Cyber Security Checklist

Click the tips below to learn how you can better prepare and protect your business from a cyber security breach.

- [ ] REFRAIN FROM PUBLIC Wi-Fi
- [ ] LIMIT THE USE OF PORTABLE TECH
- [ ] PRACTICE PRIVACY
- [ ] LOCK UP SENSITIVE DATA
- [ ] GET ORGANIZED
- [ ] START SCREENING
- [ ] ESTABLISH A ROUTINE
- [ ] GET INFORMED
- [ ] TRAIN EMPLOYEES
- [ ] CONTROL ACCESS
- [ ] STAY VIGILANT

MUTUAL OF
ENUMCLAW
INSURANCE
EST. 1898

REFRAIN FROM PUBLIC Wi-Fi

Don't use unsecure wireless networks when accessing systems storing sensitive and confidential data.

If using a personal computer to access public Wi-Fi networks while on the go, there are a number of things you can do to protect the device from hackers.

Simple public Wi-Fi security measures

Enable Secure Sockets Layer (SSL)

Before taking off on a trip, enable Secure Sockets Layer (SSL) connections on your most-used websites. SSL connections help encrypt the information exchanged on a website, making it difficult for hackers to access it. Gmail, Twitter and Facebook, for instance, have such SSL connection options. Clicking on the "Always Use HTTPS" option in Gmail and Twitter, for instance, will enable this security feature.

Turn off Wi-Fi connection

Disabling your Wi-Fi on your computer before heading out to the airport or other destinations where public networks are available is also a smart way to ensure your computer does not hook up to a public network on its own, possibly putting your online information at risk. Once you have arrived at a destination and want to access the Internet, this Wi-Fi option can be turned back on.

Use a virtual private network (VPN)

For business travelers, using a virtual private network ensures online safety while on the road. Many companies offer network access to employees while they are traveling, allowing them to hook up to the company's VPN outside the office. A VPN will help act as a shield to outside attacks.

If using public computers, please keep these steps in mind.

REFRAIN FROM PUBLIC Wi-Fi

Take caution

Public computers don't need to have anti-spyware programs installed, so taking extra precaution is necessary to ensure your personal information is kept secure.

Log out

Remembering to log out of a website is absolutely critical when using a public computer. Closing the browser window will not necessarily log a person out of a website, leaving that information accessible to the next person who uses the computer. Make sure websites, such as social networks, do not automatically save login information on the computer, as well.

Browse privately

Selecting the "browse privately" option will also erase your tracks on a public computer. Erasing the history and temporary Internet files once you are done using the computer is another smart step.

Return to Checklist

LIMIT THE USE OF PORTABLE TECH

If it is necessary to use portable devices, make sure information is encrypted and password protected.

The problem with portable tech

Companies and consumers are certain to plunge deeper into mobile computing. However, few are prepared for the security and privacy risks that arise from the rapid adoption of smartphones and tablets in every aspect of work and home life.

The issue

Smartphones and tablets are not tied to a fixed location. Plus, they come in a wide variety of customizable form factors, each model with the latest sensor and data collection capabilities. These characteristics make them significantly more complicated than desktop PCs to protect. The recent Stagefright exploit is a case in point. Stagefright exposed 950 million Android phones to corrupted video messages carrying malicious codes.

It takes time to create, test and deploy security patches for multiple operating systems on myriad handset models. And then the carriers—Verizon, AT&T, T-Mobile and Sprint in the United States and others internationally—don't exactly relish their part in the process.

Criminal forces

The discovery of fresh security flaws in mobile operating systems, and the subsequent patching exercise, is following the same trajectory as what happened with desktop computing.

So it's safe to say, there will be no shortage of freshly discovered mobile OS security flaws going forward. In a recent analysis of 7 million mobile apps on Android and iOS platforms, FireEye found a 188 percent increase in vulnerabilities since 2011 for Android and 262 percent for iOS.

The exposure redoubles when employees take their mobile devices away from work premises and connect them to networks outside a company's perimeter defenses. The devices can more easily become infected, and subsequently give an intruder access to a corporate network once the device returns inside the perimeter.

A note about encryption

The impact of a data breach can be lessened if sensitive data stored in databases is encrypted. Most of the time it isn't. When data is encrypted, hackers can't locate encryption keys on the server or extract information from running memory on a server.

Return to Checklist

PRACTICE PRIVACY

Require system users have unique usernames and passwords that change, at a minimum, on a quarterly basis.

The power of passwords

Identifying information is all over the Internet, and identity thieves do everything they can to get what they need. However, users can make it harder for them by creating-and remembering more secure, hard-to-hack passwords.

3 tips for more secure passwords

1. Have more than one

Using the same password everywhere is dangerous. Make each password different. A simple trick is to use the last four letters of the website or company name somewhere within the password. Associating the site with the password will make it easier to remember.

2. Get creative

Names spelled backwards, birth dates, pets' names, or phone numbers are highly common and easily breakable choices for passwords. Either avoid them or invent a new approach, such as typing one row up, so "kip" becomes "i80".

3. Make a template

Passwords that follow a format, but contain different characters are both memorable and hard for hackers to guess. A certain number of letters, followed by a special character like a pound sign, then followed by a group of numbers is just one example; UIO#1206 or SJO#0817 both follow the same format, but could be used for different sites. Just make sure that the letters and numbers are meaningful enough to be memorable.

Other helpful password suggestions

Password manager software

Using strong passwords that vary on different accounts is good advice for online security and privacy. The problem is, it's not easy to remember all those hard-to-crack passwords without a cheat sheet that could be pilfered.

A dedicated password manager software can help you store and organize different passwords and PIN codes. Some even allow you to create one master password, and then update variations and/or work as form fillers to automatically enter log-in information.

Password strength checkers

Strong passwords ideally contain at least 12 characters and mix uppercase and lowercase letters, numbers and symbols. Although passwords with at least eight characters have long been advised, studies show that hackers using automated programs and their own ingenuity can break an eight-character password in a few hours, whereas adding four keystrokes could raise that to a theoretical 17,000 years.
No matter how long, it's wise to gauge password strength with free checkers.

Return to Checklist

LOCK UP SENSITIVE DATA

Keep all confidential information stored in a safe place.

Don't forget the basics

Today with the various cyberthreats, the focus is often too much about computer security. It's imperative you implement concrete policies on employee theft, visitors in the office and physical building security.

A safe work environment is an effective work environment

The practice of good office security coupled with sound control practices is essential to office safety and data security.

Here are a few keys:

- Pay attention to office security before, during, and after hours
- Keep well-lit the opening, closing and parking areas for employees, clients and visitor security
- Enforce visitor security with clear check-in, check-out procedures
- Lock file cabinets and areas where sensitive data and financial records are kept
- Keep servers and sensitive computer data in separate locked areas

Return to Checklist

GET ORGANIZED

Only collect and keep data that is absolutely necessary.

Improper data retention on databases is a problem

In the Epsilon breach, for example, hackers accessed sensitive information from consumers who opted out of services. That data should have been deleted.

Be sure to establish a protocol for the removal of unnecessary data on a regular basis.

Don't use sensitive data in nonproduction databases for testing

This practice, particularly the use of whole tables with real data, should be avoided at all costs. Testing datasets that do not relate to real data are the best way to limit your exposure.

Stop improperly deleting data backups and database dumps from server

Administrators often dump tables from the database on the same server, and then they simply delete them, instead of executing a secure deletion. Hackers have discovered that those dumps actually provide decrypted, sensitive consumer data that's easy to recover.

Check web server settings

Database backups can be found online when there are improper settings on a web server directory. Administrators often dump databases on the Internet web server and leave them in the folder, where Google finds them, indexes them, and data are exposed. Ensure secure deletion after dumping database data on a publicly available Internet server.

Secure your email

In general, email as it is the most insecure method of communication we use. It can be intercepted and falsified. When the stakes are high, remember to use additional methods of verification and encrypt any sensitive information that you send via email.

Return to Checklist

START SCREENING

Have all employees who can access sensitive information sign a confidentiality and security document.

Vet and verify

Employees play a key role in the security of our business. Good hiring practices are critical to success. This includes the proper vetting, verification, on-boarding, orientation and training of employees. It is especially important to have good security practices when an employee leaves the company, whatever the reason.

Screening tips for employers

- Keep background screening limited to relevant positions. For example, check driving records only for positions that involve operating a vehicle.
- Develop specific criteria for performing background checks and put it in writing.
- Evaluate the use of background checks when hiring new employees. By eliminating unnecessary screening, employers can eliminate the risk of a costly legal battle.

Return to Checklist

ESTABLISH A ROUTINE

Review data practices and security procedures at least once a year.

General security tips to consider

- Implement a "clean desk" policy so sensitive information isn't just sitting out for anyone to take or copy
- Have shredders available and shredding policies in place for documents with personal identifiers such as Social Security numbers and other sensitive information
- Require the use of secure passwords
- Develop policies and audit practices against posting passwords on notes near computers
- Set all workstations to have automatic screen time-outs that require passwords to regain access

Use machine learning and predictive analytics

Tracking exploitable high-value assets, user behavior, and flagging abnormal or malicious activities is the most effective and fastest way to identify the critical security events that need immediate action and/or remediation.

Security tips pertaining to database security

- Test databases that are part of an Internet web portal. SQL injection and Cross Site Scripting are the most common exposure on many systems, and they are most likely leveraged by hackers
- Monitor database servers for intrusion activities from system and application requests
- Implement firewall and perimeter protection that can filter web attacks such as SQL injection and XSS.

Return to Checklist

GET INFORMED

Perform an overall security assessment to pinpoint weaknesses.

Security as a path taken, rather than a destination reached

Reviewing these recommended steps will help you better understand the risks posed to your business.

Build a solid foundation

1. Understand your threat environment—Operating risk vs. Fraud

Operating risk is anything that can go wrong with your business. This can be human error, a computer crash or a flood.

Fraud is a type of operating risk, but should be considered separately as it's a deliberate act and requires a different management treatment.

What internal and external operating risks and fraud opportunities is your business exposed to?

2. Understand the tenets of security risk management

If we think of your business as a pie chart, one slice may be product development; another may be sales and marketing; another operations and systems. Whatever your business, Security Risk Management should be in that pie chart—as an integrated slice of your business. Integration is tenet No. 1.

3. Know your security team

Your security team starts at the top:

CEO/Principal/Owner
If the top of the house doesn't understand his or her invested stake, no one will.

Officers/Executives
They determine roles and model security-conscious behavior. This is how a protection culture is built.

System Admin/Technical
The nuts and bolts of your tech security.

Legal Counsel and Compliance
To keep the whole team abreast of changing legal and compliance considerations.

Employees
Similar to the top of the house, if people doing your business and handling your data aren't on-board and executing, the best policies in the world are useless.

4. Establish security policies and practices

When drafting policies, ask yourself what assets need to be protected. What is valuable in your business? Computer code or cash, real estate or heavy metals, your type of business will guide you. With policies to protect those assets in place, publish them. Communicate them to everyone on your team and train employees in implementing them.

5. Continuity of Business and Disaster Recovery Planning

Have a plan to mitigate risk during a power failure or computer crashes

Six steps to follow:

- Identify threats to your business continuity
- Assign responsibility and ownership of business continuity to appropriate members of your management team and insure that all threats are covered
- Develop a realistic plan
- Have data backup and off-site storage in place now
- Test the plan
- Review and update the plan as needed and at least annually

6. Employees/Staff Privacy Policy/ Privacy on Information Regulation

Many businesses are regulated. They have a legal and ethical requirement to maintain privacy of employees and customer records. Know your industry. Certain records, like protected health information, require very specific protections. Plan for them.

Build sound management practices

1. Have a "How-to Plan" for managing an information breach

When a breach happens it's critical to:

- Identify — Escalate to the appropriate management and subject matter expert resources within the organization to initiate the launch of a deliberate breach response plan
- Investigate — Implement a structured process and appropriate resources to determine source, scope, duration and cause
- Report and notify — Inform both internally and externally as company policy, your contractual commitments and the law may require.
- Remediate and recover — Stop the immediate information leakage and fix the problem.
- Assist — It makes moral, business and financial sense to help the people your breach may have jeopardized. This can be through offering a victim assistance service which is appropriate to the facts, circumstances and nature of the breach and compromised information. This may include providing them with the opportunity to review their credit reports and on-going credit and public records monitoring through reputable services.

Return to Checklist

TRAIN EMPLOYEES

Educate staff about how to follow security best practices and spot potential data exposures.

Start a culture of security

Begin educating employees about your organization's data security practices during new-hire orientation sessions. Make the discussion about more than just login credentials and help desk phone numbers. Use it as an opportunity to discuss the company's commitment to protecting sensitive company and customer data.

Give HR, IT and managers the tools they need to begin engaging new employees in a two-way conversation about data protection and the organization's expectations.

New-hire orientations are also a good time to present new workers with a copy of the processes and procedures they'll need to follow to safely access sensitive data within your corporate network.

It's vital to emphasize to new employees that data security is important, as well as to follow up with frequent reminders and point-in-time instruction to provide reinforcement.

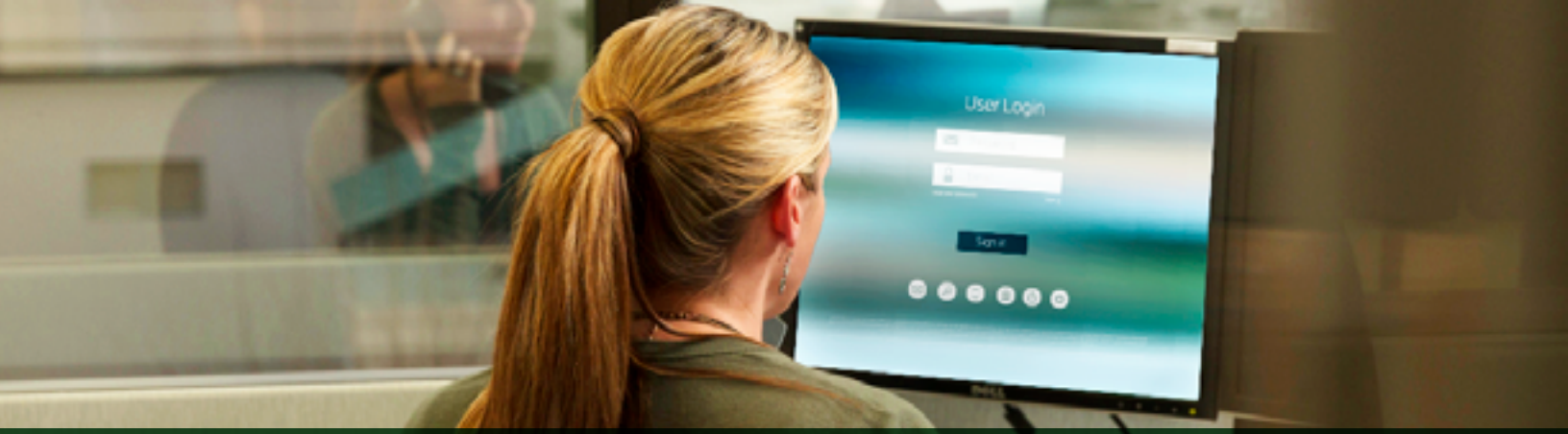
Management can create an environment where employees feel comfortable to ask questions and get clarification on any procedures they don't fully understand by being proactive in raising the topic of conversation in a non-threatening way.

HR can take steps to provide training when an employee's job duties change in such a way that warrants a different perspective or level of security. New supervisors will need to understand any expanded obligations on being attentive to the security practices of every role in his or her group, as well as specific reporting requirements like mandatory notification from state laws.

Managing security related to personnel turnover

Hiring and firing are the two critical times when you need to have tight employee practices in place. Make sure your company has a policy and operational execution against that policy that looks at data protection, remote access and computer account privileges during terminations that provide for securing company property, password changeovers within the company and outside vendors coupled with a good theft prevention plan.

Return to Checklist



CONTROL ACCESS

Regulate physical access to computers, reduce the number of privileged accounts and record all the logins and activities.

Database security

Database security is an essential element of overall security maturity at enterprise level. Underestimating its value and not dedicating sufficient attention to developing a comprehensive data security plan can, in many instances, lead to data compromise.

- Install proper access controls — Ensure proper integration of databases and resources that require access. Not having proper access controls in place often leads to a breach
- Limit credentials — It can be a problem when database access with the highest privilege is granted to all team members. Hacking these accounts can open all doors to the whole network. Limiting credentials, especially on critical systems, adds another layer of protection
- Insist on proper authentication — Applications can bypass authentication. Ensure that all applications require proper authentication

Check and double-check third-party contracts

If you hire third-party vendors or consultants, make sure their data practices are as safe as your own – especially if they handle or have access to sensitive data within your organization.

All contracts with third parties that handle your data should address specific data-handling and security practices. A must-have clause: If data is lost or otherwise compromised, your company will be notified within 24 hours or less of discovery.

Six security steps to help mitigate the risk from third-party vendors

If your company depends on collaborating with third-party contractors and suppliers, follow these steps to better protect yourself from a breach.

CONTROL ACCESS

1. Implement restrictive access controls

This may include restriction to certain times of day, or maintenance windows. Access may also be restricted to occur through a separate VPN (or like) device, where monitoring and logging can occur at a much higher level of fidelity.

2. Implement Two-Factor Authentication

Have third-party vendors provide two means of identification from separate categories of credentials. The first, perhaps being a physical token, like a card, and the second is something memorized, like a security code.

3. Designate IP addresses

Only allow the third party to use a designated IP address and protocols necessary for the communication. This limits the ability of the attacker to launch attacks from the attacker IP addresses, using stolen credentials.

4. Ensure environment

Enforce that their environment is configured to alert to geolocation, time, number of devices connected to, etc. If the vendor does not have a need to conduct Remote Desktop Protocol, then that should be explicitly prohibited, or alerted as a high fidelity event if attempted, at a minimum.

5. Implement application whitelisting

Do your best to prevent unauthorized programs from running on systems touched by the third-party vendor.

6. Audit more

Continuously inspect all third-party accounts, especially privileged accounts. Ensure that the third party is verifying, in writing, the continuing need for a specified account credential.

Return to Checklist

STAY VIGILANT

Be attentive around network intrusions and keep antivirus software up to date.

Install antivirus, anti-spyware and firewalls

Keeping computers in good-working order not only enhances the online experience, it can help make attacks from malware, viruses and spammers more obvious.

Here are four steps to help keep you protected:

1. Turn on Automatic Updates

This will make sure you have the latest software patches, which are usually published to fix known bugs and security flaws.

2. Run an antivirus program

Make sure to run an antivirus program and set it to automatically update and scan your system, at least once a week.

3. Search for malware

Run some kind of malware, or hostile software, removal program. There are several free programs available for personal use that will scan your system and help keep your computer safe.

4. Run a firewall

Don't believe the myth that they slow down your computer significantly. Windows, Linux and Mac all have built-in firewalls, which are far better than nothing at all.

Security Software

Without some type of anti-virus or anti-malware software, even surfing the Internet can be risky. For the best protection, opt for more comprehensive security suite products that may be labeled as "total," "platinum" or "360" versus those simply noted as anti-virus or anti-malware.

Don't forget to install security software on your smartphones and tablets, which are increasingly vulnerable to malware attacks. Many service providers have free antivirus and malware protection software, but some offer no-cost security suite products, especially for customers who bundle various services.

STAY VIGILANT

Firewalls and Router Security

A firewall is software or hardware that checks information coming from the Internet or a network, and then either blocks it or allows it to pass through to your computer, depending on the computer's settings.

Check privacy settings

A good first step is to check the privacy settings on Facebook, Google Groups, Windows or anywhere else. Virtually any website can track your online activity without your knowledge, and many online services offer different levels of control to prevent the potential sharing of your online searches and website visits. Although setting up privacy controls at individual websites can be time-consuming, it can help protect you.

What you need to know about ransomware

What is it?

Ransomwear is a type of malicious software designed to block access to a computer system until a sum of money is paid. There is little debate that ransomware is a common form of attack. Almost everyone at least knows someone who has been a victim of ransomware.

How to get it

Ransomwear can be tricky to avoid especially now that clicking a link in an email or opening an attachment is unnecessary for it to infect your system. These days, it is embedded in websites of companies that just didn't take the time or effort to secure their Website. Or, the malicious code is delivered by an advertisement that the attacker buys on the legitimate Website. All you have to do in order to become infected is browse a regular Website. Even if you don't click a single link, the ransomware can download onto your computer. Current versions don't install in the traditional manner, so it sneaks by most of the defense tools we have in place. If you pay the ransom, you get your files unlocked. While earlier versions requested larger sums of money for ransom, current demands are for smaller amounts such that most businesses can pay it quickly without waiting for insurance.

How to beat it

The secret about ransomware is that you do not have to pay the ransom if you have a recent backup. Many companies find themselves without a backup and have to wrestle with paying a ransom or suffering a loss. Having a solid, accessible backup is a basic IT function. Unfortunately, a large percentage of companies respond to ransom demands because it was assumed (but not verified) that a viable backup existed.

Return to Checklist

SOURCES

"5 Reasons Why Cyber Security Matters for SMBs" By Matt Cullina

"What You (and Your Employer) Should Know About Background Checks" By IDT911

"15 Unsafe Security Practices That Lead to Data Breaches" By Ondrej Krehel, IDT911

"Convenience of mobile computing comes at a security cost" By, Rodika Tollefson, ThirdCertainty

"Public Computers: Convenience vs. Security" By Matt Cullina

"Steps to Smarter Security" By Brian McGinley, IDT911

"Clean That Machine: Tips on Keeping Your PC Up and Running Fast" by Ondrej Krehel

"Six Privacy Safeguard Tips" By Eduard Goodman

Return to Checklist