THE HARTFORD

SMALLBIZ AHEAD

TCIA
THE CLIENT'S INSURANCE AGENCY

HOW TO SAFEGUARD YOUR BUSINESS FROM DATA BREACHES

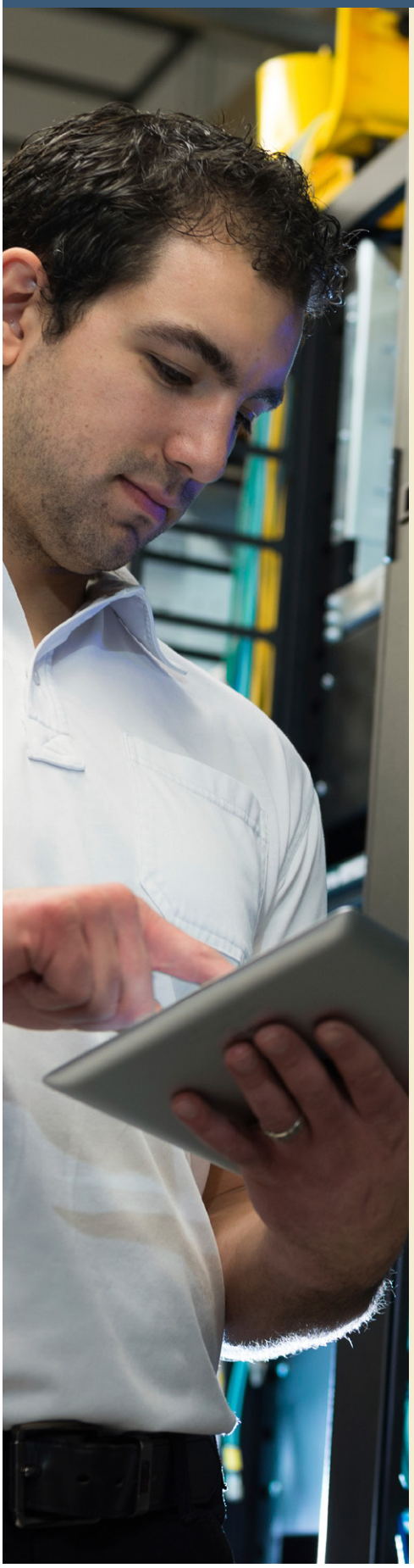


TABLE OF CONTENTS

INTRODUCTION

If you're like many small business owners, when you hear the words "data breach" you think of the highly publicized incidents involving large corporations that have gotten a lot of attention from the media. Such as:

- Target store's 2013 breach in which up to 110 million records were compromised and hackers made off with roughly 40 million credit and debit card numbers, leaving Target to pay over $250 million in damages.
- Sony Online Entertainment, which saw 102 million customer records compromised in 2011 and ultimately paid $171 million in damages. The hackers responsible have yet to be identified.
- Anthem insurance, in which nearly 80 million records were compromised, some included Social Security numbers.

What rarely makes the news are the many hacking incidents involving small businesses. The likelihood that a small business will fall victim to a potentially costly data breach is staggeringly high. The fact is that 74 percent of small and midsize businesses reported an information security breach in 2015.

Unfortunately, the underreporting of small business data breaches is likely the primary reason that most small business owners don't believe they're at risk for a cyber attack. In fact, 82 percent of small business owners say they're not targets for attack.

Not only are these attacks incredibly common, but they can also be devastating. With an average cost of a data breach being $4,000,000, it's easy to understand why 60 percent of small businesses fold within six months of falling victim to data theft. This cost doesn't even factor in the significant additional and unavoidable costs of investigating and remediating a data breach.

It can take a considerable amount of money to make the necessary security upgrades to technology as well as to plan and execute a communications strategy to restore a business's reputation after a data breach.

According to a Ponemon Institute study, 57 percent of people who had received a breach notification letter said that they lost trust and confidence in the business after finding out the business was breached. Even worse, 31 percent said they ended their relationship with the breached business.

It's important for business owners to understand that in the event of a data breach, few customers or potential customers will see the business as a victim. Instead, they'll see the business as untrustworthy and unprofessional. According to Visa, the customer's perspective is: "I gave my information to you, you exposed/lost it, and now it's your fault. Period."

Bottom-line: Any small business could be the target of a data breach and if the attack is successful, the odds are heavily weighted toward the business going under as a result. A data breach could leave a small business owner facing perhaps hundreds of thousands of dollars in legal fees.

Luckily, there are steps business owners can take to mitigate the risk of a data breach and help avoid the damages that would likely follow. This e-book serves as a guide to explain the common risks that data breaches pose to small businesses, the precautionary measures one can take to help prevent a data breach, as well as steps a business owner can take to help minimize the damage after a breach has occurred.

CHAPTER 1: THE RISKS

SECTION 1. WHY SMALL BUSINESSES ARE LIKELY TARGETS

Small businesses are a hacker's preferred target for data theft for the following reasons:

- Small businesses typically have lax security standards
- Many small businesses don't monitor server networks and data on a regular basis
- Most small businesses assume they won't be attacked
- Few small businesses have an IT specialist or department
- Many small business owners and employees operate on unsecure Wi-Fi
- Most small businesses don't train employees on cyber security best practices

SECTION 2. THE FALLOUT FROM A DATA BREACH

Did you know that 60% of small businesses that fell prey to data theft closed within six months?

The fallout from a data breach can be devastating to a small business. Remember from earlier, 60 percent of small businesses that fell prey to data theft closed within six months. Businesses that are victims of a data breach can be required to take time consuming and expensive actions including hiring a private firm to perform a mandatory forensic examination; providing credit monitoring services to affected customers, vendors and employees; paying liability fraud charges and Payment Card Industry (PCI) compliance fees. These are in addition to coming up with a communications plan and the resources required to repair the damage to their brand.

Possibly most devastating of all is that after a breach, businesses may not be able to accept credit card transactions until after the breach has been identified, investigated and remediated. This means a business might not be able to accept credit card payments for possibly several weeks or even months. For businesses that depend on credit card transactions for the bulk of their payments, this is a serious threat to their survival. Here's a closer look at what businesses could go through after a data breach occurs.

Mandatory Forensic Audit

In the event that a small business triggers a warning that they've been breached, the Payment Card Industry Data Security Standard (PCI DSS) requires an audit by a third-party PCI DSS security examiner. The security examiner's role is to inspect and review the company's business practices, habits, transactions, and security procedures to try to establish if, when, and where there was a data breach. This forensic audit can take a couple of days or up to several weeks, during which time the business being audited can expect the following:

- A complete review of its security policy. (You DO have a security policy, don't you? See Chapter 2, Section 2 if you don't yet have a security policy in place.)
- Security weakness tests for every computer, server and network connection the company uses to conduct business.
- Manual inspection of all virus and security software to ensure that they're up-to-date and properly installed.
- Wireless network testing to see if any unauthorized computers are accessing a business's wireless network.
- Phone line security testing to ensure that there are no listening modems or other security threats on the business's phone lines.

It's not uncommon for hackers to wait several years before using stolen data like Social Security numbers because they know most monitoring services usually only last one year.

Credit and Identity Monitoring for Affected Customers

If a customer's information is stolen in a data breach, there's a chance that their credit score will be negatively impacted. Even though the customer is technically not at fault, it can still be very difficult for them to clear their credit score and it can take several years to get the score back to where it was.

There's also the possibility of customers becoming victims of identity theft. If a customer's information, such as a Social Security number,

is stolen in a breach, the customer will likely want to monitor for signs of possible identity violations such as sudden changes in arrest or driving records. Most hackers who commit data breaches are aware of the standard one-year timeframe for credit and identity theft monitoring after a breach. In the case of identity theft, it's not uncommon for hackers to wait several years before using stolen data like Social Security numbers because they know most monitoring services usually only last one year.

It's important to mention that credit and identity theft monitoring for affected customers isn't legally required of the company that has been involved in a data breach. Still, it's something that often is provided by companies after a breach has occurred and customers are beginning to expect it. By not providing these services to customers, you could set yourself up for an even bigger struggle when it comes to reestablishing your company's reputation.

Liability Fraud Charges

There's some debate over who's responsible for the damages that are incurred as the result of a data breach. It's possible for businesses to be held liable for the fraudulent charges that were made with stolen customer credit card information. For many businesses without adequate insurance, these liability fraud charges could be great enough to destroy them. In the event of Target's data breach, a lawsuit was filed with an estimated **$1 billion in remediation costs**.

Updating Point-of-Sale Systems

Once a business suffers a data breach, chances are the business will need to update or completely replace its Point-of-Sale systems. The PCI DSS may remove the business's ability to handle any credit card transactions until such upgrades are in place. Not only can this be costly–and look bad–but it can render a business incapable of handling transactions for several days to possibly months.

SECTION 3. THE TYPES OF ATTACKS THAT SMALL BUSINESSES CAN EXPECT

There are 3.5 new cyber security threats created every second. It seems like any form of online interaction leaves businesses open to bombardment by thousands of different cyber-attacks. It's imperative that small business owners gain familiarity with the common types of cyber-attacks being perpetrated. These attacks can range from online advertisements that install malicious code onto a computer, password-cracking schemes that allow access to an entire computer network, to sophisticated multidimensional attacks that scrape information from a business's point-of-sale software database and more. Read on for a more in-depth look at the different types of cyber-attacks for which small business owners should be on the lookout.

Malware

Malware is a broad term used to describe malicious software designed to gain access or cause damage to a computer. Rarely is malware created just to cause damage. Often it's an insidious attack that gains access to a computer in order to steal data such as personal information and credit card numbers. There are several types of malware that business owners need to know about.

- **Adware**. This type of malware often comes bundled with free or pirated versions of software. The adware is designed to launch advertisements and pop-up ads on websites that the infected computer goes to. Often, advertisers sponsor it as a means for generating traffic and revenue. These advertisements can be a nuisance and slow down performance of the computer. It's common for adware to be bundled with spyware.
- **Spyware**. This malicious software spies on the activities of the infected computer without the user's knowledge. It monitors user's activity on the computer to see what files are opened, the websites visited and the types of data being stored. Spyware also records the keystrokes and data that's displayed and saved. Recording keystrokes is one way that spyware can open up gateways to larger hacking and data breach

attacks. Spyware can also perform additional malicious activities and functions including lowering security settings and disrupting network connections.

- **Trojan Horses**. Also known simply as "Trojans," this type of malware has the appearance of a normal file or computer application, but when downloaded, it gives a third-party remote access to the user's computer. Once access is achieved, the third party can then harvest passwords, identification data, financial records and other sensitive information. Trojans can also alter computer settings to reduce security and allow access for the installation of even more malware.

It may sound overly simple but it takes a hacker only five minutes to hack a lowercase only password with six characters or fewer.

Password Attacks

A password attack is like a modern day, digital lock pick. There are several methods that hackers can use to increase the likelihood of learning someone's password, these include guessing based on researching the person they're attempting to hack, running a dictionary attack or something called a "brute force attack."

One of the earliest techniques for cracking passwords was simply guessing. It may sound overly simple but it takes a hacker only five minutes to hack a lowercase only password with six characters or fewer. For slightly more complex passwords, a hacker may use a dictionary-like program that automatically guesses password options. This dictionary list may consist of actual words in the English language, or some of the most common passwords. Most people assume that their password is unique, but in reality, nearly 75 percent of the internet population uses passwords that are listed in the top 500 most common passwords.

As security protocols for passwords have increased, so too has the sophistication of the software that hackers use to discover them. Something called a "brute force attack" uses every combination of letters, symbols and numbers and attempts to guess the password. The simpler a password is, the easier it is for the brute force attack software to guess it. An eight-character password containing both upper and lowercase letters can take about four months to crack. When character count is increased to 10 upper and lowercase letters, it can take over

100 years to crack. Because of how long it can take to crack more complex passwords, a new method of hacking was created where victims unknowingly give hackers their passwords. This technique is called phishing.

Phishing

Phishing emails are sent by malicious users in an attempt to gain information such as credit card numbers, Social Security numbers, home addresses, or passwords. The way it works is the malicious user will send an email in the guise of a reputable source and claim that the recipient of the email must follow a link, which is included in the email, and the recipient clicks the link and then shares sensitive data.

For example, in 2003, there was a prevalent phishing scheme that posed as an automated email from eBay, informing users that their accounts were about to be suspended if they didn't update their credit card information. The email contained a link that the user was supposed to follow, where they would then be taken to a screen where they could update their credit card information. The email itself looked similar to an eBay notification, replicating colors and language used by the eBay brand. The webpage that users landed on after clicking on the link also closely resembled eBay's website. It was easy for an unsuspecting user to fall for the ruse and input their credit card information.

Today, phishing techniques have become far more sophisticated. With the emergence of social media, most people have some form of their identity posted online. For professionals or members of LinkedIn, that information can include their employer, employee email, employee phone number, employment history, and vendors with whom they work. From that information, a malicious user can concoct a phishing email by posing as a vendor that an employee has worked with. To gain trust, the phisher references specific details like the employee's name and phone number. The malicious user then requests information that, to the victim, makes sense for a vendor to request. Sometimes, the phisher may falsely pose as a vendor, notify the recipient that a payment wasn't correctly transferred, and request financial information such as credit card numbers or bank accounts to correct the transaction.

Pharming

Pharming is an even more sophisticated malicious technique being used to gain confidential data. With pharming, the naming system in a server is hacked so that users think they're accessing legitimate sites when they're actually being redirected to fraudulent ones. Once on the fraudulent site, users are prompted to provide sensitive data such as credit card information or Social Security numbers.

Drive-By Downloads

Drive-by downloads aren't exclusive to computers, they can also infect smartphones and tablets.

Most business owners believe that as long as they aren't downloading anything from unsecure websites, they can't contract a computer virus or some other form of malware. Unfortunately, "drive-by" downloads make it possible for websites to upload small bits of malicious code onto a user's computer. The small bit of code then contacts a malicious server that installs even more powerful malicious software onto the end user's computer. All the while, the end-user is unaware that any of this is happening. These drive-by downloads often result in standard malware programs that'll alter security settings to open up the computer to further attacks as well as steal important information such as credit card numbers, passwords and user activity habits.

Drive-by downloads aren't exclusive to computers, they can also infect smartphones and tablets. Additionally, drive-by downloads can be combined with phishing techniques and advertisements placed on reputable websites for a devastating multipronged attack. This can happen through a standard phishing email or an advertisement that directs recipients to a website infected with a drive-by download. In the case of advertisements, it's very common for smartphone users to accidentally click an advertisement when scrolling on a website, thus activating the malicious drive-by download.

Point-of-Sale System Hacking

Point-of-sale hacking of businesses has received a lot of attention from the media. A point-of-sale attack involves hackers scraping the data that is stored at the endpoint of a point-of-sale terminal, like when a credit card is swiped at

a store register. This data is vulnerable for only a microsecond before it becomes encrypted. In that microsecond, hackers are able to steal it, send it to several servers and then retrieve it. The reason hackers send it to several terminals is because it makes it that much more difficult to trace the culprit. Worst of all is that a point-of-sale terminal can be infected with malicious software for months before it's discovered.

So, how do point-of-sale terminals become infected? By any number of the means mentioned above. All that it takes is for one source of malicious software to gain access to part of a business's server, computer systems, or network for it to begin searching and gain access to the point-of sale terminal. Something as simple as a phishing email could be the start of a malicious process that ultimately leads to a virus infecting a point-of-sale terminal and scraping customer credit card information for possibly months before it's discovered.

Home Depot and Target may make for huge payoffs to hackers, but those attacks require much effort and sophistication. Small businesses on the other hand, are the far more accessible, low hanging fruit and offer hackers quick wins.

SECTION 4. COMMON SECURITY MISTAKES MOST BUSINESSES MAKE

Once business owners gain an understanding of the different types of security threats, it may be a little easier for them to detect the flaws in their own security. It's important to remember that if huge companies such as Target and Home Depot can spend millions on security and still succumb to data breach attacks, then it stands to reason that small businesses are even more vulnerable and should work to beef up their precautionary measures every chance they get. Home Depot and Target may make for huge payoffs to hackers, but those attacks require much effort and sophistication. Small businesses on the other hand, are the far more accessible, low hanging fruit and offer hackers quick wins.

What follows is a list of some of the most common mistakes small businesses make that leave them susceptible to data breach attacks.

Not Creating Timed Log Outs

There's a reason why online banking websites quickly log out inactive users. Leaving an unattended device or computer logged in to a secure database or website greatly increases the likelihood of malicious or detrimental use. The most obvious risk is that anyone who walks by the unattended computer can access critical software and data. This could be a malicious employee or customer, or even a burglar.

A lesser known risk is something called a "man in the middle attack" or "sidejacking." This involves the user logging in to an online platform or application, and a hacker impersonating the user by gaining access to the session cookie. From here, the hacker is able to interact with the online platform as if he was the user. Timed log outs can help reduce the risk of these attacks because they can end a session, and a hacker's chance of gaining access and retrieving data.

Poor Password Standards

Ranking as one of the top security mistakes business owners make is poor password standards. This can involve any of the following:

- Passwords shorter than eight digits
- Passwords that don't have various cases, numbers and symbols (example: 4HNJfw3!)
- Using the same password for multiple platforms and applications
- Using a password that's based on a personal hobby or interest
- Reusing an old password after an automated password update
- Following a common format of an uppercase letter, lowercase letters and then numbers
- Not changing passwords regularly
- Not using a password manager
- Using 1-part authentication as opposed to 2-part authentication

At some point, many software companies will cease to support, update and patch outdated versions of their programs and software.

Using Outdated Software

Business owners and employees might be reluctant to update software and programs because they know every aspect of their current software inside and out. Unfortunately, so do hackers. The longer a program exists after its release, the more time hackers have to find all the vulnerabilities and loopholes in that program.

At some point, many software companies will cease to support, update and patch outdated versions of their programs and software. This is when the software becomes even more risky to use, as hackers take advantage knowing that anyone still using the outdated software is vulnerable to certain attacks. Hackers may even create easy to use kits to help others launch attacks at anyone still using the outdated software.

Trusting Public Wi-Fi

Just because a public Wi-Fi source is password protected doesn't mean it's secure. If a person simply has to go up to the counter at a coffee shop to find out what the Wi-Fi password is, then it's easy to say that there's basically no security. Using a network that's shared by multiple people, especially people you don't know, opens you up to huge security problems.

It doesn't require a lot of skill for a hacker who's sharing a Wi-Fi network with you to hack into and monitor all the data that you're transferring over the internet. Hackers can also easily gain access to your computer and upload malicious software while sharing a Wi-Fi network.

In addition to the dangers of using public Wi-Fi sources, you may also be duped into using a hacker's hotspot. Sometimes, hackers will open up a Wi-Fi hotspot of their own in a gathering place like a coffee shop. They then name the Wi-Fi hotspot something similar to the coffee shop's name. Unsuspecting users who log on to this hotspot essentially give the hacker access to all of their information.

Not Encrypting Data before Storing it in the Cloud

When data is placed in cloud storage, it's automatically encrypted by the storage provider. When it's accessed by the owner via password, the cloud storage provider decrypts the data. Unfortunately, this data is far more vulnerable than most users are led to believe. Most of the time, when personal photos of celebrities are leaked; it's because the celebrity's cloud storage account has been hacked. In other words, someone simply hacked the account password and downloaded the data.

Even though the data may have been encrypted, the cloud storage provider decrypts it, believing the malicious hacker is the appropriate user. Failing to encrypt data *before* loading it into a cloud storage platform is one of the most common mistakes business owners make when trying to secure data. One of the easiest ways for a hacker to gain access to a user's cloud storage is with sidejacking or man-in-the-middle tactics.

Not Creating a Security Policy

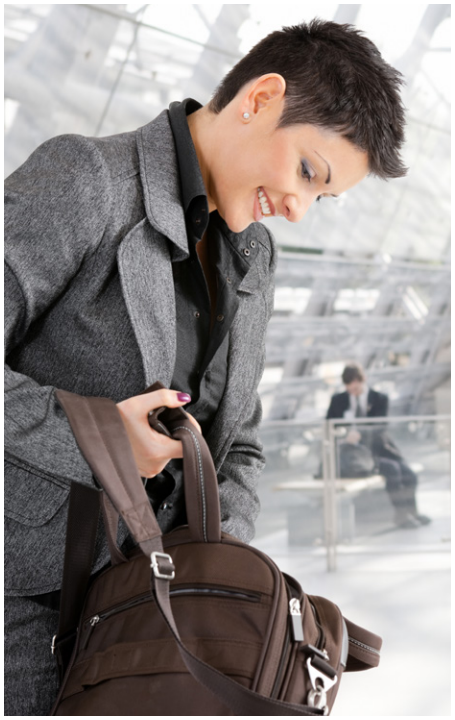
It's difficult for a company or business to prove that data security is a top priority if they don't have a documented data security policy in place. In the event of a breach, one of the first things that the mandatory forensic audit will review is the company's data security policy.

Not Updating Point-of-Sale Systems

As is the case with any type of outdated software, old Point-of-Sale systems are susceptible to hackers who have had the time to become intimately familiar with all the vulnerabilities and loopholes through which they can gain access to credit card data and other valuable information in the system. Unlike using an outdated or unpatched version of Microsoft Windows, business owners using outdated or unpatched Point-of-Sale systems are subject to major fines.

If a data breach does occur, the forensic audit will find outdated Point-of-Sale software. If this happens, it may then be very difficult to regain customer trust, or to convince credit card companies to allow you to handle transactions.

Not Providing Locks for Devices



Sometimes data theft happens the old-fashioned way and someone just flat out steals a device. Businesses are susceptible to theft when they don't do the following:

- Register devices with manufacturers and activate tracking
- Provide keys and lockable cabinets for storing devices at the end of the day
- Lock all office doors when not being used and at the end of the day
- Provide carrying bags for all employee devices
- Train employees on theft prevention strategies

Poor BYOD Policies

Bring your own device (BYOD) is becoming more common among businesses that have multiple employees. Unfortunately, poorly structured BYOD policies leave doors open for hackers and data breaches. BYOD policies that don't have guidelines for software updates, IT support and encrypted data options can expose businesses to some major vulnerabilities.

CHAPTER 2: THE DEFENSES

SECTION 1. BEST PRACTICES FOR PREVENTING DATA BREACHES

Unfortunately, there's no silver bullet for preventing data breaches; securing your business from hackers requires a holistic approach. Most data breaches are the result of an "inside job." No, this doesn't mean that your employees are double-dealing with some secretive hacker agency. It just means that most

data breaches are caused by internal sources, such as employees and business owners who don't follow good data security practices.

What follows is an in-depth guide to many best practices for preventing data breaches. Once you've learned the best practices, continue reading to learn how to create your own security policy and employee handbook.

> Most data breaches are the result of an "inside job."

About Passwords

Change passwords every 3 months. Consider changing passwords every three months as a best practice. These changes should be significant enough that they cannot be guessed by someone who knew the previous password. For example, if your current password is "redcardriver01," don't update it to "redcardriver02." Make the changes more significant by changing the password to something such as "BlueBicycleRider#11."

Make passwords long and varied. Typically, strong passwords are at least 10 characters long and contain symbols, upper and lowercase letters and numbers. This is what's considered a strong password. An example of this would be "RedCarDriver01!"

You can take this strategy one step further by creating a password "phrase." So, instead of "RedCarDriver01!," you might use "DidIDriveARedCarIn2001?." The increased number of characters makes the chance of cracking the password significantly more difficult.

If you want to increase the security of your password even further, you can swap numbers, symbols and letters that are similarly shaped. An example of this would be "D1d1Dr1v3@R3dC@r1n2ooI?"

You can also make completely random passwords by simply following shapes and patterns on your keyboard. For example, "ZsEfVbHuKoKmJyGvFeSz" is what you get when you type diagonally on the keyboard using only letters moving from left to right and then right to left. If you were to add on several numbers and symbols, this password would likely be incredibly strong, easy for you to remember and difficult to crack.

Be sure to use significantly different passwords for each of your accounts. Using the same password for every account opens the floodgates to attackers once one password is cracked.

Never use browser-based password storage systems. Storing passwords online with your web browser can increase the chances of a breach whether it's by a hacker accessing the passwords remotely or a malicious user logging on to your computer physically. This is because most web browser-based password managers store your password on your computer in an unencrypted form.

You CAN write down your passwords to help remember them–you just have to do it safely. Get a sheet of graph paper and write your passwords on it so that they're going in different directions as they would in a word search puzzle. Once you have written the passwords down, fill the rest of the graph paper with words, letters, symbols and numbers. You should be able to simply jog your memory for your passwords by looking at the sheet, but to anyone else it'll be extremely difficult.

Use a dedicated password manager. Some professions require employees to manage tens to hundreds of passwords for various logins. Because best practices state that you should always use a different password for different applications and programs, it can quickly become overwhelming to try to remember multiple, strong passwords. In situations such as these, consider using a dedicated password management program.

Unlike browser-based password managers, dedicated password management software can store your passwords in encrypted form in cloud-based storage or on your own computer.

Unlike browser-based password managers, dedicated password management software can store your passwords in encrypted form in cloud-based storage or on your own computer. They can also help randomly generate passwords and ensure that passwords are automatically changed periodically. With a password management application, you only need to enter one password to log in to the interface. From there, the password management software will store all of your passwords and input them automatically into web applications and programs.

Password management applications can also be used to store credit card information. In addition to helping protect passwords and credit card numbers, these programs can help prevent against phishing attacks. For example, if you open the link contained in a phishing email that leads you to a website that looks similar to your bank website, your password manager will know that it's not the actual website and it won't upload the password.

Here are a few popular password management applications:

- Dashlane
- LastPass
- Keepass

About Remote Access and Public Wi-Fi

Never use public Wi-Fi. Always assume the public Wi-Fi sources aren't secure, even if they're password-protected.

Turn off sharing in your settings panel when using public Wi-Fi. Sharing allows you to perform functions such as accessing remote printers, sharing files and allowing remote logins, which are all very important procedures that deserve good security.

Turn off network discovery. This will make it harder for anyone to see that your computer or mobile device is on the network.

Use HTTPS whenever you can. HTTPS stands for *hypertext transfer protocol secure* and offers an extra layer of security and encryption over standard web browsing which is labeled as HTTP. To know if you're using HTTPS, just take a look at the web address in your browser field. If the site is secure, the letters "HTTPS" will appear at the beginning of the website name. Most websites that accept information and passwords will automatically be HTTPS. For example, Facebook.com and amazon.com use HTTPS. If you're on a website while using public Wi-Fi and you need to exchange any sort of information, double check to make sure that it has HTTPS. If it doesn't, hold off on exchanging that information until you're able to get to a more secure Wi-Fi hotspot, perhaps one in your home or office.

Disable Wi-Fi when you're in a public place and don't use the internet. This will reduce the amount of time that your device is connected to the unsecure public network and decrease the chances of you being hacked.

Make sure that the basic firewall that your computer or mobile device comes with is enabled. Enabling your firewall, if it isn't already enabled, will make it far more difficult for malicious users to gain access to your system.

Use a virtual private network when you're not on your home or work network. A virtual private network (VPN) adds a level of security to your web browsing by running all of your web activity through a private network even though you're using a public one.

Here are three popular VPN services:

- private Internet access
- proXPN
- WiTopia

About Bring Your Own Device (BYOD)

Consider that you may not want to make your BYOD policy mandatory for employees because it requires the installation of invasive software and the loss of privacy for the device owner.

Also, consider giving employees who wish to use their own devices an acceptable use agreement policy and have them sign-off on the agreement. This policy would cover information such as the requirements for malware and antivirus software, firewall specifications, password security, device location software, and clearly defined, separate containers for personal and business data. This acceptable use agreement would acknowledge that the owner of the device relinquishes privacy and control over what's done on the device and that all data on the device can be wiped at the business owner's request if the employee leaves the company or is fired, loses his or her device, or if IT detects a breach on the device.

Ensure that all spyware and antivirus software that's installed on employee computers is also installed on employee personal devices that are being used for work purposes.

Another BYOD best practice is to ensure that all spyware and antivirus software that's installed on employee computers is also installed on employee personal devices that are being used for work purposes. Be sure the software is installed in a manner that ensures the owner of the device isn't able to alter security features and settings.

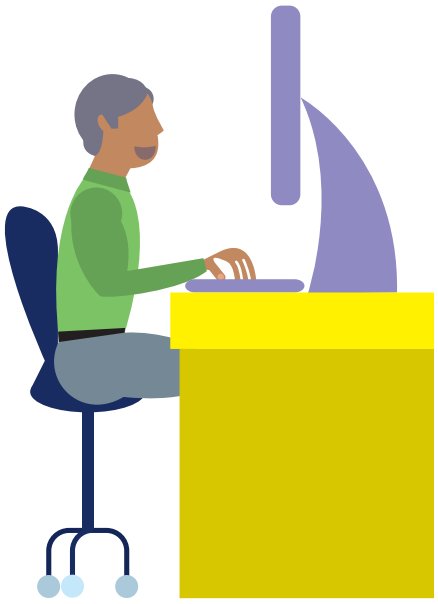
Typically, companies with strong BYOD practices insist that personal devices used for business be registered and ID'd just as any other company device would be.

They also require that all policies that apply to standard work computers in regards to data storage, password strength and Wi-Fi usage apply to all personal devices that are used for work.

Another important BYOD best practice is the installation of mobile device management (MDM) software that allows owners to monitor and manage mobile devices. MDM software can allow for tracking of mobile devices that may be lost or stolen and it gives remote access to all data on the device. In the event of theft or loss, MDM software enables the user to wipe the entire hard drive of the device. Managers can also be given the ability to encrypt data on the device, remove user access to the device and disable the ability to transfer any data.

The three popular MDM applications are:

- Mobile Device Manager Plus
- Hexnode MDM
- SimpleMDM



About Antivirus Software

There's a difference between antivirus and anti-malware software. A virus is a string of code that copies itself and does damage to a computer. Viruses were much more popular in the 1990s, but have now taken a backseat to other types of attacks such as

Trojans and worms. Malware is a broadly used term to describe any type of malicious software that could attack your computer.

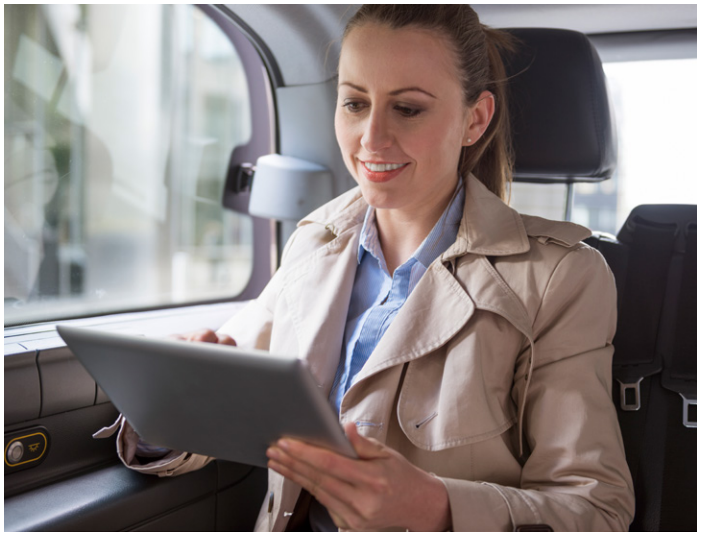
Consider installing antivirus and anti-malware software on all PCs. This software can be installed at the administrative level so that all settings are fixed and cannot be changed by employees. You'll need software to handle both malware and viruses. Nowadays most "antivirus" software handles malware as well. The term "antivirus" has lately become a catch all term that now seems to encompass all major threats and not just viruses.

There are two types of antivirus and anti-malware programs: on demand and on access. Upon access, programs are always running and will help ensure that you don't go to a website that contains malicious software or that you don't install a program that has been infected. These on access programs will either block you from going to malicious websites, or post a warning on your screen about the threat.

On demand programs work by scanning your entire system or by scanning specific areas for threats at scheduled times. An on-demand program will not be running at all times. Instead, it can be used routinely to check and see if anything has slipped past the on access program. This strategy ensures that your computer will be able to continue running quickly while also being protected.

Some popular antivirus and anti-malware programs include:

- Malwarebytes anti-malware
- Norton antivirus
- McAfee
- Avast



Do Macs need antivirus and anti-malware software? It might seem reckless to come out and say, "No, Macs don't need antivirus and anti-malware software." But, what can be said is that Macs make up a very

small percentage of the vast number of computers that are in use–and hackers are opportunistic. So it's rare that hackers target Macs because there are far fewer of them compared to the number of computers in use with Microsoft Windows operating systems.

Because of how Mac operating systems are created, it's very difficult for malware to spread throughout the computer. Additionally, all Mac operating systems since OS X 10.8 Mountain Lion have a gatekeeper function that prevents Mac users from installing non-Apple approved applications.

If, however, your business uses Macs to handle highly sensitive data and is an obvious target for hackers, then purchasing antivirus and anti-malware software may help provide some additional security.

If you do want to install antivirus and anti-malware software on your Mac these are popular programs:

- SentinelOne
- Sophos Anti-Virus

About Data Storage

Consider restricting access to portable storage units such as USBs and portable hard drives to only employees who absolutely need to use them. If you're going to allow employees to use USBs and portable hard drives a good practice is to ensure they're password-protected. Some storage units have numeric key codes built-in to the exterior of the device. Unless the code is input manually on the exterior keypad, the data is unreadable and the device cannot be used.

Portable storage devices can also be outfitted with features that allow them to be wiped remotely.

Portable storage devices can also be outfitted with features that allow them to be wiped remotely. This is handy in the event that a device is lost or stolen as it allows the owner to remotely clear all of its data. Along with remote clearing, portable storage devices can also come with features that allow all activity to be tracked. This can be exceptionally useful if the inception point of a data breach is on a portable storage unit.

You can also encrypt USB devices on all Microsoft Windows computers that are running Vista or a more recent operating system by using BitLocker. BitLocker will enable password protection to encrypt and decrypt the data on the flash drive.

If you're a Mac user, you can encrypt USB drives and make them password-protected as long as you are running OS X 10.7 "Lion" or more recent. (You're running the most recently updated operating system, right?)

If you have a file saved in only one location then it's not backed up. To be safe, consider storing data on your computer as well as in the cloud and possibly even a secured portable drive. Before storing data on the cloud, it's important to encrypt. Most cloud storage units automatically encrypt data that's being stored. Unfortunately, anyone who has your password will be able to decrypt this data. Consider using a personal encryption software program to add an extra layer of protection to the data you're storing on the cloud.

About Accepting Credit Card Payments over the Internet

Unless you have a strong background in web development and IT, it may be best if you set up an account with a third-party merchant to handle online credit card transactions, as opposed to creating your own merchant account and building your own checkout portal.

When you use a third-party vendor, the entire transaction process takes place off your website and the third-party merchant handles all credit card and personal information. This can greatly reduce your involvement in the handling of highly sensitive information. In order to handle and process credit card payments, third-party merchants who handle online credit card transactions must adhere to the standards set forth by the payment card industry.

Most third-party merchants require no set up costs. Instead, they make their money by charging a small percentage of each of your transactions. Typically, these transactional charges are less than 3 percent.

Four popular merchants that handle online credit card payments are:

- PayPal
- Stripe
- Chase Paymentech
- Flagship

About Securing Point-of-Sale Devices

Businesses that use point-of-sale devices (PoS) and employ data security best practices update their PoS devices to meet current PIN transaction security standards. A recent notable update means all their devices are now equipped with a chip reader as opposed to the traditional magnetic strip swipe reader.

Routinely check your credit card reading device for the following signs of tampering:

- Missing manufacturer labels
- An inconsistency between electronic serial numbers and the serial numbers printed on the label on the bottom of the device
- Damaged seals
- Extra wiring
- High-volume of magnetic strip reader fails and debit card declines

If you notice any of these telltale signs, contact the manufacturer immediately.

If you notice minor details or changes in appearance or function of the credit card reader, contact the manufacturer.

Consider installing security mounts so that card readers cannot be moved. This will help limit a malicious user's ability to tamper with the card reader.

You may also want to keep all readers locked in a storage device and require all managers to check them 'in' and 'out' and record their whereabouts at the beginning and end of every shift.

Peel off all sticker overlays on credit card readers. These overlays aren't standard on credit card readers anymore and are often used to cover up signs of damage or tampering.

Get to know the devices that you are using. 3-D printing has advanced to the point where malicious users can duplicate the plastic shell of a credit card reader very easily. If you notice minor details or changes in appearance or function of the credit card reader, contact the manufacturer. You may be dealing with a 3-D printed clone in place of a stolen reader.

Don't allow any other devices to be placed near the credit card reader. Sophisticated attacks can involve smartphones being placed near your readers to capture customer information.

Consider purchasing devices directly from manufacturers or authorized resellers only. Often, credit card readers sold online through non-authorized resellers have been tampered with and contain malicious software or hardware that'll be used to steal credit card information.

Consider purchasing PoS software that encrypts and tokenizes all credit card information. ShopKeep is an example of popular PoS software that does this.

Best practices for using mobile phones with card reader attachments to accept payments are:

- Use hardware that immediately encrypts all data upon swipe or chip insert.
- Provide mobile devices for all employees and regulate their usage by employing the same best practices that you do for standard card readers and work computers.
- Ensure that all operating systems and applications are up-to-date.
- Never manually input credit card numbers.

Here are a couple of popular providers of credit card reading devices:

- Verifone
- MagTek

These are popular mobile device credit card processing service providers:

- Square
- PayPal

About Cyber Liability and Data Breach Insurance

One of the best and easiest ways to protect your business from a data breach and manage the fallout, is with cyber liability and data breach insurance. With the exponential growth of hacking incidents targeting businesses, this coverage is growing in popularity and being viewed more and more as a necessity.

In the event of a breach, data breach coverage can help cover expenses and in addition, may include services to help manage and mitigate the fallout. Often, these policies include options that will:

- Help notify customers in the event of a data breach
- Cover the legal expenses that result from a breach
- Help with advertising costs to repair a business's reputation
- Help identify the breach and mitigate its damages

Data breach insurance can also help business owners prevent breaches from happening in the first place. Look for policies that include support for employee training, assistance in setting up network security, help creating security policies and procedures and incident response planning.

Talk to an insurance agent to learn more about how cyber liability and data breach insurance can help strengthen your business's data security.

SECTION 2. HOW TO CREATE A SECURITY POLICY

Now that you're aware of some best practices for safeguarding your business against data breaches, it's time to create a security policy. The scope of your security policy can be determined by the assets that your business handles. For example, although timed logouts after no activity help increase security, they can also be a nuisance. If you run a graphic design business and use Microsoft Outlook to interact with customers and other employees, you probably don't need to set a timed logout for every 15-minutes. If you run an accounting firm however and your employees have access to a remote company hard drive that they store all the data on, you may want to enforce a 15-minute logout along with two-step verification for passwords when accessing that hard drive.

The scope of your security policy can be determined by the assets that your business handles.

The following is an outline you can use to begin creating a security policy for your business. This information can help you determine the specific security measures you may implement for your particular business. Document these measures in your security policy document.

1. Introduction

In the introduction of your security policy, describe all the types of information that your business handles, even if it's not critical for security reasons. Then list which categories of information are most sensitive and why they need protection.

2. Purpose

Here describe the purpose of your security policy. The description doesn't have to be complex. You can start by stating something like, "The purpose of this document is to define the risks and procedures for securing and handling a data breach."

3. Scope

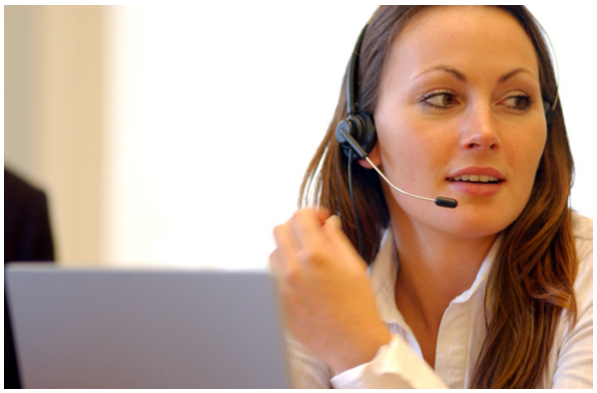
For scope, you can start by answering and elaborating on these questions:

- Who does this policy apply to?
- Is this policy only for employees or is it for vendors and contractors?
- Does this policy extend to customers and clients and cover how they can interact with your business and its data?

4. Relationships to other policies

What other policies do you have that may need to align and integrate with this one? Do you have a vendor hiring policy that must integrate security policies from this data breach policy? List these policies and how each works to support and be supported by your data security policy.

5. Responsibilities



Describe who's responsible for what aspects of your data security program. Start by answering these questions:

- Who are the parties responsible for implementing and enforcing this policy?
- What are their responsibilities?
- What are the responsibilities of the people who were listed in the scope of this policy?
- Is someone responsible for updating antivirus software, managing Bring Your Own Device (BYOD) equipment, etc.?

6. Compliance

What happens when individuals don't comply with this security policy? Describe how policy violations will be handled.

7. Definition of an Incident

Give a broad definition of what would be classified as a data security incident. Then provide about 5 to 10 examples of data security incidents your business may face.

8. Reporting an Incident

In reporting an incident, describe the process for reporting incidents and to whom are they reported? Include what details should be included in an incident report.

You may want to require:

- Employee name
- Date
- Location
- Incident type
- Number of people involved

9. Investigation and Risk Assessment

What's the procedure for your investigation into a possible data breach incident?

How will you assess the risk and the impact of a breach?

10. Containment and Recovery

Who's on your incident management team and what's the course of action they'll take in the event of a data breach?

11. Notifications

Who'll be responsible for notifying customers and clients whose data may have been compromised? Which customers will be notified?

For example, will you notify all customers, only those who are compromised or only those who interacted with your business within a certain timeframe of the data breach?

12. Review

Who'll review the incident, methodology and results once the breaches are contained?

13. Definitions

Include definitions of any specific key terms that you use in the policy.

If you decide to purchase data breach and cyber security insurance, your insurance company may help you write your policy. Also, note that your insurance company may handle some of the actions listed in this policy document, such as containment and recovery.

SECTION 3. EMPLOYEE GUIDELINES AND TRAINING

Hackers are constantly looking for opportunities to steal data. They'll often go after the lowest hanging fruit–unsuspecting and untrained employees.

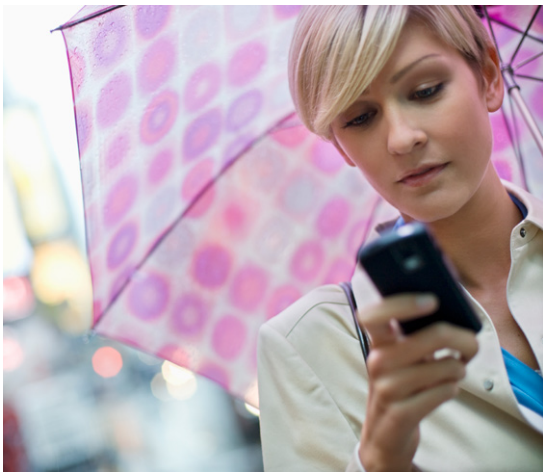
Employee mistakes are one of the most common ways that data breaches occur. Whether it's an employee falling for a phishing email or using an insufficient password, employees (and owners) are the most likely causes for data breaches. One of the most important things a business owner can do to protect his or her operation is to provide data security guidelines to all employees.

Documenting and providing data security guidelines to employees is a definitive first step toward leading a team that incorporates data security best practices in their daily work. Remember, hackers are constantly looking for opportunities to steal data. They'll often go after the lowest hanging fruit–unsuspecting and untrained employees–because it's the easiest route to valuable data. Businesses that turn security best practices into everyday habits create a culture of data safety and are much less vulnerable to a breach.

Begin creating your data security guidelines document by grabbing relevant sections from the "About..." sections of this e-book. Choose the practices that are relevant to your business. For example, if your employees only need to remember two passwords, you probably don't need to include password management software into your guidelines. Likewise, if you don't accept online payments, you don't need to include that section either. Adding information to your guidelines that isn't relevant to your business can confuse employees and divert their attention from the pertinent information.

Help your employees learn to recognize hacker tactics and eliminate risky workplace practices that can open the door to data breaches. Consider sharing the sections of this e-book on malicious threats and common mistakes small businesses make with your employees. Discuss the material with them to ensure they fully understand the information you provided. Once you have reviewed the guidelines with your employees, ask them if they're aware of any data security risks at your business that aren't covered in the guidelines. Review the document regularly and update it as needed. Provide employees with a copy of your security guidelines that they can keep for reference purposes.

For most businesses, reviewing data security guidelines with employees may suffice. However, if your business handles high volumes of sensitive data it may be a strong target for hackers. You may benefit from hiring a data breach consultant and purchasing data breach insurance. Both of these options can give you access to in-depth employee training by experts in the field of data breach and cyber security.



CHAPTER 3: WHAT TO DO WHEN YOU DISCOVER A DATA BREACH

When a breach happens, it's important to act quickly but also to choose your remediation actions carefully. The process for managing a data breach can be divided into four major steps:

- Investigation of the breach
- Containment the breach
- Notification of those affected
- Reputation management (public and customer relations)

The following section will explore each action in detail. Before reading on, it's worth taking the time to assess whether your business, and you, can actually handle a data breach successfully without external help. In some cases, hiring a data security specialist, or simply purchasing data breach insurance may be your best option.

SECTION 1. IS YOUR BUSINESS CAPABLE OF HANDLING A DATA BREACH?

If your business doesn't have a dedicated IT department or specialist, then you may not be equipped to handle a data breach effectively using in-house resources. Understand that even if your business has an IT department or specialist, a data breach may require the undivided attention of your IT department and could pull important IT resources away from regular business operations for several days, possibly even months. Because the risks to the viability of your business are so high after a data breach, if you don't have the excess resources in place to handle the breach internally, consider purchasing data breach insurance and perhaps hiring a data breach consultant.

Not only will a data breach insurance policy or a data breach specialist help provide the technical expertise required to handle an attack, they may also assist with customer and public relations when it comes time to notify affected individuals and, if necessary, handle the media.

With that said, here are the steps businesses might take to handle a suspected data breach.

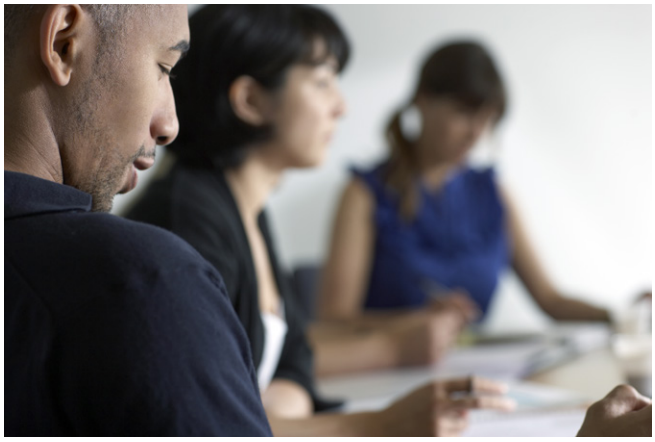
SECTION 2. HANDLING A DATA SECURITY BREACH IN-HOUSE

This section includes the four steps that your business may want to take after a breach has occurred. Consider following these four steps in the order listed, to help you identify and determine:

- Whether you're dealing with a breach or computer or software glitch
- The severity of the breach
- Who in your business should be notified
- Which law enforcement agencies should be notified
- How to notify customers and other effected individuals

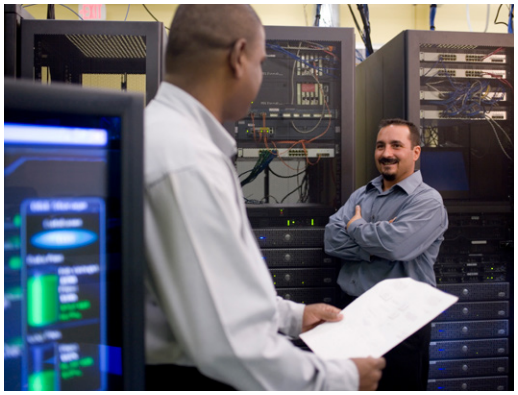
Step One: Investigating a Data Breach

It's important for business owners to recognize the warning signs that indicate a breach may have occurred. Malware and antivirus software can help alert you to intrusive and malicious software. However, a combination of robust, updated software and close monitoring of all network activity makes for a stronger defense that's more likely to discover breaches earlier.



To spot a breach, keep your eyes open for any computer or network activity that's out of the ordinary or doesn't make sense. If it seems

that your computer or network has developed a mind of its own, there's a good chance your systems have been breached. Here are some of the most common warning signs that a system breach has occurred:



- Antivirus programs are running at different settings, turned off or not automatically updating
- New widgets are found on your web browser or operating system toolbars
- New software or programs have appeared and you don't remember installing them
- Settings for computers, security, logins or applications have changed
- Log-in experience to computer for any application is different or suddenly unexplainably difficult
- Applications or programs automatically launch themselves after your computer boots up

If you notice any of these signs, or an indication that your computer or system is operating in a way that it's not intended to, begin your investigation. The first step is to determine if you are dealing with a malicious attack or a software glitch.

To determine if your computer has a software glitch:

- Perform online research on all recently installed software.
- Call the customer support hotlines for all software you have installed on your computer and report the computer behavior you're experiencing.
- Check for any updates or patches for software or operating systems that you are running.

If your search for a software glitch turns up with no results, it's safe to assume that you are dealing with a malicious attack.

- Double-check all malware and antivirus software.
- Contact your malware and antivirus software providers and explain the symptoms that you're noticing.
- Perform online research on the symptoms you're noticing.

At this point, you'll have likely determined whether you're dealing with a software glitch or malicious attack. In the event of a software glitch, the software provider should be able to provide assistance to correct the issues. In the event of a malicious attack, further investigation is required.

The U.S. Department of Justice recommends that businesses ascertain the following information in order to fully scope out the magnitude of a data breach. You should investigate and document:

- The affected number of computer systems
- The apparent origin of the incident, intrusion or attack
- Any malware used in connection with the incident
- Any remote servers to which data was sent
- The identity of any victims

Incidents such as peculiar emails, phone calls, package deliveries, physical break-ins, vandalism, or suspicious employee, customer or vendor behavior should also be logged and included in the investigation.

Step 2: Containing a Data Breach

If you think of a breach as being similar to an oil spill, then the first step you take after identifying the spill would be to block off the point of the leak or reroute the oil. With a data breach, your primary goal during the containment phase is to shut off all possible avenues that the breach could be coming in through and to halt traffic to affected areas.

The U.S. Department of Justice recommends the following steps for containing the data breach:

- Rerouting network traffic
- Isolating all parts that would compromise the network
- Obtaining an uninfected backup copy of all critical data and restoring it on a new network after abandoning the previous, infected network

- Locating the origin of the attack and, if possible, contacting the service provider of the network that the attack came from
- Altering the configuration of a network
- Changing all passwords

All activities that are done to contain the breach and all costs associated should be recorded. This information will be important for any criminal investigations and when reporting damages.

Step 3: Notifying Those Affected by a Data Breach

Notification of a data breach can be the make or break point for a business's reputation. Failing to properly notify individuals and customers can increase the impact of the breach and lead to bad publicity. The four main parties that likely require notification in the event of a data breach are people within the business (employees, customers, vendors, etc.), law enforcement, legal agencies and any other individuals who may be affected.

Most data breaches are unlawful and therefore law enforcement should be notified.

Begin by notifying individuals listed in your data breach policy. There may be no need to alert every single employee at your business unless the data breach somehow interferes with their job responsibilities or affects them personally. You can provide detailed reports to all managers, security coordinators and IT personnel. These reports could include the details about the initial investigation of the data breach, the scope of the breach and current actions that are being taken to contain the breach.

Most data breaches are unlawful and therefore law enforcement should be notified. Law agencies such as local police, FBI and Department of Homeland Security have a strong interest in data breach attacks. It's in your best interest to contact these agencies as they may have access to tools and resources that private consulting groups may not. They may also be able to advise you on when it's time to notify customers and other affected individuals. Notifying these affected individuals too soon could impair the investigation and tip off those responsible for the breach. Coordinating with law enforcement can help mitigate the damage of the breach, speed up a system recovery and foster goodwill between you and your customers.

In addition to notifying law enforcement agencies, you might also contact your attorney. If your lawyer doesn't specialize in data breach, he or she should be able to put you in contact with someone who does. To reduce the likelihood of fines or penalties, it may help to bring in legal support early to ensure the steps you take are lawfully sound.

The standard timeframe that a business has to notify affected individuals about a data breach is 60 days. Depending on the state in which you do business, and the state where your customers live, this timeframe can vary. This is one of the reasons that notifying law enforcement and your lawyer is imperative. They should be able to advise you on the correct timing of required notifications.

> Discussing the scope of the breach and its origin will help demonstrate that you're fully aware and in control of the situation and that you're acting with transparency.

To ensure affected parties receive your timely notifications, you'll want to send your communications in multiple formats such as an email, delivered mail and automated phone call. You'll also need to staff a response team to handle incoming emails or phone calls from customers reaching out with concerns about the data breach.

Step 4: Reputation Management–Customer and Public Relations

One of the most important factors in managing fallout from a data breach is to ensure that customers hear about the breach from you and not from the media. It's important to provide them with the right messaging, information and level of transparency. Being the first to notify the customers about the breach, and doing it in a professional and caring manner, can go a long way toward maintaining goodwill and a positive public image.

Oleksandr Maidaniuk, head of quality assurance solutions of Ciklum Interactive Solutions lists these basic rules for notifying the public, your customers and vendors about a data breach.

1. Be open and sincere. Admit if the fault was on the company's side and accept responsibility.
2. Provide details. Explain why the situation took place.
3. Mitigate. Make conclusions from the breach and describe solutions for affected users. If possible, prepare a special offer for the affected audience.

4. Educate. Explain how to prevent similar issues in the future.
5. Invite to dialogue. Involve your clients, industry experts, analysts and media people to the broader discussion about the source of the problem.

Steps 1 and 2 can be handled in your initial notification to affected individuals. Consider hiring a PR firm to manage crisis communications and protect your image if there's a chance that the media will pick up the story of your breach. A PR firm can help craft and convey effective messaging to help the media and broader audience understand what's going on in a way that preserves the reputation of your business.

Step 3 can be handled by providing credit and identity monitoring for affected individuals, depending on what information was lost in the breach. If only credit card information was lost, then there's no need for identity theft monitoring. In your initial notification, make it clear to customers that you'll be providing services to help them correct any damage that may occur as a result of the data breach.

Step 4 is where you assure affected individuals, and if necessary the public, that you have reviewed and renewed your security protocols. Resist providing details of these protocols, as you won't want that information landing in the hands of other hackers. But do let it be known that you have taken every measure possible to prevent another breach from happening.

With step five, it's best practice to answer all questions presented to you. No affected or concerned individual is too small to respond to and no question is off-limits. Discussing the scope of the breach and its origin will help demonstrate that you're fully aware and in control of the situation and that you're acting with transparency.

CONCLUSION

Data breaches have the potential to be completely devastating to a business and others who are affected. If your business handles any form of customer data, whether it's emails, credit card numbers, addresses and phone numbers, Social Security numbers or other personal information, it's imperative that you take the necessary steps to secure that data and prevent data breaches. With this e-book, you now have information on:

- Common threats that can result in data breaches
- Best practices for ensuring data security
- Important steps to take when a potential data breach is discovered

There's enough information here to help you ascertain whether or not your business is capable of handling a data breach with in-house resources or whether to contact an insurance agency about purchasing data breach coverage.

Business success is about more than earning profits by providing outstanding products, exceptional service and customer value. You must also protect your customers' best interests, privacy and security. So congratulations, with this e-book, you've taken a major step toward ensuring the longevity of your business and the security of your employees', vendors' and customers' information.

Now it's time to take the next big step which is to review and update your company's data security strategy.

LEARN MORE.
For more information, visit us at **sba.thehartford.com**.

Business Insurance
Employee Benefits
Auto
Home

Information and links from this e-book are provided for your convenience only. Neither references to third parties nor the provision of any link imply an endorsement or association between The Hartford and the third party or non-Hartford site, respectively. The Hartford is not responsible for and makes no representation or warranty regarding the contents, completeness or accuracy or security of any material within this e-book or on such sites. Your use of information and access to such non-Hartford sites is at your own risk. You should always consult a professional.

The Hartford® is The Hartford Financial Services Group, Inc. and its subsidiaries, including Hartford Fire Insurance Company. Its headquarters is in Hartford, CT.

16-1272 © December 2016 The Hartford. All rights reserved.