MANAGING BUSINESS RISK IN THE CYBER THREAT MINEFIELD

A Guide to Cybersecurity for Business Owners

By Chris Schneider, CEO,
Adams Brown Technology Specialists

ADAMS BROWN
Technology Specialists
above+beyond

www.adamsbrowntech.com

TABLE OF CONTENTS

INTRODUCTION

Growing up in a small town it was ingrained in me to give back. That's what people in a small-knit community do. When someone needs help, you help. I have carried this with me throughout life, and it's why I care so deeply about protecting hard-working people from falling victim to bad actors.

Whenever I read a news headline about yet another company being hit by a cyberattack, I can't help but think of those people who lost hard-earned money and are having to spend an exorbitant amount of time to correct a situation that could have likely been prevented. That's when my desire to help out kicks into overdrive. However, this problem is more than one person.

Cybersecurity is a business problem. It's also a strategy problem. If you are going to protect yourself, you have to know where you are vulnerable. What you've done in the past is likely not enough so things need to change. I recognize this is easier said than done. Why invest in something that's not an immediate problem? Why spend time preventing something that will probably never impact you to begin with? You do it because, I promise you, it's easier and less expensive to do what it takes now to protect your company and data than it is after you have to deal with a breach.

In order for us to get to a better place, business and IT leaders have to be willing to get a little uncomfortable. Until then, they'll just continue to roll the dice and take a chance. Is that a gamble you're willing to take? I hope not.

The reality is that we will continue to see cyber incidents that could have and should have been prevented as long as there is...

- A prideful IT leader with a "we don't need help" mentality
- A continued lack of awareness from the top to the bottom
- Little accountability or proof that proactive tasks are getting done
- An IT department being overworked
- Too much trust without verification
- An absence of procedural training across the board
- A security tool with prohibitive costs
- Underestimation of the threats
- Overestimation of one's ability to recover
- A business leader that sees cybersecurity as an expense

Do any of those hit a little too close to home? If so, this eBook is designed to help you. Keep reading to see why you need to focus on cybersecurity and get tips and advice to help you secure your company data from identifying your risk, to training your team, to testing your systems and much more.

When it comes to your cybersecurity, don't wonder if you're safe — make sure you have the security you need in place and a plan to recover if something were to happen. Use the information contained within to start your journey.

CHRIS SCHNEIDER,
CEO of Adams Brown
Technology Specialists.

CHAPTER 1

Cybersecurity is Likely Your Biggest Business Risk

Today's world has become more interconnected. Think about it. You get email on your watch. The website you had open on your desktop can be waiting for you on your phone to pick up where you left off. You can use your devices to see where your loved ones are and ensure they are safe. This provides peace of mind to many people. But as technology aims to make your life easier, it comes with tremendous risk.

Businesses like yours, regardless of size or industry, face an ever-growing threat of cyberattacks like:[1]

A stolen laptop of a healthcare executive that led to more than $200,000 in remediations, monitoring and operational improvements.

The small family-owned construction business that had $550,000 transferred out of company bank accounts after an employee opened an email they suspected was from a supplier but was actually an impostor account with malware.

The data of a government contracting firm that was sold on the dark web leading to more than $1,000,000 in losses including being offline for several days, new security software licenses, a new server and more.

These few examples alone show that cybersecurity is no longer just an IT issue – it's a business issue – an issue that requires attention from all organizational levels. As a business owner, you must first realize that these risks are real, and then proactively protect your companies from online threats.

CYBERSECURITY'S IMPORTANCE CANNOT BE OVERSTATED

It's a combination of an increase in cyberattacks along with an increasing reliance on technology that has made it imperative for businesses to prioritize cybersecurity. Every company, from small startups to large corporations, must have a strong cybersecurity plan to protect its data, assets and reputation.

With the rise of cloud computing, mobile devices and the Internet of Things (IoT), businesses are becoming more interconnected and reliant on technology. While these technologies bring many benefits, they also increase the risk of cyberattacks. A single vulnerability in a business's network or device can expose the entire system to cyber threats.

Cyberattacks have become more sophisticated and prevalent in recent years. According to a study by Hiscox, a global insurance company, the average cost of a cyberattack for a business is around $200,000. This amount can be much higher for larger organizations, where a data breach can cost millions.

[1] National Cybersecurity Alliance Small Business Cybersecurity Case Study Series

That's why you need to protect sensitive data. Think about all the data you have from customer information to financial data to intellectual property. What impact would it have on your business if this data were to become inaccessible? Public knowledge? Lost forever? The damage to your business's reputation and customer trust will be substantial. Not only will you lose clients, but the loss of sensitive customer information can result in legal action.

A cyberattack can also disrupt business operations, leading to downtime and a loss of revenue and productivity. Significant financial losses can set you back years. In a worst-case scenario, it could cause you to close your doors.

GOVERNMENT REGULATIONS MANDATE CYBER PROTECTIONS

Governments worldwide have introduced laws and regulations that place significant responsibilities on businesses that collect, store and process sensitive data. There are data protection regulations you must follow such as the European Union's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA). They require businesses to protect personal data and provide individuals with control over how data is used. This includes implementing appropriate security measures to protect against unauthorized access, disclosure or misuse of personal data.

There are also industry-specific regulations. Certain industries have specific regulations that require businesses to maintain particular cybersecurity standards. The following are some of the bigger laws that may impact your business:

Healthcare. The Health Insurance Portability and Accountability Act (HIPAA) sets national standards for the privacy and security of protected health information.

Finance. The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to implement measures to protect customer data, including the development of written information security plans.

Energy. The North American Electric Reliability Corporation (NERC) develops and enforces standards for the reliable operation of the bulk power system in North America, including cybersecurity requirements.

Defense. The Defense Federal Acquisition Regulation Supplement (DFARS) imposes cybersecurity requirements on contractors doing business with the Department of Defense, including the implementation of the NIST SP 800-171 security controls.

Retail. The Payment Card Industry Data Security Standard (PCI DSS) sets requirements for the protection of credit card data, including network security, vulnerability management and access control.

Companies listed on stock exchanges or operating in regulated industries may have cybersecurity disclosure requirements, too. The U.S. Securities and Exchange Commission (SEC) requires public companies to disclose cybersecurity risks and incidents with material impact.

There are also breach notification requirements that mandate all businesses notify individuals whose personal data has been compromised in a data breach. While there is no federal breach notification law in the U.S., many states have their own laws. These laws vary by state but generally require businesses to notify affected individuals of a breach in a timely manner.

CYBERSECURITY PROVIDES PROTECTION

Cybersecurity protects against a wide range of security threats. It helps prevent unauthorized access and protects data from theft or exposure. By investing in cybersecurity measures, you can reduce your risk of being hacked or compromised, protect your customers' data and maintain the trust and loyalty of your clients.

A cybersecurity program consists of a comprehensive set of policies, procedures and technologies designed to protect computer systems, networks and data from unauthorized access, use, theft or damage.

A well-designed cybersecurity program (discussed further in future chapters) can help to reduce risk by:

- **Identifying and assessing the risks that the business faces**
- **Testing and monitoring the effectiveness of the controls**
- **Implementing controls to mitigate those risks**
- **Having a plan for responding to a cyberattack**
- **Educating employees on cybersecurity best practices**

By implementing a well-designed cybersecurity program, you can better protect yourself against a wide range of security threats and maintain the confidentiality, integrity and availability of data and systems. Bad actors are looking for easy targets. Don't be one of them!

CHAPTER 2

Cyberattacks Prove Costly

Cyber threats have become increasingly sophisticated and frequent. Cybercriminals are continually developing new methods to gain access to sensitive data and businesses must stay one step ahead to protect themselves.

$8 trillion

The total cost worldwide of all cybercrime damage in 2023.[2]

$4.35 million

The average cost of a data breach in 2022.[3]

15%

The year-over-year increase in cyber damage the next three years.[2]

46%

How many cyberattacks target small businesses.[4]

The best way to protect yourself, your company's reputation, your financial stability and your operations is by understanding the most common cyberattacks used. With knowledge comes power. Once you understand how you will likely be targeted, you can take proactive steps to protect your company's digital assets and decrease the risk of a successful attack. Proactive is the keyword here. Proper cybersecurity helps prevent attacks, and it's what will help you lessen the costly damages that businesses face when simply reacting to an attack after it occurs.

Cyberattacks are any attempt by cybercriminals to compromise a company's data or network for personal gain. These attacks can cause significant harm to a company, leading to financial losses and damaged reputations.

PHISHING WREAKS HAVOC ON BUSINESSES

When you look at the tremendous cost of cyber damage, it's even more staggering when you realize 90% of data breaches occurred as a result of one type of cyberattack – phishing.[5]

[2] 2022 Official Cybercrime Report
[3] 2022 IBM Cost of Data Breach Report
[4] 2021 Data Breach Investigations Report
[5] U.S. Federal Bureau of Investigation

This kind of attack is where criminals pretend to be a reputable organization in order to obtain sensitive information such as account credentials (email, bank, etc.) and credit card numbers. This can be done in a number of ways including:

Email phishing. An attacker sends an email that appears to be from a legitimate source, like a bank or popular website. The email often asks the user to click on a link or download an attachment. Doing so takes them to a fake website that steals sensitive information. It is the most common type of phishing attack.

Spear phishing. More targeted than email phishing, it's aimed at a specific individual or organization. The attacker will often use information gathered from social media or other sources to make the email appear more legitimate.

Smishing. Carried out via text message, the attacker will send a text message appearing to be from a legitimate source, such as a bank or a government agency. The message often links to a fake website designed to steal sensitive information.

Vishing. This attack is carried out via voice call where the attacker will pose as a legitimate source, such as a bank or government agency, and ask the user to divulge sensitive information over the phone.

Clone phishing. This type of attack involves the attacker creating a fake website that looks identical to a legitimate one. The user will often be directed to the phony website via a link in an email or text message.

The financial losses from phishing are staggering. It is the most common cybercrime and in 2022, there was an estimated 88.9 billion spam emails daily, a 3.07% increase from the year prior.[6] That translates into a tremendous number of opportunities for your team members to fall victim to phishing, opening your company up to significant financial losses and potential regulatory fines.

Typically, there are two goals the bad actors have in mind when sending out phishing campaigns. These include:

Email Hijacking. A form of man-in-the-middle attack, which we outline later, in which the hacker compromises and gains access to a target's email account.

Ransomware. Depending on your endpoint and network security, one-click could provide a bad actor access to your company network.

[6] The State of the Email Ecosystem in 2022

You Know It's Phishing When...

Since the impact of phishing attacks on small businesses can be devastating, it's important that you look for some common red flags. Here are a few things that will alert you that a communication received is a possible phishing scam:

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

How to Protect Yourself from Phishing

You can take a number of actions to protect your company from phishing scams that start with employee education as well as a few technical solutions. Here are some security measures designed to prevent phishing attacks from succeeding.

- **Educate employees to identify and avoid phishing attacks.** Train them on how to recognize suspicious emails or messages. And make sure they never click on links or download attachments from unknown sources.
- **Implement multi-factor authentication for all company accounts.** This requires employees provide a second form of identification, such as a code sent to their phone, and their login credentials to access company systems. It works by denying attackers access even if they have obtained login credentials. It's also valuable in remote work environments as will be discussed in the next chapter.
- **Execute advanced email security solutions.** These solutions use machine learning algorithms to detect and block suspicious emails before they reach employee inboxes. This can be especially effective in preventing attacks that use sophisticated social engineering techniques. Also, having systems that report suspicious logins or emails being sent at suspicious times is key to identifying if you have been compromised.
- **Develop and implement proper change procedures.** Identify specific changes that should not be solely based on email communications. A couple of examples include a vendor changing a banking account number or an employee redirecting their payroll to a different bank. These actions should require someone to pick up the phone or speak face to face with an individual or entity to verify it is a legitimate change.
- **Develop and implement an incident response plan.** Outline the steps to take in the event of a phishing attack. Be sure to include how to contain the damage, investigate the incident and restore normal operations. Having a well-defined incident response plan can help minimize the impact of a phishing attack and reduce the time it takes to recover.

Companies must stay vigilant to protect assets. It's how you can minimize financial losses and damages to the company's reputation.

MALWARE IS COMMON IN PHISHING & OTHER CYBERATTACKS

Malware can be spread through infected email attachments, malicious websites or vulnerabilities in software. It's how bad actors steal your identity and try and extort money, disrupting your business operations and potentially landing you in legal hot water. And with 560,000 new pieces of malware detected daily, for more than 1 billion total malware programs,[7] it's likely going to hit your company at some time.

[7] The State of Malware in 2023

Malware is a type of software that cybercriminals use to gain access to a company's network, steal sensitive data or disrupt the network's operations.

A number of different types of malware are being used today, including these that are seen most often:

- **Viruses.** Viruses replicate themselves and spread from one computer to another inside files. It's triggered by accessing the file. Once a virus infects a system, it can damage files, steal information and cause various other problems. It's one of the most common types of malware.
- **Worms.** Like viruses, worms are self-replicating malware that can spread through a network. However, you don't need to open a file or click on anything to trigger it. You can get one simply by being on the same network with a device that is infected. Worms also cause severe damage by consuming system resources, degrading network performance and stealing sensitive information.
- **Trojan horses.** Here malware disguises itself as legitimate software. Once installed, it can perform various harmful activities, such as stealing passwords and personal information, deleting files and even taking control of the computer system.
- **Adware.** This software displays unwanted advertisements on a computer or mobile device. While not always malicious, adware can still be a nuisance and a security risk. It spreads when someone downloads a free program or by going to website that takes advantage of vulnerabilities in the internet browser.
- **Spyware.** It's designed to capture virtually everything done on a computer or device without the user's knowledge or consent. This can include keystrokes, browsing history and login credentials. It's hard to find and is often installed on a computer without the user's consent when they download internet software, web browser tools, ad blockers and other types of freeware.
- **Ransomware.** Files on a computer or network are encrypted by ransomware making them inaccessible to the user. The attacker then demands payment in exchange for the decryption key. It comes when users visit fake websites, open unexpected attachments or click on a malicious link in an email, social media post or instant messenger.

You Know It's Malware When...

Hopefully, you have antivirus software that alerts you to malware being on the computer telling you that a file has been blocked. It's actually difficult to tell that malware is on your computer once it's there, but here are a few signs to look for:

- Slow performance where your computer is taking longer to start up or open applications
- Popup ads that you see are increasing or appearing where you normally wouldn't see them
- Unusual activity on the network where there is unnecessary activity or servers may be sending out spam emails
- Unexpected changes to your device settings that you didn't make, like new toolbars in your web browser
- Antivirus software alerting you to malware or blocked sites

How to Protect Yourself from Malware

As with phishing, you need to make sure your employees are trained to not click on potentially malicious links and to protect their usernames and passwords. In addition, consider:

- Document policies and procedures outlining the data you have and how it is secured
- Install advanced endpoint and network security (AI, machine learning, XDR, MDR, etc.)
- Utilize a Security Operations Center or SOC to watch your network
- Keep your software up to date and run regular reports to prove it
- Use strong passwords (at least 12 characters long with uppercase letters, lowercase letters, numbers and symbols)
- Back up all data and test regularly

81% of company data breaches are caused by poor passwords.[8]

Considering the damages malware attacks can have on your business along with the potential price you may be forced to pay to regain access to your systems, you cannot take malware lightly.

OTHER CYBERATTACKS YOU MIGHT SEE

The prevalence of phishing and malware has led some bad actors to try and evade detection by using more uncommon types of attacks to get your valuable information. While the following are more uncommon, you may find that you need to take additional actions to protect your company from them.

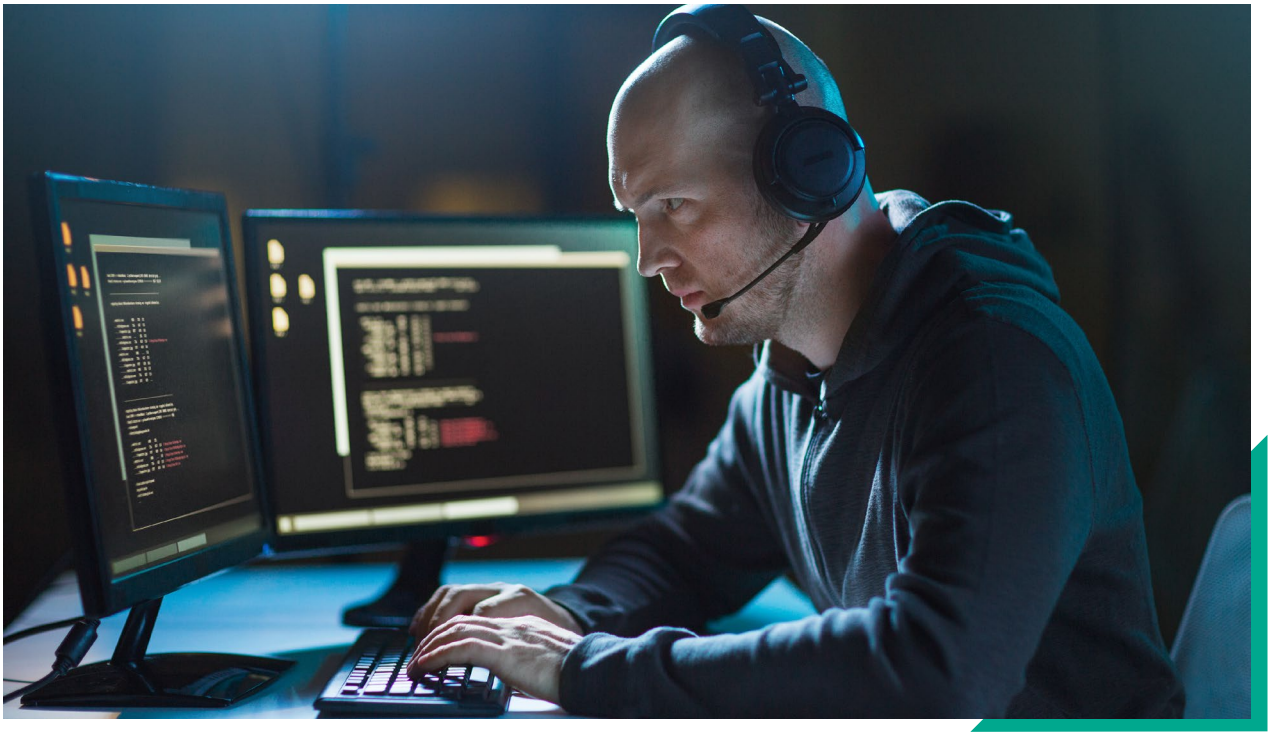
- **Denial-of-service (DoS) attack.** A network or server is overwhelmed with traffic making it unavailable to legitimate users. Cybercriminals use botnets, which are networks of infected computers, to carry out these attacks.
  - *Signs of an attack* include an inability to access websites or services, a slow network or connection speed, error messages or unresponsive servers or systems.
  - *Protect yourself* by using firewalls and intrusion prevention systems to filter out malicious traffic.
- **Man-in-the-middle (MITM) attack.** Cybercriminals intercept communication between two parties like a company and a client. Sensitive information is then stolen including passwords, credit card details and other confidential information. For example, email hijacking, is where the hacker compromises and gains access to a target's email account. The attacker then silently monitors the communications between the client and the provider and uses the information for malicious purposes. Once they identify a way to leverage the information they have gathered, they start reaching out to individuals you have emailed previously and try to get them to reroute payments to a different location. To keep these conversations under your radar, they will create rules within your email platform and sometimes even operate out of your trash or junk mail folders.

[8] Verizon Data Breach Investigations Report

- *Signs of an attack* include unusual network activity like high amounts of data transfers, suspicious network requests, SSL/TLS certificate warnings, unusual web browser behavior and suspicious logins.
- *Protect yourself* by using secure communication methods, such as SSL/TLS encryption, whenever possible. Use only secure Wi-Fi networks to avoid opening up sensitive data on public Wi-Fi networks. And keep all software up to date so vulnerabilities in older software versions cannot be exploited.

- **Brute force password attacks.** This is a straightforward approach where the attacker uses automated software to try all possible combinations of characters until the correct password is found. This method is time-consuming but effective against weak passwords.
  - *Signs of an attack* include multiple failed login attempts, unusual activity on your account, password change requests, unusual IP addresses and a slow or unresponsive system.
  - *Protect yourself* by requiring strong passwords and implementing a lockout policy that locks out users after a certain number of failed attempts.
- **Insider threats.** A growing concern for businesses as they involve employees or contractors who have access to sensitive information and may intentionally or unintentionally leak or steal it. Insider threats can take many forms, including data theft, sabotage or unauthorized access to sensitive information.
  - *Signs of an attack* include unusual data access or access outside of normal job duties, unusual system changes, unusual behavior by an employee and breaches in security policies.
  - *Protect yourself* by implementing access controls that limit the amount of data employees or contractors can access. Conduct background checks on new employees and contractors and also regularly monitor network activity for any signs of suspicious behavior.

The less common attacks are harder to pull off successfully. However, the payoff for doing so may be higher. A sophisticated, targeted attack like one of these is often directed at higher-value targets. The more value a bad actor sees in your company's data, the more creative they will get. That's why you need to understand your risk.



CHAPTER 3

Know Your Risk

Assessing your cybersecurity risks is an essential step in protecting systems and data. It involves identifying potential vulnerabilities, evaluating the likelihood and potential impact of a cyberattack and developing a plan to mitigate and manage these risks. This comprehensive review of your company's digital assets, including your computer systems, networks and data storage, helps you understand where your vulnerabilities are so you can build a roadmap to a strong cyber defense position.

RISK ASSESSMENTS UNCOVER & PROTECT VULNERABILITIES

A cybersecurity risk assessment enables you to make informed decisions, target risk mitigation and take proactive measures to protect the business from cyber threats.

The following details the five steps used in many cybersecurity risk assessments to analyze the threats and vulnerabilities to discover possible risks:

1. **Vulnerability testing.**
   The process of identifying and assessing security vulnerabilities in software applications, computer systems, networks or infrastructure. It involves the use of automated tools and manual techniques to scan and analyze systems for known vulnerabilities. The goal is to identify weaknesses that could potentially be exploited by attackers to gain unauthorized access, disrupt services or compromise the confidentiality of systems and data.

2. **Simulated ransomware attacks.**
   A controlled and planned exercise conducted by organizations, simulated attacks help you test your preparedness and response capabilities in the event of a real ransomware attack. This is done using internal or external security professionals to simulate the behavior and techniques used by real ransomware attackers like sending phishing emails, deploying malware, etc.

3. **Testing of employee base.**
   Here you evaluate if employees are aware of and adhere to your cyber policies through surveys, incident response drills, simulations and more. By assessing any potential weaknesses that can be exploited, you can see where you need to tailor training programs, improve policies and enhance your overall security awareness to mitigate the risk of human error.

4. **Policy and procedure review.**
   By examining and evaluating the effectiveness, adequacy and compliance of your cybersecurity policies and procedures, you can ensure they are robust, relevant, compliant and effectively communicated. Documentation and guidelines that govern your company's approach to cybersecurity are assessed through reviews of training, policies, procedures and the like. This too helps you see where gaps and inconsistencies may exist.

5. **Simulated phishing attacks.**
   It involves sending simulated phishing emails to employees and measuring their response to determine the level of awareness, vigilance and adherence to security protocols. This is also a way to raise awareness and educate employees on phishing to help you create a culture of cyber vigilance.

The results from each of these steps come together to provide you with a clear picture of your current strengths and weaknesses so you can decide which areas, if any, need additional focus. But cybersecurity is not a one-and-done proposition. Once your risk assessment is done and safeguards put in place, it's important to build strong ongoing support services to stay on track. New threats are emerging daily, and unknown risks and vulnerabilities can become evident quickly as your business grows. Your risk is constantly evolving.

CASE STUDY

20% OF EMPLOYEES CLICKED SIMULATED ATTACK EMAIL

The challenge:
A 100-person company was concerned with its cybersecurity and the technology proficiency of its workforce. Company leaders were afraid limited cybersecurity awareness among employees posed a significant risk to the company and its security.

The resolution:
As part of a cybersecurity assessment, we ran a simulated phishing attack. The results were:

- Over 50% of the team opened the simulated phishing email
- 20% of employees clicked on the malicious link in the phishing email

Thankfully it was merely a simulation! However, the exercise highlighted the ease with which a malicious actor could seize credentials and potentially dominate the system. Consequently, this revelation prompted the creation of a comprehensive priority roadmap that demanded urgent attention.

The impact:
Company leaders have initiated monthly cybersecurity training sessions for all employees, educating them on potential threats. Concurrently, monthly phishing tests continue to be conducted. Within six months, the click-through rate on these tests plummeted to less than 2%, representing tangible progress and a significant reduction in the company's risk profile.

REMOTE WORK COMES WITH ADDITIONAL RISKS

As remote work options were necessary for a period of time as a result of COVID-19 and still remain popular today, you need to understand that remote work increases the attack surface for cybercriminals. Employees working from home or other remote locations use various devices and networks to access company resources. This makes monitoring and controlling security more challenging. And they often use personal devices, have an unsecured home network and have insufficient backup systems. They may also use unsafe public Wi-Fi networks that cybercriminals can easily hack. This is the risk you have to manage.

There are expected to be 36.2 million American employees working remotely by 2025.[9]

A cyberattack on remote workers may have less to do with unsafe networks or software and more to do with a lack of day-to-day interaction with one another. In recent years there has been an increase in what is known as Business Email Compromise or CEO fraud. This occurs when an employee receives an email asking them to transfer money to a seemingly familiar account. However, the account is not legitimate. And since the request came from a manager, who might normally pop their head in an office for this face-to-face request but does it via email or text today, an employee ends up transferring the money before realizing it was a fraudulent request.

Take proactive measures to safeguard your company by:

- **Establishing a remote work policy.** One of the first steps to safeguard your company is establishing a remote work policy outlining the expectations and responsibilities of remote workers. This policy should include guidelines for using personal devices and networks, password requirements and handling of sensitive information. And it should include a face-to-face or phone requirement for any transfer of funds or sensitive information. The policy should also address cybersecurity training for remote workers which must include how to identify and report phishing attacks and other cybersecurity incidents.

- **Using secure remote access.** This is critical for protecting company resources from unauthorized access. Business owners should implement multi-factor authentication and virtual private networks (VPNs) to ensure that only authorized users can access company resources. With a VPN encrypting traffic between the remote worker's device and the company's network, it is more difficult for cybercriminals to intercept sensitive information.

- **Providing company-issued devices.** These devices are typically more secure than personal devices because they come pre-installed with security software and are managed by IT professionals. As a result, you control access to company resources more easily.

Whether your employees are hybrid, remote or in-office, you want to lower your risk of an intruder getting into your business network via an unsecured home network. Bad actors go after the biggest weaknesses they see. Make sure targeting your remote workers isn't one of them. With proper training, tools and technology, you can turn them into the first line of defense for keeping scammers at bay.

[9] Upwork's Future Workforce Pulse Report

CASE STUDY

REMOTE EMPLOYEE VULNERABILITY

The challenge:
A medium-sized manufacturing company that championed work flexibility, allowed several employees to work remotely. These employees could access the company's network from their home setups. However, multi-factor authentication (MFA) was not required for remote access due to budgetary constraints, remote employees' concerns about efficiency and the IT department's assurances about existing security measures. This leniency in security became a ticking time bomb.

The resolution:
As part of a cybersecurity assessment, The security lapse materialized when a remote employee's "secure" home network was infiltrated. The attacker gained access after the employee, lacking the latest security patches, clicked on a phishing link. To make matters worse, the employee had saved their company login credentials in their browser. With no MFA in place and the credentials compromised, the hacker smoothly connected to the company's internal system using VPN. Rapidly, they started extracting valuable intellectual property and sensitive client Personal Identifiable Information (PII). By the time the intrusion was identified, significant data had been extracted.

The company had to address not only the immediate breach but also its underlying causes. An extensive forensic investigation took place to trace the attacker's actions. Then there was a comprehensive review of their current security infrastructure. Recommendations were given to the CEO/President to:

1. Enforce MFA across all remote access points.
2. Regularly update and patch employee systems.
3. Conduct continuous cybersecurity training, emphasizing potential risks like phishing.
4. Adopt a more skeptical approach to perceived security assurances and carry out independent security assessments.

The impact:
The breach left an indelible mark on the company. Beyond the tangible financial losses and the costs of remediation, the company grappled with reputational damage. Trust, once lost, is challenging to rebuild. However, the silver lining emerged in the form of valuable lessons. The company now understood the importance of balancing flexibility with robust security. They have since implemented rigorous security protocols, ensuring every remote worker is as secure as one at the headquarters. The breach served as a stark reminder: that cutting corners on security can come at a high price.

ISN'T IT HANDLING THIS?

Maybe. Or, maybe not. While cybersecurity is about protecting a lot of your information technologies, it differs from IT services in terms of responsibilities and focus. Your IT team is tasked with things like managing and maintaining your computer systems, networks, hardware and software. They make sure everything is working for your users and help them when technical issues arise. And they handle all upgrades and backups, too. Your IT department is busy, and they do not have time for testing, checking, reporting and other proactive tasks needed to prevent a security incident or prove the security in place is working. This is where things start to fall apart because they tell business leaders everything is in good shape and they do not need any help. But what does good shape mean?

Cybersecurity professionals protect digital assets from unauthorized access, theft or damage. They identify vulnerabilities, develop security policies and procedures, monitor for security breaches and much more. And keeping up with a constantly changing cyber threat environment is challenging itself.

So, your IT team may be handling cybersecurity. However, in today's environment, IT professionals need to put down their pride and welcome help. This is no longer a single-person or single-team type of issue. What you see in most cases, especially for small and mid-size businesses, is a hybrid approach.

Have internal IT professionals or leaders working alongside outsourced cybersecurity resources. Together, they align cybersecurity with the technology and internal procedures you already have.

As a business owner, you can no longer simply ask the IT department if they are making daily backups and think your cybersecurity needs are met. You cannot rely on the ways you have always done things working for you today. Change is essential. Policies and procedures must be in writing and available to stakeholders like your board and lenders. Your IT budget needs to include cybersecurity costs for security software and infrastructure, employee training, compliance requirements and incident response and recovery. Work to make sure that IT or someone in your company, is paying attention to cybersecurity and has the resources to do so.

Auditing where you are today to see what is needed to secure yourself from cyberattacks is a necessary step.

START WITH A CYBERSECURITY ASSESSMENT

Before you can address cybersecurity threats, you first need to understand what risks you face and where your specific needs lie. That's where a cybersecurity audit comes into play. A cybersecurity audit is a systematic evaluation of your company's existing IT infrastructure, policies and procedures. It aims to identify potential risks and vulnerabilities that could be exploited by cybercriminals.

An effective cybersecurity audit begins with an inventory of all hardware and software, including servers, computers, mobile devices, applications and data repositories. This inventory allows you to pinpoint where sensitive data resides and how it's being protected. From there, an analysis of your network architecture will identify potential security gaps, like unsecured wireless networks or unencrypted data transfers.

The audit will also review your company's security policies and procedures. For example, are employees trained regularly on safe online behaviors? Do you have a robust password policy? Is there a plan for handling security breaches? These are just a few of the questions an audit can help answer.

Additionally, a cybersecurity audit will consider the compliance requirements your business must meet. This can include specific industry regulations or general privacy and data protection laws. Non-compliance can lead to fines and reputation damage, making this aspect of the audit extremely important.

By conducting a cybersecurity audit, you can get a clear picture of your current security status and understand where improvements are needed. It is a critical first step in crafting an effective cybersecurity strategy. The audit not only assesses risks but also uncovers your needs, making it easier to allocate resources effectively and prioritize actions that will offer the greatest protection against cyber threats. It's an important foundational approach to a proactive cyber strategy for your business.

CASE STUDY

SCAN FOUND 500+ VULNERABILITIES

The challenge:
A medium-sized manufacturing company that championed work flexibility, allowed several employees to work remotely. These employees could access the company's network from their home setups. However, multi-factor authentication (MFA) was not required for remote access due to budgetary constraints, remote employees' concerns about efficiency and the IT department's assurances about existing security measures. This leniency in security became a ticking time bomb.

The resolution:
Using advanced AI security software, we:

- Scanned over 20,000 endpoints, identified vulnerabilities and simulated potential ransomware attacks.
- Detected over 30,000 vulnerabilities across 35 networks and 15 locations.
- Brought attention to 90% of the vulnerabilities that existed.

Penetration testing and ransomware simulation showed how easily a bad actor could gain control of credentials and exert unwarranted control over the system. This led to a detailed roadmap of priorities for immediate attention.

In parallel, a dark web scan revealed over 1,700 compromised credentials, leading to immediate password changes for affected users.

A thorough review of policies and procedures showed critical deficiencies such as a lack of cybersecurity training, inadequate network segmentation, insufficient checks for patching and backups and a glaring absence of multi-factor authentication.

A comprehensive roadmap was developed to create or update policies and remedy these concerns. Over the next six months, the district painstakingly worked on patching vulnerabilities and modifying its technology and processes to close security gaps.

The impact:
The school district made substantial strides in mitigating its cybersecurity risk. Their technology assessment served as a crucial starting point. Now, they conduct regular scans to verify the success of the changes made and to identify new, emerging vulnerabilities. They are now equipped with a more secure digital environment, a thorough understanding of the system vulnerabilities and a plan to continuously enhance their cybersecurity measures.

CHAPTER 4

Preparing for Cyberattacks

You probably have heard the saying, “It’s better to be safe than sorry.” This is one of those instances where those words ring true. The fact is that cyberattacks are going to happen. Your business will likely be a target sooner than later. Regardless of size or industry, no business is immune, so it’s a matter of time. That’s why one of your top priorities should be preparing for an attack before it happens. This is how you will protect your data and assets, mitigate financial risks and ensure your business can continue operating.

Developing a cybersecurity plan should start with a risk assessment to identify potential vulnerabilities. It should include a clear response strategy for potential attacks, ongoing staff training on cybersecurity practices and routine audits to ensure the effectiveness of the security measures in place. The necessary measures needed to ensure compliance with relevant data protection regulations should also be factored in.

KEY POLICIES & PROCEDURES TO ADOPT

Businesses should have policies addressing critical areas of cybersecurity. Here are a few policy areas you’ll want to consider:

- **Passwords.** Outline requirements for strong passwords and password storage.
- **Email security.** Detail the rules for using email, especially attachment usage and how to identify phishing emails.
- **Data security.** Provide rules for handling sensitive data, such as how to store it, who has access to it, how it is secure, how that security is tested and how to dispose of it.
- **Technology usage.** Explain how to use technology, for example, what websites are not allowed and how to report suspicious activity.
- **Employee training.** Show how you will train team members on cybersecurity best practices and how to use technology securely.
- **Business Continuity Plans.** Outline all of the hardware and software systems you need to operate your business. Then, walk through each of those and determine what your plan is to minimize downtime in the event of a failure, breach or disaster.
- **Incident response.** This shows how you intend to respond to a cybersecurity incident or disaster from how to detect and contain the damage to notifying affected parties to recover from the incident.

Whether included in another policy or in a standalone one, you’ll want to dictate that regular security updates and patches are part of routine operations to ensure that all systems are up-to-date. These policies should be updated regularly and shared with team members at least annually, requiring their signature stating they read and understand them.

TEST SYSTEMS BEFORE YOU'RE ATTACKED

It is essential to test your cybersecurity defenses regularly. It's how you find vulnerabilities and ensure what you have in place to protect your systems is working as intended to either stop or lessen the impact of an attack. In addition, it gives you valuable insights into the effectiveness of your cybersecurity training programs.

The exact type of testing you need will depend on the size and complexity of your organization, the sensitivity of your data and the level of risk you are willing to accept. Implementing a comprehensive cybersecurity plan isn't just about warding off cyber threats—it's about securing your business's reputation, trust and ultimately, its success.

CHAPTER 5

Responding to a Cybersecurity Incident

Despite employing the best preventive measures, a cybersecurity breach can still occur. It is essential to have a proactive strategy in place for such scenarios to minimize the potential damage and swiftly restore normal operations.

WHAT TO DO IF A BREACH OCCURS

In the event of a cyber breach, it's important to take immediate action to contain the damage and mitigate the impact. The following are some steps companies should take:

1. **Identify the extent of the breach.** Start by determining what data was accessed or stolen, who was affected and how the breach occurred.

2. **Contain the breach.** Once you know the extent of the breach, contain it to prevent further damage. You want to disconnect affected systems from the network to prevent the spread of malware or other malicious activity. But also consider changing passwords and possibly even notifying legal counsel and law enforcement.

3. **Contact your cyber insurance carrier.** If you carry cyber insurance, you'll want to reach out as soon as possible so the insurance company can begin its investigation and provide assistance to mitigate damage. Depending on your policy, they may be able to provide advice on how to respond, financial assistance to cover the costs of responding to the breach and legal representation if needed.

4. **Assess the damage.** What was the impact of the attack? Start by looking at who specifically was impacted including customers, employees or partners. But also consider things like lost revenue, the cost of repairing damage and the impact on the company's reputation.

5. **Notify appropriate parties.** If sensitive information is compromised, the business owner should notify those affected immediately. The notification should include details of the breach, the types of data that were compromised and what steps the business is taking to address the issue. This is where you can tell them what support, if any, you are providing to protect themselves from any potential risk.

6. **Preserve evidence.** You need to preserve evidence of the cyberattack, including logs, emails and other relevant information. This information can help during the investigation of the incident and the identification of the responsible parties.

7. **Investigate the attack.** You should aim to find out how the cyberattack occurred so you can determine how to prevent future cyberattacks.

8. **Prevent future attacks.** Implement measures to prevent future breaches, including more robust security measures, providing additional employee training, updating policies and procedures and conducting regular security audits.

Working through the magnitude of things that need to be done in the event of a cyberattack is why it's crucial to have a plan in place before it happens.

KNOW WHOM TO CALL UPON FOR HELP

In addition to a plan, you should have a ready-to-assemble team consisting of experts who can work together to help you respond quickly and effectively. Here are some of the key roles you should rely on:

Chief information security officer (CISO). Regardless of the exact title, this person is responsible for the security of your information. They can help investigate the attack, mitigate damage and prevent future attacks.

Cybersecurity firm. Hopefully, you have an existing relationship with a firm. If not, you will need to find one quickly. Count on them to provide expert advice and assistance in investigating the attack to limit damages. They can also play a large role in helping with a strategy to prevent future attacks.

Lawyer. Rely on legal counsel to provide advice on the implications of the attack, such as notification requirements and potential liability.

Public relations specialist. This could be an internal or external role, but this person(s) can help you communicate with the public in an accurate, timely and transparent way. They will make sure you are mindful of the relationships you need to preserve and handle any media narrative if it ends up in the news. They are experienced in crisis counseling and can provide counsel to protect your reputation.

Insurance company. If you have cyber insurance, pull upon the resources available to make sure you're doing what is needed to get financial assistance for you and those impacted.

Your team will help you stay calm while acting quickly. They can help you communicate effectively with everyone involved, limit exposure and ensure you're better protected if a cyberattack happens again.

NOTIFICATION & REPORTING OF ANY ATTACKS

The necessity of notifying and reporting cyberattacks cannot be overstated. Affected parties must be promptly informed if their sensitive data has been compromised. This is where your team can help you with the right messaging to protect your company as well as those impacted.

The notification should be clear and comprehensive and cover items like:

- What happened
- What data was compromised
- What steps are you taking to protect customers, employees, partners and yourself
- What steps can they take to protect themselves

You must also clarify you are willing to answer any questions that people may have and how they go about asking them.

If you are offering something to help those affected people protect themselves, explain what it is and how they get it. This could be something like free credit monitoring, identity theft protection, discounts, etc. Rely on your insurance company here if any offer is covered in your policy.

Finally, be sure to apologize—a sincere apology goes a long way. Let people know that you are sorry this happened and that it's creating an inconvenience for them. It shows respect and helps repair relationships and restore trust.

A well-prepared response strategy is as crucial as a robust cybersecurity plan in the fight against the ever-evolving landscape of cyber threats.

CHAPTER 6

The Future of Cybersecurity

Cybersecurity is a complex and ever-changing landscape. As we delve deeper into the digital era, the evolution of cybersecurity becomes more dynamic, mirroring the rapidly transforming technology landscape. As technology advances, so too do the methods and tools used by cybercriminals. Businesses must be ready to adapt their cybersecurity strategies to these changes, keeping their finger on the pulse of emerging trends and developments.

NEW TRENDS IN CYBERSECURITY

More than 2,200 cyberattacks happen each day.[10] That means someone is attacked every 39 seconds. And that number continues to rise.

While many of the tried-and-true methods cyber criminals use, like phishing and malware, still work, they are always looking for new ways to attack data.

The future of cybersecurity highlights the growing importance of privacy and compliance in an increasingly regulated digital landscape. Here are a few of the latest trends you may want to adapt your strategy to address or include:

- **LinkedIn.** Phishing emails made to look like they were from the popular networking platform are on the rise with 42% of employees clicking on emails from the most imitated brand globally.[11] New employees who have changed their job status on LinkedIn are the big targets. Cybercriminals pretending to be senior staff attempt to get personal information, or they ask employees to buy gift vouchers or call a number to discuss some job requirements.

- **Cloud security.** With the increased popularity of cloud computing, there are new security challenges. Misconfigurations, unauthorized access, insecure APIs and data breaches are some of the risks associated with cloud environments. You have to consider the data stored and processed outside of your control.

- **Internet of Things (IoT) security.** All those physical devices we have that are connected to the internet create additional vulnerabilities that have to be considered and planned for. Insecure or poorly configured IoT devices can be exploited, leading to data breaches, privacy violations and even physical harm in certain contexts.

[10] The State of Cybersecurity in 2023
[11] Q1 2021 Phishing Report

- **Cyberwarfare.** This is how nations, state-sponsored groups and other entities are increasingly attacking their adversaries. It represents a complex and evolving landscape that blurs the boundaries between military, political and technological domains. This presents challenges to you since you will have to be able to defend yourself against attacks that are designed to cause maximum damage.

- **New legislation.** In addition to specific laws and regulations in effect today that vary from jurisdiction and industry, the legislative landscape continues to evolve rapidly as governments adapt to emerging cyber threats. For example, a law being developed by the House of Representatives, The National Cybersecurity and Critical Infrastructure Protection Act of 2023, would create a cybersecurity czar to oversee the nation's cybersecurity efforts if it is ever introduced and passed. Organizations should stay updated with relevant regulations in their jurisdictions and ensure compliance.

- **Zero trust security.** This model assumes that no user device can be trusted by default and that all access to resources must be verified regardless of whether they are on your network or not. This means that users and devices must constantly prove their identity and meet specific security requirements before they are granted access to sensitive data or systems.

Cyber awareness can help you keep up with emerging trends so you can evaluate their impact on your business. You can do so by reading industry publications, attending cybersecurity events or networking with cybersecurity experts. See below for a list of resources.

USING ADVANCEMENTS TO PROTECT FROM CYBERATTACKS

Technology can also help businesses improve their cybersecurity posture and protect themselves from the ever-growing threat of cybercrime. Several of these advancements are redefining the future of cybersecurity:

- **Artificial intelligence (AI) and machine learning (ML).** They are increasingly being leveraged for predictive threat modeling and real-time response to cyber-attacks. These technologies enable automated and smart security measures, enhancing the capacity to detect and neutralize threats even before they cause significant harm.

- **Blockchain technology.** Its distributed ledger system ensures transparency, security and privacy, and is particularly beneficial for transactions and data transfers. By leveraging blockchain technology, businesses can create tamper-proof and decentralized networks resistant to cyber-attacks.

- **Quantum computing.** While it threatens to disrupt current encryption techniques, making existing cybersecurity measures obsolete, it also offers the potential for enhanced security protocols, giving rise to the field of quantum cryptography.

Moreover, a holistic approach to cybersecurity incorporating humans, processes and technology is emerging. While technical defenses are essential, employee awareness and a robust security culture are equally crucial for effective cybersecurity. Future strategies will stress more on creating a balanced focus on all these aspects.

CONCLUSION

Go Protect Your Business

With a grasp of emerging trends and the critical role of cybersecurity in the modern era, the time to spring into action is now. Invest your efforts in shaping a solid cybersecurity framework for your business, adopting cutting-edge technologies and trends. Embrace the principles of being informed, vigilant and adaptable. Remember, cybersecurity is not a one-off task, but a perpetual journey that evolves with your business and the constantly changing tech environment. By staying a step ahead, you safeguard your business and sustain its reputation, trustworthiness and long-term success amid the expanding digital landscape.

Cybersecurity is an essential aspect of modern business operations.

In this progressively digital world, cybersecurity forms the backbone of any business operation. The surge in cyber-attacks reinforces the fact that all businesses, regardless of their size or domain, must guard their systems and data proactively. Implementing the best practices defined in this ebook can drastically decrease your chances of falling victim to a cyberattack and also help limit the potential damage, should one occur.

Nonetheless, it's worth noting that cybersecurity is an intricate, ever-evolving domain. For a business owner, keeping abreast of the latest threats, methodologies and technologies can be daunting. Use a team of skilled cybersecurity professionals to help you evaluate your current security position, spot vulnerabilities and enforce powerful safeguards to mitigate risks.

Cybersecurity is not only a defensive measure but also a proactive investment in the long-term success, resilience and sustainability of a business. By prioritizing cybersecurity, you can protect your assets, reputation and customer trust, ensuring a secure foundation for growth and innovation.

Checklist for Better Security

ADAMS BROWN
Technology Specialists
above+beyond

By following these steps and regularly reviewing and updating cybersecurity measures, you can significantly reduce the risk of a successful cyberattack and minimize the potential damage if one does occur.

TECHNOLOGY

- [ ] Keep all software and systems up-to-date with the latest security patches
- [ ] Implement multi-factor authentication for all accounts
- [ ] Use firewalls and antivirus software to protect against cyberattacks
- [ ] Implement email filters to prevent spam and phishing emails from reaching employees
- [ ] Use encryption for sensitive data, both in transit and at rest
- [ ] Use virtual private networks (VPNs) to access company networks and systems remotely
- [ ] Use intrusion detection and prevention systems to monitor network traffic for potential attacks
- [ ] Use role-based access control to ensure employees only have access to the data and systems they need to perform their job duties
- [ ] Use secure file transfer protocols (SFTP) to transfer sensitive data
- [ ] Use secure cloud storage providers to ensure data is encrypted in transit and at rest

PEOPLE

- [ ] Address the cybersecurity talent gap and build the resources you need to stay safe
- [ ] Use strong, unique passwords for all accounts and encourage employees to do the same
- [ ] Educate employees about cybersecurity best practices, including identifying and reporting suspicious activity
- [ ] Conduct background checks on all new hires to reduce the risk of insider threats
- [ ] Conduct regular security awareness training for employees

PROCESSES

- [ ] Address compliance regulations
- [ ] Limit access to sensitive data and ensure access is granted on a need-to-know basis
- [ ] Back up data regularly and store it securely
- [ ] Monitor systems for unusual activity and investigate any suspicious activity immediately
- [ ] Conduct regular cybersecurity assessments to identify potential vulnerabilities and proactively address them
- [ ] Develop an incident response plan to ensure all employees know what to do in the event of a cyberattack
- [ ] Develop and regularly test a disaster recovery plan to ensure critical systems and data can be quickly restored in the event of a disaster
- [ ] Use secure file transfer protocols (SFTP) to transfer sensitive data
- [ ] Use secure cloud storage providers to ensure data is encrypted in transit and at rest

Remember that despite taking all necessary precautions, a breach can still occur. You still need to have a response plan.

Additional Resources

ADAMS BROWN
Technology Specialists
above+beyond

To keep up with the latest security threats, subscribe to security newsletters and follow security blogs and websites. Here are a few, of many, to consider:

- Adams Brown Technology Specialists' blog: www.adamsbrowntech.com/resources/blog
- CISO Magazine: www.cisomag.com
- SC Media: www.scmagazine.com
- ThreatPost: www.threatpost.com
- Infosecurity Magazine: www.infosecurity-magazine.com
- Krebs on Security: www.krebsonsecurity.com
- Security Magazine: www.securitymagazine.com
- ZDNet's cybersecurity blog Zero Day: www.zdnet.com/blog/security
- Wired's cybersecurity section: www.wired.com/category/security

Looking for a deeper read, the following are a few good books:

- The Art of Deception by Kevin Mitnick
- The Hacker's Handbook by Marcus Ranum
- Cybersecurity for Beginners by Raef Meeuwisse

The following events provide great opportunities to learn from cybersecurity experts:

- BlackHat
- Defcon
- Be sure to check for local events in your community, too

If you're a regular podcast listener, you might want to try:

- CyberWire Daily hosted by Dave Bittner
- Security Now hosted by Steve Gibson
- Smashing Security hosted by Graham Cluley and Bruce Schneider

About the Author

Chris Schneider, CEO of Adams Brown Technology Specialists,

is a problem solver who uses technology as a tool to help businesses achieve their goals and operate as efficiently as possible. He believes that all stakeholders must have a clear understanding of the "why" and "how" when it comes to technology plans and implementation. By building technology plans and managing implementation strategies, he supports companies and their IT departments. This is done with a focus on gaining trust and buy-in from across the organization by utilizing clear communication with team members within the business.

ADAMS BROWN TECHNOLOGY SPECIALISTS

Adams Brown Technology Specialists is a team of experienced cybersecurity experts who can help you assess your current security posture, identify vulnerabilities and implement effective measures to mitigate risks. You can be confident your business is secure and your customer's data is protected, allowing you to focus on what matters most—growing your business.

www.adamsbrowntech.com

ADAMS BROWN
Technology Specialists
above+beyond