30 tips for Cybersecurity Awareness Month

Cybersecurity best practices for your business



WIPFLI

Are your cybersecurity measures where they should be?

Data breaches are happening more frequently and costing businesses more each year.

Wipfli's 2025 collection of the most timely and relevant 30 cybersecurity security best practices, released during Cybersecurity Awareness Month in October, can help you navigate the threats and challenges that are an unavoidable part of business life all year round.

No matter how far along an organization's information security practices are in their development and enforcement, these tips can provide you with assurance or important starting points to tighten up your policies and processes. Your efforts need to be ongoing and nimble, as the cybercriminals are set on confounding the latest defenses.

Read on to learn about everything from the biggest targets for cybercriminals to how AI and other tools can help propel — and thwart — attacks, and how you can help protect your business 24/7. We've collected all 30 tips in one convenient e-book.

The global average cost of a data breach in 2025 was $4.4M

2025 saw an 84% uptick in phishing emails on a weekly basis.

An estimated 3.4B spam emails are sent every day.

Organizations that used AI security extensively saved 1.9M compared to organizations that didn't.



© Wipfli

TIP #1

Protect personal devices from cyberattacks



Incidents of malware and other cyberattacks have exploded in recent years, preventing businesses from accessing their data.

Organizations that allow employees to use personal devices for work face an even higher risk of a breach. Indeed, some 87% of businesses are dependent on their employees being able to access business apps from their devices.

Organizations must balance the cost-saving advantages of not issuing phones and tablets to employees, as well as the convenience of employees being able to use their own devices for work, against the added vulnerabilities.

A user who does not understand their company's bring-your-own-device (BYOD) security policy creates exposure for themselves and the business. Because fewer than half of U.S. companies have established a policy, the potential for problems is high. Employees may not adhere to the same security standards they would when using a company-owned device.

More than 60% of data breaches are attributable to a lost or stolen device. A single missing device containing sensitive data is enough to jeopardize an entire business. While all users should protect devices with multifactor authentication to create obstacles for potential criminals, a mobile device management solution is critical in BYOD security so that administrators can lock or wipe a device in case the device is lost or stolen.

NEXT STEPS

- **Develop a BYOD security policy that is reasonable for employees while protecting your interests:** It should spell out what the business will access and what it won't access. The policy should also define measures for when a device goes missing or when an employee leaves the company.
- **Look into a mobile application management system:** You can customize controls based on how apps are used, the type of user, the application, the network or the time of day. You can also specify which apps are approved and which ones are banned.
- **Consider an organizationwide mobile content management system:** It keeps you in control of secure company data while user information on personal devices remains private.

© Wipfli

TIP #2

Make the most of multifactor authentication



Effective cybersecurity risk management requires continuous improvement. Remote and hybrid work, plus multiple access points to your business network or cloud services and applications, have made multifactor authentication (MFA) an indispensable practice.

MFA protects against attacks that use easily guessed or stolen passwords.

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

These critical defense layers make it harder for attackers to infiltrate your systems. Most are familiar with one-time codes and facial recognition in addition to passwords. But biometric verification using a wider array of traits is gaining ground. It includes everything from retina and iris scanning to earlobe and hand geometry to fingerprint scanning, digital signature scanning and voice authentication. Biometric device components include a reader, a database and software to convert the scanned/biometric data into a standardized digital format and compare match points of the observed data with stored data.

You can also use single sign-on (SSO) with MFA enabled to help reduce the number of authentication sources that need to be secured with MFA. SSO uses a central authentication server to confirm a user's identity and provide access to the associated applications or resources. It allows you to enhance security and streamline operations in settings where users frequently need to access multiple services.

NEXT STEPS

- **Inventory all platforms:** MFA should be used broadly across your organization. Identify all platforms where employees have access to remote company data and resources, including email, VPN, remote desktop platforms, cloud solutions, corporate bank accounts and collaboration software.
- **Implement MFA solutions:** For any of your identified remote access and internal admin accounts, you'll need to implement MFA solutions. Some organizations require more than one solution, as deploying MFA on internal admin accounts can be more technically challenging. Your vendors should also enable MFA.
- **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.

© Wipfli

TIP #3

Defend against AI-generated cyberattacks

Once attackers have identified a piece of infrastructure to go after, they can use generative AI to shape and execute attacks wherever they choose. They can generate social engineering campaigns or use AI to generate scripts that will be used as part of an attack.

From a defensive standpoint, you can employ machine learning to look at huge quantities of data about attacks to identify patterns of what suspicious activity looks like and start monitoring in real time for those activities that have been indicators of compromise elsewhere.

Because AI will help increase the quality of phishing schemes against individuals to trick them into divulging information, organizations and employees need to be cognizant of what those social engineering attempts look like to identify them and function as a kind of human firewall. AI-generated messages may be more specific and better crafted toward their target compared to human-generated attacks. They'll include language inflections and terminology that will mimic a real person much more closely than before.

Deepfake attacks are another AI development. These generate media, such as videos or images, to impersonate specific real people and carry out fraud or disinformation campaigns. In the workplace, actual audio could be fed into an AI model, which can synthesize speech, saying whatever the attacker instructs it to and that sounds just like a known individual.

It's also crucial to assess your organization's AI security practices when adding AI tools into your workflow. If you have excessive sharing settings, bad actors could use AI to quickly access sensitive information from unauthorized accounts, shortening the time between network compromise and data exfiltration.

NEXT STEPS

- **Increase your level of scrutiny:** The tell-tale signs of email or text-based phishing attempts may disappear with AI-generated campaigns. These better-crafted messages won't include the kinds of spelling, grammar and other language issues that often raise red flags about malicious intent. So, in the absence of the usual tipoffs, ask yourself if this person is someone who would normally contact you or have any reason to contact you. Would it make sense to engage with them? Checking the "from" field will still be a useful way to help verify the sender's authenticity.
- **Check with an actual sender or caller:** If you receive email or voice messages that give you pause about their authenticity, get in touch with the person through an out-of-band channel (don't reply to the email or call the number provided) to verify the request is real. Any outreach that seems like a scam should be reported to your cybersecurity team.
- **Review your vendors:** It's equally important to review your vendors' AI usage alongside your own. Your organization must understand how vendors are using your data within their AI modules or large language models.
- **Monitor your policies and procedures:** As your organization adopts AI solutions, it's essential to update your security policies, acceptable use policies and procedures for proper enforcement. You also need to review your security architecture to ensure you have the right policies in place to prevent unauthorized access to sensitive data by AI tools.

© Wipfli

TIP #4

Strengthen your email security

Email has always been a chief attack vector favored by cybercriminals. Its exposure to the internet along with historically weak security makes gaining unauthorized access to email accounts relatively easy.

Common ways to recognize BEC — business email compromise — scams include highlighting time urgency and positioning the sender as authoritative (impersonating a CEO, CFO or another C-suite executive). The threat actor may make an unusual-sounding request seem legitimate by providing a plausible reason for it and clear instructions on how and when to meet the request, which may involve transferring a specific sum of money.

For all the vulnerabilities, there have also been many improvements in email security. Here's how to make it harder for attackers to exploit your email system.

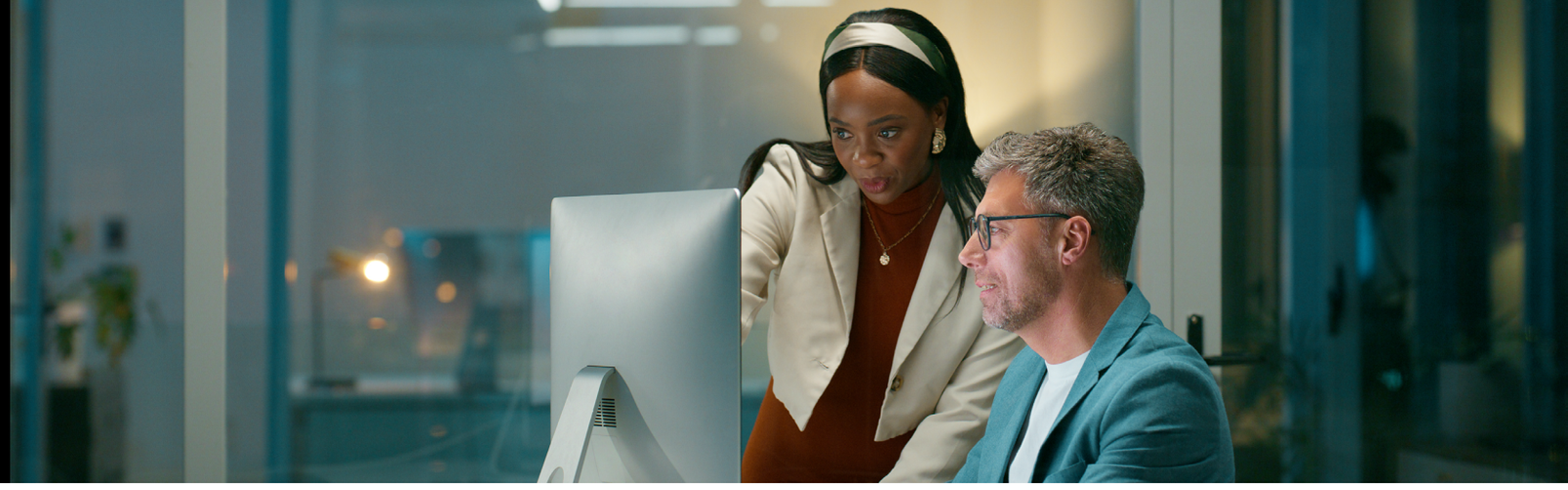
NEXT STEPS

- **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-prem 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 :** We can't reiterate strongly enough how important MFA is. Enforcement is critical to 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 the instruction to wire $75,000 to an escrow account is a scam. It's especially important to enable these on mobile email platforms where the apps just display the sender's name and don't show you the full email address by default.
- **Consider higher-level security monitoring:** Systems such as Microsoft 365 contain behavioral analytics tools that enable your team to identify indicators of compromise in a timely manner. You should be able to see when hackers are getting into employee email though alerts about "impossible travel" by your employees. If a U.S. user's login suddenly appears to be coming from Romania, it would be flagged as a compromised email. An additional layer includes "security information and event management" that combs through the log activity of every device. AI helps do automated threat hunting based on all the collected log data. Tools can also verify that links and attachments are safe before a user is allowed to access them.
- **Train your users to detect phishing attempts:** Security awareness training should be mandatory for all and ongoing. Repeat your reminders for how to detect suspicious messages — and how to respond, whether it's forwarding to IT or verifying the request with out-of-band authentication.

© Wipfli

TIP #5

Resist multifactor authentication bypass attacks



While MFA is increasingly available and accepted for reducing cyber risks, the criminals seeking to thwart it are also getting better. MFA is necessary, but it doesn't guarantee the security of your accounts and systems.

Attackers are working on new approaches to thwart MFA as quickly as users are adapting it. Their techniques include:

- **MFA bombing attacks:** When a criminal breaches a user's password, they trigger the MFA system to send push notifications for login approval repeatedly, hoping to exhaust the victim into approving the request.
- **Web traffic interception:** Cybercriminals use fake websites or proxy servers to trick victims into revealing their credentials and MFA codes.
- **SIM swapping:** SIM swapping allows attackers to bypass MFA by hacking phone carriers and assigning SIMs to their own devices. Using stolen credentials, they get the carrier to assign the SIM to their phone and, as a result, MFA codes are sent to the attacker's phone instead of the legitimate user's.

NEXT STEPS

- **Make sure legacy authentication portals are disabled:** Early-stage portals don't support MFA, so turn them off.
- **Enforce MFA on every available external login portal possible:** If there is a username and password on your website or for your employees to log in, it absolutely has to have MFA on it. If employees are using personal devices, it's also important to have them create an added layer of protection against these attacks by adding MFA to their carrier accounts as well.
- **Take advantage of authenticator apps-based MFA:** Authenticator apps generate time-based, one-time passwords on a device, adding an extra layer of security and helping eliminate SMS vulnerabilities. They can also streamline the MFA process by securing all accounts in one app.
- **Remove options allowing for push notifications:** Having users input a number from tools such as authenticator apps is much more secure than bypassing MFA by clicking on a push notification.
- **Review your conditional access policies:** Some companies skip MFA for Microsoft logins from a company IP or mobile device. If you allow single-factor authentication, check for process vulnerabilities.

© Wipfli

TIP #6

Stay on top of 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.

A Verizon study of hacking-related breaches found that 80% of breaches were linked to passwords. The most common methods for compromising accounts are lost or stolen credentials and password guessing.

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

Smart businesses are shifting away from relying solely on passwords as an access tool, both because of security weaknesses and out of a recognition that users are frustrated with frequent reset requirements. Having MFA requirements in place that may still include a password is a sound approach to enabling access and protecting your systems and data. The passwordless Windows Hello authentication system that relies instead on PINs is also gaining traction.

Take measures to help ensure that the rules around password use are strong and enforced. Preventing the use of weak or reused passwords at your organization is vitally important.

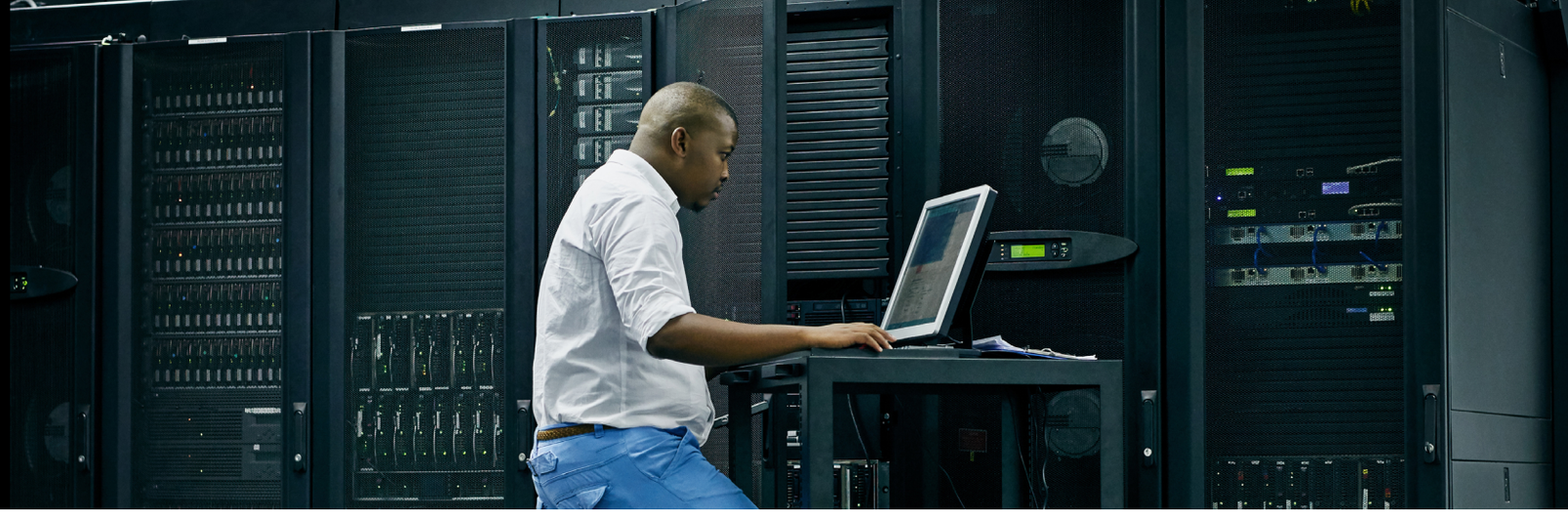
NEXT STEPS

- **Implement password filtering:** 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.
- **Encourage passphrases over 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.
- **Increase your minimum password length:** If passphrases are adopted as a standard, 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 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.

© Wipfli

TIP #7

Install a trustworthy data backup system



Businesses depend on their valuable data gathered and stored for years. It can all be lost in an instant as a result of external and internal threats.

Whether it's a ransomware attack or data lost to thieves or natural disasters, your proprietary information and customer database are at risk of being stolen and sold off without the right protections in place.

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. If your organization isn't able to recover their data, the result may be a loss of confidence in your organization and 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 help protect your organization from ransomware attacks. Without quick data recovery, precious time and money are lost.

Data backups offer versatility, reliability and peace of mind. Don't put your reputation and your entire business at risk in the event of data loss due to a breach or any other threat.

NEXT STEPS

- **Designate a backup administrator:** Assigning a single person helps ensure accountability for setup, maintenance and periodic testing.
- **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:** This can help ensure multiple backups that are on-site or off-site, and those that are air gapped, are safe from a malware intrusion. Keep an eye out for immutable backups, a newer feature that prevents backup data from being modified or encrypted.

© Wipfli

TIP #8

Don’t skip the basics

You surely know that keeping information secure is neither an ad hoc nor on-the-fly endeavor. The keys to helping ensure resiliency in the face of threats from cybercriminals and natural disasters require a plan based around structure, documentation, monitoring and accountability.

Your organization may focus on some aspects of information security more than others, so it makes sense to take stock of efforts on a regular basis. Does your business adequately address the core components of an effective information security program? You need an effective, holistic program to keep your data and systems as safe as possible.

NEXT STEPS

- **Shore up your program management:** Be sure this includes a formalized risk assessment cycle, which involves identifying your risks, implementing mitigation strategies, training the relevant people, reassessing them once they are complete — and repeating the cycle from the top.
- **Secure your network:** Track your application inventory. That inventory should include third-party connections and APIs, as they are extensions of your environment. Understand every entity that connects to your network to keep it secure. Annual due diligence should assess the security controls of your third-party vendors, either by examining their audit review or sending them a security questionnaire about their practices. Questions should cover: 1) patch management, 2) offboarding procedures at the end of relationships with third parties or employees (be sure people who shouldn’t have access don’t have access to your information), 3) where third parties store your data encryption practices so it isn’t accessible to outsiders and 4) practices around the data you’ve shared with third parties when the relationships end (return it or delete it?).
- **Shore up your program management:** Use a formalized risk assessment cycle, which involves identifying your risks, implementing mitigation strategies, training the relevant people, reassessing them once they are complete — and repeating the cycle from the top.
- **Implement vulnerability management:** Establish a notification setup to handle zero-day vulnerabilities. When a high-profile, urgent fix is needed for a previously unknown attack, be sure your IT team is fully and promptly alerted to the need for patching and remediation.
- **Ensure strong data control:** Regularly perform access reviews, not only for your Microsoft login credentials, but also for any software that users maintain access to. Your software administrators should be periodically verifying what the user access levels are and whether they need to be updated, given that people transfer jobs and responsibilities. Loop administrators into the offboarding process, so when someone leaves the organization, they can verify what software they had access to and remove that access.
- **Regularly monitor and test the environment:** Have an independent party review your security controls. Consider a 24/7 SOC (and an outsourced test of those controls should be done at least annually). An independent party can connect to your organization and see all firewall activity. If an intruder gets in, they shut down that activity.

© Wipfli

TIP #9

Protect the organization with a password manager

Cybercriminals don't always need a breach to gain an initial foothold in your organization. Employees seldom choose strong, complex passwords, and 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 login at many, even hundreds, of websites). If your users are reusing passwords, both your organization and partner organizations could be at risk.

Given the range 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. Here are their benefits:

- 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 login 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 randomly generated by the password manager, relieving the employee of having to compose a new password for every site or service.
- 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.
- They enable employees to share login credentials with colleagues without disclosing what the password is. If someone with access to your organization's banking information leaves, teammates who also access the account don't need to change and share the password with others. Permission is simply denied to that departing employee.

NEXT STEPS

- **Use an enterprise-level password manager application:** This relieves the user of the issues related to password management discussed above.
- **Implement a single password manager for the entire organization:** Don't let employees use personal, standalone password managers for accessing your organization's assets or services. If an individual leaves the organization, those company passwords leave with them. Meanwhile, employees should not be keeping passwords for sites they access for personal reasons.
- **Select the most appropriate 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. Base your decision on factors such as ease of administration, effectiveness and cost.

© Wipfli

TIP #10

The flexibility of a hybrid or remote workforce comes with challenges for both workers and employers

For Q1 2025, four in 10 jobs allowed some amount of remote work.

48% of job seekers reported that they would like a hybrid role.

With so many organizations managing a workforce with a large share of people working remotely on any given day, it's critical for yours to implement the right technology and security controls to protect that workforce and your organization's data.

Without a roadmap that prioritizes your organization's challenges and factors in technology, your employees will look for workarounds. For example, if your organization hasn't implemented a cloud storage solution, employees may turn to personal Dropbox or Google Drive accounts that don't have proper security controls configured. Because services like these are beyond the control of your organization, the risk of a sensitive data leak increases.



NEXT STEPS

- **Make the most of MFA:** Remote work and multiple access points to your business network make MFA more critical than ever. Beyond passwords and one-time codes, biometric verification using a wider array of traits, from retina and iris scanning to voice authentication and earlobe geometry, is gaining ground.
- **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 MFA.
- **Migrate legacy file servers and applications to the cloud:** Cloud-hosted data is accessible anywhere, which is vital for hybrid and remote workers. By migrating your physical office environments to cloud solutions — which 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 the technology you rely on enables voice, video and text communication for users from anywhere, as well as allows secure file storage and sharing across your organization. Collaboration options include Microsoft Teams, Google Workspace and Webex Teams.

© Wipfli

TIP #11

Revisit employee access and authorization

Properly managing employee access to your organization's data and resources is vital to ensuring the security of your systems and assets. Failure to have the proper methods in place can lead to data breaches and security risks for your organization, and a host of associated expenses.

Do your employees have access to more information than they need to perform their job duties? How do you monitor authorization levels? Your business could be at risk when people share information with others who don't have that access, from the loss of trade secrets, pricing strategies and other competitive information to lowered morale and trust.

What's more, many organizations are wasting money by paying for more licenses than they need. By reviewing access rights and restricting them appropriately, you can help reduce risk, costs and inefficiencies.

NEXT STEPS

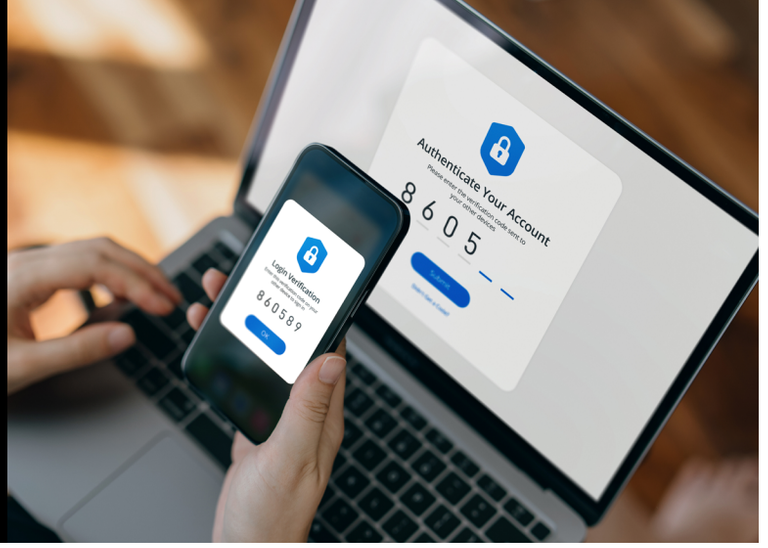
- **Review access and authorization rights on a regular basis:** This is not a set-it-and-forget it endeavor. Review these rights wherever appropriate — on your network, in your accounting systems, in your ERP systems — to make sure the user really needs that access level, and determine how often you will do so. Setting a regular cadence further reduces risk.
- **Regularly review licensing:** Ensure counts are accurate and that 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 process owner in that approval process.



© Wipfli

TIP #12

Know when to use PINs vs. passwords



Organizations that stay on top of evolving security protocols are incorporating the simpler-to-remember PINs (personal identification numbers) into their platforms and sometimes replacing passwords as an authentication tool altogether.

But before you can adopt PINs, you must have the right security foundations in place and be certain your systems are up to date. Currently, an estimated 15%-25% of organizations have adopted the full Windows Hello authentication system that includes PINs on their PCs.

People tend to think of a PIN as a simplified password, but it's more complicated than that. Passwords can be transmitted across systems, whether that's through the internet or from a system to a server. So, when a password gets compromised, a hacker using that same password and login credentials can move from one system to another.

With a PIN, the number used is local to a specific system. It is tied to a single system and a single device. Because a PIN is not transferred, broadcasted or transmitted from system to system to system, in the event that device is compromised, only that particular system is affected. The breach can go nowhere else.

NEXT STEPS

- **Be sure your trusted platform module (TPM) is working properly:** Your organization needs a functioning TPM in its computers, a kind of secure cryptoprocessor designated to carry out cryptographic operations in order to deploy a PIN system.
- **Activate Windows Hello for Business in your PC network:** The Hello PIN is backed by the TPM chip. The chip includes multiple physical security mechanisms to make it tamper resistant.
- **Encourage PIN use:** The comparatively short length of a PIN compared to a password is appealing to users. Another plus: It doesn't need to be changed regularly for security. But never permit anyone to use the same PIN on more than one device.
- **Consider combining PIN and password use:** Setting up a system so a password is still required at restart, along with a PIN, provides an extra layer of protection.

© Wipfli

TIP #13

Elevate data privacy awareness training

Be sure everyone in your organization is clear on the distinctions between data privacy and data security.

- Data privacy centers on the organization's proper use of personally identifiable information, including their responsibilities over that data, how it was obtained, on what and who it was collected about, how it is stored and secured, and how it is disposed of.
- Data security is one piece of data privacy, as it considers an organization's responsibility over the protection of its data from unauthorized access.

Effective cybersecurity risk management means continuous improvement on all fronts. This includes enhancements 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.

It's clear that data privacy and security go together, but remember that data privacy is the fundamental reason why you invest so much in cybersecurity protections. Keeping employees attuned to this may strengthen their response to phishing and other social engineering attacks.

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. And use the opportunity to also cover the data privacy goals and requirements relevant to your organization.

NEXT STEPS:

- **Identify relevant data privacy goals:** Be sure your organization's mission statement and business strategies discuss the importance of 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.
- **Include 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 Protection 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 reasons why:** It's generally accepted that adults learn new things best when they also understand why they need to learn them. Thus, be sure to introduce any and all new data privacy elements in your enhanced curricula and provide context for your employees. When employees understand the necessity of data privacy, they'll be far more likely to do their part in helping to protect data and your organization.

© Wipfli

TIP #14

Mitigate risk in collaboration software



Remote and hybrid work continues 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 an indispensable 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. But beware of cloud collaboration platforms with out-of-the-box settings to allow open or easy sharing.

Organizations that fail to provide employees with a centralized set of secure collaboration tools are setting up an environment in which workers use unapproved apps and software and thus create vulnerabilities. It's up to your organization to implement collaboration solutions that restrict open sharing to avoid becoming an easy target for cybercriminals.

You can use tools to make sure each collaborator can only access what they need to on a project, limiting risk.

NEXT STEPS:

- **Review the 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 with your configuration questions.
- **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 for help in setting up and monitoring 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 critical questions to answer when taking steps to protectyour sensitive data.
- **Configure restrictions on the 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. Engage an experienced third party if there is uncertainty about how to properly configure sharing.
- **Implement an ongoing review:** 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.

© Wipfli

TIP #15

Combat the cyber labor shortage

Even as other segments of the tech labor market are shedding jobs, cybersecurity continues to experience a significant shortage of skilled workers.

2025 estimates suggest that there is a 4.8 million shortfall in cybersecurity professionals. Compounding the shortage is the nearly static number of people in the cyber workforce, with a year-on-year increase of just 0.1%.

Because few business leaders feel confident that they have the right security talent in place, many are open to outsourcing roles to help ensure their organization is doing all they can to protect their data and their systems.

NEXT STEPS

- **Look into outside managed services for help:** With permanent cybersecurity hires difficult to procure, you can find the help you need for the short or long term by working with outsourced cybersecurity pros. Using outsourced professionals may be the most cost-effective approach for organizations, especially with the more limited budgets of small or midsized organizations.
- **Consider fractional leadership:** A virtual chief information security officer (vCISO) can provide the strategic capabilities needed for a sound, effective cybersecurity operation. For smaller organizations, a full-time CISO may not even make financial sense given more limited needs. A vCISO can provide the gravitas needed for your business with a more limited commitment of time and without incurring full-time costs.



© Wipfli

TIP #16

Be sure your vCISO is separate from your IT operations

Chief information security officers (CISOs) are expensive because they are imperative and in high demand and as such can be cost prohibitive for many midsized organizations. Even if you have the budget, CISOs are in short supply. Most businesses need the expertise a CISO brings to the table, but not necessarily for 40 hours a week.

That's when a virtual chief information security officer (vCISO) may be the right move, especially in light of increasing regulatory mandates for oversight of your data security program. 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.

Having a vCISO in place to address vendor due diligence requests, respond to a security incident or enhance your information security program is necessary to reduce risk on a variety of fronts: financial, reputational and technical compliance. Your ability to obtain cybersecurity insurance (or receive payout in the event of a damaging breach) may even require proof that your organization's data security practices are overseen by a vCISO.

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 data breach, you need someone who's "been there and done that" to set your course.
- **Segregate your vCISO from your IT functions:** You need a separation of duties between your data security operations and your information technology team. While individuals in those areas work closely together, their goals are not always aligned with regard to mitigating risk. IT may be more focused on how to get more and better technology in the hands of users, and the data security side is zeroing in on potential new security holes created in those acquisitions.
- **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, 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:** View the vCISO as an extension of your executive team. The vCISO will be presenting progress and key performance indicators about your cybersecurity program's effectiveness and may be escalating issues to the rest of the C-suite.

© Wipfli

TIP #17

Protect against nation-state attacks



Nation-states are increasingly buying tools and services from the dark web while tools developed by nation-states are also making their way onto the black market.

Research shows a 100% rise in “significant” nation-state incidents between 2017 and 2020. An analysis of over 200 cybersecurity incidents associated with nation-state activity since 2009 shows that enterprises are now the most common target (35%). Often, organizations are targeted by nation-state attackers in a ransomware operation to gain funding or in an espionage campaign to obtain intellectual property.

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)

Nation-state attackers often target supply chains. The SolarWinds breach discovered in 2020, for example, underscores the necessity 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 that no malicious code is contained in the update.
- **Test your defenses yearly:** Conduct a red or purple team exercise to verify your defenses. Cybersecurity personnel can detect and respond to advanced attackers that are targeting your network or that are already in your network.

© Wipfli

TIP #18

Make cybersecurity a part of your operations



Many organizations treat cybersecurity as an annual checklist. Efforts are focused on meeting regulatory requirements and reviewing security policies, but effective cybersecurity goes beyond a yearly activity.

Cybersecurity should be embedded into operations and supported by continuous monitoring and proactive processes that help maintain defenses. By integrating cybersecurity into your organization's core functions, you'll be better equipped to respond to evolving threats and protect data as you innovate and grow.

NEXT STEPS:

- **Develop your cybersecurity program:** Operationalizing cybersecurity starts with a program that identifies the key operations you need to perform and at what frequency. What needs to be done daily to be proactive about monitoring threats and reducing the time attackers will have in your systems? What should be done weekly or monthly to help you manage risk, identify vulnerabilities and respond to the latest threats? What should be done quarterly or annually to update and improve your cybersecurity operations?
- **Outsource where needed:** Effective cybersecurity operations require the right processes, tools and people, which can be challenging for organizations with limited resources. Outsourcing certain functions with a managed services provider can help you build a more cost-effective, scalable cybersecurity program.

© Wipfli

TIP #19

Safeguard your digital supply chain



Securing your organization's digital supply chain, reliant on the cloud and SaaS providers that are integral to most business operations, is critical. Commonly used third-party software supply chain components are highly prized targets for cybercriminals.

Cloud services have unique risks that need to be qualified alongside those risk attributes you may have already considered in third-party risk assessments of legacy vendors and service providers.

This means you can't stop at typical vendor due diligence like accrediting cloud service providers' commercial insurances (especially cyber liability coverage) and ongoing financial viability. Your review scope must expand to consider cloud-specific cybersecurity requirements. It must also place an even greater emphasis on a providers' business continuity and disaster recovery capabilities in concert with your own continuity plans for outages.

To maintain your information's confidentiality, integrity and availability in the cloud, review cloud-specific risk attributes, such as data segmentation, virtualization security, data sovereignty and secure coding practices. 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 the cloud service provider's risk profile:** Use knowledge of service provider and user controls to estimate the cybersecurity risk of cloud-shared information. Measure this against information sensitivity and control strength and compare it to the information's risk profile on the internal network.
- **Emphasize continuity/recovery plan viability:** Take a deep dive into both the service provider's business continuity and technology disaster recovery plans, as well as your own.
- **Plan for your security key recovery:** In an outage, recovering security keys and configuration data may be difficult. You need to be prepared to restore your active directory environment from scratch and transfer it to an offline server to retrieve your keys.

© Wipfli

TIP #20

Stabilize the cyberthreat moving target with a cybersecurity risk assessment

The only constant is change. It's a truth that drives businesses' growth and also applies to the constantly evolving cyberthreat spectrum. Variants to well-known threats are regularly emerging along with entirely new exploits and attack tactics.

Complacency around cybersecurity risk management can lead to serious consequences, even the demise of the business itself. If your business loses access to its network or other systems, the impact may be severe.

While gaining a complete picture of your risk can seem elusive given the changing threats, an important way to stabilize the moving target is by conducting a cybersecurity risk assessment.

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 level of protection after you add new business locations, applications or other new processes. 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 risk management journey are much easier to discern and plan for. A risk assessment strategy provides needed structure and accountability.

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 larger-impact cyber risks first, and that it acknowledges 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 that it's still based on relevant assets and threats. Update its methodology and risk-scoring routines to pace improvements advanced by trusted sources, such as NIST.

© Wipfli

TIP #21

Conduct ransomware simulations to bolster your defense

A ransomware attack restricts access to your data by encrypting it, requiring the victim to pay a ransom in order to regain access to their own data.

No industry is immune, as perpetrators know an organization's data is highly valuable and perhaps irreplaceable, though smaller businesses receive a disproportionate share of the damage. Currently, some 82% of ransomware attacks are aimed at small and midsized businesses, as criminals perceive them as less prepared to defend themselves.

Conducting attack simulations can help ensure that employees know their responsibilities. They promote critical communication within your organization and can reduce incident resolution time.

When relevant parties know how to react and who needs to get involved, you can greatly reduce the impact of the ransomware attack. You'll want to address these common questions:

- Can we identify when ransomware first infects a computer on our network?
- How much time elapses between the initial infection and alerting our security team and responding to the alert?
- If ransomware does infect a user's computer, how much data on our network will be encrypted?
- Are our backups secured and safe from encryption during an attack?
- Do we have places on our network where we can't see ransomware activity?

NEXT STEPS:

- **Simulate a ransomware attack through a tabletop exercise or live simulation:** 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 amount of data loss).
- **Facilitate follow-up:** 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. In addition, software tools can help you test your defenses for real, which can supplement the benefits of a tabletop exercise alone.
- **Test your employees' skills:** Use software that can simulate and distribute emails that look like genuine requests from a customer, when in reality, they are attack emails. This helps you understand the areas of exposure internally. But be sure to initiate the emails in a testing mode.

© Wipfli

TIP #22

Level up your defenses with threat-informed testing

Focus your cybersecurity budget to invest in the solutions that are going to have the most impact against the threats that you're facing.

Penetration tests are helpful in identifying vulnerabilities in your network. But what happens when you have implemented your remediations? It's time to start thinking about a red or purple team exercise.

These are adversarial, emulation-based services that mimic attacks that a particular company is likely to face, such as sending them realistic but benign ransomware that helps to see if the security investments they've made are working adequately. They assess whether your controls prevent an attacker from achieving their objective (e.g., obtaining proprietary data or personally identifiable information).

In a red team exercise, the front-line security team won't know this is being done because the test is being conducted to see whether the team security systems prevent successful attacks.

A purple team exercise is collaborative between the attackers and your network defenders. Both sides work together to understand your network and the controls you have in place. After a simulated attack, the attackers work with the defenders to review antivirus and network logs. The goal is to tune your defenses and make sure they're working to prevent malicious activity.

NEXT STEPS

- **Evaluate the state of your network security program:** Red and purple team exercises are not for every organization and are 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 already have an endpoint detection and response (EDR) 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.
- **Consider purple team before a red team approach:** The purple team exercise may be better accepted in your organization because of its collaborative nature, and because it is a time-limited and less-costly option. Purple team pricing may range between $15,000 to $25,000 over a couple of days, while red team is likely to be an engagement lasting a few months, with costs ranging from $35,000 to $100,000.
- **Conduct a red team or purple team exercise:** A red team exercise provides a test for your network defenders and your EDR 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 and reveals your EDR capabilities in preventing malicious activity.

© Wipfli

TIP #23

Set up a security operations function apart from IT

In stepping up your cybersecurity efforts, it's essential that data security operations be separate from traditional IT functions. Whether that security chief is a dedicated, in-house employee or a part-time, virtual security pro, their duties need to be segregated from your IT team, which has priorities that can conflict (or not align) with security decision-making and practices.

Increasingly, regulatory scrutiny is also resulting in moves to solidify separate security oversight.

A security operations capability requires someone to follow regular procedures to validate that security controls are functioning. Specifically, they 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 defective controls identifying an anomaly.

Security operations bring 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, that may not be feasible, but your security chief can create and communicate a security operations mindset.

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. 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 unexpected logins or password changes.
- **Check your patches:** As vulnerabilities in operating systems and applications are regularly identified, patches are being pushed out promptly to address them. Regularly review your systems to make sure patches are applied.
- **Verify backup completion:** Isolated backups are critical to ensuring an organization's ability to recover from devastating attacks. Too often, organizations have failed backups that they don't know about. Review your backup status daily 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 — firewalls, EDR and other infrastructure such as Active Directory and event logs on servers — capture big amounts of security event data. 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 looks like, you might get away with reviewing it manually. Otherwise, set up automation for the heavy lifting and to alert you to anomalies. Check daily to ensure it's configured and running properly.

© Wipfli

TIP #24

Develop and communicate your Bluetooth use policy



Bluetooth access is not just a convenience for employees. In remote work environments, many find that wired headsets or earbuds are simply not adequate for picking up voices during meetings.

Hi-def wireless earbuds, such as AirPods, that are designed to be paired with a mobile device via a Bluetooth connection are the go-to choice for many because of their higher sound quality.

If your company has eschewed Bluetooth use as a risk management strategy, consider revisiting that policy. From a threat modeling perspective, it may make sense for many organizations to allow Bluetooth use if other risk reduction methods are in place. The fact is that the likelihood of an attack that could exploit your devices over Bluetooth is low. The Bluetooth protocol doesn't go beyond 100 meters, so the requirement of close physical access to a device keeps security concerns manageable.

NEXT STEPS

- **Implement security requirements:** These measures should include encryption and the disabling of discoverable mode. Use PINs as an extra layer of protection if Bluetooth accessories support this feature.
- **Instruct users to pair devices at home or the office:** Because computers are most vulnerable when being paired with a new device, threat actors could be looking to intercept the wireless connection process, so it's important to pair new devices in the office or at home before going to a public location. And remind people never to accept unexpected pairing requests.
- **Be sure to communicate acceptable Bluetooth parameters to your employees:** Include the policy in your training materials.
- **Make sure employees know to turn off Bluetooth connectivity when they aren't using it:** Reiterate the message periodically, as it's easy to forget.

© Wipfli

TIP #25

Establish a data governance framework



Establishing a data governance framework provides a source of truth on key data elements of your organization. It also identifies who can view and modify data and details the data retention policy.

Creating this framework is critical as organizations face new data privacy regulations and increasingly rely on data analytics to help optimize operations and drive decision-making.

While data accuracy and quality are business process issues that must be tackled, questions around its security and accessibility are just as important. The framework should ensure that data is consistent and trustworthy and doesn't get misused.

Businesses should give focused attention and resources to ensure that data access corresponds with the correct role or individual and that external sharing is set up in accordance with the appropriate security measures.

NEXT STEPS

- **Define your goals and assess your current situation:** You need to create clear objectives and a detailed assessment of your current approach to managing data. These could include improving data quality and reducing compliance risks such as oversharing. To further these ends, identify where your sensitive data currently resides in your systems and who has access to it.
- **Create policies and processes:** To implement the framework, you need to develop guidelines that delineate your approach to data governance. Share them appropriately within your organization and with external entities that need or require assurance of the elements involved in your data governance. Spell out what the data can and cannot be used for.
- **Communicate the framework:** Once the framework is created, your organization needs to make sure that everyone who needs to know about the framework understands their responsibilities in relation to it.
- **Monitor the framework:** Watch over the framework to track the achievement of your targeted goals and to be alerted when your data is not being used as intended. Tools such as Microsoft Purview can help you with your data.

© Wipfli

TIP #26

Augment your antivirus tools with EDR



There is no one-size-fits all security solution, and antivirus software alone is no match for today's sophisticated attacks. You need an approach to combatting ransomware, supply chain software disruptions and other attacks that uses the most up-to-date technology and meets your specific needs.

It should have the capability to use machine learning and inspect your system's memory to automatically interrupt an attack.

The urgency is indisputable: While all organizations are vulnerable, smaller businesses are most at risk. In 2021, 82% of ransomware attacks were targeted at businesses with less than 1,000 employees and 76% of those attacks were deployed outside of working hours. The average ransom was between 1% and 1.5% of gross revenue.

Endpoint detection and response (EDR) is an important option in helping you identify malicious processes and system events running within your computers. EDR can protect your workstations and servers, but it has its limits as it will not secure your network devices or cloud services, which require different tools. EDR's constant monitoring identifies abnormal processing activity, detects suspicious events and alerts your security team.

If your organization relies on old-school virus protection and has not yet had a disruptive attack, it's easy to slip into complacency about the risk level you face. You may have been more lucky than protected up until now. So, amid the ever-expanding range of cyberattacks, how should your organization protect itself?

NEXT STEPS:

- **Select an EDR solution:** Work with your security team to evaluate leading EDR solutions and deploy the right one for your environment. It should deploy on both workstations and servers and rely on AI machine learning.
- **Monitor on-premises and cloud environments:** EDR can monitor your entire attack surface, so make sure you implement it across all assets — both on premises and in the cloud – and that your team is trained to respond.
- **Consider even higher-level security monitoring:** When using systems such as Microsoft 365, tools are available to find evidence of hackers getting into employee email. It should be able to look for "impossible travel" scenarios. If a U.S. user's login suddenly appears to be coming from Romania, it would be flagged as a compromised email.

  An additional layer includes "security information and event management" that combs through the log activity of every device, including network infrastructure such as firewalls and routers, to identify malicious network traffic. AI helps do automated threat hunting based on all the collected log data.

© Wipfli

TIP #27

Know where sensitive data resides and monitor its use

As a piece of your overall data governance framework, your approach to storing and sharing your sensitive data needs to be a top priority. Data is accumulating rapidly and developing a plan for how to identify and categorize it, where to store it and who can access it can be very challenging.

Many organizations don't understand the risks they face by not protecting their data adequately. This includes personal information related to your employees and customers, M&A information and financial records. And the challenges are growing as individuals create and share data across organizational or regional boundaries. There are multiplatform considerations to tackle as well with sensitive information residing 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 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 protect your data:** You'll want to do this while making sure that user productivity and the ability to collaborate isn't hindered. 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 to prevent accidental oversharing of sensitive information.
- **Implement a monitoring and alert system:** An ongoing monitoring operation keeps your organization aware if something unexpected, and risky, is being done with your data. Monitoring tools such as Microsoft Purview can be an important prevention asset as it applies sensitivity labels and implements policy with regard to external sharing, retention periods and who can edit versus view sensitive data. Hiring an outside team can help you augment your security.
- **Automatically retain, delete and store data and records:** Make sure to do so in a compliant manner so you don't run afoul of regulators. Microsoft Purview includes a useful data retention component as well.

© Wipfli

TIP #28

Level-set cyber controls and consider cyber insurance



Because fall is when many organizations build budgets for the year ahead, this could be an opportune time to reevaluate your cybersecurity. Start by benchmarking your cybersecurity controls to trusted definitive baselines, such as the NIST Cybersecurity Framework or the PCI Data Security Standard.

This will help you identify whether any must-have protections to thwart the latest cyberthreats are missing from your arsenal.

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

These baselines and the best practices listed in this e-book are also important to set in place as many are requirements for securing cyber insurance.

You'll want to purchase cyber insurance to hedge against the downside risk costs if cyberattacks such as ransomware and data exfiltration bots unexpectedly overwhelm your cyber defenses. And as threats increase in severity and cost, it's important to review your cybersecurity insurance coverage to help ensure that it's accurate.

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. You should also regularly review your cybersecurity insurance and the controls required to obtain a policy, such as MFA, EDR data backup testing and employee training.
- **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.
- **Consider captive insurance to manage cyber risk:** Most organizations should at least carry data privacy breach, network liability and data ransomware/extortion coverages, with limits consistent with their risk appetite. Creating a captive program gives you more financial control as you manage risk.

© Wipfli

TIP #29

Leverage AI in your cybersecurity

Organizations are using machine learning defensively to look at huge quantities of data about attacks that have happened elsewhere to identify patterns showing what suspicious activity looks like.

You can monitor your own systems in real time based on that AI input to proactively look for evidence of that kind of activity directed at your business.

AI has accelerated how malware developers are carrying out attacks, but also how defenders can identify them. EDR tools are increasingly relying on AI, along with real-time analytics, to discern legitimate, good behavior from potentially malicious behavior. They cannot only detect an attack, they can also disrupt an attack before damage is inflicted.

NEXT STEPS

- **Look into AI-driven anti-malware tools:** AI used in malicious software can avoid detection and adapt to changing environments, which makes it harder to identify as malware. Anti-malware tools relying on AI will be a valuable tool in staying ahead in the cat-and-mouse game with attackers. Anti-malware looks at what's running in memory and other processes, identifying malicious activity that may be very deep in the system.
- **Find cybersecurity specialists who are well versed in AI developments:** The cost for risk reduction will be far less than the consequences of a ransomware attack, which can threaten an entire business. Contracting for an outsourced service may be a more cost-efficient route than trying to add permanent hires with these skills.
- **Level up your threat hunting:** An additional tool includes "security information and event management" that combs through the log activity of every device used by your organization. AI helps do automated, proactive threat hunting based on the collected log data to thwart malicious activity.



© Wipfli

TIP #30

Implement zero trust architecture concepts

Securing your network now means implementing zero trust concepts.

Zero trust is intentional, requiring your organization to be proactive. 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."



Cybersecurity pros traditionally were more focused on defending the firewall with the presumption that the threat landscape existed outside the perimeter. Assets inside the network were presumed to be trustworthy. This approach is not sufficient and needs to evolve; organizations must recognize that an attacker could have a foothold on their network through a compromised workstation, vulnerable wireless connection, stolen credentials or other vulnerability.

NEXT STEPS

- **Use least-privileged 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 who 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 access requests 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 1) implement end-to-end encryption, which can protect data even if a workstation is compromised, 2) put network segmentation in place to make it harder for an unauthorized user to traverse your entire network, 3) secure how you use local administrative accounts to make it harder for attackers to escalate privileges and 4) continuously monitor for threats and indicators of compromise to make sure you can interrupt attacks and evict attackers.

© Wipfli

Become a more cyber-resilient business

If these tips have raised your awareness of areas where you need to beef up your cybersecurity measures, you may also be feeling unsure of which to tackle first. With the cyber landscape constantly evolving, it's important to stay vigilant in reducing 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.

ADVISORY & ACCOUNTING

WIPFLI

© Wipfli