YEO & YEO

TECHNOLOGY

Cybersecurity eBook

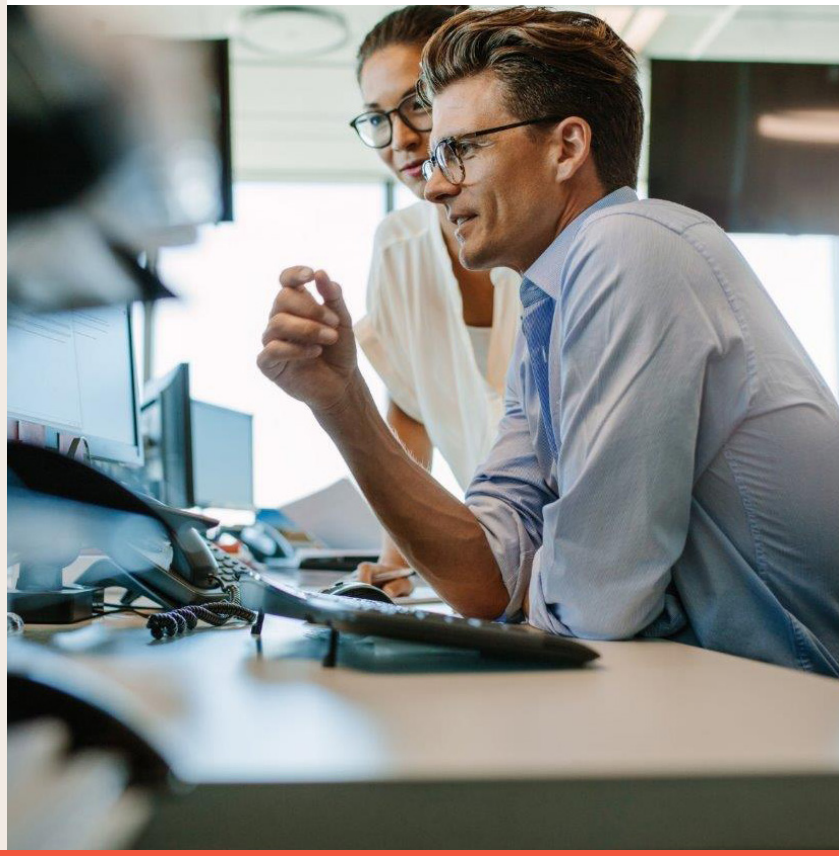
INSIGHTS & TIPS FOR BUSINESSES & ORGANIZATIONS

Contents

INTRODUCTION

As our reliance on technology grows, the risk of individual and commercial cyberattacks increases as well. Hackers now have more opportunities to steal sensitive data than ever before.

Yeo & Yeo Technology understands the importance of protecting your business assets. We're here to help by providing holistic services like managed IT, software, security awareness training, and IT consulting to clients throughout Michigan and beyond. Our expertise in technology spans more than 30 years, and our skilled professionals are ready to offer cybersecurity solutions to enhance and protect your business.



Types of Cyberattacks to Watch For

Cyber threats are evolving at a rapid pace – tactics and attack methods are changing and improving daily. The following are a variety of cyberattack methods to be aware of and information to help protect your business against them.

PHISHING

Many people are familiar with phishing schemes, even if they do not know the term. Phishing is a type of cyberattack that involves maliciously misleading someone into providing confidential information through the illusion of a trusted source.

HOW IT WORKS

Cybercriminals are constantly looking for ways to steal personal information. Let's look at a specific example of a common phishing attempt that people often experience.

A phisher creates a fake website that incorporates elements that very closely resemble the company they are attempting to impersonate, such as logos, content, and overall branding. These sites typically include the original domain address but have one extra letter, a slightly misspelled word, etc. – small changes that one might easily miss.

The cybercriminal then sends a message to the user of that company with a link to the fraudulent site, urgently asking them to click on the link to address a hacked account, unauthorized purchase, etc. When the user clicks on the link, they are directed to the website where the attacker (who is monitoring the page) steals their login credentials to gain access to secured areas on the legitimate site.

When the user logs in, an undetected malicious web code activates to seize the user's session cookies. Once this occurs, a reflected XSS attack executes, providing the offender privileged access to the network. When the cybercriminal receives access to the network, its data is compromised.

COMMON RED FLAGS TO LOOK FOR IN PHISHING SCAMS INCLUDE:

- Misspellings or grammatical errors
- A sense of urgency in the message
- A request to click on a link or provide private information

It is vital for one to keep a watchful eye on every email and message for red flags that may indicate a phishing attempt.

TYPES OF PHISHING

1. **Basic phishing:** Email is the most common form of general phishing that involves a scammer sending a dishonest message to a random user, prompting them to click on a fraudulent link. A cybercriminal might send a fraudulent email to a user promoting a free account upgrade and ask them to provide login credentials, banking details, etc., to claim the offer.
2. **Spear phishing:** Spear phishing is a method that targets individuals of an organization, requiring prior research into the target's background. A spear phisher might send an email that includes the victim's name and level of authority to make it appear more "personal."EMU Foundation
3. **Smishing and vishing:** While phishing primarily utilizes emails to target an individual, smishing uses text messaging and vishing employs phone calls and voicemails. A smishing attempt might seem more believable depending on the type of language a cybercriminal uses, making it easier to click on the link provided in the text message. Vishing can be even more difficult to detect as cybercriminals might call about your car warranty or even record your voice and ask a question that requires a "yes" answer. For example, they might ask, "Is this [insert name]?" or "Can you hear me properly?" Once the victim answers, "yes," the cybercriminal then creates a voiceprint of the answer and uses it to pose as the victim when verifying identity in their accounts.
4. **Whaling:** Whaling is another form of a targeted attack aimed specifically at senior-level executives. Instead of generic phishing emails, whaling is a bit more high-level; a scammer might craft an email with a solid understanding of business language and tone, prompting the professional to conduct a secondary act like wire or transfer funds.

EMERGING TRENDS

Today, cybercriminals have become adept at disguising their emails and websites to look like legitimate businesses. As society continues to place a focus on the mobile market, cybercriminals will develop scams that are increasingly sophisticated. Today's scams are now designed for mobile devices and are often shorter and more direct than those designed for desktop computers.

Cybercriminals looking to enter cybercrime can now "rent" phishing kits from Phishing-as-a-service (PaaS) to create malicious content and software for cyberattacks. This service operates similarly to the legitimate business model, Software-as-a-service (SaaS).

Phishing attacks increased by 29% worldwide in 2021.

IMPACT AND ACTION

Business professionals – beginners and seasoned – are common targets of phishing scams due to their primary communication and business data existing within email platforms. They also maintain large email accounts, so cybercriminals may find them easy targets for their schemes.

The effect of a successful phishing attempt is critical and often detrimental to businesses of all sizes.

- Financial losses
- Damaged reputation
- Disruption of operational activities
- Loss of staff

Yeo & Yeo can provide your business with email protection solutions such as email spam filtering, archiving, encryption, advanced threat protection, and more. Organizations and individuals must stay vigilant to protect their assets, and partnering with experts like Yeo & Yeo Technology is the first solution.

MALWARE

Malware is malicious software designed to damage or gain access to a computer system. Once it is on the computer, malware can collect personal information, delete files, and even take control of your computer. Malware can take the form of a worm that digs deep into a system and replicates itself between devices, or a virus that requires a user to click on a link, attachment, etc.

A 2022 Verizon Data Breach Investigations Report found that over 80% of data breaches involve stolen credentials.

HOW IT WORKS

Cybercriminals have a variety of programming languages they can choose from to create their malicious programs. These coding languages differ based on the intent behind the creation. For example, Python is the most commonly used language that targets remote servers. Mobile malware is often developed using JavaScript because many Android apps are created using the same language.
When a user clicks or downloads a false link or program, the malware's code begins to execute the tasks for which it was created. These tasks can include:

- Self-replication
- Blocking access to files or the system (can force the user to make a payment to regain access)
- Installing applications that commandeer the system without the user's knowledge and monitoring the user's behavior
- Damaging the system's critical elements, rendering the device inoperable
- Malware can also be camouflaged as programs meant to help you, such as PDF converters, MP3 files, and more.

TYPES OF MALWARE

1. **Adware:** Adware (advertisement-supportive software) displays unwanted pop-up advertisements on a user's device, intended to generate clicks.
2. **Worms:** Worm malware is a self-contained virus intended to replicate itself once it enters a user's device. Its purpose is to burrow through the user's operating system (OS) without their knowledge and exploit hidden vulnerabilities.
3. **Ransomware:** This type of malicious malware is designed to damage a system and halt its function until a ransom is paid to the cybercriminal. This may also be known as denial of service (DoS), in which a cybercriminal invades a network to disrupt the service.
4. **Rootkits and botnets:** A rootkit is software that is installed on a user's computer without their knowledge via exploitation of the system's vulnerabilities. Once installed, a cybercriminal uses a robot (also known as "Bot") within the software to take complete control over the computer system while remaining anonymous. This system is then added to a network of controlled computers called "botnets."
5. **Fileless malware:** Fileless malware uses legitimate programs to infect a computer system. It does not rely on established files and leaves no footprint, making it more difficult for a user to detect and remove the malware.

6. **Malvertising:** Malvertising is the act of injecting malicious code into legitimate advertisements on publishers' websites, redirecting users to the cybercriminals' false sites.
7. **Spyware:** Spyware is discreetly installed on a user's device and spies on their behavior. This software is designed to steal valuable information, usage data, etc., and share the report with advertisers, data firms, or external sources.
8. **Trojans:** Trojan malware is downloaded to a user's system, disguised as a legitimate program that might appeal to the system's owner. Trojans are used to gain unauthorized access to the user's private data.

EMERGING TRENDS

Cybercriminals constantly develop new methods to steal confidential information, leading to the continued construction of a professional cybercrime "business model." The market for ransomware now consists of ransomware-as-a-service (RaaS). Cybercriminals are hired to act as payment negotiators, malicious code developers, and more, to effectively execute malware cyberattacks.

IMPACT AND ACTION

Malware attacks can cause substantial damage to businesses as they not only lose the protection of their assets but are often forced to pay a ransom to regain access. This results in significant financial losses as well as loss of the public's trust in their security.

Yeo & Yeo Technology provides **managed IT services** to help you build a stronger network, by combining standard preventative maintenance with comprehensive, real-time monitoring of your network and devices.

The banking, manufacturing, education, and healthcare industries are often the highest targeted victims of malware simply due to the basic need for their services. If these industries are prevented from providing their assets to the public, cybercriminals believe they will be more likely to pay a ransom to resume business.

PASSWORD ATTACKS

A password attack is a type of cyberattack in which cybercriminals attempt to guess or brute force their way into a victim's account by trying out different combinations of usernames and passwords.

HOW IT WORKS

Passwords create a wall of security between the user's account and external sources, but they can be an easy way for cybercriminals to hack into a user's system.

Cybercriminals often implement various techniques to explore private passwords, including brute force, guessing, and more. Once the attacker solves the password, they use that information to log into the user's account (typically multiple accounts) and gain access to their private data to use or share with their external sources.

If a victim uses a password consisting of only seven characters, an attacker can crack it in 31 seconds.

TYPES OF PASSWORD ATTACKS

1. **Man-in-the-Middle (MitM):** This kind of attack involves a third party intercepting the user's data while in transit.
2. **Brute force:** The main method of brute force attacks involves experimenting with various combinations of letters, numbers, and symbols – character by character – to "guess" the correct password.
3. **Dictionary:** A dictionary password attack consists of filtering through a list of common words and phrases that a user might incorporate into their passwords.
4. **Credential stuffing:** When a data breach occurs and the user does not change their credentials immediately, an attacker might use credential stuffing – the act of attempting former usernames and passwords – to gain access to the account.
5. **Keyloggers:** A keylogger is a program designed to track a user's every keystroke and report it back to the attacker. They will apply any keystrokes used for logins to steal the user's data and access their account.

EMERGING TRENDS

As society continues to see an increase in cyber breaches, many cybercriminals are quickly taking advantage of the credential stuffing method – stealing users' passwords before they have a chance to change them.

IMPACT AND ACTION

If a company does not have the resources necessary to appropriately detect a data breach, it can experience substantial financial loss, leading to costly recovery solutions. Yeo & Yeo's **SEIM Solutions** provide businesses with rigorous cybersecurity by monitoring their network every second of the day, 365 days a year.

If a threat is discovered, an alert is immediately sent to your internal IT team or our help-desk where our cybersecurity professionals can isolate, diagnose, and remediate potential cyberattacks.
Common target victims of password attacks are individuals who reuse the same password across various platforms and businesses. Cybercriminals will often seek accounts and systems like these that are "easy" to hack into.

Time it Takes a Hacker to Brute Force Your Password in 2022

Number of Characters	Number Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467 bn years	11tn years	438tn years

SOCIAL ENGINEERING

Social engineering is one of many tactics cybercriminals use to steal confidential information. This technique appeals to the user's natural instinct to trust others and manipulates that person into willingly providing personal data.

HOW IT WORKS

At its core, social engineering aims to take advantage of the victim's personal interests or emotional intelligence. This technique tricks the victim into revealing sensitive information or performing actions that will ultimately help the cybercriminal gain access to systems or data.

For example, a cybercriminal may use fear by convincing the victim they are under criminal investigation for tax fraud, or empathy by requesting the victim provide login credentials quickly or else employees will not be paid this week.

TYPES OF SOCIAL ENGINEERING

1. **Baiting:** This tactic involves providing the victim with an enticing promise, luring them into a trap designed to steal information or infect their system.
2. **Scareware:** Scareware most commonly manipulates people into believing they need to perform a specific action based on the fear that something bad will happen.
3. **Pretexting:** Cybercriminals are typically known as "bad actors." Using this technique, they will create believable stories and personas to persuade the victim into revealing information.
4. **Spear phishing:** As mentioned previously, spear phishing specifically targets individuals at an organization. In the context of social engineering, a cybercriminal might impersonate upper management or other trusted entity to urge employees to provide sensitive information or money to assist the company.

EMERGING TRENDS

"Deepfake" entertainment has risen in recent years due to its manipulation of artificial intelligence (AI) and high believability. Cybercriminals see deepfake entertainment as an opportunity to spread misinformation, discredit trusted sources, and spark outrage and hatred. For example, a cybercriminal may impersonate a grandchild on a video call using their image and likeness to extract money or sensitive information from a grandparent.

IMPACT AND ACTION

Due to the foundation of social engineering – manipulating people with stories, identity theft, and believability – this form of cybercrime is one of the biggest threats to a company's security. Yeo & Yeo Technology offers **Security Awareness Training** – an excellent way to educate employees on building a human firewall capable of preventing social engineering attacks.

It is part of our human nature to trust others and instinctively behave out of emotion. However, one can reduce their chances of falling into a social engineering trick by remaining vigilant and analyzing suspicious messages, phone calls, links, etc.

ZERO-DAY EXPLOITS

A zero-day exploit occurs when a cybercriminal exploits software vulnerabilities and releases malware without the victim's knowledge before they have an opportunity to create a patch for the security flaw.

HOW IT WORKS

Cybercriminals focusing on zero-day exploits may use a variety of techniques to find vulnerabilities in a system's code. They might manually sift through code on various systems, buy them on the black market, use bots to sort through code automatically, and more. Once a security flaw has been discovered, they quickly determine the most efficient plan of attack and develop a malicious program to exploit it. Then, they begin to infiltrate the system, remotely executing false code to compromise the machine.

TYPES OF ZERO-DAY EXPLOITS:

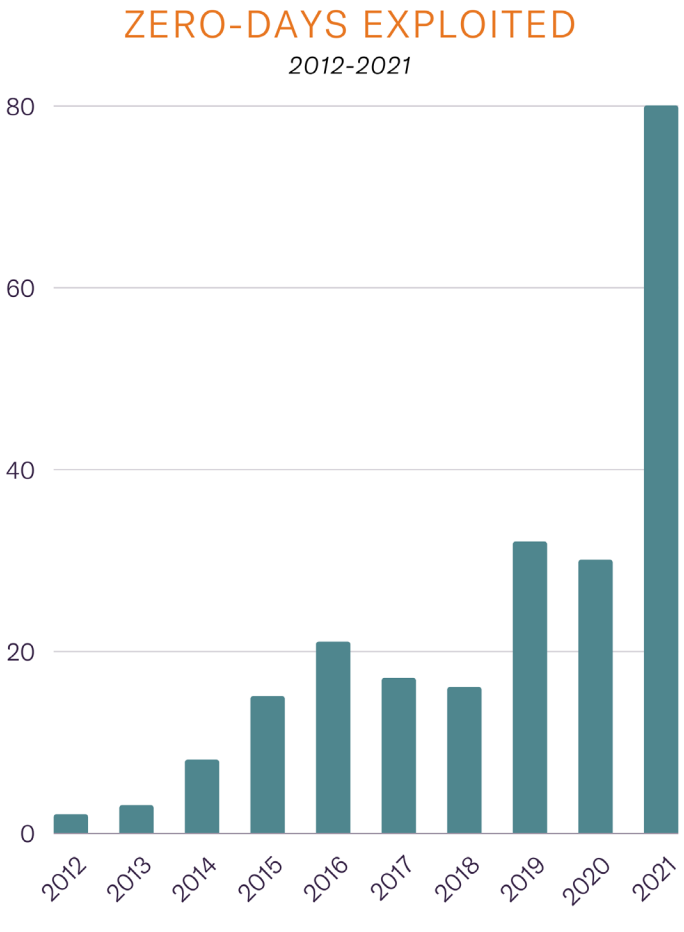
1. **Zero-day vulnerability:** The security flaw or fault that exists within a system – typically discovered after a cyberattack.
2. **Zero-day exploit:** The action of creating code or malicious software to exploit a system's vulnerabilities.
3. **Zero-day attack:** The cybercriminal steals valuable data from the system to sell or use it for other malicious purposes.

EMERGING TRENDS

Countries that do not have the talent or infrastructure to carry out cybercrimes are purchasing exploits sold on the black market, skyrocketing the rates of zero-day attacks.

IMPACT AND ACTION

The zero-day attack is perhaps one of the most damaging cyberattacks to exist because it operates by exploiting vulnerabilities before the business has a chance to protect its network. Yeo & Yeo Technology's **YeoDefense (EDR & XDR)** solutions are a smart addition to your cybersecurity team. Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) are designed to replace legacy, reactive approaches to cybersecurity.



REMOTE WORK VULNERABILITIES

Cybercriminals are taking advantage of the more recently implemented workplace model, remote work. With the increased use of home networks to complete work containing confidential information, vulnerabilities and cyberattacks grow as well.

According to LinkedIn, 25% of all jobs in North America will be remote by the end of 2022.

HOW IT WORKS

Remote workers need strong, reliable connectivity to successfully conduct business on the go or at home. They must also follow strict policies regarding concealing confidential information when they're not in the office. This can present a challenge for many companies that may have weak cybersecurity. Business professionals and small companies are at risk for remote work vulnerabilities due to the recent transition to the remote/hybrid model. New owners simply may not have the resources and funding to focus on cybersecurity, whereas work-from-home employees might not have a secure home network to protect their data from data breaches. Additionally, companies that enforce the bring-your-own-device (BYOD) policy might be saving on equipment costs. However, they also open the door to confidential business information and an employee's personal information to cohabitate, leading to various cyberattacks – and thousands of dollars wasted in data breach recovery.

TYPES OF REMOTE WORK VULNERABILITIES

1. **Lack of protocols:** When a business does not have clear, strict guidelines regarding remote work, it can become an easy target for cybercriminals to hack into its system and steal sensitive data. Established IT solutions are critical in maintaining a secure network.
2. **Unsecured home network:** An unsecured home network is an invitation for cybercriminals to hack into a user's system and access business information. Businesses can conduct cybersecurity training with employees to help reduce risk.
3. **Insufficient backup systems:** As today's workforce continues to focus on virtual productivity, a business must implement appropriate backup and recovery solutions to avoid cyberattacks or losing vital data from the system.
4. **Location of work may reduce security:** Remote work may present network security risks based on the employee's location alone. For example, if an employee works in a coffee shop, they're using public Wi-Fi, putting the company's information in jeopardy.

EMERGING TRENDS

More companies are choosing to implement remote work into their business model, leading us into a more technology-reliant society. Businesses are increasingly hiring freelancers to complete a portion of their projects, leading to further remote work vulnerabilities if they do not have secure IT solutions in place.

Cybercriminals are now targeting video conferencing platforms such as Zoom, Microsoft Teams, and more to gain access to sensitive information shared by businesses during virtual meetings.

IMPACT AND ACTION

Remote work offers benefits and challenges. Many companies are seeing a significant morale boost within their teams due to remote work. However, if they do not have the proper cybersecurity solutions in place, they can risk becoming the victim of cybercrime.

Equipping employees with the right tools when working from home takes many forms. To support workstation safety and productivity, ergonomic workstations, laptops, monitors, and docking stations may be provided. Similarly, equipping employees with virtual protection is important as well.

Whether your employees are hybrid, remote, or in-office, Yeo & Yeo Technology equips you with a layered approach to security that can lower your risk of an intruder getting into your business network via an unsecured home network.

CHECKLIST FOR REMOTE/ WORK-FROM-HOME EMPLOYEES:

- ✓ Do not open suspicious emails/texts, etc.
- ✓ Report suspicious messages to the IT department
- ✓ Utilize company-provided equipment for work purposes
- ✓ Do not share work devices
- ✓ Create a unique passcode for each work-related account
- ✓ Ensure home networks are secure
- ✓ Ensure your systems are up to date and patched. Our **YeoCare Managed Service** plans include patch management to keep your systems secure.
- ✓ Reach out to the IT department if you have any questions/concerns

Cybersecurity Statistics

600%

The rate that cybercrime increased during the COVID-19 pandemic.

$6 Trillion

The expected 2021 total cost worldwide of all cybercrime damages

Phishing attacks account for

90%

of all data breaches.

233 days

The average time financial institutions took to detect and address data breaches

95%

of organizations claim to provide phishing awareness training, but

30%

trained just a portion of their user base

90%

of healthcare staff in 2020 did not receive any updated cybersecurity training while working from home due to the COVID-19 pandemic.

Assessing Your Cybersecurity Risks

Yeo & Yeo Technology is committed to staying ahead of the curve to protect our clients from cyberattacks. While cybercriminals are always searching for new ways to exploit vulnerabilities, our team of experts is constantly working to develop new defenses using advanced technologies. By assessing your cybersecurity risks, you can identify threats quickly and block them before they can cause harm.

STEPS TO REDUCE POTENTIAL RISKS

Every business must take essential steps to mitigate risk and improve cybersecurity within their organization. Reference our checklist below to assess your IT solutions:

1. **Identify your assets and devices:** If your company is constantly growing, you"ll want to determine exactly which applications your business is connected to and who may still have access after a departure.
2. **Identify threats and vulnerabilities:** This may consist of running security tests throughout your infrastructure to discover potential vulnerabilities that a cybercriminal might exploit. For example, you may consider analyzing and regularly changing account credentials every three months.
3. **Assess the impact an attack would have:** Analyze various scenarios in which your company would experience a cyberattack - what potential software could be exploited? Who is involved in the recovery process? Be sure to ask these questions and assess how an attack could affect your business.
4. **Make a plan:** Preparation is key to minimizing damage when a cyberattack occurs. Follow these steps to develop a plan of defense and recovery: Prioritize risks, develop controls, develop continuous monitoring, reevaluate the plan regularly, and have backups in place.

TOP INDUSTRIES THAT MAY BE VULNERABLE TO CYBERATTACKS:

Finance: Cybercriminals target companies in finance due to the nature of the industry. They're often looking to receive financial payouts and will utilize any cyberattack available to do so. Some factors that make them more susceptible to targets:

- Increase in cashless transactions makes it easier for cybercriminals to intercept.
- To manage the cost of compliance, many financial institutions rely on third-party vendors for cybersecurity solutions.
- Cyberattacks significantly impact operations, so financial entities are more likely to pay a ransom.

Healthcare: The healthcare industry operates on confidentiality, making it attractive to cybercriminals. Factors that make the healthcare industry an enticing target:

- Limited technology budgets
- Sensitive patient information
- Attacks that steal, manipulate, or otherwise compromise patient information can negatively impact healthcare facilities' credibility and operations.

Small businesses: Small businesses are susceptible to cyberattacks due to their lack of resources to implement cybersecurity precautions. According to Security magazine in an article published in 2022, 60% of small business victims will permanently close within six months of a cyberattack. Additional factors that make small businesses an easy target for cybercriminals:

- Limited budget for cybersecurity solutions
- Restricted number of staff dedicated to IT
- Many first-time owners have sparse knowledge of which cybersecurity solutions are best suited for their business.

Education: The recent transition to online learning has made the education industry an appealing target for cybercrime. Some components that make the education sector appealing to cybercriminals:

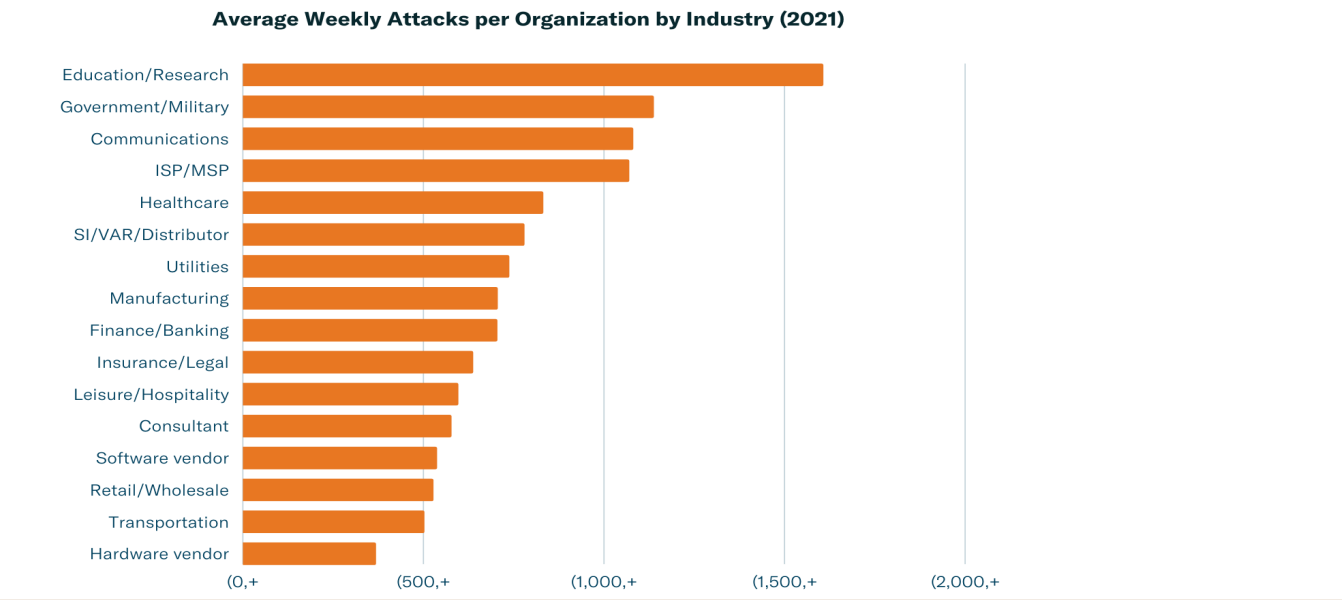
- Education has introduced technology as a core factor in children's learning programs.
- Teachers often utilize their own devices which may reduce cybersecurity.
- Education experiences frequent budget-related circumstances that limit resource availability for different departments, including IT.

Government: Many government entities are targeted with ransomware attacks due to their high-level profiles. In addition, cybercriminals aim to steal data from this sector due to their vast amount of confidential information. Factors that lead cybercriminals to government agencies:

- Government institutions contain highly sensitive information.
- State and local governments often do not have the same high-level budget as federal institutions.
- Many government organizations lean on third parties and contractors to manage specific sectors of their departments.

Manufacturing: As manufacturing organizations transition to conducting more work online, they may not have the expertise and resources needed to enforce high-quality security practices. Elements that make the manufacturing industry an easy target for cybercriminals:

- Manufacturers cannot afford to go offline at any point, making them more prone to ransomware attacks.
- Many multinational manufacturers have thin IT solutions to protect against cybercrime.
- Many manufacturing facilities tend to operate on outdated IT systems.



What to Do if a Breach Occurs

If a data breach occurs in your system, don't panic. Learn about the benefits of cybersecurity insurance and how to address cyberattacks if your business does not have insurance yet. Follow the steps outlined to manage a breach and determine the best practices you can take to recover any lost assets.

- ☑ **Contact your provider:** If your business has cyberinsurance, it's vital that you contact your cyberinsurance provider as soon as possible if your team detects a data breach. Many providers will be able to notify your customers of the breach, recover any compromised data, repair damage to computer systems, and more.
- ☑ **Contain the breach:** A few signs of a cyberattack include unusual or unexpected password changes, inbox activity, or account access from various sources. Once you've found the affected system, isolate the system(s) by disconnecting from the internet, limiting site traffic, disabling remote access, etc.
- ☑ **Report the attack to applicable parties:** You'll need to document the entire incident from the moment you noticed the attack to provide your team with as many details as possible. Your team may include a C-suite representative, HR, IT, PR, lead investigator, and anyone with a specific responsibility to manage the crisis. Review your state's laws for guidelines on when and how you can notify your customers about the data breach.
- ☑ **Investigate how the attack occurred and implement measures to prevent it from happening again:** How did the cyberattack occur? What events led to the attack? Determine any recent changes or transitions made to accounts or technologies that might have established your business as a target, and begin to implement measures to prevent it from happening in the future.
- ☑ **Conduct a thorough analysis of existing public info, sites, or content to ensure no private information was posted accidentally:** Many cybercriminals steal data to sell on the dark web for a large price. You'll want to take advantage of various resources that can provide information as to what was stolen from your business and where it might've been posted.
- ☑ **Consult with a legal team to determine state laws revolving around data breaches:** Your incident response team will help you conduct a thorough analysis of your system and what caused the attack. Cyberattacks are handled differently in each state, so be sure to check with your team about specific steps you can take to manage the crisis in your area.

General Tips to Enhance Your Cybersecurity

Cybercriminals target anyone with a network, online account, or any connection to technology. From top industries to remote employees to everyday consumers, it's essential to implement strategies to improve overall cybersecurity. Here are a few ways you can enhance cybersecurity within your organization.

EMAIL SECURITY SOLUTIONS

Whether communicating with co-workers, clients, or vendors, the majority of business transactions are conducted via email. Phishing emails often appear to come from legitimate sources and can be difficult to spot, making business professionals prime targets of phishing scams.

Yeo & Yeo Technology offers security protection solutions for your entire email infrastructure including:

- Email encryption
- Gateway defense
- Fraud protection
- Email archiving

USE A SECURE BUSINESS VIRTUAL PRIVATE NETWORK (VPN)

A VPN can provide your employees with an encrypted connection to your network whether they're in the office or remote. A VPN can prevent web traffic from entering your network, keeping your business assets secure.

CONSIDER A MANAGED SERVICE PROVIDER

Partnering with a managed service provider can significantly reduce the chances of a cyberattack within your network. Yeo & Yeo Technology's proactive IT solutions are tailored to your business needs and can support your existing IT infrastructure, or be fully managed by our team of engineers and technicians.

ADDRESS CYBERATTACKS EFFICIENTLY WITH CYBERSECURITY INSURANCE

While general insurance liability covers physical injuries or property damage, it does not cover damage sustained during a cyberattack. Cybersecurity insurance assists with:

- Notifying customers about a data breach
- Finding the root cause
- Recovering compromised data
- Implementing measures to prevent future attacks

Cybersecurity insurance can help your team address and recover assets from cyberattacks in an efficient and timely manner. Ask your response team to assess a cybersecurity insurance policy for your business and delve into precisely what is covered and what coverage you need. Check with your team to learn about the insurer's requirements as well.

12 Ways to Prevent Cyberattacks Checklist

While cyberattacks can happen to any business, there are proactive measures you can take to reduce your chances of a system security breach.

- ☑ **Security assessment:** You can complete a security assessment by analyzing any existing vulnerabilities, risks, and potential impact an attack might have.
- ☑ **Spam email:** If your business conducts transactions and communications primarily through email, Yeo & Yeo can help you choose the right service to reduce your staff's exposure to spam email.
- ☑ **Passwords:** Conduct a thorough analysis of your login credentials for each account your business is connected to and remove any unnecessary access.
- ☑ **Computer updates:** Updating your connected software is a smart way to consistently reduce your chances of a cyberattack. Yeo & Yeo provides managed IT services to ensure your systems are always up to date.
- ☑ **Firewall:** Schedule a call with Yeo & Yeo to learn how you can implement Intrusion Detection and Intrusion Prevention features into your system.
- ☑ **SIEM/Log management:** Meet compliance requirements and protect against cyberattacks by managing all event and security logs within your network via YeoSecure.
- ☑ **Security awareness:** Training your team on security awareness on a regular basis is critical to protecting your business.
- ☑ **Backups:** Be sure to systematically back up all of your data and have an offline copy. Test your backups regularly.
- ☑ **Encryption:** Encrypt any vital file on all devices used, whether active or inactive to prevent unauthorized access.
- ☑ **Advanced endpoint and detection response:** Yeo & Yeo's team of experts can work with you to evaluate your current attack response and help implement corrective measures and solutions in the event of a cyberattack through XDR and EDR solutions.
- ☑ **Multi-factor authentication:** Multi-factor authentication is an excellent way to provide an additional layer of protection for your accounts.
- ☑ **Mobile device security:** Be sure to analyze the security of your staff's mobile devices. Cybercriminals are now targeting mobile devices to steal business data.

Conclusion & Additional Resources

Jeff McCulloch,

President, YYTECH

With a focus on operational efficiency and process improvement, Jeff McCulloch, President, strives to deliver maximum value to clients through right-fit technology solutions and exceptional service delivery.

Joining Yeo & Yeo in 1996 as a software specialist and holding several management positions since, Jeff has more than 25 years of experience in business development, product management, and business operations within high technology companies. Throughout his professional career, he has managed multi-scale technology engagements and support solutions for manufacturers and distributors, financial/credit unions, healthcare institutions, state and local government, retail, nonprofits, and small to mid-size businesses throughout Michigan.

Jeff is a member of Ingram Micro Trust X Alliance, serving as past secretary, Vice President, and President. He is a member of Central Michigan University's Cybersecurity Advisory Board, Saginaw Career Complex's Cybersecurity Program Advisory Committee, and is co-chair of Delta College's Advisory Information Technology Committee.

While cybercrime continues to thrive, there are many steps you can take to reduce security vulnerabilities and improve online safety. Yeo & Yeo Technology offers the right staff, expertise, and experience needed to protect your business and prevent cyberattacks. You can choose to utilize our services in addition to your existing IT products and internal network team, or as a standalone solution.

Yeo & Yeo provides an abundance of information surrounding technology solutions. Check out our resources, including the latest blog articles and eBooks **here.**

If you'd like to learn more about Yeo & Yeo's cybersecurity solutions, **get in touch** with us today.

Let's thrive.

We're here to help. But first, we're here to listen. No matter the need, we build a right-sized, customized path to help you get there.

VISIT
yeoandyeo.com/technology

CALL
989.797.4075

CONNECT