30 tips in days

Cybersecurity
best practices
for your business

WIPFLI

How are you keeping up with changing cyber trends?

During the month of October, Wipfli shared 30 cybersecurity tips in 30 days. For over five years, the firm has put together this annual list of 30 best practices — each year's tips reflecting the evolving cyber needs and challenges of businesses as they navigate a digital world. Cyberattack methods have changed, data breach costs have risen and cyber insurance requirements have tightened.

Cybersecurity is more important than ever, and businesses are starting to catch up. Accordingly, this year's 30 tips in 30 days offered a mix of basic, moderate and advanced cybersecurity best practices. No matter where your organization's information security program is in its maturity, you can benefit from these tips. Now, we've collected all 30 in one e-book.

Read on to learn everything from who cybercriminals are targeting, to what methods they're using and how you can help protect your business.

43% **of data breach victims are small and medium-sized businesses**

13% **is how much data breach costs have risen in only two years**
(now at $4.35 million per data breach)

46% **of the world's cyberattacks target the U.S.**

78% **of companies expect cyber regulatory requirements to increase annually**

TIP #1

Simulate ransomware attacks to improve your defense

Ransomware is a type of malware that restricts access to your data by encrypting it.

The bad actor will require the victim to pay a ransom in order to regain access to their own data. Perpetrators don't care what industry you are in; they know an organization's data is highly valuable to that specific organization. It's part of why ransomware attacks are on the rise and currently are the most prominent malware threat.

Understanding what to do when an attack occurs by simulating the attack will help ensure that employees know their responsibilities, that critical communication will occur and that the incident will be resolved in a timely manner.

When you know how to react, how quickly to react and who needs to get involved, you can greatly reduce the impact of the ransomware attack.

You'll want to answer these common questions:

- When should you contact law enforcement?
- Does the insurance company need to get involved? Are they dictating which forensic company you use?
- Who can help you determine the extent of the malware encryption?
- What do you tell your employees, customers, clients, patients and/or stakeholders?

If you're able to document and anticipate the activities that will need to take place during an attack, you're then able to help ensure all groups can resolve the incident as soon as possible and address all aspects of an attack.

NEXT STEPS

- **Simulate a ransomware attack by performing a tabletop exercise**: An exercise allows participants to walk through each step and learn how to identify what is encrypted, what is the impact to the organization and what options they can offer management for resolving the attack. (e.g., pay the ransom or recover the data prior to the encryption within X amount of time with X data loss). The tabletop exercise should allow discussion on all topics, such as what is impacted technically, communications requirements and resolution options. Once you discuss the exercise topics, document the process to respond to the ransomware attack. Should one occur, you'll have a methodical process to follow.
- **Test your employees' skill at recognizing emails that may contain ransomware malware**: Use software that can simulate and distribute emails that look like genuine requests from a customer when in reality they are attack emails so that you can understand the areas of exposure internally. Initiate the emails in a testing mode.

TIP #2

Protect your hybrid workforce

During the height of the COVID-19 pandemic, close to 70% of full-time employees were working from home.

Now, in 2022, 35% of employees have the option of working remotely full time, , while 58% have the option of working remotely at least one day a week. With so many organizations composed of a hybrid workforce, it's critical for yours to implement the right technology and security controls to protect that workforce.

Without a roadmap that identifies and prioritizes your organization's challenges and plans around technology, your employees will start looking for workarounds. For example, if your organization hasn't implemented a cloud storage solution, your employees might end up creating personal Dropbox accounts that don't have proper security controls configured. Because services like these are beyond the control of your organization, it can increase the risk of a sensitive data leak.

NEXT STEPS

- **Implement a secure VPN**: A VPN allows your employees to have access to everything they need to do their jobs whether they're at the office or working remotely. Make sure you protect your VPN connection with multifactor authentication (MFA), which , which requires employees to authenticate a second set of credentials to gain access. (Example: To sign into the VPN, they enter their email password and then a code texted to their mobile phone.)
- **Migrate legacy file servers and applications to the cloud**: Cloud-hosted data is accessible anywhere, which makes it great for hybrid and remote workers. By migrating your physical office environments to cloud solutions — ones that you control and can configure security around — you enable employees to securely access data from wherever they are working.
- **Use business communication technology:** Make sure to implement technology that enables voice, video and text communication between users from anywhere, as well as allows secure file storage and sharing across your organization. This includes options such as Microsoft Teams, Google Workspace and Webex Teams.
- **Implement conditional access policies and mobile device management**: By setting access policies, you help ensure employees have access to what they need and not every bit of data your organization produces. With mobile device management, you can also help ensure that certain workers have access to sensitive data from external devices.

TIP #3

Implement password best practices

Weak, easily guessed or reused passwords are the cause of the majority of data breaches worldwide.

Previous data breaches, hacker forums and the simple guessing of weak passwords in a password spray attack are just some of the ways passwords can be exploited by a bad actor.

Once a valid password is found, those bad actors will conduct a credential stuffing attack across multiple resources, attempting to log in to hundreds of different sites with the same credentials, knowing that many users will reuse passwords.

Even if breached passwords are hashed (i.e., encrypted), this is little protection, as hardware specifically dedicated to cracking passwords is becoming more powerful, efficient and cheaper every year. Wipfli's own in-house hardware used in penetration testing is capable of many billions of guesses per second.

Yet passwords are still the basic authentication mechanism for the vast majority of organizations. Passwords can be secure if steps to prevent the use of weak passwords are implemented.

NEXT STEPS

- **Encourage the use of passphrases rather than passwords**: Passphrases are comprised of several memorable words in random order, perhaps combined with a few character replacements. This produces a string that is much harder to guess or crack than those based on a single word with modifications or additions.
- **Implement password filtering**: You should implement password filtering regardless of whether you use a password or a passphrase, but note that it's especially important if passwords are the de facto standard. Password filters prevent users from setting a password that contains easily guessed strings such as months, seasons, years, sports teams, etc., which is the primary way that bad actors guess user passwords.
- **Increase your minimum password length**: If passphrases are adopted as a standard, the minimum password length can be extended to 16, 20, 24 or even 30 characters without undue burden on users. Conversely, increasing the minimum password length may have the alternate effect of encouraging passphrases use over passwords.
- **Use MFA:** Regardless of the strength of a user's password, there is always the possibility it will be compromised in some manner. MFA provides a second, distinct verification of the user's identity.

TIP #4

Supplement your antivirus with XDR

Ransomware and other malware have become so sophisticated that they can evade detection by traditional antivirus technologies.

In 2021, 66% of midsize organizations were hit by ransomware, up from 37% in 2020. The average ransom payout was $812,000, with 10% of organizations paying over $1 million to recover their data.

So, what can help your organization protect itself from ransomware? Extended detection and response (XDR) is a great option in helping you identify malicious processes and system events running within your computers. XDR stretches across your entire organization, providing visibility across your network, endpoints, cloud solutions and more.

It constantly monitors all of this in order to identify abnormal processing activity, detect suspicious events and alert your security team.

NEXT STEPS

- **Select an XDR solution**: Work with your security team to evaluate leading XDR solutions and deploy one within your environment.
- **Train employees**: Ensure your team has the knowledge and capability to respond to alerts generated by XDR.
- **Monitor on-premises and cloud environments**: XDR has the ability to monitor your entire attack surface, so make sure you implement it across all assets — both on premises and in the cloud.

TIP #5

Stabilize the cyberthreat moving target with a cybersecurity risk assessment

Organizational change is a constant. It's how businesses reach new heights. Unfortunately, the cyberthreat spectrum also constantly changes.

The near-continuous emergence of variants to well-known threats, as well as entirely new exploits and attack tactics, should remind organizations that complacency around cybersecurity risk management can lead to serious consequences, even the end of the business itself.

Though it may seem like you're chasing a target that never seems to slow down enough for you to gain a complete picture, the cybersecurity risk assessment process offers you a way to stabilize the image within your crosshairs.

This process is so well respected, and so highly trusted, because when applied correctly, it dramatically reduces both the planning horizon and the level of effort required to navigate your security roadmap. Your roadmap is essential to controlling the impacts of existing cyberthreats, updating risk profiles to reflect organizational changes, and avoiding impacts of cyberthreats that emerge in the future, so you want it to be easily navigable.

By performing a cybersecurity risk assessment, you gain an excellent baseline reference to benchmark and qualify whether your cybersecurity controls and management capabilities provide the same amount of protection after you implement new business locations, applications or other new ways of doing things. These results similarly inform next steps around variant or newly emergent cyberthreats.

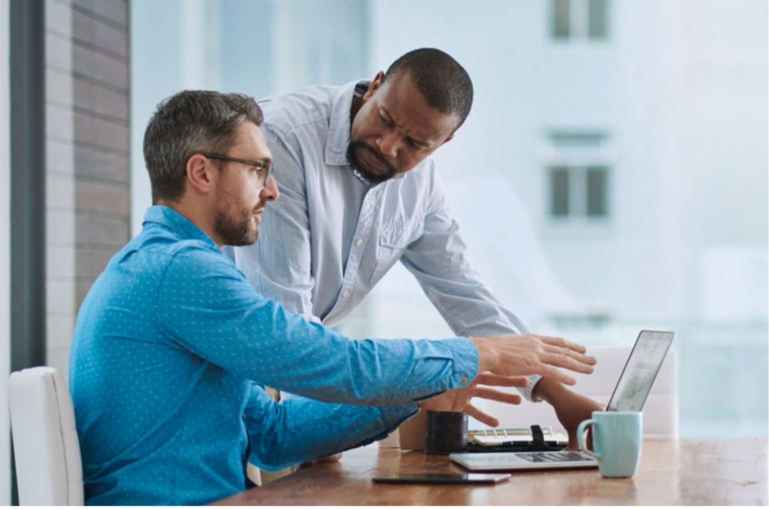
Without a cybersecurity risk assessment, you're forced to consider everything that's proposed, or that could happen, from scratch. But with an assessment, both your starting point and waypoints along the journey toward effective cybersecurity risk management are much clearer and easier to discern.

NEXT STEPS

- **Identify vulnerable assets and credible threats**: Compress the scope of the cybersecurity risk assessment to include only credible cyberthreats, and only those organizational assets vulnerable to them.
- **Measure and prioritize cybersecurity gaps and business enablers**: Maximize business benefits by planning the enterprise security roadmap such that its cadence and sequence mitigate the larger-impact cyber risks first, and that it respects potential future business use cases.
- **Reference the cybersecurity risk assessment**: Use cybersecurity risk assessment results to guide your thinking in response to newly announced business changes and emergent cyberthreats. Estimate your future cyber risk profile on the basis of your current one — is what you have sufficient for the future, or do you need reinforcement?
- **Sustain the cybersecurity risk assessment**: Periodically renew the cybersecurity risk assessment to confirm it's still based on relevant assets and threats, and update its methodology and risk-scoring routines to pace improvements advanced by trusted sources such as the NIST.

TIP #6

Pump up your data privacy awareness training



When it comes to effective cybersecurity risk management, continuous improvement is what it's all about.

These include improvements such as leading-edge detection of new attack signatures, the expansion of incident response playbook coverages and the addition of MFA for more applications. It can also include the addition of data privacy components to role-based security training provided to employees.

Data privacy focuses on when, where and how personal data is collected, shared and used. Security, on the other hand, is more about protecting personal and other data from unauthorized access, sustaining data integrity and ensuring that the data is available for its authorized purpose.

It's clear that data privacy and security go together, but with data privacy being the ultimate reason you invest so much in cybersecurity protections, how much stronger could employees' resistance to phishing and other social engineering attacks be if they are more aware of this?

Think of it this way: You want employees to master your security processes and technology; is there a reason why you wouldn't also want them to also embrace the reasons why?

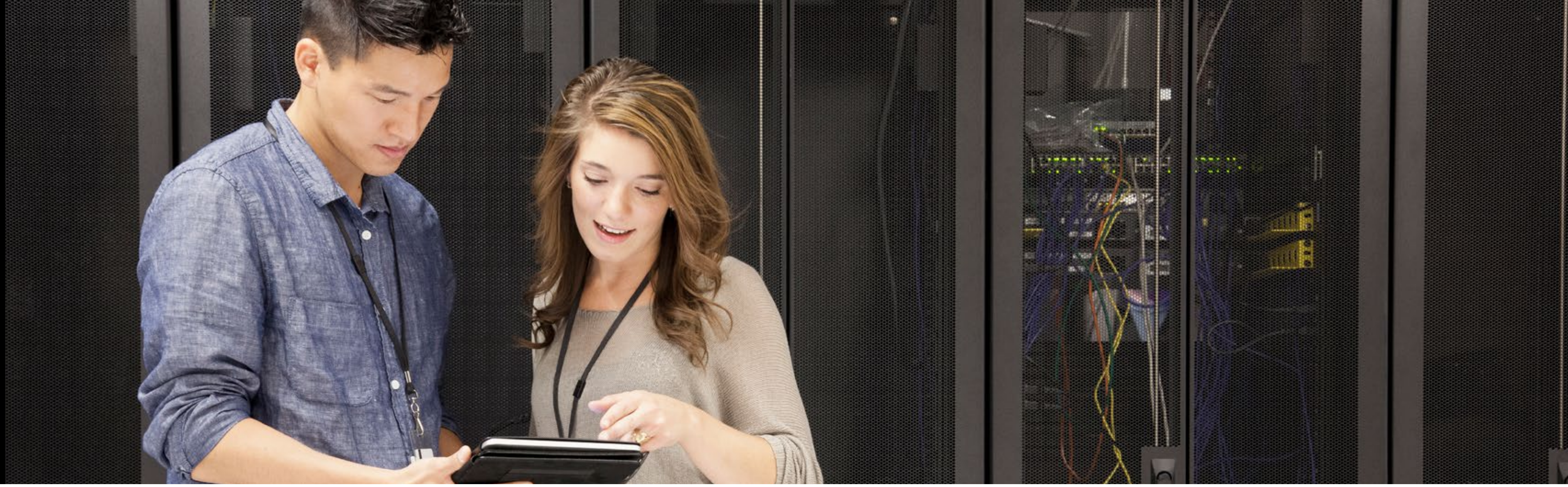
Best security management practices include periodically refreshing security awareness training content so that it's up to date and covers all relevant current threats and attack tactics. The next time you do this, please take the opportunity to also supplement your curriculum with coverage of the data privacy goals and requirements relevant to your organization.

NEXT STEPS

- **Identify relevant data privacy goals:** See what your organization's mission statement and business strategies say about valuing and protecting the interests of your customers. In today's customer-centric business climate, it is customer caring and commitment that drive data privacy goals.
- **Identify relevant data privacy requirements:** Review relevant data privacy laws and regulations to ensure you're focused on compliance. The U.S. Computer Fraud and Abuse Act and the Children's Online Privacy Protections Act apply to all industries. All 50 U.S. states now have data-breach notification laws, and sectoral regulations such as GLBA and HIPAA could also be important.
- **Build enhanced data privacy coverage into security training curricula:** Apply the knowledge you gain within the action steps above to outline and summarize your knowledge for sharing with others via the slides or in-person presentations you use to deliver security training to your colleagues.
- **Share the reason why:** It's generally accepted that adults learn new things best when they also understand the reason why they need to learn. Thus, be sure to introduce the new data privacy elements in your enhanced curricula and place them in perspective for your students.

TIP #7

Implement zero trust architecture concepts



Hard to earn and easy to destroy, trust is crucial not only in interpersonal relationships but in computer systems, too.

The problem is that networks and systems were designed from the beginning to trust all users and transactions. In most networks, trust was given and never earned. But now, cybercrime has changed that. If you want to secure your network, you've got to understand and implement zero trust concepts.

Zero trust is intentional, and you have to be proactive about it; it doesn't just happen. According to Microsoft, zero trust is an integrated approach "that explicitly and continuously verifies every transaction, asserts least privilege, and relies on intelligence, advanced detection, and real-time response to threats."

NEXT STEPS

- **Use least privilege access**: Users should only have the level of access they need to complete their job tasks. Having excessive permissions may be convenient, but it's a major security risk. If that user account gets compromised and has more access than necessary, that extra information is at risk. Multiply this by the number of users that have excessive permissions.
- **Verify permissions explicitly**: When establishing access for a user, at a minimum you need to verify the requesting user is who they say they are. This is typically accomplished with MFA. Zero trust takes it a step further by considering additional data sources. Is the request for access coming from a location you expect? Is the request for access coming from a device you trust and know to be in good health? Is the user authorized to access information with this level of classification? Zero trust means you need to interrogate the access request more stringently.
- **Assume you've already been breached**: You'll need to use a variety of techniques to do this, but in zero trust, you have to assume that attackers are already in your network. Some of the things you can do include:
  - Implement end-to-end encryption, which can protect data even if a workstation is compromised.
  - Put network segmentation in place to make it harder for an unauthorized user to traverse your entire network.
  - Secure how you use local administrative accounts to make it harder for attackers to escalate privileges.
  - Continuously monitor for threats and indicators of compromise to make sure you can interrupt attacks and evict attackers.

TIP #8

Secure your organization with a security operations function

Security operations is the function of combining cybersecurity processes with ongoing traditional IT capabilities to reduce your organization's exposure to cybersecurity risks.

A security operations capability requires someone to follow regular procedures to validate that security controls are functioning. Specifically, you want to review the overall system to make sure any deviations are identified in a timely manner and promptly addressed.

Deviations could be regularly occurring controls not being performed or detective controls identifying an anomaly.

Security operations brings a structured process to identifying these deviations. In large organizations, it's not uncommon to have a team dedicated to security operations. In smaller organizations, it may not be feasible to have a dedicated security operations team, but you can structure the activities and establish a security operations mindset. While this isn't an all-inclusive list of security operations, here's a primer of some of the blocking and tackling to get your own security operations function working.

NEXT STEPS

- **Define your key systems that need to be monitored**: A first step in any security operations function is understanding what infrastructure you have and its importance in supporting your business objectives. You need to identify your most important assets and prioritize your efforts on monitoring those.
- **Review privileged accounts:** Privileged and administrative accounts are among the most sensitive components of your IT system. These allow the highest levels of permissions and let whoever is logged in to that account modify your applications and data. A security operations function should be looking at those accounts to identify any unauthorized use. This could include logins or password changes when you're not expecting those types of actions.
- **Ensure you apply patches**: Vulnerabilities in operating systems and applications are constantly being identified, and patches are being pushed out as quickly as possible to address those vulnerabilities. A key security function is to regularly review your systems to make sure those patches have been applied.
- **Verify backup completion**: Isolated backups are critical to ensuring an organization's ability to recover from devastating attacks such as ransomware. Too often, organizations have failing backups that they don't know about. It's a critical function to review your backup status on a daily basis to make sure you have something from which you can attempt a recovery.
- **Identify and respond to suspicious activity**: Hackers and cybercriminals are constantly attacking systems and looking for their next victim. Defensive security solutions such as firewalls, endpoint detection and response (EDR) and other infrastructure such as Active Directory and event logs on servers capture huge volumes of security event data. This data can help identify instances of unauthorized access attempts and whether they succeed. The challenge is to review this volume of data in a timely manner. If you have a limited attack surface and a clear understanding of what an unauthorized access attempt would like, you might get away with reviewing it manually. Otherwise, you'll need automation to do the heavy lifting and alert you to anomalies. If you do have this automation in place, a daily check to make sure it's configured properly and running is a great idea.

TIP #9

Use a password manager

Cybercriminals don't always need a breach to gain an initial foothold in your organization.

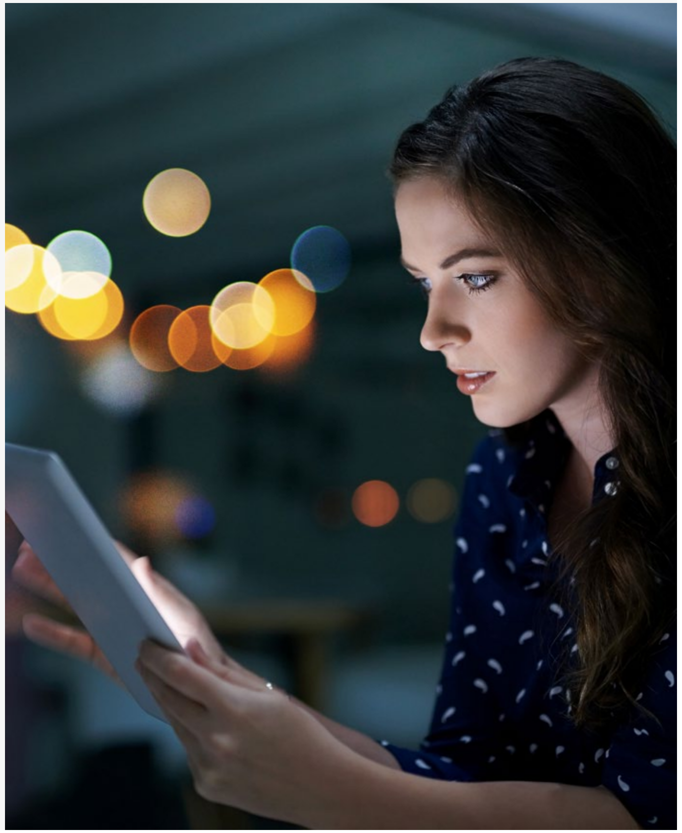
Left to their own devices, employees seldom choose strong, complex passwords. Further, they tend to choose passwords composed of common elements such as months, seasons and years, which an attacker can easily guess.

Employees also tend to reuse passwords across websites and different services, so one service or website that is compromised can lead to many in what's called a credential stuffing attack, the automated use of a breached password to attempt a log in at many, even hundreds, of websites. If your users are reusing passwords, both your organization and partner organizations could be at risk.

Given the number of online services that most people use, plus the number of breaches that occur on a yearly basis, the question becomes not how to stop credential breaches but how to minimize their potential impact. The most effective way to do so is with a password manager.

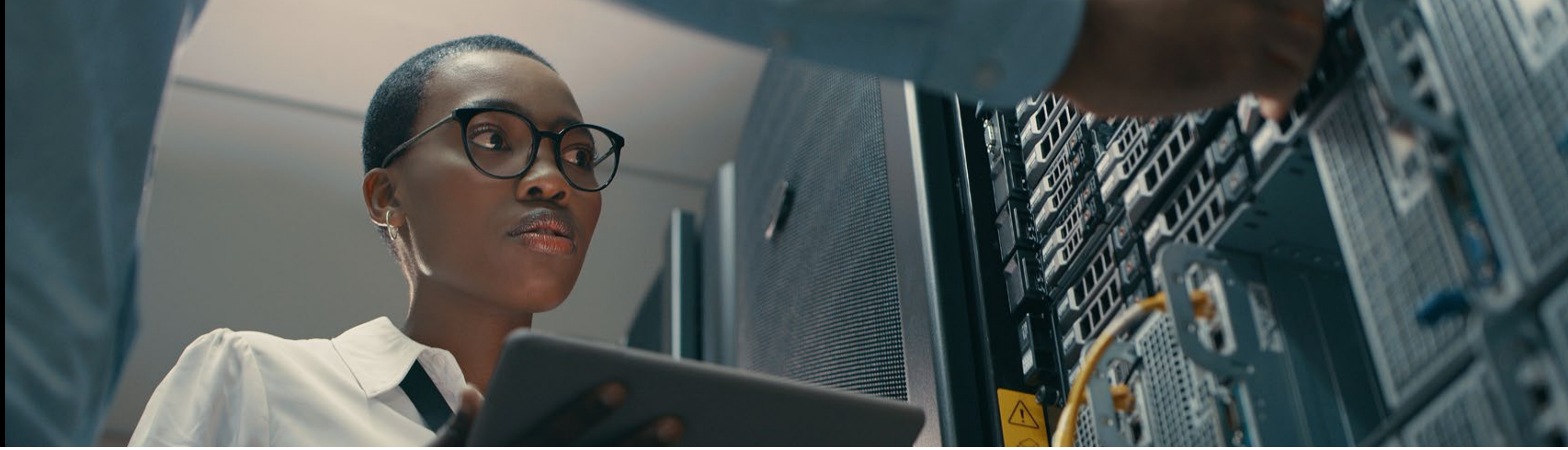
NEXT STEPS

- **Implement a password manager for the entire organization:** Password manager applications relieve the user of several issues related to password management.
  - » They encourage the use of longer, more complex or even random passwords, since users don't have to commit them to memory. Depending on the particular password manager, users may only have to remember one or two passwords: one for their initial network logon and one for the password manager itself. Some password managers can also implement single sign-on. Having the password manager set very complex passwords prevents password spray attacks, as these passwords can't be guessed by an attacker.
  - » They make it much easier to use unique passwords per login, as unique passwords can be generated by the password manager itself, relieving the employee of having to compose a new password for every site or service. This helps prevent credential stuffing attacks.
  - » They provide safe, encrypted storage for a user's passwords, keeping them off Post-it Notes or notepads and out of text, Word and Excel files, which could themselves be compromised.
- **Select the right password manager for your organization:** Password managers can take on many forms: standalone applications for each user, applications that integrate with a web browser or centralized applications managed for the entire organization by your IT department.
- **Choose whichever manager is most appropriate for your organization's needs:** Base your decision on factors such as cost, ease of administration and effectiveness.



TIP #10

Back up your data



Your organization's information is valuable. Your clients are relying on you to ensure their confidential and even nonconfidential data is safe and recoverable.

They trust that you will protect and back up the data regardless of any incident that may damage the primary copy of that data. Not being able to recover their data may result in loss of confidence in your organization and in loss of business.

Even if your data is outsourced to a third-party provider, you are responsible for ensuring that the safety and recoverability of the data meets your organization's needs, no matter if the data is in multiple locations or in multiple formats.

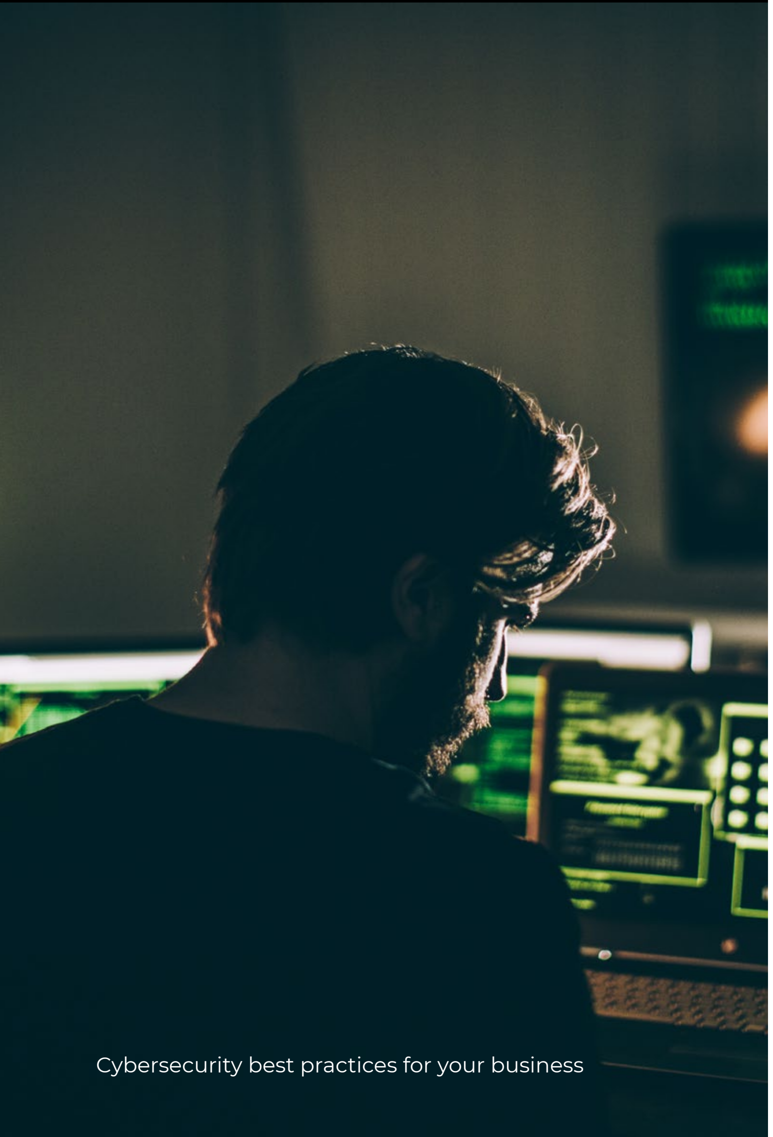
Being able to recover from different types of incidents means first identifying the type of data that is critical, how it is backed up and how it will be recovered. For example, copies of the data that are air gapped from the primary data helps protect your organization from cyberattacks such as ransomware. Without being able to recover data quickly, precious time and money are lost, and you have to spend dollars on recovery versus spending time on new development and new sales.

NEXT STEPS

- **Select a backup tool**: Choose a backup tool that allows for easy recovery and recovery testing. The reason you are backing up is for the reassurance that you can recover if/when it is necessary.
- **Choose multiple tools, if necessary**: Choosing multiple tools can help ensure multiple backups that are onsite or offsite, and those that are air gapped, are safe from a malware intrusion.
- **Ensure the backup allows for full recovery, not just file recovery**: If the primary data center needs to be recovered at an alternate location, it may be necessary to recover to new hardware. Recoveries should be tested to the alternate data center.

TIP #11

Protect against nation-state attacks



Nation-state attacks typically come from three different sources:

- The nation itself (such as Russia, China, Iran or North Korea)
- Groups that are linked to a government (these attacks are also called state-sponsored attacks)
- Cybercriminal gangs in a country that allows them to operate freely (these attacks are also called state-ignored attacks)

Research shows that 35% of nation-state attacks target enterprises, and they are often fueled by international competition. Often, organizations are targeted by nation-state attackers in a ransomware operation to gain funding or an espionage campaign to obtain intellectual property.

Many nation-state attackers are also targeting supply chains. The SolarWinds breach discovered in 2020 particularly underscores the importance of understanding your software supply chain. Why? Because a nation-state attacker may not target your organization directly but rather target a company that can push updates into your network to gain initial access.

NEXT STEPS

- **Audit your defensive posture:** Audit your current information security posture. Do you have a defense-in-depth posture to defend against advanced attackers?
- **Understand the threat:** Invest in threat intelligence and understand the threat actors interested in your business, product or data. Use this intelligence to create a defense-in-depth architecture.
- **Deploy software updates:** Many attackers can use vulnerabilities in older products, so make sure to regularly test and implement security updates from vendors.
- **Protect your supply chain:** Review and test software updates from vendors to ensure no malicious code is contained in the update.
- **Test your defenses yearly:** Conduct a red or purple team exercise to verify your defenses and cybersecurity personnel can detect and respond to advanced attackers who are targeting your network or already in your network.

TIP #12

Know where sensitive data resides and what is being done with it

Data is exploding. It's being created, stored and shared everywhere, and that's what makes discovering and managing it so challenging.

Many organizations don't have the information to understand the risks they face. Protecting data has become more challenging as people work in new ways, including creating and sharing data across organizational or regional boundaries. Customers now need to protect sensitive information on devices, software as a service (SaaS) applications and cloud services, in addition to on-premises environments.

If your organization doesn't know where your sensitive data resides, and you don't have controls in place to ensure that all categories of data are handled appropriately, you could experience damage to critical business relationships due to unauthorized access to sensitive client data.

Plus, the number of regulations organizations must comply with to protect sensitive data continues to grow. The cost of not complying with data regulations could result in fines and lower credibility with regulators and customers.

NEXT STEPS

- **Implement a strategy for protecting and managing sensitive data**: Before your organization can protect and govern its sensitive data, you first have to know where it resides, how it is being used and shared, what the associated privacy and regulatory risks are, and even whether the data is still needed.
- **Apply sensitivity labels to classify and protect your data**: You'll want to do this while making sure that user productivity and their ability to collaborate isn't hindered. Make sure you understand your data landscape and identify sensitive data across your hybrid environment; apply flexible protection actions, including encryption, access restrictions and visual markings; and detect risky behavior so you can prevent accidental oversharing of sensitive information.
- **Automatically retain, delete and store data and records:** Make sure to also do so in a compliant manner so you don't run afoul of regulators.

TIP #13

Review external sharing practices

Long before the pandemic, organizations were familiar with distributed teams. Now it's all about the hybrid workplace.

Remote and hybrid work continue to drive the need for organizations to provide collaboration solutions to work without limits, work on the go and work securely, from anywhere.

The ability to share files with external users (guests) is a great feature that allows you to securely collaborate with people outside your organization, such as your business partners, vendors, clients or customers — if it is set up and managed appropriately. Collaboration solutions with open sharing present an easy target for cybercriminals, especially if you are not aware of or control your external sharing practices.

Do you know where your business-critical and sensitive data resides and what is being done with it? Do you have control of this data as it travels inside and outside your organization?

Many cloud collaboration platforms have out-of-the-box settings to allow open or easy sharing, which lets employees share any information with anyone in or outside your organization. Your employees may not know the level of security that exists (or doesn't exist) for the information they share.

By establishing and reviewing external sharing practices, you can provide the right information to the right audience.

NEXT STEPS

- **Review external sharing configuration and settings**: Review the external sharing settings (if enabled) and their limits, keeping in mind the configuration can be different for each collaboration solution and set at different levels within the solution. Check your application provider's documentation or engage an experienced third-party vendor if you're uncertain on how to configure.
- **Know whether data is being shared externally**: What information is being shared with external users and how much? Most collaboration solutions have auditing functions that provide the ability to log and search for external sharing. An even better solution is to set up alert policies that identify activities performed by users based on the conditions you define. You can also engage a third party if there is uncertainty about how to set up and monitor activity.
- **Identify locations of sensitive information:** Is there information in cloud applications that is sensitive and should have limited or no sharing? Where specifically does that information reside, and who has access? These are very important questions to ask and answer in order to make sure you are protecting your sensitive data.
- **Configure restrictions on sharing of sensitive information**: Discuss protecting sensitive information with your IT department or IT service provider. Implement best practices by following the cloud application vendor's guidance to secure your sensitive information. Here, too, you can engage an experienced third party if there is uncertainty about how to properly configure sharing.
- **Implement an ongoing review of stored information and best practices**: Regularly take inventory of shared information, since sensitive information may be added in new places. Frequently check your cloud application provider's best practices for updated information.

TIP #14

Review user privileges and administrative accounts

Employee accounts with excessive privileges are a real risk in many organizations. So is having too many administrative accounts and not tracking who has access to them.

For example, if an individual account has global administrator access and it gets compromised by a phishing attack, password spray attack or ransomware — all incredibly common attack methods — the cybercriminal gains access to basically your entire company. These takeovers can lead to lost production time and millions of dollars in ransom, recovery and lost productivity.

NEXT STEPS

- **Adjust access levels**: Keep your individual account at the same access level your users have. Keep your admin accounts separate, and use different passwords for them.
- **Keep your vendor account access minimal**: Don't give vendors access to a greater scope than what they need. Disable/delete them when you no longer work with them.
- **Review C-level access**: C-suite execs are highly targeted by cybercriminals, so make sure their accounts don't have excessive privileges. Only give them access to what they need.
- **Review application privileges**: Who has ability to authorize check runs or modify payroll? Who can issue a wire transfer? Reviewing these privileges not only helps limit fraud but also helps protect against cybercrime. Fewer people with access to sensitive functions limits the damage that can be done.
- **Make a list of administrative accounts and review it regularly**: Inventory your admin accounts and keep the list current on an ongoing basis. At minimum, perform an annual review of who has access to these accounts and determine whether they still need these access levels.
- **Monitor all login activity associated with administrative accounts**: Investigate any activity that appears out of the norm.
- **Require strong passwords and MFA**: Make sure admin accounts each have a unique password that follows strong password requirements. Implement MFA for all for all administrative access to add a second layer of security.

TIP #15

Manage employee access and authorization

Employees sometimes have access to more information than they need to perform their job duties, which raises the risk they will unknowingly share that information with others.

This leads to a host of problems, from the impact on morale if sensitive information is accidentally shared with other employees, to the loss of trade secrets, pricing strategies and other competitive information. On top of that, many organizations are paying for licenses they don't need.

By reviewing access rights and restricting them appropriately, you can help reduce risk, costs and inefficiencies.

NEXT STEPS

- **Review access and authorization rights on a regular basis**: Review these rights wherever appropriate — on your network, in your accounting systems, in your ERP systems — to make sure the user really needs that access level, and determine how often you will do so. Setting a regular cadence further reduces risk.
- **Regularly review licensing**: Ensure counts are accurate and only those who need the licenses have them.
- **Assign an owner to your line of business software**: Involve that individual in the approval process for granting access to systems. Have this individual review the list of people who have access at least annually, if not biannually. If individuals need access to new functionality in your systems, involve the owner in that approval process.

TIP #16

Enhance your email security

Email has always been a big attack vector favored by cybercriminals.

It's exposed to the internet and has historically bad security — and it's easy to manipulate inattentive users with specifically crafted spear phishes. No wonder it's a favorite target. However, there have been a lot of improvements in email security, so you can make it harder for attackers to exploit your email system.

NEXT STEPS

- **Use a cloud-based email system:** Legacy, on-premises email systems require maintenance and security patching — something many organizations struggle to do promptly. If you're still using an on-premises email system that you need to maintain, it's time to move to a cloud-based, SaaS enterprise email system such as Microsoft 365. The cloud provider takes care of the platform and handles security patching so you don't have to.

- **Use MFA:** If you've been reading these tips closely, you know how strongly we feel about MFA. It's critical that you enforce this on your email accounts to help combat credential attacks that let attackers take control of your email account.

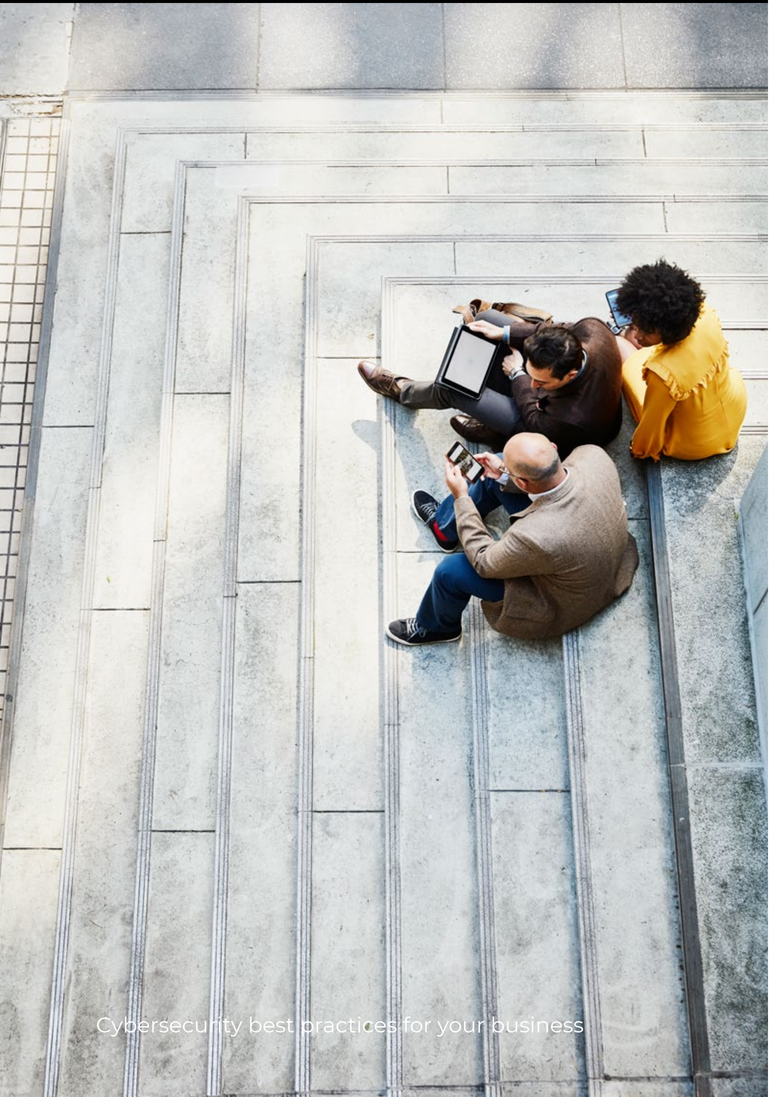
- **Implement email authentication:** Three technologies — Sender Policy Framework (SPF); Domain-based Message Authentication, Reporting and Conformance (DMARC); and DomainKeys Identified Mail (DKIM) — all work together to help make it harder to deliver fraudulent emails to potential victims. If you're not familiar with these technologies, work with your email provider or an experienced administrator to enable them in your environment.

- **Enable external email warnings:** Email systems should be configured to alert message readers that emails originated outside of the organization. This is critical to helping users identify when a cybercriminal is impersonating the CFO and they are not really directing you to wire $75,000 to an escrow account. It's especially important to enable these on mobile email platforms where the apps just display the sender name and don't show you the full email address by default.

- **Train your users to detect and question spear-phishing attempts:** Security awareness training is table stakes. We have to be educating users on how to detect suspicious messages. Moreover, we need to be training them on how to respond accordingly. Whether it's forwarding to IT or verifying the request with out-of-band authentication, train your users on how to respond, and create a culture of professional skepticism when reacting to phishing emails.

TIP #17

Reduce risk around using personal devices



Organizations have seen improved productivity and cost savings by allowing employees to use personal mobile devices for work.

The bring your own device trend continues to rise, trend continues to rise, with 75% of employees using their personal mobile phones for work. But while many vendors offer mobile applications, they may not properly protect the information that is stored in applications on personal devices.

Unprotected information can easily be obtained by cybercriminals when devices are left unencrypted or unprotected by a passcode. Plus, there is the risk the employee will lose or misplace the device. Organizations need to take steps to reduce these risks.

NEXT STEPS

- **Define policies for personal device usage:** This includes how to securely access organization data, as well as the types of information that should be available on personal devices.
- **Implement MDM to protect information:** It's a good idea to implement a mobile device management (MDM) solution. This solution places organization information in a separate container on the device, automatically applies a passcode to that information and allows for remote removal of the information in the event of employee separation or that the device is lost or stolen. It also ensures encryption is enabled on the device before organization information is stored, as well as prevents sharing of information to other apps.
- **Provide guidance on personal device use:** Make sure employees know they need to regularly update mobile operating systems and apps, avoid using risky public Wi-Fi and avoid leaving devices unattended and unlocked. Provide this guidance on a regular basis to remind employees of the importance, as well as help new employees navigate the policies.

TIP #18

Use a secure configuration baseline

This is a bit more of an advanced cybersecurity technique. A secure configuration baseline really has two main components: 1) the actual baseline secure configuration and 2) an ability to identify deviations from the secure configuration.

The secure configuration is an organization's defined security settings to be applied to workstations, servers and network infrastructure. Once those settings are configured, you can't assume they'll always be that way. It's possible that an employee makes a modification to a security parameter as a matter of convenience or a simple mistake. What you should really be worried about is that hackers will start modifying some of your settings during an attack.

You should have a process to periodically compare what's actually in place to your approved baseline. You can do this manually or you can automate it, but either way, it's imperative to be able to detect an unauthorized security configuration as close to time of change. Whether it was an innocent mistake that weakens your security posture or is an indicator of compromise, you need to know so you can get it fixed ASAP.

NEXT STEPS

- **Inventory your systems:** The first step is making sure you understand your systems and the different makes and models of infrastructure that make up your environment. You should also know how many of each so you can help identify when unauthorized devices might be connected to your network.
- **Define the parameters of your baseline:** Once you have your inventory defined, you can build the set of parameters and values that will make up your configuration baseline. You'll probably have to do some research, or you might want to engage some consulting help with specialists. In addition to the computer infrastructure itself, you might consider key business applications, just in case there are security settings you want to monitor there.
- **Establish how you'll monitor:** Automated or manual, you'll need to designate some resources to monitor your secure baseline. This involves regularly inspecting the current state settings and comparing them to your baseline.
- **Ensure you have an investigation process:** When you identify a deviation where some setting in the current state doesn't match what's defined in your baseline, you'll need to investigate the change. Did that change move you to a more secure posture or less? Who made the change? Was the change authorized? Any time there's an unauthorized change, it could be an indicator of compromise, so link this to your incident response process.

TIP #19

Understand and manage your vulnerabilities

New vulnerabilities are continuously discovered and announced.

Sometimes software developers are able to release new software versions that address vulnerabilities before cybercriminals are using them to exploit your networks. Other times, though, hackers find the vulnerabilities first and start exploiting them before the software vendor can release a fix and you can get your systems updated.

This is why vulnerability management processes are so critical to helping ensure your cybersecurity. To keep pace with the hackers, you need to continuously scan your environment and look for security holes that need to be patched. Thankfully, there are tools that can help automate the process to identify missing security patches and deploy the software updates.

NEXT STEPS

- **Implement a continuous vulnerability management utility:** In order to identify security vulnerabilities, you'll need to scan for them. Utilities such as Tenable.io are specifically designed to regularly scan your systems and report any identified vulnerabilities.
- **Define thresholds for patch application:** Not all vulnerabilities are created equal. Vulnerabilities on internet-facing systems that directly lead to remote code execution and have publicly available exploits are much more severe than vulnerabilities that can theoretically lead to memory dumps on internal file servers. You'll need to set priorities and expectations for a patching cadence so that your most vulnerable and highest-risk systems get patched first.
- **Develop testing processes:** Patches can introduce risk, so it's important to validate patch compatibility with key systems. To do this, you'll need to establish a test environment for your critical systems and apply the patches there first. Running through some validation steps to make sure the patches don't negatively affect your key systems can save a lot of headaches.
- **Consider automated patch distribution systems:** Depending on the size of your environment, it's quite possible that you won't be able to manually roll out patches to all your workstations and servers. As your organization continues to grow, you may need to look for automated patching systems or a managed services provider to handle it for you.
- **Develop management reporting:** Staying current with patches and managing your vulnerabilities takes constant diligence. Management reporting will help you track and report your progress. If you're falling behind and not meeting your thresholds, management reporting can help make the case for additional resources to get back on track.

TIP #20

Stay up to date on threat intelligence

Cybercriminals are constantly developing new tools, methods and exploits to take advantage of vulnerabilities.

To more effectively discover and respond to attacks, your organization must stay up to date with recent threat intelligence.

Failing to stay current can leave you open to attacks and compromise, since the attacks may use methods you're not aware of. This can lead to massive sensitive data loss, disruption of services, destruction of critical infrastructure and the theft or loss of large sums of money.

Staying current doesn't have to be a huge undertaking. Active threats are routinely identified and reported by government agencies, including US-CERT and the FBI, as well as numerous private companies. They also typically include guidance and instructions to protect against and mitigate attacks.

NEXT STEPS

- **Identify respected organizations that provide reliable threat information:** Some may require fee-based membership for full access, and some may come as a part of a service. You can also choose organizations based on your industry. For example, InfraGard has industry-specific chapters you can join. Other valuable threat intelligence sources include SANS Institute, Internet Storm Center/DShield and US-CERT.

- **Leverage an ISAC as one of your sources:** The National Council of ISACs comprises information-sharing and analysis centers in different industries whose purpose is to share information around cyberthreat prevention, protection, response and recovery. Examples of ISACs include the MS-ISAC for state, local, tribal and territorial governments; Health-ISAC for the healthcare industry; and FS-ISAC for financial services firms.

- **Use the information provided:** Apply information obtained from (but not limited to) these sources to continuously evolve your cybersecurity program and stay ahead of new threats.

TIP #21

Implement managed detection and response

For cybercriminals, traditional viruses have fallen by the wayside in favor of fileless malware that runs in memory.

During the first half of 2022, organizations worldwide were hit with 236 million ransomware attacks. Cybercriminals know your data is valuable to you and that you'll likely pay to get it back.

Because ransomware and other modern attacks can evade detection from traditional antivirus technologies, your organization needs automated and artificial intelligence-based solutions that can identify abnormal activity occurring within your computers and networks.

Many organizations are now using managed detection and response (MDR) to do so. MDR leverages both automation and outsourced specialists to monitor your environment, identify security incidents and respond quickly to mitigate threats and evict attackers. It's also much more cost effective than hiring and retaining dedicated security operations staff, especially considering that due to the cyber labor shortage, only 68% of open cybersecurity jobs actually get filled.

NEXT STEPS

- **Select an MDR solution:** Choose a solution that aligns with your organization's internal and external needs. For example, cyber insurance carriers are increasingly requiring their policy holders to have EDR, which is a component of any MDR service, so you're covered in more ways than one by taking the extra step to go with MDR.
- **Find a managed security services provider:** This provider can supplement your team and provide the expertise to identify threats in your network. With the labor shortage, you'll likely want to outsource parts of your security to vendors with the expert staff needed to help protect your organization.
- **Monitor your entire attack surface:** Ensure your MDR solution and team are monitoring all your assets — both on premises and in the cloud.

TIP #22

Baseline your cyber controls and assess your cyber insurance

There's no need to wait until New Year's Day to act on your resolution to up your cybersecurity protections — or back them up with the right, and right amount of, cyber insurance.

Fall is often when organizations build budgets for the coming year, so now might be the best time to take stock of your cybersecurity.

Benchmarking your cybersecurity controls to trusted definitive baselines such as the NIST Cybersecurity Framework, HIPAA, HITRUST and the PCI Data Security Standard should be your first step. This will help you quickly identify whether any leading-edge protections to thwart the latest cyberthreats are missing from your arsenal.

Once you have the right cybersecurity controls in place, it's time to perform independent third-party testing to re-baseline the controls' performance. This gives you confidence that they're doing what you need them to do. Make sure to also establish the updated reference baselines you'll need to readily detect unauthorized access attempts and other attacker intrusions.

You can use these updated baselines to inform your cyber insurance strategies. You'll want to purchase cyber insurance to hedge your downside risk costs incurred if cyberthreats such as ransomware and data exfiltration bots unexpectedly overwhelm your cyber defenses. It's essential to not only buy enough coverage but also to buy the right types of cyber insurance. Ensure that policy limits are consistent with your risk appetite, and that your policies provide benefits for all cyber incidents that your risk assessments identify as relevant to you.

NEXT STEPS

- **Perform a security assessment:** Audit and assess your security to identify gaps in your cybersecurity program.
- **Reinforce cyber defenses:** Be proactive in identifying gaps and weaknesses in your cyber defenses, and implement new/additional capabilities to bridge these gaps.
- **Re-baseline:** Engage independent third-party testing to update cyber defense performance reference baselines and adjust cyber insurance policies in response to changes from the past.
- **Confirm cyber insurance coverages and limits:** Most organizations should at least carry data privacy breach, network liability and data ransomware/extortion coverages, with limits consistent with their risk appetite.

TIP #23

Secure your digital supply chain

Your past experiences with vendors and service providers might have painfully pointed out the importance of securing your organization's supply chain for physical goods and services. But what about your digital supply chain?

When you think of cloud service providers as part of the digital supply chain, you can apply lessons learned to help ensure the resiliency of business processes that depend on them. Cloud services present unique risks that must be qualified on top of those risk attributes you may have already considered in third-party risk assessments of legacy vendors and service providers.

This means that you can't stop at accrediting cloud service providers' core cybersecurity control capabilities, commercial insurances (especially cyber liability coverage) and ongoing financial viability, as you've been doing for all vendors/service providers.

Your cloud service provider review scope must expand to consider cloud-specific cybersecurity requirements. It must also place an even greater emphasis on cloud service providers' business continuity and disaster recovery capabilities in concert with your organization's own plans for supplementing (or replacing) cloud services when they unexpectedly become unavailable or constrained.

Any risk review should strive to assure you that implementing services won't unacceptably raise your risk profile. If it could, then you need to map and implement additional controls required to reduce related risks to tolerable levels prior to the go-live date. Performing a risk review of cloud service providers is no different; make sure to benchmark their risk profiles against your own.

Finally, to ensure the confidentiality and integrity of the information being shared in the cloud, and to ensure the reliable ongoing availability of dependent business processes, make sure you also review cloud-specific risk attributes. These include data segmentation and partitioning, virtualization security, data sovereignty, and secure coding practices, among others. Take extra care when confirming the viability of associated recovery plans.

NEXT STEPS

- **Classify the cloud service:** Is it Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS)? Moving from SaaS to PaaS to IaaS is called "down the stack," and the further down the stack your subscribed cloud service lies, the more responsibility you must take for the design, application and effectiveness of the associated cybersecurity controls.
- **Identify all essential service provider and user entity controls:** Review assurance reports from the cloud provider to identify their controls. Those they direct must exist at the user entity to protect the information to be shared into the cloud.
- **Establish and benchmark the cloud service provider's risk profile:** Use service provider/user entity controls knowledge to estimate the level of cybersecurity risk that information shared into the cloud will be exposed to. Measure this in context of information sensitivity and controls strength, and benchmark to the information's risk profile when it's on the internal network.
- **Emphasize continuity/recovery plan viability:** Deep-dive both the service provider's business continuity and technology disaster recovery plans, as well as your own. Any gaps or insufficiencies you accept will create weakness in your digital supply chain.

TIP #24

Level up your defenses with red and purple team exercises

Penetration tests are great methods to identify vulnerabilities in your network and show the risk associated with them.

What happens when you have implemented your remediations? It's time to start thinking about a red or purple team exercise.

A red team exercise emulates an adversary that may attack your organization and sees whether your controls prevent the adversary from achieving their objective, such as obtaining proprietary information or personally identifiable information.

It can challenge the assumption that your enterprise and extended detection and response (EDR or XDR) capabilities will mitigate the threat and tests whether your network defenders can identify and respond to a breach.

A purple team exercise is a collaborative exercise in which the attackers collaborate with your network defenders to understand your network and the controls you have in place. The red team will define a set of tests to make sure your controls are working as anticipated and make sure your network defenders can identify the red team's malicious activity.

NEXT STEPS

- **Evaluate the state of your network security program:** A red and purple team exercise is not for every organization and is best suited for those that have a mature cybersecurity program. Some questions to help you evaluate whether a red or purple team exercise is right for you: Have you conducted a recent penetration test? Do you have an EDR or XDR solution? Do you have an incident response plan?
- **Assess whether you need a penetration test versus a red team/purple team exercise:** What is the end goal of the engagement? Do you want to see whether there are vulnerabilities in your network? If so, a penetration test may be right for you. Do you want to see if your cybersecurity controls can detect and respond to an intrusion? In that case, a red or purple team exercise may be right for you.
- **Conduct a red team or purple team exercise:** A red team exercise is less collaborative and provides a test for your network defenders and your EDR or XDR capabilities, as the organization may or may not choose to disclose the red team exercise to their security personnel. A purple team exercise makes sure your network defenders can see the attacks happening in real time or your EDR or XDR capabilities can detect and prevent malicious activity.

TIP #25

Understand the cyber implications of vendor risk management

One of many things we've witnessed in the past two years is just how fragile and interconnected our supply chain is.

As you think about your vendors and key suppliers, which of those are you most dependent on? Many organizations think about financial stability and brand reputation when evaluating partners for a business relationship. Have you done enough to validate that they also have adequate cybersecurity measures in place and that they will likely be able to withstand cybersecurity attack and still meet your expectations?

NEXT STEPS

- **Inventory your key partners and suppliers:** Get started with building an inventory of your key suppliers and business partners. It's a good step, too, to record the type of information you share with them. If you're providing personally identifiable information such as payroll data for employees or medical information about customers, this raises the risk profile of the relationship.

- **Evaluate their cybersecurity safeguards and practices:** It's important to discuss cybersecurity controls and your expectations for what safeguards are in place to protect the data you share with your business partners. Similarly, it's important to understand what additional controls and safeguards are in place to help them withstand an attack. If the company can't provide you with a SOC report, or some other form of assurance around cybersecurity controls, you might need evaluate them independently if the risk warrants it.

- **Negotiate cybersecurity attack notice requirements:** If you have key vendors and suppliers, you'll want to make sure they are required to give you notice of cybersecurity events they experience that could disrupt your business operations. Depending on the importance of the supplier, you'll need to think through how quickly they should notify you of disruption. Is 10 days sufficient notice, or will too much commerce be lost by then? 36 hours? 24 hours? Find the right number and make sure the notice period is defined in your contract.

- **Identify alternatives:** In the event that one of your key suppliers is taken down by a cybersecurity attack, you'll need alternative suppliers in place to make sure your business cycles aren't interrupted.

- **Regularly evaluate:** This isn't a once-and-done activity. You'll need to regularly reassess your key partners and suppliers to identify whether there have been any material changes in their cybersecurity posture. Are they still carrying enough insurance? Have they had any attacks? If so, what was the impact? Have they implemented any new systems that required changes in the cybersecurity safeguards? The point is to identify any changes that increase your exposure to attacks affecting your suppliers and therefore your own resilience.

TIP #26

Address regulatory requirements affecting cybersecurity

Cybersecurity attacks have become such a significant and ongoing threat that a variety of regulatory and oversight bodies have introduced cybersecurity requirements for their constituents.

The HIPAA Security Rule, PCI Data Security Standards and FFIEC requirements have long been established and should be well known by now. Other regulatory requirements are in early stages of implementation and could have large impacts if they apply to your organization.

The Department of Defense (DoD) is working on implementing Cybersecurity Model Maturity Certification (CMMC) requirements into its acquisition rules.

The National Association of Insurance Commissioners has defined a model law for cybersecurity requirements, and each state is in process of implementing these requirements. The Federal Trade Commission has defined cybersecurity safeguards required for nonbanking financial institutions. Even large organizations with complex supply chains and distribution networks, such as automotive manufacturers, are mandating their own cybersecurity programs.

NEXT STEPS

- **Research your industry and look for specific cybersecurity requirements:** The U.S. doesn't have one overarching federally mandated cybersecurity law, so each industry is creating its own standards and requirements. You'll need to do some research to understand what applies to you. It's always a good idea to consult specialists if you're unsure what applies to your organization.
- **Review contracts to identify contractual obligations:** Sometimes contracts you have with your customers will specify what cybersecurity requirements apply to you. This is especially true with contracts with the DoD or prime contracts that flow down CMMC requirements. You'll want to review contracts with your major customers to make sure you understand whether your customers have dictated cybersecurity requirements.
- **Obtain top-down support:** By gaining top-down support for cybersecurity, you can more effectively obtain budget and organizational commitment to a comprehensive security program. After all, significant portions of your revenue stream may be dependent on meeting these cybersecurity requirements.
- **Conduct an assessment to identify gaps:** These regulatory requirements for cybersecurity practices are high hurdles to clear. Almost no organization has everything in place right out of the blocks. You'll want to conduct a gap assessment to identify what you're missing and develop a remediation plan to ensure you comply with the requirements.
- **Work with specialists to implement required safeguards:** It's not uncommon for an organization to need help meeting these cybersecurity requirements. There's usually a lot of interpretation that needs to be made to take a general regulatory statement and apply it to your environment. Be sure to work with a specialist experienced in the given regulation to make sure you get it right and can defend the judgements you made in designing your controls and implementing safeguards.

TIP #27

Don’t forget about physical security

With so much of the world online these days, it can be easy to overlook the security of physical spaces such as your organization’s offices.

But criminals are still interested in gaining unauthorized, physical access to restricted areas such as server rooms, or in stealing company documents and computers to retrieve sensitive data. They often use social engineering techniques to do so.

This can result in not only robbery but also malware installation, data breaches, corporate espionage and the loss of access control in and out of your property due to stolen identification.

NEXT STEPS

- **Train employees on how to prevent tailgating and piggyback rides:** Criminals will often gain unauthorized entry to restricted spaces by tailgating (slipping in behind someone when entering a restricted area) or piggybacking (using social engineering to convince someone to provide access to a restricted area). Employee training is critical to being able to identify social engineering techniques, as well as overcoming common courtesies such as holding the door open for someone right behind you when they should have to swipe a keycard to get through that door.
- **Make sure everything is locked:** Lock devices, doors and drawers to help prevent unwanted access. Also, test automatic locks and keypads on a regular basis. Keypad batteries die, leaving doors automatically unlocked for fire safety reasons and allowing an opportunity for a breach.
- **Shred documents:** Frequently shred documents with any sensitive information and ensure these shredded documents are disposed of properly. Many organizations have locked containers throughout offices that allow employees to insert documents to later be shredded by authorized personnel.

TIP #28

Involve the experts in your incident response planning

When was the last time you took a long road trip and didn't consult a map either before or during the drive? The prudent, risk-managed response is never, or at least rarely.

This logic extends to incident response planning — the process of pulling together a roadmap that helps you implement a cybersecurity incident management capability in alignment with your organization's unique requirements (i.e., mission, size, structure and functions). Just as when you're successfully navigating your way cross country, your guiding principle here should be "begin with the end in mind." You want your incident response plan to be informed by the knowledge and experience of best-practice experts and resources who have been there before. This approach not only enables you to get the right things right the first time but also launches nascent incident response capabilities to much higher levels quickly and efficiently.

Every incident response plan should map the incident response lifecycle: prepare, detect, analyze, contain, eradicate, recover and lessons learned. Minimum plan components should include incident severity classification criteria, the incident response team roster, forensic evidence handling standards, lists of topical internal and external resources, and procedures or playbooks that guide technical response steps specific to the threat scenarios likely to impact you.

The best way to embed all this quickly, and with maximum utility and efficiency, is to look beyond the boundaries of your own planning horizon to resources such as NIST and the US-CERT, as well as third-party incident response planning experts, and then engage this knowledge around your planning effort. Equally as important is keeping an existing incident response plan up to date. These same external resources have already encountered and taken in the leading edges of the current threat spectrum, and as a result, are readily available to respectively advise or inform.

NEXT STEPS

- **Commit to a standards-based planning approach:** Practice makes perfect, and as a result of the exacting process for their acceptance, standards represent unassailable planning criteria that you can trust have already proven successful many times over.
- **Bring specialized resources into the planning process:** Why go it alone? And why waste the time associated with trial and error? Reach outside and rely on trusted experts as both process enablers and force multipliers to most quicky home in on what's most important to you.
- **Focus on the highest-risk, leading-edge threat scenarios:** While your incident response plan should evolve over time, today's cyberthreats are such that you need playbooks for certain incident scenarios nearly immediately. As a result, it's critical that you quickly identify and implement these at the very beginning — expert knowledge enables this to happen.
- **Plan your work, work your plan:** Train and test, absorb lessons learned and then train and test some more until you can do it in your sleep. External experts are highly skilled at compressing this cycle.

TIP #29

Use multi-factor authentication

MFA is still as relevant now as it was years ago when it first became a recommended best practice.

Why? Because it protects data against lost or stolen passwords and equipment. It reduces the surface area of attack for cybercriminals trying to access your organization's data. And it improves security so that remote employees can access systems and resources from anywhere.

MFA is also increasingly required by regulations (e.g., HIPAA, CMMC, FFIEC) and cyber insurance providers, who are making it a condition of policy renewal and underwriting.

NEXT STEPS

- **Inventory all platforms:** Identify all platforms where employees have access to remote company data and resources. This can include email, VPN, remote desktop platforms, cloud solutions and collaboration software.
- **Implement MFA solutions:** For any of your identified remote access and internal admin accounts ,you'll need to implement MFA solutions. Note, some organizations require more than one solution, as deploying MFA on internal admin accounts can be technically more challenging and requires specialized solutions.
- **Review vendor account logins:** Your vendors should also have MFA enabled, further increasing the level of security throughout your organization.
- **Engage third-party expertise:** A third party can audit and implement MFA solutions around your organization, from online collaboration platforms to security systems to line-of-business software.

TIP #30

Use a vCISO to provide strategic security direction

Whether it's addressing vendor due diligence requests, responding to a security incident or enhancing your information security program, your vCISO provides both the oversight and ongoing assistance your organization needs. If you have a regulatory requirement to hire a CISO, the vCISO can fill that requirement.

Chief information security officers are expensive and, candidly, most midsize organizations can't justify having one as a full-time executive.

As vital as it is, hiring a chief information security officer (CISO) is a huge challenge for every industry. They're in high demand but short supply, and they command a significant salary. At the same time, most businesses need the expertise a CISO brings to the table, not the 40 hours a week that come with a full-time position.

Enter the [*virtual* chief information security officer]() (vCISO). A vCISO's fractional ownership model gives you part-time access to senior executive cybersecurity leadership and risk management capabilities. In other words, the CISO position is filled on a part-time basis by a consultant, and this person commits to providing strategic cybersecurity direction and helping organizations enhance their cybersecurity posture.

NEXT STEPS

- **Engage a specialist provider of vCISO services:** Work with a firm that has the resources and experience necessary to provide executive-level oversight for strategic cybersecurity issues. Whether you need to meet industry-specific cybersecurity requirements to move into a new market and drive growth, or restore customer confidence after a cybersecurity breach, you need someone who's "been there and done that" to set your course.
- **Set priorities and cybersecurity program objectives:** Your vCISO needs to interact at the executive level and understand your business objectives. This is critical to aligning the cybersecurity program to support your business growth.
- **Dedicate resources to do the work:** By definition and structure, the vCISO isn't a doing role. It's oversight and strategic direction for your cybersecurity program. The vCISO will structure initiatives, track progress and clear roadblocks on initiatives. You'll need to dedicate staff time to doing the work and making progress on the cybersecurity initiatives.
- **Ensure vCISO agenda time at executive and board meetings:** It's important that you view the vCISO as an extension of your executive team. The vCISO will be presenting progress and key performance indicators about your cybersecurity program effectiveness, and may be escalating issues to the rest of the C-suite. Without interaction and support of the executive team, the vCISO won't be effective driving the change you need in your cybersecurity program.

Become a more cyber-resilient business

How many of our 30 tips has your business already implemented? With the cyber landscape constantly evolving, there's always room to improve defenses and reduce risk. At Wipfli, our goal is to help you ensure the confidentiality, integrity and availability of your information assets.

Learn more ▸

With our cybersecurity professionals at your side, you can:

- Increase your resistance to cyberattack
- Securely access your programs and data, regardless of device or location
- Leverage highly available, fault-tolerant cloud solutions
- Recover from cybersecurity attacks and system outages
- Grow your business with industry-specific cybersecurity compliance programs
- Address SOC for Cybersecurity and enhance disaster recovery and business continuity

Perspective changes everything. WIPFLI