THINK IT THROUGH

CYBERSECURITY

Cybersecurity Checklist

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

- □ Avoid 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

Avoid public Wi-Fi

Don’t use unsecured wireless networks when accessing systems that store sensitive or 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.

Take simple public Wi-Fi security measures:

Enable Secure Sockets Layer (SSL).

Before taking off on a trip, enable 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. Most social media and email platforms offer 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.

Disable Wi-Fi on your computer before heading out to the airport or other destinations where public networks are available. This will 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, Wi-Fi can safely be turned back on.

Use a Virtual Private Network (VPN).

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

Avoid public Wi-Fi

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

Take caution.

Public computers don't always have anti-spyware programs installed, so extra precautions are 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 you out of a website, which means your information could be accessible to the next person who uses the computer. Make sure websites, especially social networks, don't automatically save your login information on the computer.

Browse privately.

Selecting "browse privately" or "incognito window" will erase your tracks on a public computer. Deleting the history and temporary Internet files once you're done using the computer is another smart step.

Return to Checklist

Limit the use of portable tech

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

Portable tech is problematic.

Few companies or consumers are prepared for the security and privacy risks that arise from using smartphones and tablets in every aspect of work and home life.

New technology means new issues.

Smartphones and tablets aren't 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 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 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 are at work.

The discovery of fresh security flaws in mobile operating systems (OS), and the subsequent patching exercises, are following the same trajectory as what happened with desktop computing.

It's safe to say there will be no shortage of freshly discovered mobile OS security flaws going forward. In an analysis of 7 million mobile apps on Android and iOS platforms, FireEye found a significant increase in vulnerabilities since 2011.

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

Limit the use of portable tech

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. Furthermore, when data is encrypted, most states do not require notification after a potential data breach becomes known.

Return to Checklist

Practice privacy

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

Passwords are powerful.

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.

Tips for more secure passwords:

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.

Get creative.

Names spelled backward, 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."

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.

Practice privacy

Other helpful password suggestions:

Consider password manager software.

Using strong passwords that vary for different accounts is good advice to improve 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.

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

Use 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. 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.

While it’s important to focus on computer security, it’s imperative you also implement concrete policies on employee theft, visitors in the office, and physical building security.

A safe work environment is an effective work environment.

Good office security coupled with sound control practices is essential for office safety and data security.

Here are a few keys:

- Pay attention to office security before, during, and after hours.
- Keep entrances, exits, and parking areas well-lit for the security of employees, clients, and visitors.
- Enforce visitor security with clear check-in and 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's absolutely necessary.

Improper data retention 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 don't relate to real data is the best way to limit your exposure.

Stop improperly deleting data backups and database dumps from the server.
Administrators often dump tables from the database on the same server, and then 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 exposes data. Ensure secure deletion after dumping database data on a publicly available Internet server.

Secure your email.
In general, email 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 your business. Good hiring practices are critical to success. This includes proper vetting, verification, onboarding, orientation, and training of employees. It's 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 policies 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.

Consider these general security tips:

- 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, monitoring user behavior, and flagging abnormal or malicious activities are the most effective and fastest ways 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 (XSS) are the most common exposures on many systems, and they're 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 is a path, not a destination.

Reviewing these recommended steps will help you better understand how your business is vulnerable to risk.

Build a solid foundation.

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 approach.

How is your business exposed to internal and external operating risks or opportunities for fraud?

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.

→

Get informed

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 Administrators/Technical Support
These employees are the nuts and bolts of your tech security.

Legal Counsel and Compliance
They help 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.

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. Once you institute policies to protect those assets, make sure to also publish them. Communicate them to everyone on your team and train employees in implementing them.

Plan for continuity of business and disaster recovery.

Have a plan to mitigate risk during power failures or computer crashes.

Steps to follow:

- Identify threats to your business continuity.
- Assign responsibility and ownership of business continuity to appropriate members of your management team and ensure 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.

Get informed

Know industry regulations regarding employee privacy.

Many businesses are regulated. They have a legal and ethical requirement to maintain the 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.

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 experts 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 affected parties both internally and externally, as required by law, company policy, and contractual commitments.

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. Consider offering a victim assistance service that’s appropriate to the facts and circumstances of the breach and the nature of the compromised information. This may include providing victims with the opportunity to review their credit reports and ongoing credit and public records monitoring through reputable services.

Return to Checklist

Train employees

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

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 in order to safely access sensitive data within your corporate network.

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

By proactively engaging on the topic in a nonthreatening way, management can create an environment where employees feel comfortable asking questions or getting clarification on procedures they don't fully understand.

HR should provide training when an employee's job duties change in such a way that warrants a different perspective or level of security. New supervisors should fully understand additional responsibilities. Expanded obligations may include being attentive to subordinates' security practices, as well as state law and mandatory notification requirements.

Train employees

Manage security related to personnel turnover.

Hiring and firing are two critical times when you need to have tight employee practices in place. Make sure your company maintains and executes a policy that considers data protection, remote access, and computer account privileges during terminations. The policy should allow for securing company property, outline the process for password changeovers within the company, and address needs for outside vendors. Finally, maintain a comprehensive theft prevention plan.

Return to Checklist

Control access

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

Improve database security.

Take precautions to avoid data compromise.

Database security is an essential element of overall security maturity at the 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 the highest privilege of database access is granted to all team members. Hacking these accounts can open 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.

Control access

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.

Security steps to help mitigate the risk from third-party vendors:

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.

Implement two-factor authentication.

Have third-party vendors provide two means of identification from separate categories of credentials. The first can be a physical token, such as a card. The second can be a memorized security code or something similar.

Designate IP addresses.

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

Manage the environment.

Configure a vendor's environment to alert to geolocation, time, number of devices connected, 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.

Implement application whitelisting.

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

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 programs, anti-spyware software, 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.

Steps to help keep you protected:

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.

Run an antivirus program.
Make sure to run an antivirus program and set it to automatically update and scan your system, preferably on a daily basis.

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.

Run a firewall.
Don’t believe the myth that they slow down your computer significantly. Windows, Linux, and Mac all have built-in firewalls.

➡

Stay vigilant

Install security software.

Without some type of antivirus 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 antivirus 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, and some offer no-cost security suite products, especially for customers who bundle various services.

Use firewalls and router security.

A firewall is software or hardware that checks information coming from the Internet or a network, 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.

Stay vigilant

What you need to know about ransomware:

What is it?

Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid. It's becoming an increasingly bigger concern for business owners as cybercriminals continue to shift their target from consumers to enterprise networks. This malicious software has the potential to bring an organization's operations to a halt, blocking access to important information and sometimes wiping out all of a company's existing data in the long term.

How to get it:

Ransomware can be tricky to avoid. You don't have to click a link in an email or open an attachment in order for it to infect your system. The attacker can embed malicious code in an unsecured website, or purchase an ad on a legitimate website and embed it with code. 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 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, and most businesses can pay quickly without waiting for insurance.

How to beat it:

The secret about ransomware is that you don't have to pay the ransom if you have a recent backup. Many companies find themselves without a backup and have to decide between paying a ransom or suffering a loss. Having a solid, accessible backup is a basic IT function. Unfortunately, a large percentage of companies are forced to 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 CyberScout

15 Unsafe Security Practices That Lead to Data Breaches by Ondrej Krehel, CyberScout

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, CyberScout

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