marketing plans
    - Business leads and inquiries

    - Product design and development plans
    - Legal, tax and financial correspondence

2 **Catalog Your Inventory**

Once you've identified your data, keep a record of its location and move it to a more appropriate location as needed.

3 **Develop a Privacy Policy**

Privacy is important for your business and your customers. Continued trust in your business practices and products, combined with secure handling of your clients' unique information, impacts your profitability. Your privacy policy is a pledge to your customers that you will use and protect their information in ways that they expect and that adhere to your legal obligations.

Your policy starts with a simple, clear statement describing the information you collect about your customers (e.g., physical addresses, email addresses and browsing history) and what you do with it. There are a growing number of regulations protecting customer and employee privacy, which often carry costly penalties for privacy breaches. You will be held accountable for what you claim and offer in your policy.

That's why it's important to create your privacy policy with care and post it clearly on your website. It's also important to share your privacy policies, rules and expectations with all employees and partners who may come into contact with that information. Your employees need to be familiar with your privacy policy and what it means for their daily work routines.

Your privacy policy should address the following types of data:

- **Personally identifiable information**—Often referred to as PII, this information includes things such as first and last names, home or business addresses, email addresses, credit card and bank account numbers, taxpayer identification numbers, patient numbers and Social Security numbers. It can also include gender, age, date of birth, city of birth or residence, driver's license numbers, and home and cellphone numbers.

- **Personal health information**—Whether you're a health care provider with lots of sensitive patient information or you manage health or medical information for a small number of employees, it's vital that you protect that information. A number of studies have found that most consumers are very concerned about the privacy and protection of their medical records. They do not want their health information falling into the hands of hackers or identity thieves who might abuse it for financial gain. They also do not want co-workers prying into their personal

health details, and they don't want future employers or insurers finding out about any medical conditions or history.

- **Customer information**—This includes payment information such as credit or debit card numbers and verification codes, billing and shipping addresses, email addresses, phone numbers, purchasing history, buying preferences and shopping behavior.

4 Protect Data Collected on the Internet

Your website can be a great place to collect information such as transactions and payments, purchasing and browsing history, newsletter sign-ups, online inquiries and customer requests.

This data must be protected, whether you host your own website and manage your own servers, or whether your website and databases are hosted by a third party, such as a web hosting company.

If you collect data through a website hosted by a third party, be sure that the third party fully protects that data. Apart from applying all the other precautions that have been described, such as classifying data and controlling access, you need to make sure any data collected through your website and stored by the third party is sufficiently secure. That means any data is protected from hackers and outsiders as well as employees of the hosting company.

5 Create Layers of Security

Protecting data, like any other security challenge, is about creating layers of protection. The idea of layering security is simple: you cannot and should not rely on just one security mechanism—such as a password—to protect something sensitive. If that security mechanism fails, you have nothing left to protect you.

When it comes to data security, there are a number of key procedural and technical layers you should consider.

- Inventory your data.

  o As described above, you need to conduct a data inventory so you have a complete picture of all the data your business possesses or controls. It's essential to get a complete inventory, so you don't overlook sensitive data that could be exposed.

- Identify and protect your sensitive and valuable data.

  o Data classification is one of the most important steps in data security. Not all data is created equal, and few businesses have the time or resources to provide maximum protection to all their data. That's why it's important to classify your data based on how sensitive or valuable it is, so that you know what your most sensitive data is, where it is located and how well it's protected.

  Common data classifications include the following:

HIGHLY CONFIDENTIAL:

This classification applies to the most sensitive business information that is intended strictly for use within your company. Its unauthorized disclosure could seriously and adversely impact your company, business partners, vendors, and customers in the short and long term. It could include credit card transaction data, customer names and addresses, card magnetic stripe contents, passwords and PINs, employee payroll files, Social Security numbers and patient information (if you're a health care business).

SENSITIVE:

This classification applies to sensitive business information that is intended for use within your company. Information that you consider to be private should be included in this classification. Examples include employee performance evaluations, internal audit reports, various financial reports, product designs, partnership agreements, marketing plans and email marketing lists.

INTERNAL USE ONLY:

This classification applies to sensitive information that is generally accessible by a wide audience and is intended for use only within your company. While its unauthorized disclosure to outsiders should be against policy and may be harmful, the unlawful disclosure of the information is not expected to negatively impact your company, employees, business partners, vendors and the like.

- **Control access to your data.**

  o No matter what kind of data you have, you must control access to it. The more sensitive the data, the more restrictive the access. As a general rule, access to data should be on a need-to-know basis. Only individuals who have a specific need to access certain data should be allowed to do so.

  o Once you've classified your data, begin the process of assigning access privileges and rights—that means creating a list of who can access what data, under what circumstances, what they are and are not allowed to do with it, and how they are required to protect it. As part of this process, a business should consider developing a straightforward plan and policy—a set of guidelines—about how each type of data should be handled and protected based on who needs access to it and the level of classification.

- **Secure your data.**

  o In addition to administrative safeguards that determine who has access to what data, technical safeguards are essential. The two primary safeguards for data are passwords and encryption.

    ▪ Passwords should be the strongest they can reasonably be. Employee training on the basics of secure passwords and their importance is a must.

    ▪ Passwords alone may not be sufficient to protect sensitive data. Businesses may want to consider two-factor authentication, which often combines a password with another verification method, such as a PIN. Some popular methods of two-factor identification include the following:

      • Something the requestor individually knows as a secret, such as a password or a PIN.

      • Something the requestor uniquely possesses, such as a passport, physical token or ID card.

      • Something the requestor can uniquely provide as biometric data, such as a fingerprint or face geometry.

  o Encryption has been used to protect sensitive data and communications for decades, and today's encryption is affordable, easy to use and highly effective in protecting data from prying eyes.

    ▪ Encryption encodes or scrambles information to such a degree that it is unreadable and unusable by anyone who does not have the key to unlock the

data. The key is like a password, so it's very important that the key is properly protected at all times.

- Encryption is affordable for even the smallest business, and some encryption software is free. You can encrypt an entire hard drive, a specific folder on a drive or just a single document. You can also use encryption to protect data on a USB or thumb drive and on any other removable media.

- Because not all levels of encryption are created equal, businesses should consider using a data encryption method that is certified by the Federal Information Processing Standard, which means it has been certified for compliance with federal government security protocols.

- **Back up your data.**

  o Just as critical as protecting your data is backing it up. In the event that your data is stolen by thieves or hackers, or even erased accidentally by an employee, you will at least have a copy to fall back on.

  o Put a policy in place that specifies what data is backed up, how it is backed up, how often it's backed up, who is responsible for creating backups, where and how the backups are stored, and who has access to those backups.

  o Businesses have many backup options, whether it's backing up to an external drive in the office, or backing up online so that all data is stored at a remote and secure data center.

  o Remember, physical media—such as a disc or drive used to store a data backup—is vulnerable no matter where it is located, so make sure you guard any backups stored in your office or off-site, and make sure that your backup data storage systems are encrypted.

6 — Plan for Data Loss or Theft

Every business has to plan for the unexpected, and that includes the loss or theft of data from your business. Not only can the loss or theft of data hurt your business, brand and customer confidence, it can also expose you to the costly state and federal regulations that cover data protection and privacy. Data loss can also expose you to significant litigation risk.

That's why it's critical to understand exactly which data or security breach regulations affect your business and how prepared you are to respond to them. Understanding these regulations will make it easier to launch a rapid and coordinated response to any loss or theft of data.

At the very least, all employees and contractors should understand that they must immediately report any loss or theft of information to the appropriate company officer. No loss should be ignored. So even if you have sensitive data that just can't be accounted for, such as an employee who doesn't remember where he left a backup tape, it may still constitute a data breach and you should act accordingly.

Keep in mind that you may need to report a breach to your customers as well. All states and the District of Columbia have data breach notification laws dictating how businesses must alert their customers that a breach has occurred.

Scams and Fraud

New telecommunication technologies may offer countless opportunities for businesses, but they also offer cyber criminals many new ways to victimize your business, scam your customers and hurt your reputation. Businesses of all sizes should be aware of the most common scams perpetrated online.

Action Items

1 Train Employees to Recognize Social Engineering

Social engineering, also known as "pretexting," is used by many criminals, both online and off, to trick unsuspecting people into giving away their personal information or installing malicious software onto their computers, devices or networks. Social engineering is successful because criminals do their best to make their work look and sound legitimate, sometimes even helpful, which makes it easier to deceive users.

Most social engineering occurs over the telephone, but it frequently occurs online as well. Information gathered from social networks or posted on websites can be enough to create a convincing ruse to trick your employees. For example, LinkedIn profiles, Facebook posts and Twitter messages can allow a criminal to assemble detailed reports on employees. Teaching people the risks involved in sharing personal or business details on the internet can help you prevent both personal and organizational losses.

Many criminals use social engineering tactics to get individuals to voluntarily install malicious computer software, such as fake anti-virus software, thinking they are doing something that will make them more secure. Fake anti-virus software is designed to steal information by mimicking legitimate security software. Users who are tricked into loading malicious programs on their computers may be providing remote control capabilities to an attacker or unwittingly installing software that can steal financial information.

The malware can also make system modifications that make it difficult to terminate the program. The presence of pop-ups displaying unusual security warnings and asking for credit card or personal information is the most obvious method of identifying a fake anti-virus infection.

2 Protect Against Phishing and Online Fraud

Phishing is a technique used by online criminals to trick people into thinking they are dealing with a trusted website or other entity. Businesses face this threat from two directions—phishers may be impersonating them to take advantage of unsuspecting customers, and phishers may be trying to steal their employees' online credentials.

Attackers often take advantage of current events and certain times of the year, such as the following:

- Natural disasters

- Epidemics and health scares

- Economic concerns

- Major political elections

- Holidays

Businesses should ensure that their online communications never ask their customers to submit sensitive information via email, personal visits or phone. Make a clear statement in your communications reinforcing that you will never ask for personal information via email so that if someone targets your customers, they may realize the request is a scam.

Employee awareness is your best defense against your users being tricked into handing over their usernames and passwords to cyber criminals. Explain to everyone that they should never respond to incoming messages requesting private information. If a stranger claims to be from a legitimate organization, verify his or her identity with the stated company before sharing any personal or classified information.

Also, to avoid being led to a fake site, employees should know to never click on a link sent by email from an untrustworthy source. Employees who need to access a website link sent from a questionable source should open an internet browser window and manually type in the site's web address to make sure the emailed link is not maliciously redirecting to a dangerous site.

This advice is especially critical for protecting online banking accounts belonging to your organization. Criminals commonly target business banking accounts more than any other sector. If you believe sensitive information has been revealed, make sure to do the following:

- Report it to the appropriate people within your organization.

- Contact your organization's financial institution and close any accounts that may have been compromised (if you believe financial data is at risk).

- Change any passwords you may have revealed, and if you used the same password for multiple resources, make sure to change it for each account.

3 Don't Fall for Fake Anti-virus Offers

Fake anti-virus, "scareware" and other rogue online security scams have been behind some of the most successful online frauds. Make sure your organization has a policy in place explaining what the procedure is if an employee's computer becomes infected by a virus.

Train your employees to recognize a legitimate warning message (using a test file from eicar.org, for example) and to properly notify your IT team if something bad or questionable has happened.

If possible, configure your computers to prohibit regular users from having administrative access. This will minimize the risk of them installing malicious software and help them remember that adding unauthorized software to work computers is against policy.

4 Protect Against Malware

Businesses can experience a compromise through the introduction of malicious software, or malware. Malware can make its way onto machines from the internet, downloads, attachments, email, social media and other platforms. One specific malware to be aware of is key logging, which is malware that tracks a user's keyboard strokes.

Once installed, key logging malware can record keystrokes made on a computer, allowing hackers or thieves to see passwords, credit card numbers and other confidential data. Keeping security software up to date and patching your computers regularly will make it more difficult for this type of malware to infiltrate your network.

5 Guard Against Malicious Software

Despite progress in creating more awareness of security threats on the internet, malware authors are not giving up. Effective protection against viruses, Trojans and other malicious software requires a layered approach to your defenses. Anti-virus software is a must, but should not be your only line of defense. Instead, deploy a combination of techniques to keep your workplace safe.

Also, be careful with the use of thumb drives and other removable media. These media could have malicious software pre-installed that can infect your computer, so make sure you trust the source of the removable media devices before you use them.

Combining the use of web filtering, anti-virus signature protection, proactive malware protection, firewalls, strong security policies and employee training significantly lowers the risk of infection. Keeping protection software up to date along with your operating system and applications increases the safety of your systems.

6 Be Aware of Spyware and Adware

Spyware and adware, when installed, will send pop-up ads, redirect you to certain websites and monitor websites that you visit. Extreme versions can even track what keys are typed. Spyware can cause your computer to become slow and also leaves you susceptible to data theft. If you are subject to endless pop-up windows or are regularly redirected to websites other than what you type in your browser, your computer is likely infected with spyware.

To remove spyware, run a full scan of your computer with anti-virus software and, if necessary, run a legitimate product specifically designed to remove spyware. To avoid being infected with spyware, limit cookies on your browser preferences, never click on links within pop-up windows and be wary of free downloadable software from disreputable or unrecognized sources.

7 Verify the Identity of Information Seekers

Ensure that you train employees to never disclose customer information, usernames, passwords or other sensitive details to incoming callers. When someone requests information, always contact the person back using a known phone number or email account to verify the identity and validity of the individual and his or her request.

Network Security

Securing your company's network consists of the following three key elements:

1 Identifying all devices and connections on the network

2 Setting boundaries between your company's systems and others

3 Enforcing controls to ensure that unauthorized access, misuse or denial-of-service events can be prevented or rapidly contained and recovered from if they do occur

Action Items

1 Secure Internal Network and Cloud Services

Your company's network should be separated from the public internet by strong user authentication mechanisms and policy enforcement systems such as firewalls and web filtering proxies. Additional monitoring and security solutions, such as anti-virus software and intrusion detection systems, should also be employed to identify and stop malicious code or unauthorized access attempts.

- Internal network—After identifying the boundary points on your company's network, each boundary should be evaluated to determine what types of security controls are necessary and how they can be best deployed. Keep the following in mind:

   o Border routers should be configured to only route traffic to and from your company's public IP addresses.

   o Firewalls should be deployed to restrict traffic only to and from the minimum set of necessary services.

   o Intrusion prevention systems should be configured to monitor for suspicious activity crossing your network perimeter.

   In order to prevent bottlenecks, all security systems you deploy to your company's network perimeter should be capable of handling the bandwidth that your carrier provides.

- **Cloud-based services**—Carefully consult your terms of service with all cloud service providers to ensure that your company's information and activities are protected with the same degree of security you would intend to provide on your own. Request security and auditing from your cloud service providers as applicable to your company's needs and concerns.

  o Review and understand service level agreements for system restoration and rebuild time.

  You should also inquire about additional services a cloud service can provide. These services may include backup and restore services and encryption services, which can be very attractive to businesses.

2 Develop Strong Password Policies

Generally speaking, two-factor authentication methods, which require two types of evidence that you are who you claim to be, are safer than using just static passwords for authentication. One common example is a personal security token that displays changing passcodes to be used in conjunction with an established password. However, two-factor systems may not always be possible or practical for your company.

Password policies should encourage your employees to employ the strongest passwords possible without creating the need or temptation to reuse passwords or write them down. That means using passwords that are complex, long (at least 10 characters) and that are closely guarded by those who know them.

3 Secure and Encrypt Your Company's Wi-Fi

Your company may choose to operate a wireless local area network (WLAN) for the use of customers, guests and visitors. If so, it is important that such a WLAN be kept separate from the main company network so that traffic from the public network cannot cross the company's internal systems at any point.

Internal, nonpublic WLAN access should be restricted to specific devices and specific users to the greatest extent possible while still meeting your company's business needs. Where the internal WLAN has less stringent access controls than your company's wired network, dual connections—where a device is able to connect to both the wireless and wired networks simultaneously—should be prohibited by technical controls on each such capable device (e.g., basic input-output system (BIOS)-level LAN/WLAN switch settings). All users should be given unique credentials with preset expiration dates to use when accessing the internal WLAN.

Additionally, due to demonstrable security flaws known to exist in older forms of wireless encryption, your company's internal WLAN should only employ Wi-Fi Protected Access 2 (WPA2) encryption.

4 Encrypt Sensitive Company Data

Encryption should be employed to protect any data that your company considers sensitive, in addition to meeting applicable regulatory requirements on information safeguarding. Different encryption schemes are appropriate under different circumstances. However, applications that comply with the OpenPGP standard provide a wide range of options for securing data on disk as well as in transit. If you choose to offer secure transactions on your company's website, consult with your service provider about available options for a secure sockets layer (SSL) certificate for your site.

5 Regularly Update All Applications

All systems and software, including networking equipment, should be updated in a timely fashion as patches and firmware upgrades become available. Use automatic updating services whenever possible, especially for security systems such as anti-malware applications, web filtering tools and intrusion prevention systems.

6 Set Safe Web Browsing Rules

Your company's internal network should only be able to access those services and resources on the internet that are essential to the business and the needs of your employees. Use the safe browsing features included with modern web browsing software and a web proxy to ensure that malicious or unauthorized sites cannot be accessed from your internal network.

7 Make Sure Remote Access is Secure, if Enabled

If your company needs to provide remote access to your internal network over the internet, one popular and secure option is to employ a secure virtual private network (VPN) system accompanied by strong two-factor authentication, using either hardware or software tokens.

8 Create a Safe-use Flash Drive Policy

Ensure employees never put any unknown flash drive or USB into their computers. Businesses should set a clear policy so employees know they should never open a file from a flash drive they are not familiar with, and that they should hold down the Shift key when inserting the flash drive to block malware. By doing so, you can stop the flash drive from automatically running.

Website Security

Website security is more important than ever. Web servers, which host the data and other content available to your customers on the internet, are often the most targeted and attacked components of a company's network. Cyber criminals are constantly looking for improperly secured websites to attack, while many customers say website security is a top consideration when they choose to shop online.

As a result, it is essential to secure servers and the network infrastructure that supports them. The consequences of a security breach are great, including loss of revenue, damage to credibility, legal liability and loss of customer trust.

The following are examples of specific security threats to servers:

- Cyber criminals may exploit software bugs in the server, underlying operating system or active content to gain unauthorized access to the server. Examples of unauthorized access include gaining access to files or folders that were not meant to be publicly accessible and being able to execute commands and install malicious software on the web server.

- Denial-of-service attacks may be directed at the server or its supporting network infrastructure to prevent or hinder your website users from making use of its services. These attacks can prevent a user from accessing email, websites, online accounts or other services.

- Sensitive information on the server may be read or modified without authorization.

- Sensitive information on back-end databases that are used to support interactive elements of a web application may be compromised through the injection of unauthorized software commands. Examples include structured query language (SQL) injection, lightweight directory access protocol (LDAP) injection and cross-site scripting (XSS).

- Sensitive unencrypted information transmitted between the web server and the browser may be intercepted.

- Information on the server may be changed for malicious purposes. Website defacement is a commonly reported example of this threat.

- Cyber criminals may gain unauthorized access to resources elsewhere in the organization's network with a successful attack on the server.

- Cyber criminals may also attack external entities after compromising a server. These attacks can be launched directly (e.g., from the compromised server against an external server) or indirectly (e.g., placing malicious content on the compromised web server that attempts to exploit vulnerabilities in the browsers of users visiting the site).

- The server may be used as a distribution point for attack tools, pornography or illegally copied software.

Action Items

1 | Address the Security Aspects of a Public Server

Because it is much more difficult to address security once deployment and implementation have occurred, security should be considered during the initial planning stage. Businesses are more likely to make decisions about configuring computers appropriately and consistently when they develop and use a detailed, well-designed deployment plan. Developing such a plan will support web server administrators in making the inevitable trade-off decisions between usability, performance and risk.

Businesses also need to consider the HR requirements for the deployment and continued operation of the web server and supporting infrastructure. The following points should be in a deployment plan:

- Types of personnel required—for example, system and web server administrators, webmasters, network administrators and information systems security personnel

- Skills and training required by assigned personnel

- Individual (i.e., the level of effort required of specific personnel types) and collective staffing (i.e., overall level of effort) requirements

2 | Implement Security Practices and Controls

Appropriate management practices are essential to operating and maintaining a secure web server. Security practices include the identification of your company's information system assets and the development, documentation and implementation of policies, as well as guidelines to help ensure the confidentiality, integrity and availability of information system resources. The following practices and controls are recommended:

- A companywide information system security policy

- Server configuration, change control and management

- Risk assessment and management

- Standardized software configurations that satisfy the information system security policy

- Security awareness and training

- Contingency planning, continuity of operations and disaster recovery planning

- Certification and accreditation

3 Ensure Operating Systems Meet Security Requirements

The first step in securing a web server is securing the underlying operating system. Most web servers operate on a general-purpose operating system. Many security issues can be avoided if the operating systems underlying web servers are configured appropriately. Default hardware and software configurations are typically set by manufacturers to emphasize features, functions and ease of use at the expense of security.

Because manufacturers are not aware of each organization's security needs, each web server administrator must configure new servers to reflect their business's security requirements and reconfigure them as those requirements change.

Using security configuration guides or checklists can assist administrators in securing systems consistently and efficiently. Initially securing an operating system generally includes the following steps:

- Patch and upgrade the operating system.

- Change all default passwords.

- Remove or disable unnecessary services and applications.

- Configure operating system user authentication.

- Configure resource controls.

- Install and configure additional security controls.

- Perform security testing of the operating system.

4 Ensure the Server Meets Security Requirements

In many respects, the secure installation and configuration of the web server application will mirror the operating system process discussed above. The overarching principle is to install the minimal amount of web server services required and eliminate any known vulnerabilities through patches or upgrades. If the

installation program installs any unnecessary applications, services or scripts, they should be removed immediately after the installation process concludes.

Securing the web server application generally includes the following steps:

- Patch and upgrade the web server application.

- Remove or disable unnecessary services, applications and sample content.

- Configure web server user authentication and access controls.

- Configure web server resource controls.

- Test the security of the web server application and web content.

5 Ensure that Only Appropriate Content is Published

Company websites are often one of the first places cyber criminals search for valuable information. Still, many businesses lack a web publishing process or policy that determines what type of information to publish openly, what information to publish with restricted access and what information should not be published to any publicly accessible repository.

Some generally accepted examples of what should not be published or what should at least be carefully examined and reviewed before being published on a public website include the following:

- Classified or proprietary business information

- Sensitive information relating to your business's security

- Medical records

- A business's detailed physical and information security safeguards

- Details about a business's network and information system infrastructure—for example, address ranges, naming conventions and access numbers

- Information that specifies or implies physical security vulnerabilities

- Detailed plans, maps, diagrams, aerial photographs and architectural drawings of business buildings, properties or installations

- Any sensitive information about individuals that might be subject to federal, state or, in some instances, international privacy laws

> ### Consider the risks before using active content.
>
> Static information resided on the servers of most early websites, typically in the form of text-based documents. Soon thereafter, interactive elements were introduced to offer new opportunities for user interaction. Unfortunately, these same interactive elements introduced new web-related vulnerabilities. Different active content technologies pose different vulnerabilities and their risks should be weighed against their benefits.

6 Take the Proper Steps to Protect Web Content

Although information available on public websites is intended to be public (assuming a credible review process and policy is in place), it is still important to ensure that information cannot be modified without authorization. Users of such information rely on its integrity even if the information is not confidential.

Content on publicly accessible web servers is inherently more vulnerable than information that is inaccessible from the internet, and this vulnerability means businesses need to protect public web content through the appropriate configuration of web server resource controls. Examples of resource control practices include the following:

- Install or enable only necessary services.

- Install web content on a dedicated hard drive or logical partition.

- Limit uploads to directories that are not readable by the web server.

- Define a single directory for all external scripts or programs executed as part of web content.

- Disable the use of hard or symbolic links.

- Define a complete web content access matrix identifying which folders and files in the web server document directory are restricted and which are accessible, and by whom.

- Disable directory listings.

- Deploy user authentication to identify approved users, digital signatures and other cryptographic mechanisms as appropriate.

- Use intrusion detection systems, intrusion prevention systems and file integrity checkers to spot intrusions and verify web content.

- Protect each back-end server (e.g., database server or directory server) from command injection attacks.

In addition, the network infrastructure (e.g., firewalls, routers and intrusion detection systems) that supports the web server plays a critical security role. In most configurations, the network infrastructure will be the first line of defense between a public web server and the internet. Network design alone, though, cannot protect a web server.

The frequency, sophistication and variety of web server attacks perpetrated today support the idea that web server security must be implemented through layered and diverse protection mechanisms, an approach sometimes referred to as "defense in depth."

7 Use Proper Technologies to Protect Sensitive Data

Public web servers often support technologies for identifying and authenticating users with differing privileges for accessing information. Some of these technologies are based on cryptographic functions that can provide a secure channel between a web browser client and a web server that supports encryption. Web servers may be configured to use different cryptographic algorithms, providing varying levels of security and performance.

Without proper user authentication in place, businesses cannot selectively restrict access to specific information. All information that resides on a public web server is then accessible by anyone with access to the server. In addition, without some process to authenticate the server, users of the public web server will not be able to determine whether the server is the authentic web server or a counterfeit version operated by a cyber criminal.

Even with an encrypted channel and an authentication mechanism, it is possible that attackers may attempt to access the site by brute force. Improper authentication techniques can allow attackers to gather valid usernames and potentially gain access to the website. Strong authentication mechanisms can also protect against phishing attacks, in which hackers may trick users into providing their personal credentials, and pharming, in which traffic to a legitimate website may be redirected to an illegitimate one. An appropriate level of authentication should be implemented based on the sensitivity of the web server's users and content.

8 Commit to Maintaining Web Server Security

Maintaining a secure web server requires constant effort, resources and vigilance. Securely administering a web server on a daily basis is essential. Maintaining the security of a web server will usually involve the following steps:

- Configuring, protecting and analyzing log files

- Backing up critical information frequently

- Maintaining a protected authoritative copy of your organization's web content

- Establishing and following procedures for recovering from compromise

- Testing and applying patches in a timely manner

- Testing security periodically

Email

Email has become a critical part of our everyday business, from internal management to direct customer support. The benefits associated with email as a primary business tool far outweigh the negatives. However, businesses must be mindful that a successful email platform starts with basic principles of email security to ensure the privacy and protection of customer and business information.

Action Items

1 Set Up a Spam Email Filter

Email is the primary method for spreading viruses and malware, and it is one of the easiest to defend against. Consider using email-filtering services that your email service, hosting provider or other cloud providers offer. A local email filter application is also an important component of a solid anti-virus strategy. Ensure that automatic updates are enabled on your email application, email filter and anti-virus programs. Ensure that filters are reviewed regularly so that important emails and domains are not blocked in error.

2 Train Employees How to Responsibly Use Email

Employees must be trained to identify risks associated with email use, how and when to use email appropriate to their work, and when to seek professional assistance. Employee awareness training is available in many forms, including printed media, videos and online training.

Consider requiring security awareness training for all new employees and refresher courses every year. Simple efforts create a work environment that is educated in protecting your business and can include monthly newsletters, urgent bulletins when new viruses are detected and even posters in common areas to remind your employees of key security and privacy to-do's.

3 Protect Sensitive Information Sent Over Email

Since email in its native form is not designed to be secure, incidents of misaddressing or other common accidental forwarding can lead to data leakage. Businesses that handle this type of information should consider whether such information should be sent via email, or at least consider using email encryption.

Encryption is the process of converting data into unreadable format to prevent disclosure to unauthorized personnel. Only individuals or organizations with access to the encryption key can read the information. Other cloud services offer secure web-enabled drop boxes that allow for secure data transfer for sensitive information, which is often a better approach to transmitting between companies or customers.

4 Create an Email Retention Policy

Another important consideration is the management of email that resides on company messaging systems and your users' computers. From the cost of storage and backup to legal and regulatory requirements, companies should document how they will handle email retention and implement basic controls to help them attain those standards. Many industries have specific rules that dictate how long emails can or should be retained, but the basic rule of thumb is only as long as it supports your business efforts. Many companies implement a 60-90 day retention standard if not compelled by law to use another retention period.

To ensure compliance, companies should consider mandatory archiving at a chosen retention cycle end date and automatic permanent email removal after another set point, such as 180-360 days in archives. In addition, organizations should discourage the use of personal folders on employee computers (most often configurable from the email system level), as this will make it more difficult to manage company standards.

5 Develop an Email Usage Policy

Policies are important for setting expectations with your employees or users, and for developing standards to ensure adherence to your published polices. Your policies should be easy to read, understand, define and enforce. Key areas to address include what the company email system should and should not be used for, and what data is allowed to be transmitted. Other policy areas should address retention, privacy and acceptable use.

Depending on your business and jurisdiction, you may have a need for email monitoring. The rights of the business and the user should be documented in the policy as well. The policy should be part of your general end-user awareness training and reviewed for updates on a yearly basis.

Mobile Devices

If your company uses mobile devices to conduct company business, such as accessing company email or sensitive data, pay close attention to mobile security and the potential threats that can expose and compromise your business networks.

Many organizations are finding that employees are most productive when using mobile devices, and the benefits are too great to ignore. While mobility can increase workplace productivity, allowing employees to bring their own mobile devices into the enterprise can create significant security and management challenges.

Data loss and data breaches caused by lost or stolen phones create big challenges, as mobile devices are now used to store confidential business information and access the corporate network.

Top Threats Targeting Mobile Devices

Data loss—An employee or hacker accesses sensitive information from a device or network. This can be unintentional or malicious, and is considered the biggest threat to mobile devices.

Social engineering attacks—A cyber criminal attempts to trick users into disclosing sensitive information or installing malware. Methods include phishing and targeted attacks.

Malware—Malicious software that includes traditional computer viruses, computer worms and Trojan horse programs. Specific examples include the Ikee worm, targeting iOS-based devices, and Pjapps malware that can enroll infected Android devices in a collection of hacker-controlled "zombie" devices known as a "botnet."

Data integrity threats—Attempts to corrupt or modify data in order to disrupt operations of a business for financial gain. These can also occur unintentionally.

Resource abuse—Attempts to misuse network, device or identity resources. Examples include sending spam from compromised devices or denial-of-service attacks using computing resources of compromised devices.

Web- and network-based attacks—Launched by malicious websites or compromised legitimate sites, these target a device's browser and attempt to install malware or steal confidential data.

Action Items

A few simple steps can help ensure company information is protected. These include requiring all mobile devices that connect to the business network be equipped with security software and password protection, and providing general security training to make employees aware of the importance of security practices for mobile devices.

1. Use Security Software on All Smartphones

Security software specifically designed for smartphones can stop hackers and prevent cyber criminals from stealing your information or spying on you when you use public networks. This software can detect and remove viruses and other mobile threats before they cause you problems. It can also eliminate annoying text and multimedia spam messages.

2. Make Sure All Software is Up to Date

Mobile devices must be treated like personal computers in that all software on the devices should be kept up to date, especially the security software. This will protect devices from new variants of malware and viruses that threaten your company's critical information.

3. Encrypt the Data on Mobile Devices

Business and personal information stored on mobile devices is often sensitive. Encrypting this data is another must. If a device is lost and the SIM card is stolen, the thief will not be able to access the data if the proper encryption technology is loaded on the device.

4. Have Users Password-protect Mobile Devices

In addition to encryption and security updates, it is important to use strong passwords to protect data stored on mobile devices. This will go a long way toward keeping a thief from accessing sensitive data if the device is lost or hacked.

5 Urge Users to Be Aware of Their Surroundings

Whether entering passwords or viewing sensitive or confidential data, users should be cautious of who might be looking over their shoulders.

6 Employ Safe Strategies for Communicating

Consider the following:

- Avoid opening unexpected text messages from unknown senders. As with email, attackers can use text messages to spread malware, phishing scams and other threats among mobile device users.

- Don't be lured in by spammers and phishers. To shield business networks from cyber criminals, businesses should deploy appropriate email security solutions, including spam prevention, which protects a company's reputation and manages risks.

- Click with caution. Just like on stationary computers, social networking on mobile devices and laptops should be conducted with care and caution. Users should not open unidentified links, chat with unknown people or visit unfamiliar sites. It doesn't take much for a user to be tricked into compromising a device and the information on it.

7 Set Reporting Procedures for Lost or Stolen Equipment

In the case of a loss or theft, employees and management should all know what to do next. Processes to deactivate the device and protect its information from intrusion should be in place. Products are also available for the automation of such processes, allowing businesses to breathe easier after such incidents.

8 Ensure Devices Are Wiped Clean Prior to Disposal

Most mobile devices have a reset function that allows all data to be wiped. SIM cards should also be removed and destroyed.

Cyber Security and Employees

The first line of defense against cyber threats is a well-trained workforce. Security awareness training teaches employees to understand system vulnerabilities and threats to business operations that are present when using a computer on a business network.

Security Training

A strong IT security program must include training IT users on security policies, procedures and techniques, as well as the various management, operational, and technical controls necessary and available to keep IT resources secure. In addition, IT infrastructure managers must have the skills necessary to carry out their assigned duties effectively. Failure to give attention to the area of security training puts a company at great risk because security of business resources is as much a human issue as it is a technology issue.

Technology users are the largest audience in any organization and are the single most important group of people who can help to reduce unintentional errors and IT vulnerabilities. Users may include employees, contractors, foreign or domestic guest researchers, other personnel, visitors, guests, and other collaborators or associates requiring access. Users must do the following:

- Understand and comply with security policies and procedures.

- Be appropriately trained in the rules of behavior for the systems and applications to which they have access.

- Work with management to meet training needs.

- Keep software and applications updated with security patches.

- Be aware of actions they can take to better protect company information. These actions include proper password usage, data backup, proper anti-virus protection, reporting any suspected incidents or violations of security policy, and following rules established to avoid social engineering attacks and deter the spread of spam, viruses and worms.

A clear categorization of what is considered sensitive data versus nonsensitive data is also needed. Typically, the following data is considered sensitive information that should be handled with care:

- Government-issued identification numbers (e.g., Social Security numbers and driver's license numbers)

- Financial account information (e.g., bank account numbers and credit card numbers)

- Medical records

- Health insurance information

- Salary information

- Passwords

The training should cover security policies for all means of access and transmission methods, including secure databases, email, file transfer, encrypted electronic media and hard copies.

Employers should constantly emphasize the critical nature of data security. Regularly scheduled refresher training courses should be established in order to instill the data security culture of your organization. Additionally, distribute data privacy- and security-related news articles in your training, and send companywide communication on notable data privacy-related news as reminders to your employees.

Access Controls

Both client data and internal company data are considered confidential and need particular care when viewed, stored, used, transmitted or disposed. It is important to analyze the role of each employee and set data access control based upon those roles. If a role does not require the employee to ever use sensitive data, the employee's access to the data should be strictly prohibited.

However, if the role requires the employee to work with sensitive data, the level of access must be analyzed thoroughly and be assigned in a controlled and tiered manner following "least-privilege" principles, which allow the employee to access only data that is necessary to perform his or her job.

If your organization does not have a system in place to control data access, the following precautions are strongly recommended. Every employee should remember the following:

- Never access or view client data without a valid business reason. Access should be on a need-to-know basis.

- Never provide confidential data to anyone—client representatives, business partners or even other employees—unless the employee is sure of the identity and authority of that person.

- Never use client data for development, testing, training presentations or any purpose other than providing production service, client-specific testing or production diagnostics. Only properly sanitized data that cannot be traced to a client, client employee, customer or your organization's employee should be used for such purposes.

- Always use secure transmission methods such as secure email, secure file transfer (from application to application) and encrypted electronic media (e.g., CDs, USB drives or tapes).

- Always keep confidential data (hard copy and electronic) only as long as it is needed.

- Follow a "clean desk" policy, keeping workspaces uncluttered and securing sensitive documents so that confidential information does not get into the wrong hands.

- Always use only approved document disposal services or shred all hard copy documents containing confidential information when finished using them. Similarly, use only approved methods that fully remove all data when disposing of, sending out for repair or preparing to reuse electronic media.

Employee Departure Checklist

Create a security checkout checklist for employees who are leaving your company, regardless of their reason for leaving (voluntary or involuntary). Terminated employee accounts should be erased on all network devices and drives immediately. This is especially true for any devices that may have been taken off-site, such as laptops and smartphones.

Facility Security

Protecting employees and members of the public who visit your facility is a complex and challenging responsibility. It's also one of your company's top priorities.

The Importance of Securing Your Company's Facilities

The physical security of a facility depends on a number of security decisions that can be identified through a comprehensive risk management process. The objective of risk management is to identify an achievable level of protection for your company that corresponds as closely as possible to the level of risk without exceeding the risk.

It is easy to think about physical security of your company's facility as merely an exercise in maintaining control of access points and ensuring there is complete visibility in areas that are determined to be high-risk—either because of the threat of easy public access or because of the value of information located nearby. However, maintaining facility security also includes the physical environment of public spaces. For instance:

- Employees whose computers have access to sensitive information should not have their computer monitors oriented toward publicly accessible spaces, such as reception areas, check-in desks and waiting rooms. Employees should be trained to not write out logon information on small pieces of paper affixed to computer equipment viewable in public spaces.

- Easy-to-grab equipment that could contain sensitive or personally identifiable information, such as laptops, electronic tablets and cellphones, should be located away from public areas. If you have an environment where employees are working in a waiting room or reception area, train them to not leave these types of devices out on their desks unsecured.

- Consider using cable locks as an easy way to increase security for laptop computers. Most laptops feature a lock port for a cable, which can be connected to the user's desk. Be sure to store the key to the cable lock in a secure location away from the desk the computer is locked to.

- In cases that extremely sensitive information is stored on a laptop, consider installing tracking software. Most tracking software programs run unnoticed and allow stolen computers to be located more easily. Many also allow administrators to wipe the hard drive remotely if necessary.

- Consider implementing a badge identification system for all employees, and train employees to stop and question anyone in the operational business area without a badge or who appears to be an unescorted visitor.

Action Items

1 Safeguard Materials with Sensitive Information

Probably the most effective way to minimize the risk of losing control of sensitive information from printed materials is to minimize the amount of printed materials that contain sensitive information. Management procedures should limit the number of copies of printed reports, memoranda and other material containing PII.

Safeguard copies of material containing sensitive information by providing employees with locking file cabinets or safes. Make it a standard operating procedure to lock up important information. Train employees to understand that simply leaving the wrong printed material on a desk, in view of the general public, can result in consequences that impact the entire company and your customers.

2 Ensure Mail Security

Your mail center can introduce a wide range of potential threats to your business. Your center's screening and handling processes must be able to identify threats and hoaxes and eliminate or mitigate the risk they pose to facilities, employees and daily operations. Your company should ensure that mail managers understand the range of screening procedures and evaluate them in terms of your specific operational requirements.

3 Dispose of Trash Securely

Too often, sensitive information, including customers' PII, company financial data and system access information, is available for anyone to find in the trash. Invest in business-grade shredders and buy enough of them to make it convenient for employees. Alternatively, subscribe to a trusted shredding company that will provide locked containers for storage until documents are shredded. Develop standard procedures and employee training programs to ensure that everyone in your company is aware of what types of information need to be shredded.

4 Dispose of Electronic Equipment Securely

Be aware that emptying the recycle bin on your desktop or deleting documents from folders on your computer or other electronic device may not delete information forever. Those with advanced computer skills can still access your information even after you think you've destroyed it.

Disposing of electronic equipment requires skilled specialists in order to ensure the security of sensitive information contained within that equipment. If outside help, such as an experienced electronic equipment recycler and data security vendor, is not available or too expensive, you should, at a minimum, remove computer hard drives and have them shredded. Also, be mindful of risks with other types of equipment associated with computer equipment, including thumb drives.

5 Train Your Employees in Facility Security Procedures

A security breach of customer information or a breach of internal company information can result in a public loss of confidence in your company and can be as devastating for your business as a natural disaster. In order to address such risks, you must devote your time, attention and resources (including employee training time) to the potential vulnerabilities in your business environment and the procedures and practices that must be a standard part of each employee's workday.

And while formal training is important for maintaining security, the daily procedures you establish both in how you normally conduct business and in the way you model good security behaviors and practices are equally important. In short, security training should be stressed as critical and reinforced through daily procedures and leadership modeling.

Incident Response

Even well-implemented cyber security structures and plans may not prevent all breaches, so be sure to have procedures in place to respond to security breaches when they occur.

Types of breaches

Physical breaches—Real-world crimes such as burglaries and equipment theft, as well as any time your company's equipment is misplaced or lost in transit. Unauthorized devices may be installed on a system or network, permitting further compromises of data confidentiality and integrity. Physical breaches can also result from reselling, donating or recycling old equipment that has not been properly cleansed of potentially sensitive information.

Network and system security breaches—When computers become infected with malicious code, are accessed by unauthorized individuals remotely or are used by authorized individuals to perform malicious activity. This can also include breaches to network routers and firewalls, both within and outside your organization's boundary and control.

Data breaches—The leakage or spillage of sensitive information into insecure channels that can result from any of the types of events described above. Data breaches can also occur if sensitive information is left improperly exposed by mistake.

Breach Action Items

1 Notify Law Enforcement and Customers, if Necessary

Depending on the type of breach and your business, your company may be required to notify local law enforcement or other government authorities upon discovery of a data breach. In the event of exposure of customer information, you should notify the customers of the incident, record the data that was lost or exposed, and record the measures taken to prevent future exposure.

2 Work Cohesively Across Teams to Limit the Damage

Once your company becomes aware that a breach has occurred, technical personnel and business decision-makers should work together to decide on the most practical and effective containment plan. Containment plans will vary from one set of circumstances to the next, and they may quickly become intensive in terms of time and resources from both the technological and business impact perspectives. In any case, the containment of data breaches should be focused on determining the extent of the compromise and preserving the confidentiality and integrity of sensitive data that has not yet been stolen or disclosed.

Other issues affecting the selection and execution of a containment plan include your company's strategy for reputation risk management and your decision on whether to request outside assistance—either from local or federal law enforcement, a private consulting firm or a computer incident response organization such as US-CERT.

3 Begin Recovery Efforts

After a containment plan has been established and execution has begun, get started on eradication and recovery efforts. In the case of network and system security breaches, eradication usually means removing all instances of unauthorized software from the network and disabling all access privileges associated with users who have committed malicious activity.

Cleaning a network or system of all traces of malicious code can often entail having to completely wipe all storage media and perform a "clean install." Therefore, recovery from such a breach may be resource-intensive and require careful restoration of data from backups. Bear in mind that backups may also contain malicious code and should be carefully checked for compromise; otherwise, the security breach will be perpetuated after the recovery phase.

Key Disaster Recovery Principles

✓ **Don't wait until it's too late**—Businesses should not wait until after a disaster to think about what should have been done to protect their data. Not only is downtime costly from a financial perspective, but it could also mean the complete demise of the business.

✓ **Protect information completely**—To reduce the risk of losing critical business information, businesses must implement appropriate security and backup solutions to archive important files, such as customer records and financial information for the long term. Natural disasters, theft and cyber attacks can all result in data and financial loss, so businesses need to make sure important files are saved not only on an external hard drive or company network, but also in a safe, off-site location.

✓ **Get employees involved**—Employees play a key role in helping to prevent downtime. They should be educated on computer security best practices and what to do if information is accidentally deleted or cannot easily be found in their files.

✓ **Test frequently**—After a disaster hits is the worst time to learn that critical files were not backed up as planned. Regular disaster recovery testing is invaluable. Test your plan anytime anything changes in your environment.

✓ **Review your plan**—If frequent testing is not feasible due to resources and bandwidth, businesses should at least review their disaster preparedness plans on a quarterly basis.

✓ **Be prepared**—It is always better and less costly to invest in adequate security upfront rather than going through a costly incident response that could result in rebuilding your entire network infrastructure.

4 Hold a Debriefing Meeting

Your company should always perform a "lessons learned" meeting after the recovery phase has been successfully completed to discover, document and refine the knowledge gained during the incident handling process.

Policy Development and Management

All companies should develop and maintain clear and robust policies for safeguarding critical business data and sensitive information, protecting their reputation and discouraging inappropriate behavior by employees.

Many of these types of policies already exist for real-world situations, but may need to be tailored to your organization and updated to reflect the increasing impact of cyber space on everyday transactions, both professional and personal. As with any other business document, cyber security policies should follow good design and governance practices. Policies should be concise, clear and reviewed regularly to ensure that they stay pertinent as your business's needs change.

Action Items

1 Establish Security Roles and Responsibilities

One of the most effective and least expensive means of preventing serious cyber security incidents is to establish a policy that clearly defines the separation of roles and responsibilities with regard to systems and the information they contain. Many systems are designed to provide for strong role-based access control, but this tool is of little use without well-defined procedures and policies to govern the assignment of roles and their associated constraints. At a minimum, such policies need to clearly identify company data ownership and employee roles for security oversight and their inherent privileges.

Depending on the types of data regularly handled by your business, it may also make sense to create separate policies governing who is responsible for certain types of data. For example, a business that handles large volumes of PII from its customers may benefit from identifying a chief steward for customers' privacy information. The steward could serve not only as a subject matter expert on all matters of privacy, but also be a champion for process and technical improvements for PII handling.

2 Establish an Employee Internet Usage Policy

The limits on employee internet usage in the workplace vary widely from business to business. Your guidelines should allow employees the maximum degree of freedom they require to be productive (short breaks to surf the web or perform personal tasks online have been shown to increase productivity). At the same time, rules of behavior are necessary to ensure that all employees are aware of boundaries, both to keep them safe and to keep your company successful. Consider the following:

- Personal breaks to surf the web should be limited to a reasonable amount of time and to certain types of activities.

- If you use a web filtering system, employees should have clear knowledge of how and why their web activities will be monitored, and what types of sites are deemed unacceptable by your policy.

- Workplace rules of behavior should be clear, concise and easy to follow. Employees should feel comfortable performing both personal and professional tasks online without making judgment calls as to what may or may not be deemed appropriate. Businesses may want to include a splash warning upon network sign-on that advises the employees of the businesses' internet usage policies so that all employees are on notice.

3 Establish a Social Media Policy

Social networking applications present a number of risks that are difficult to address using technical or procedural solutions. A strong social media policy is crucial for any business that seeks to use social networking to promote its activities and communicate with its customers. At a minimum, a social media policy should clearly include the following:

- Specific guidance on when to disclose company activities using social media and what kinds of details can be discussed in a public forum

- Additional rules of behavior for employees using personal social networking accounts to make clear what kinds of discussion topics or posts could cause risk for the company

- Guidance on the acceptability of using a company email address to register for, or get notices from, social media sites

- Guidance on selecting long and strong passwords for social networking accounts, since some social media sites do not enforce strong authentication policies for users

All users of social media need to be aware of the risks associated with social networking tools and the types of data that can be automatically disclosed online when using social media. Taking the time to educate your employees on the potential pitfalls of social media use, especially in tandem with geolocation services, may be the most beneficial social networking security practice of all.

4 Identify Potential Reputation Risks

All organizations should take the time to identify potential risks to their reputation and develop a strategy to mitigate those risks via policies or other measures as available. Specific types of reputation risks include the following:

- Being impersonated online by a criminal organization

- Having sensitive company or customer information leaked to the public via the web

- Having sensitive or inappropriate employee actions made public via the web or social media sites

All businesses should set a policy for managing these types of risks and plan to address such incidents if and when they occur. Such a policy should cover a regular process for identifying potential risks to the company's reputation in cyber space, practical measures to prevent those risks from materializing and reference plans to respond and recover from incidents as soon as they occur.

Summary

A data breach could cripple your business, costing you thousands or millions of dollars in lost sales and damages. Contact Troy Benefits Consulting today. We have the tools necessary to ensure you have the proper coverage to protect your company against losses from cyber attacks.

Cyber Security Glossary

Adware: Any software application that displays advertising banners while the program is running. Adware often includes code that tracks a user's personal information and passes it on to third parties without the user's authorization or knowledge. If you gather enough of it, adware slows down your computer significantly. Over time, performance can be so degraded that you may have trouble working productively. See also **spyware** and **malware**.

Anti-virus software: Software designed to detect and potentially eliminate viruses before they have a chance to wreak havoc within the system. Anti-virus software can also repair or quarantine files that have already been infected by virus activity. See also **virus** and **electronic infections**.

Application: Software that performs automated functions for a user, such as word processing, spreadsheets, graphics, presentations and databases—as opposed to operating system (OS) software.

Attachment: A file that has been added to an email—often an image or document. It could be something useful to you or something harmful to your computer. See also **virus**.

Authentication: Confirming the correctness of the claimed identity of an individual user, machine, software component or any other entity.

Authorization: The approval, permission or empowerment for someone or something to do something.

Back door: Hidden software or hardware mechanism used to circumvent security controls.

Backup: File copies that are saved as protection against loss, damage or unavailability of the primary data. Saving methods include high-capacity tape, separate disk subsystems or on the internet. Off-site backup storage is ideal, and should be sufficiently far away to reduce the risk of environmental damage, such as floods, which might destroy both the primary and the backup if kept nearby.

Badware: See **malware**, **adware** and **spyware**.

Bandwidth: The capacity of a communication channel to pass data such as a text, image, video or sound through the channel in a given amount of time. Usually expressed in bits per second.

Blacklisting software: A form of filtering that blocks only websites specified as harmful. Parents and employers sometimes use such software to prevent children and employees from visiting certain websites. You can add and remove sites from the "not permitted" list. This method of filtering allows for more full use of the internet, but is less efficient at preventing access to any harmful material that is not on the list. See also **whitelisting software**.

Blended threat: A computer network attack that seeks to maximize the severity of damage and speed of contagion by combining methods—for example, using characteristics of both viruses and worms. See also **electronic infection**.

Blog: Short for "web log," a blog is usually defined as an online diary or journal. It is usually updated frequently and offered in a dated log format with the most recent entry at the top of the page.

Broadband: General term used to refer to high-speed network connections such as cable modem and digital subscriber line (DSL). These types of "always on" internet connections are actually more susceptible to some security threats than computers that access the web via dial-up service.

Browser: A client software program that can retrieve and display information from servers on the World Wide Web. Often known as a "web browser" or "internet browser." Examples include Internet Explorer, Chrome, Safari and Firefox.

Brute force attack: An exhaustive password-cracking procedure that tries all possibilities, one by one. See also **dictionary attack** and **hybrid attack**.

Clear desk policy: A policy that directs all personnel to clear their desks at the end of each working day, and file everything appropriately. Desks should be cleared of all documents and papers, including the contents of the "in" and "out" trays—not simply for cleanliness, but also to ensure that sensitive papers and documents are not exposed to unauthorized persons outside of working hours.

Clear screen policy: A policy that directs all computer users to ensure that the contents of the screen are protected from prying eyes and opportunistic breaches of confidentially. Typically, the easiest means of compliance is to use a screen saver that engages either on request or after a specified short period of time. See also **shoulder surfing**.

Cookie: A small file that is downloaded by some websites to store a packet of information on your browser. Companies and organizations use cookies to remember your sign-in or registration identification, site preferences, pages viewed and online "shopping cart" so that the next time you visit a site, your stored information can automatically be pulled up for you. A cookie is convenient but also presents potential security issues. You can configure your browser to alert you whenever a cookie is being sent. You can refuse to accept all cookies or erase all cookies saved on your browser.

Cyber bullying: Sending or posting harmful, cruel, rude or threatening messages, or slanderous information, text or images using the internet or other digital communication devices.

Denial-of-service attack: The prevention of authorized access to a system resource or the delaying of system operations and functions. Often this involves a cyber criminal generating a large volume of data requests. See also **flooding**.

Dictionary attack: A password-cracking attack that tries all of the phrases or words in a dictionary. See also **brute force attack** and **hybrid attack**.

Digital certificate: The electronic equivalent of an ID card that establishes your credentials when doing business or other transactions on the web. It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

Domain hijacking: An attack in which an attacker takes over a domain by first blocking access to the domain's DNS server and then putting his or her own server up in its place.

Domain name system (DNS): The DNS is the way that internet domain names are located. A website's domain name is easier to remember than its internet protocol (IP) address.

Dumpster diving: Recovering files, letters, memos, photographs, IDs, passwords, checks, account statements, credit card offers and more from garbage cans and recycling bins. This information can then be used to commit identity theft.

Electronic infections: Often called viruses, these malicious programs and codes harm your computer and compromise your privacy. In addition to the traditional viruses, other common types include worms and Trojan horses. They sometimes work in tandem to do maximum damage. See also **blended threat**.

Encryption: A data security technique used to protect information from unauthorized inspection or alteration. Information is encoded so that it appears as a meaningless string of letters and symbols during delivery or transmission. Upon receipt, the information is decoded using an encryption key.

End-user license agreement (EULA): A contract between you and your software's vendor or developer. Many times, the EULA is presented as a dialog box that appears the first time you open the software and forces you to check "I accept" before you can proceed. Before accepting, though, read through it and make sure you understand and are comfortable with the terms of the agreement. If the software's EULA is hard to understand or you can't find it, beware!

Evil twins: A fake wireless internet hot spot that looks like a legitimate service. When victims connect to the wireless network, a hacker can launch a spying attack on their transactions on the internet, or just ask for credit card information in the standard pay-for-access deal. See also **man-in-the-middle attacks**.

File-sharing programs: Sometimes called peer-to-peer (P2P) programs, these allow many different users to access the same file at the same time. These programs are often used to illegally upload and download music and other software.

Firewall: A hardware or software link in a network that inspects all data packets coming and going from a computer, permitting only those that are authorized to reach the other side.

Flooding: An attack that attempts to cause a failure in the security of a computer by providing more input, such as a large volume of data requests, than it can properly process. See also **denial-of-service attack**.

Hacker: An individual who attempts to break into a computer without authorization.

HTTPS: When used in the first part of a URL (e.g., http://), this term specifies the use of hypertext transfer protocol (HTTP) enhanced by a security mechanism such as secure sockets layer (SSL). Always look for HTTPS on the checkout or order form page when shopping online or when logging into a site and providing your username and password.

Hybrid attack: Builds on other password-cracking attacks by adding numerals and symbols to dictionary words. See also **dictionary attack** and **brute force attack**.

Instant messaging (IM): A service that allows people to send and get messages almost instantly. To send messages using instant messaging, you need to download an instant messaging program and know the instant messaging address of another person who uses the same IM program. See also **spim**.

Internet protocol (IP) address: A computer's internetwork address, written as a series of four 8-bit numbers separated by periods, such as 123.45.678.990. Every website has an IP address, although finding a website is considerably easier to do when using its domain name instead. See also **domain name system (DNS)**.

Internet service provider (ISP): A company that provides internet access to customers.

Keystroke logger: A specific type of electronic infection that records victims' keystrokes and sends them to an attacker. This can be done with either hardware or software. See also **Trojan horse**.

Malware: A generic term for a number of different types of malicious code. See also **adware** and **spyware**.

Man-in-the-middle attack: Posing as an online bank or merchant, a cyber criminal allows a victim to sign in over a secure sockets layer (SSL) connection. The attacker then logs onto the real server using the client's information and steals credit card numbers.

Monitoring software: Software products that allow parents to monitor or track the websites or email messages that a child visits or reads. See also **blacklisting software** and **whitelisting software**.

Network: Two or more computer systems that are grouped together to share information, software and hardware.

Operating system (OS): Programs that manage all the basic functions and programs on a computer, such as allocating system resources, providing access and security controls, maintaining file systems and managing communications between end users and hardware devices. Examples include Windows, Macintosh and Linux.

Password: A secret sequence of characters that is used as a means of authentication to confirm your identity in a computer program or online account.

Password cracking: The process of attempting to guess passwords, given the password file information. See also **brute force attacks**, **dictionary attacks** and **hybrid attacks**.

Password sniffing: Passive wiretapping, usually on a local area network, to gain knowledge of passwords.

Patch: A patch is a small security update released by a software manufacturer to fix bugs in existing programs. Your computer's software programs and operating system may be configured to check automatically for patches, or you may need to periodically visit the manufacturers' websites to see if there have been any updates.

Phishing: Soliciting private information from customers or members of a business, bank or other organization in an attempt to fool them into divulging confidential personal and financial information. People are lured into sharing usernames, passwords, account information or credit card numbers, usually by an official-looking message in an email or a pop-up advertisement that urges them to act immediately, usually by clicking on a link provided. See also **vishing**.

Pharming: Redirecting visitors from a real website to a bogus one. A user enters what is believed to be a valid web address and is unknowingly redirected to an illegitimate site that steals the user's personal information. On the spoofed site, criminals may mimic real transactions and harvest private information shared by users. With this, the attacker can then access the real website and conduct transactions using the credentials of a valid user.

Router: A hardware device that connects two or more networks and routes incoming data packets to the appropriate network. Many internet service providers provide these devices to their customers, and they often contain firewall protections.

Script: A file containing active content—for example, commands or instructions—to be executed by the computer.

Skimming: A high-tech method by which thieves capture your personal or account information from your credit card, driver's license or even passport using an electronic device called a "skimmer." Such devices can be purchased online for under $50. Your card is swiped through the skimmer and the information contained in the magnetic strip on the card is then read into and stored on the device or an attached computer. Skimming is predominantly a tactic used to perpetuate credit card fraud, but is also gaining in popularity amongst identity thieves.

Social engineering: A euphemism for nontechnical or low-technology means—such as lies, impersonation, tricks, bribes, blackmail and threats—used to attack information systems. Sometimes telemarketers or unethical employees use such tactics.

Social networking websites: Sites specifically focused on the building and verifying of social networks. Such sites enable users to create online profiles, post pictures and share personal data, such as their contact information, hobbies, activities and interests. The sites facilitate connecting with other users who have similar interests, activities and locations. Sites vary in who may view a user's profile—some have settings that may be changed so that profiles can be viewed only by "friends." See also **blogs**.

Spam: Unwanted, unsolicited email from someone you don't know. Often sent in an attempt to sell you something or get you to reveal personal information.

Spim: Unwanted, unsolicited instant messages from someone you don't know. Often sent in an attempt to sell you something or get you to reveal personal information.

Spoofing: Masquerading so that a trusted IP address is used instead of the true IP address. A technique used by hackers as a means of gaining access to a computer system.

Spyware: Software that uses your internet connection to send PII about you to a collecting device on the internet. It is often packaged with software that you download voluntarily, and even if you remove the downloaded program later, the spyware may remain. See also **adware** and **malware**.

Secure sockets layer (SSL): An encryption system that protects the privacy of data exchanged by a website and the individual user. Used by websites whose URLs begin with HTTPS instead of HTTP.

Trojan horse: A computer program that appears to be beneficial or harmless, but has a hidden and potentially malicious function that evades security mechanisms. "Keystroke loggers," which record victims' keystrokes and sends them to an attacker, and remote-controlled "zombie computers" are examples of the damage that can be done by Trojan horses. See also **electronic infection.**

URL: Abbreviation for uniform (or universal) resource locator. A way of specifying the location of publicly available information on the internet. Also known as a web address.

URL obfuscation: Taking advantage of human error, some scammers use phishing emails to guide recipients to fraudulent sites with names very similar to established sites. They use a slight misspelling or other subtle difference in the URL, such as "monneybank.com" instead of "moneybank.com" to redirect users to share their personal information unknowingly.

Virus: A hidden, self-replicating section of computer software, usually malicious logic, that spreads by infecting (i.e., inserting a copy of itself into and becoming part of) another program. A virus cannot run by itself; it requires that its host program be run to make the virus active. Often sent through email attachments. Also see **electronic infection** and **blended threat**.

Vishing: Soliciting private information from customers or members of a business, bank or other organization in an attempt to fool them into divulging confidential personal and financial information. People are lured into sharing usernames, passwords, account information or credit card numbers, usually by an official-looking message in an email or a pop-up advertisement that urges them to act immediately—but in a vishing scam, they are urged to call the phone number provided rather than clicking on a link. See also **phishing**.

Vulnerability: A flaw that allows someone to operate a computer system with authorization levels in excess of that which the system owner specifically granted.

Whitelisting software: A form of filtering that only allows connections to a preapproved list of sites that are considered useful and appropriate for children. Parents sometimes use such software to prevent children from visiting all but certain websites. You can add and remove sites from the permitted list. This method is safe, but allows for only extremely limited use of the internet.

Worm: Originally an acronym for "Write once, read many times," a type of electronic infection that can run independently, can replicate a complete working version of itself onto other hosts on a network and may consume computer resources destructively. Once this malicious software is on a computer, it scans the network for another machine with a specific security vulnerability. When it finds one, it exploits the

weakness to copy itself to the new machine, and then the worm starts replicating from there as well. See also **electronic infection** and **blended threat**.

Zombie computer: A remote-access Trojan horse that installs hidden code that allows your computer to be controlled remotely. Digital thieves then use robot networks of thousands of zombie computers to carry out attacks on other people and cover up their tracks. Authorities have a harder time tracing criminals when they go through zombie computers.

Sources: Federal Communications Commission, Department of Homeland Security, National Cyber Security Alliance and the Chamber of Commerce