30 tips in 30 days

WIPFLI

Cybersecurity in the new normal

The unexpected and broad disruption caused by COVID-19 opened the floodgates to cybercriminals looking to take advantage as we all focused on remaining resilient and moving our workers into a virtual environment.

The pandemic has been classified as the largest-ever cybersecurity threat.

And it has capitalized on our fears.

- Cyberattack complaints to the FBI climbed to 4,000 a day, a 400% increase.
- Phishing and social engineering attacks average 20,000-30,000 a day.
- Ransomware attacks climbed 800%.
- Remote work has increased the average cost of a breach by $137,000.
- Google blocked 18 million daily malware and phishing emails related to the coronavirus in April.

Read more: *Fraud and cybercrimes exploding during COVID-19*

The dust has not yet settled, and it's difficult to know what the new normal will look like in the coming months and years. But the cybercriminal watchdogs at Wipfli say here is where we're headed:

1. Adopting zero trust architecture
2. Better threat is intelligence needed as diverse products are implemented
3. Cybersecurity decisions need to be made through a risk-assessment lens
4. Cyber resilience must become a core part of operations
5. Employees are the weakest link in your defenses and need more training
6. Cloud security is paramount

To help you manage and respond to the biggest cyber issues — and in honor of Cybersecurity Awareness month — our team has compiled 30 cyber tips.

WIPFLI

Tip #1: Start building a solid cyber program

Organizations collect and track a lot of sensitive information regarding their customers, staff and operations, including:

- Health information
- Social security numbers
- Employee and volunteer records
- Billing information
- Intellectual property

With cybercrime on the rise during COVID-19, no one can afford to not make cybersecurity a top priority.

Steps you can take

Establish a culture of security awareness

Establishing an internal culture of security awareness is the responsibility of an organization's leadership. Too often, organizations put the responsibility on IT. To get started, you can explore and enroll employees in a cybersecurity and privacy awareness program.

Inventory your data and systems

You can't protect what you don't know about. It's important to have a complete list of all the different data you collect and systems you use. The easiest way to do this is by using a simple template. Review this inventory with stakeholders around the business and make sure you've found where all the important information is stored. And don't forget what gets scanned and printed. Those devices have storage and need to be inventoried too.

Assess your controls

Next, you'll need to assess your organization's controls to safeguard the data and potential risk to the data should it ever be compromised. This can be done in-house but is normally best left to a trusted cybersecurity partner. A trusted vendor with specialization in your industry will be able to produce a report that not only showcases where your organization is most vulnerable but also offers practical and prioritized recommendations to help your organization without you needing a tech jargon dictionary next to your desk.

Implement your plan

Now it's time to put the plan into action and remediate the findings from the report. Remember, this is a continual process and not just a single event. It's possible some of the recommendations can be performed in-house, and, where applicable, it's a great idea to do so. You'll have to keep in mind adding the responsibility of remediating these findings may not have been on your staff's current list of responsibilities or in their skillset. It may be beneficial to seek outside guidance or even outsource the remediation altogether.

WIPFLI

Tip #2: Mitigate threats due to remote workers

Organizations are more vulnerable now that the majority of the workforce is remote due to the COVID-19 pandemic, and cybercriminals are ramping up their efforts to break through your security.

A few of the things cybercriminals have been taking advantage of are:

- Email phishing: These attempts try to get your team to click a link or download a file that will expose their login data or open the gate for a ransomware attack.
- Unencrypted/insecure connections: These connections between employees and your network can allow attackers to intercept traffic and obtain sensitive information.
- Poor patch management policies: Poor patch management leaves devices vulnerable to new attacks. New vulnerabilities are identified daily, and hackers are quick to search for systems that haven't been patched in order to exploit them.
- Weak password policies: Weak passwords can make it easier for attackers to get in when policies allow for dictionary words or other easy-to-guess passwords.

Steps you can take

To help keep cybercriminals out, take these four steps:

1. Conduct regular security awareness training that teaches employees to identify and report suspicious e-mails. Additionally, instruct them on the dangers of clicking links in e-mails and downloading files, especially from sources they do not know or trust.
2. Establish a Virtual Private Network (VPN) that uses strong encryption for employees to connect to your internal environment from their homes. This will make it immensely more difficult for an attacker to intercept and view the data being sent back and forth.
3. Implement a patch management program that is able to manage updates to remote devices over a VPN connection. Also, instruct your employees to shut down their devices nightly to ensure patches are installed fully.
4. Implement a strong password policy and a password filter that prevent the use of easily guessable passwords and dictionary attacks. Additionally, implement multifactor authentication for remotely logging in to company resources.

View previous tips: https://www.wipfli.com/30-tips

WIPFLI

Tip #3: Make working from home safer

Cybercriminals aren't just trying to exploit weaknesses in employees — they're also targeting equipment and gaps in your processes. Here are a few areas open to attack:

- Improperly configured access: Giving users more permissions than are necessary can lead to more information being lost and more damage being done to your network, customers and reputation.
- Missing equipment: The likelihood of a laptop going missing is high. Lack of disk encryption makes it easy for cybercriminals to access data and network resources.
- Personal equipment: If employees conduct business operations from their personal computers, you cannot manage the security of the device, which increases the risk that your network will be compromised.
- Unencrypted emails: With more remote workers, the risk that sensitive information can be obtained from emails that aren't encrypted is even higher.

Steps you can take

- Ensure users are only given permissions to access the data needed to do their job, and give their account the lowest level of privilege that is needed for access. Configure access control lists within your environment to prevent unauthorized devices and users from being able to access sensitive systems or data. Also, do not allow users to have local administrative privileges on their computer.
- Implement full disk encryption on remote devices and encourage employees to shut down their devices at the end of the day, or even when they leave their home during the day. Remind them not to leave their computers in their cars, and to be diligent regarding their home security.
- Allow employees to conduct their duties on organization-provided computers only. It is critical that you are able to manage the security of devices connecting to your network.
- Implement an email encryption solution and require employees to encrypt their emails when sending sensitive information. Many email encryption solutions also include the ability to configure "trigger" items that, when identified in an email, will automatically encrypt if the user did not already choose to encrypt the message.

View previous tips: https://www.wipfli.com/30-tips

WIPFLI

Tip #4: Don't bet on free antivirus protections

You've seen the headlines or maybe have personal experience with a virus on your devices. We've come a long way from the "ILOVEYOU" virus of 2000 that infected more than 10 million Windows personal computers.

Cybercriminals have continuously evolved their nefarious craft so that antivirus programs, especially basic ones, are not enough.

Steps you can take

The cost of recovery, unusable device inconvenience or replacement, and the possibility of unrecoverable information for personal or company-owned mobile devices is well above the costs for one of the more robust protective solutions of today.

"Free" doesn't translate into being secure from attack. A lot of free programs have many of the advanced protections turned off.

Also, there are many reliable rating websites and organizations to help you choose one best for you that has proved itself under rigorous testing.

These sites offer historic views of the tested products along with their strengths and weaknesses for the many attack types of today.

Respected ratings organizations (e.g., Gartner, Forrester) are available for business-class solutions. These focus on not only the full endpoint protection suites for user devices but also a comprehensive enterprise-class solution suite — providing a hardy defense-in-depth approach expected for small- to medium-sized businesses, and up to the largest of global environments.

For personally owned devices, reasonably priced but comprehensive "antimalware" solutions abound and have versions for the various PC types and mobile devices.

View previous tips: https://www.wipfli.com/30-tips

WIPFLI

Tip #5: Perform a risk assessment

Generally, a risk assessment provides the information necessary to make informed decisions as to the risk-versus-benefit of each key business decision — and that includes cybersecurity decisions.

For example, a decision to use a free, ineffective antivirus solution comes with a higher risk that hackers can breach your system. A decision based upon a risk assessment can help you decide the cost of a more secure program is worth the lower risk.

Similarly, choosing whether to encrypt a database should be based on understanding the value of the data contained within it and the impact of having that breached.

Steps you can take

Risk assessment reporting should be integrated into key reports to senior management and the board of directors.

Risk management decisions are best facilitated with an understanding of the likelihood of a bad event happening as well as the business impact if it does happen. With that information, senior management can make decisions on risks to avoid, mitigate, accept or transfer.

Effective risk management is only possible with risk assessment results tailored to meet the needs of the organization, so it is important to identify any regulatory of statutory expectations.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) includes in the Identity Function and Risk Assessment (RA) Category the description: “The organization understands the cybersecurity risk to organizational operations (including mission, functions, image or reputation), organizational assets and individuals.”

The Category of Supply Chain Management (SC) includes a focus on risk assessment for suppliers and third-party partners of information systems, components and services to identify, prioritize and assess using a cyber supply chain risk assessment process.

For financial institutions, the Federal Financial Institution Examination Council (FFIEC) IT Examination Handbooks outlines its compliance expectations for risk assessments.

View previous tips: https://www.wipfli.com/30-tips

WIPFLI

Tip #6: Don't open that email

Pretty much everyone by now knows about email phishing, but even though we know about it, it's still a major risk.

In 2019, 90% of surveyed organizations faced spear phishing attacks, and 86% reported dealing with business email compromise (BEC) attacks. BEC is when an attacker impersonates an organization's executive to defraud the company and its customers, partners and/or employees into sending money or sensitive data to the attacker's account.

Steps you can take

Set up a spam filter to catch as much as you can, but be aware that no filter will catch them all.

Educate your team. And then educate them again. Run tests with a cyber expert to find holes in that training. Here are five easy ways to identify a phishing attack:

1. Look at the "from" address. Be sure you recognize it, and look closely. Then take a second look at the domain name (that's the name after the "@" symbol). Make sure it's spelled correctly. Many email solutions will label outside email as "External," and these emails should be vetted even more closely.
2. Make sure that the "reply" address matches the "from" address of the sender; otherwise it may be a spoofed email.
3. Make sure the sender is who they say they are. This is done by using out-of-band communication to contact the claimed sender. In other words, DO call your brother and make sure he actually sent you that cat video before you click on the link in the email, and DON'T email them back and ask if it is him; the attacker will always reply "yes."
4. Check that the message is well composed with the grammar and spelling you would expect from the sender, whether it's your boss, your brother or your bank.
5. Triple check all email links before you click on them by hovering your mouse over the link (without clicking on it) because your email application will show its actual destination. Look at the domain and be sure it is what you would expect. Misspelling a domain is a very common tactic (microsft.com vs. microsoft.com). At a glance, they look the same, but one will take you to Microsoft, and the other will take you somewhere you don't want to go.
6. If you're still not sure, ask IT (don't forward) and do not open it. Or contact the alleged sender through a different method to confirm it's from them.

View previous tips: https://www.wipfli.com/30-tips

WIPFLI

Tip #7: Guard against business email compromise

Cybercriminals are getting faster and more sophisticated in their attempts to steal your company's money or data.

They're using email-based schemes with highly targeted emails to convince internal employees who have the ability to access company funds to make payments or divulge other sensitive information. These have been labeled business email compromise (BEC) attempts.

These differ from the "standard" phishing attack in that the fraudster is typically targeting one person rather than blanketing an organization with a generic email.

Steps you can take

The single most effective way to prevent BEC is to verify instructions for payment information changes, wires and requests for very sensitive information by a means other than email. Picking up the phone and verifying instructions with the requestor can all but eliminate the risk of BEC.

You can also educate your team on the common types of BEC attacks to prevent them before they happen:

- Vendor payment change: The accounts payable department receives an email or letter from a vendor providing new ACH payment instructions. Your company doesn't find out it has been duped until your vendor starts making collection calls and informs you that they were not the one who sent the payment change request.
- Wire transfer: The CEO is out of town. The CFO receives an email that appears to be from the CEO, requesting they send a wire transfer to a new vendor. The message provides the payment instructions and emphasizes that the payment must be made immediately. Because the CEO is out of town, they cannot take a call. The payment is made, and the fraud isn't discovered until the CEO reviews the banking statement and asks about the large transfer.
- W-2 data request: The payroll department receives an email from an executive asking for the W-2 report for all employees. The report goes out to the fraudster impersonating the executive. The scam isn't discovered until weeks or months later, when employees find out that fraudulent tax returns have been filed on their behalf.

BEC also happens when a cybercriminal gains unauthorized access to an email account to steal information or launch a fraudulent request for funds. The top ways to prevent that is to protect your passwords with multifactor authentication, use strong passwords, update passwords and not use the same password for multiple accounts.

View previous tips: https://www.wipfli.com/30-tips

WIPFLI

Tip #8: Get serious about passwords

Data breaches have exposed MANY passwords. The haveibeenpwned.com "Pwned Password" database has, as of June 2020, over 573 million individual breached passwords. That's 573 million passwords already exposed for threat actors to use in their nefarious activities, such as credential stuffing.

Users commonly use easily guessable password constructs such as years, seasons, months and sports teams.

The National Institute of Standards and Technology (NIST) provides "modern" guidance on passwords. Passwords should:

1. Be a minimum of eight characters and a maximum length of 64 characters.
2. Have the ability to use all special characters but no special requirement to use them.
3. Restrict sequential and repetitive characters (e.g., 12345 or aaaaaa).
4. Restrict context-specific passwords (e.g., the name of the site/company/entity, etc.).
5. Restrict commonly used passwords (e.g., p@ssw0rd, etc.) and dictionary words.
6. Restrict passwords obtained from previous breach corpuses.

Steps you can take

No matter how much you train employees, some will not adhere to all six recommendations from NIST. Stopping #1 and #2 is easy, but very few authentication systems (and Microsoft Windows in particular) are able to block passwords that don't meet steps three through six.

Fortunately, third-party password filters can perform many of the functions that the NIST guidelines require and provide even more flexible options for password requirements. A few examples, both commercial and open-source, are:

- nFront Password Filter
- safepass.me
- Specops Password Policy

These solutions all install on your Windows domain controllers. They intercept password change requests, verify the proposed password against the parameters set within the application and either allow or deny the user from setting that password.

There is much debate in the security community revolving around the idea that, even with these controls in place, an eight-character password is sufficient. Many organizations use these password tools and still require a more cryptographically secure password length of 12, 14 or more characters.

View previous tips: https://www.wipfli.com/30-tips

WIPFLI

Tip #9: Protect against personal passwords

Data breaches are now seemingly part of everyday life. Hackers want personal data and passwords, both plaintext and encrypted, exposed — sometimes by first getting a hold of an employee's password on their personal email or social media account.

From an internal security standpoint, you might ask, "My Company's data hasn't been breached. Why should I care?" There are two primary reasons:

- Password reuse
- Credential stuffing

Individual users commonly reuse passwords among different services. While your password data may not have been breached, a password one of your employees used for another resource may have.

Credential stuffing is the process of taking a user's breached password and "stuffing" it into the login for many, perhaps hundreds, of sites — looking for sites where the same password was reused. If successful, the threat actor now has access to that user's resources, perhaps their online banking portal or other critical and sensitive information. Those hundreds of sites could include your external login portals.

Additionally, modern hardware is capable of cracking encrypted weak passwords in very short order. The "protection" provided by encryption is no longer a reliable protection for passwords.

Steps you can take

What can companies do to protect themselves from these issues? There are three primary things that can be done:

Use password managers

Password managers help employees generate strong, unique passwords for each and every resource an employee uses without the burden of having to remember a bunch of different passwords. This helps prevent credential stuffing when a password for a particular resource is breached; the breach of one now does not mean the breach of many.

Setting "good" passwords

In the absence of a password manager to help randomize unique passwords, selecting properly constructed passwords is important. Do not use common constructs like years, seasons, months, sports teams and other easily guessable strings that would make it easier for a threat actor to guess or crack the password. Again, password managers help in this regard by generating unique randomized passwords that do not suffer from the issue of reuse

Training

Employees should be trained in the use of a password manager if one is provided by the company, and in the selection of good passwords regardless. Employees should be taught why password reuse and credential stuffing are problems and that these issues extend past their work life. All the same issues apply to them personally as well.

View previous tips: https://www.wipfli.com/30-tips

WIPFLI

Tip #10: Back up your data

What would happen if your phone and computer were caught in a fire? Would you still have access to your pictures? How much work would you lose?

Nobody wants to be left without precious family memories or critical work documents. The best time to implement a backup strategy is before you need it.

Backing up your data is also a great way to help defend yourself from ransomware attacks, which are attacks that encrypt the files on your computer and require you to make a payment to obtain the private key to decrypt them.

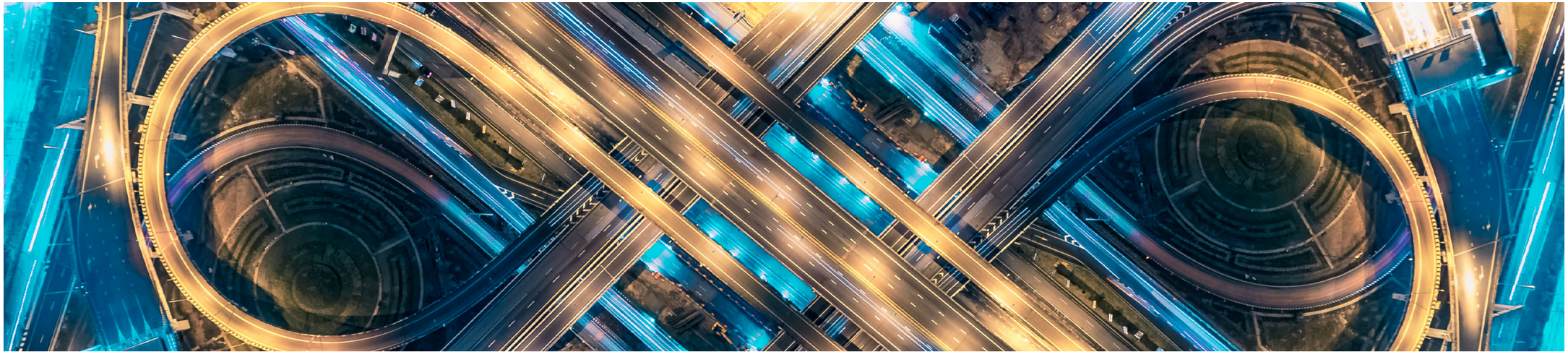
If that's not bad enough, some cyber criminals will wait until the ransomware completely propagates through your backup cycle. If you restore operating system image or program files that contain the ransomware, it will keep coming back.

If you have your data backed up to an external device or cloud storage, it is easy to simply wipe your hard drive and restore your backed-up data to the drive.

Steps you can take

1. Follow the 3-2-1 rule: Keep at least 3 copies of your data, store copies on 2 different types of storage and store at least 1 copy offsite.
2. Encrypt your backups to ensure only you have access to your confidential information. If using an online service like Google Drive, Dropbox or OneDrive, ensure that only you have access to your confidential information.
3. Keep all of your important files on a cloud drive and, once a week or so, make a copy of that folder and put it on an external drive. This makes it easy to keep track of stuff, and easy to create backups. Make sure to test your ability to download your content as well to ensure that you can successfully obtain your backed-up content before it's too late.
4. Ensure you have a backup copy of just your accounting/ERP system data (not just an image or snapshot of the disk) so you can always recover data to a new operating environment.

View previous tips: https://www.wipfli.com/30-tips



WIPFLI

Tip #11: Protect your back-up data

Security of backups is often overlooked, but it is the last and most important line of defense against attack. Attackers and ransomware often specifically target backup systems to prevent recovery of files they have maliciously encrypted or destroyed.

Steps you can take

1. Lock down access to all software, portals, files and media — such as USB drives and tapes — related to backup systems.
2. Require the use of strong passwords and multifactor authentication.
3. Store backup media in a secure location.
4. Encrypt backup data wherever it is stored — on backup servers, backup media and in the cloud. (Make sure you never lose the backup encryption key, or you will not be able to use the backups to recover.)
5. Evaluate the security measures of any third-party vendors involved in managing or storing backups.
6. Follow the 3-2-1 rule: Keep at least 3 copies of your data, store copies on 2 different types of storage and store at least 1 copy offsite.
7. Backup files that are at the greatest risk to ransomware are those directly attached to the computer getting backed up. Consider an "air gap" approach to ensure attackers cannot get to backup files. One approach is to rotate media daily, keeping a copy of the backups offline.
8. Review your backup configuration periodically to ensure all critical systems and data are protected.
9. Test your backups often to ensure the media itself works and your team knows how to recover and restore systems and data.

View previous tips: *https://www.wipfli.com/30-tips*

WIPFLI

Tip #12: Keep software up to date

Cybercriminals exploit unpatched and out-of-date software, operating systems and hardware to gain unauthorized access to systems.

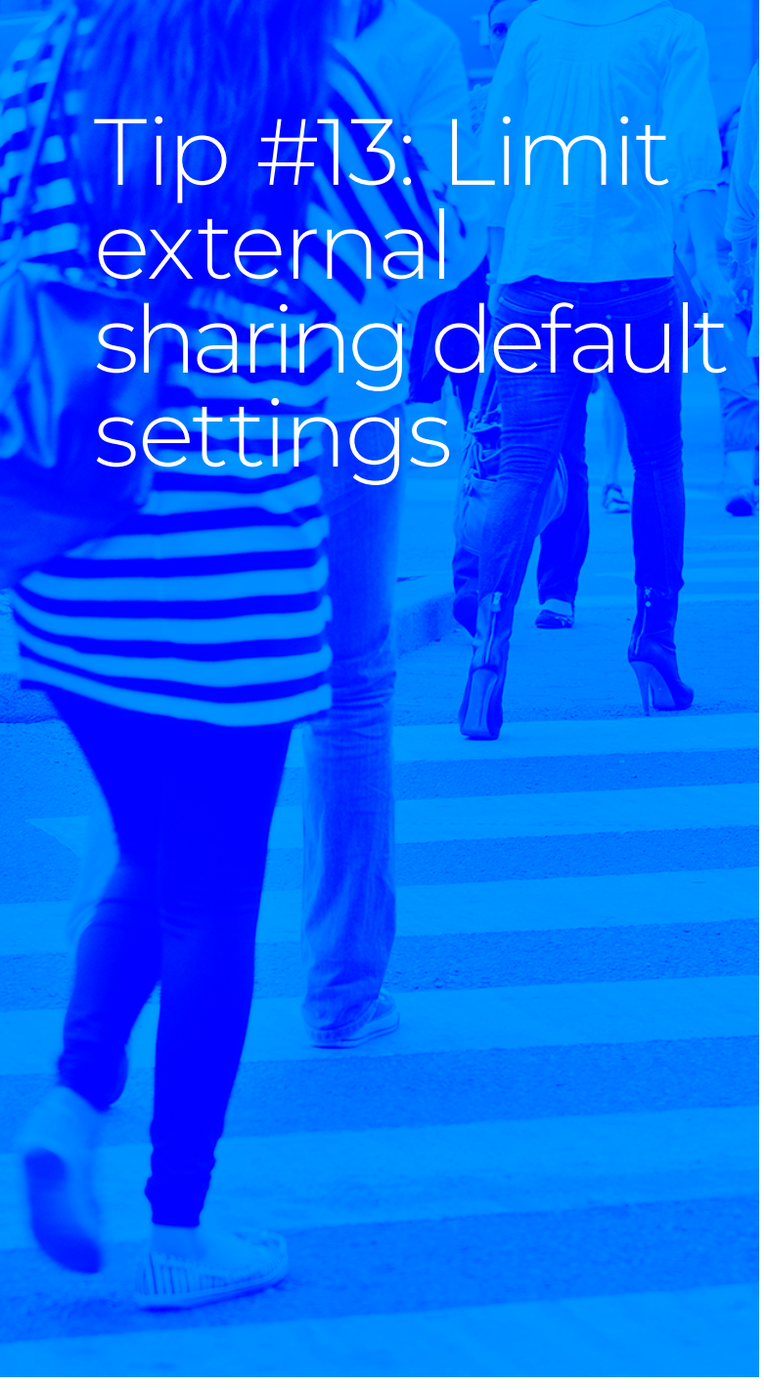
And it's not good enough to keep just one of these up to date. Cybercriminals will look for a weak link anywhere they can find it: on your laptop, a program, a Wi-Fi router or a cellphone. Leaving any of your systems unpatched and not updated opens the door for criminal access to everything.

Steps you can take

- Install updates timely once they are released.
  - Set up or verify automatic updates are configured.
  - Periodically verify the automatic update process is working properly.
- Upgrade or discard technology that has reached its end of life (EOL).
  - Once a product reaches its end of life, it is no longer supported by the vendor, meaning that when security holes are discovered, patches are not released for them. Current common EOL examples include: Windows 7 or Windows 8/8.1 and antiquated iPhones/iPADs, Android phones and tablets.
- Don't forget about network equipment and Smart devices.
  - That's right, your home router, wireless access point, SmartTV, Smart Lights and most any other devices connected to your network need updates too. The first step is to develop an inventory of all of your devices and then work through the steps previously outlined. If you run into the term "firmware," don't be intimidated by new lingo. Firmware is simply a term for the software that runs on network equipment and Smart devices. In most cases, updating to the latest version will patch known security holes. You may need to contact the vendor to be certain and/or for help with the update.
- If you are involved in IT department oversight at work, make sure you've got strong patch management policies and procedures.

View previous tips: https://www.wipfli.com/30-tips

WIPFLI



Tip #13: Limit external sharing default settings

Many cloud-based collaboration programs come with default settings that allow easy internal and external sharing of information.

That means inappropriate data sharing could be happening already without leadership or IT knowing about it.

Steps you can take

You can still achieve effective collaboration in the programs while protecting your data.

- Ask your IT department or IT support vendor:
  - Is external file-sharing enabled? If so, what files are currently being shared?
  - Is external chat-sharing enabled? If so, is it open to all external orgs or just an allowed list?
- Try it out for yourself as a test.
  - Open a file in Teams or another program, click the share button and see what options are available and what the default option is.
- Modify the settings to meet your security needs.
- If necessary, engage with a third party.
  - You might find it necessary to engage a third party if you're having difficulty determining what access various programs are providing to external and internal accounts.

View previous tips: https://www.wipfli.com/30-tips

WIPFLI

Tip #14: Harden your networks and systems

Most cyberattacks that result in full domain compromises start with the lack of hardening on many systems on the network.

Network/system hardening is the process of reducing a system's attack surface by defining secure configuration settings, disabling unnecessary services and protocols, and changing default credentials — in addition to a myriad of other items that could be employed to further reduce the system's attack surface.

A threat actor who successfully breaches the network perimeter — whether it's using a rogue device on the network, compromising a workstation via a malicious phishing email or perhaps cracking a Wi-Fi network — will take advantage of this lack of hardening to mount attacks against the network.

Steps you can take

WARNING: This is going to get a bit more technical than our usual tip!

Proper network/system hardening can prevent a cybercriminal from compromising the domain and its assets or slow them down long enough to be detected by other network controls before a compromise can occur.

Our penetration testers reveal recurring deficiencies present in almost all compromises of Windows domains. Some of the most prevalent network/system hardening issues that surface again and again include:

SMB NULL sessions enabled:

Windows domain controllers that allow SMB NULL sessions allow an unauthenticated attacker to extract Active Directory user, group and group membership information. This is invaluable reconnaissance to the attacker that can show high-value user accounts and systems that can become the target of subsequent attacks. NULL Sessions should be disabled on all domain controllers.

Insecure broadcast name resolution protocols enabled:

These protocols, typically NBNS and LLMNR, are enabled by default on the Windows system upon install. Their purpose is to give a host a way to resolve hostnames to IP addresses when DNS doesn't return a value. An attacker can intercept and spoof responses to these requests and force the victim host to interact with the attacker. If you don't rely on these protocols for name resolution, both should be disabled.

Lack of SMB signing:

SMB signing is a component of the SMB protocol that digitally signs packets to ensure packets are valid only for the hosts intended. Once an attacker is interacting with a victim host, one of the things the attacker will look for is the victim authenticating to the attacker. If SMB signing is disabled on a host, the attacker can relay captured credentials to a second victim machine. If the relayed credentials provide administrative access, the second victim machine has now been compromised. SMB signing should be enabled on every host that allows it.

Local administrator credentials shared:

Once an attacker has compromised a machine, the credentials for local users in the form of hashed passwords (including the local administrator) are now in the attacker's possession. The attacker can then use that password hash to test for its validity on other machines on the network. Local administrator passwords are commonly shared among machines, so the compromise of one can result in the compromise of several, or many. Microsoft knows this is a challenge and can introduce vulnerability, so they created a solution to help. Check out the local administrative password solution (LAPS) and consider implementing it within your organization.

Lack of network segmentation:

Large, flat networks increase the chances of an attacker to capture and relay credentials. Network segmentation, which is the process of placing different classes of assets on different network subnets, limits the broadcast domain to as few different asset classes as possible. Typically, user workstations, administrative user's workstations, servers, domain controllers and other back-end servers would be on different subnets. Consider the case of a compromised user workstation: If that workstation is located on a flat network with devices of all classes, it will see broadcasts from all classes of users and devices. If that workstation was isolated on a network segment only with other user workstations, it would not see broadcasts from users with elevated privileges, potentially leaving the attacker with only user-level credentials to work with. Consider segmenting flat networks to isolate an attacker as much as possible.

View previous tips: https://www.wipfli.com/30-tips

WIPFLI

Tip #15: Protect privileged accounts

Privileged accounts are a prime target of cybercriminals because, through them, they can gain widespread access to your data and systems.

Privileged accounts are what used to be commonly called “superuser” accounts, aka the ones that have the highest level of access to a system, such as a server and local endpoints. The account holders are the ones that typically configure, manage and support a system. That means these types of accounts are often unrestricted or lightly restricted.

Estimates vary from 50% up to 80%, but most cyber experts agree that the majority of breaches stem from misuse of privileged accounts.

Steps you can take

1. Identify and start to track privileged accounts. Make sure you look at your leadership team in addition to your IT team.
2. Identify accounts that don’t need that higher level of access and start to downgrade them. The more accounts you have, the greater the chances a hacker can get in.
3. Never use a shared administrator account. This takes away from individual accountability and limits your ability to attribute any errors or breaches to the responsible party. Wherever possible, create individual accounts for your administrators and power users.

You can also download a free guide on Privileged Account Management for the Financial Services Sector that was created by the U.S. National Institute of Standards and Technology in collaboration with experts from the financial services sector and technology vendors.

View previous tips: https://www.wipfli.com/30-tips

WIPFLI

Tip #16: Ditch antiquated software and hardware

As companies roll out new versions of software, hardware and devices, they eventually stop providing support for old versions. That means they will stop making updates — such a security patches — on those products.

Some manufacturers are very transparent about their support plans and proactively communicate with customers. A good example of this is the Microsoft Windows 10 Operating System. Their website says they will provide upgrades for five years and basic maintenance support for 10 years. This means that you will want to start planning for that upgrade before the end of support on October 14, 2025.

But not all manufacturers are as transparent as Microsoft, so you can't rely on them and, instead, set up a system to keep yourself informed.

Steps you can take

Here are tips on how you can keep informed about the end of support for a particular device, application or operating system:

- Check with the manufacturer: A search for the manufacturer, including the words "security advisory" should point you to results containing the manufacturer's website where they maintain a list of announced security and functionality updates to fix discovered vulnerabilities.
- Subscribe to newsletters: Most of these websites also contain areas where you can sign up for alerts. To make sure the alerts don't get lost in your inbox, you should create a location within your email (such as a separate folder) and create a rule to place notifications from these services into a special area so you can refer to them whenever possible.
- Periodically search for end of support: Set a recurring time on your calendar to periodically conduct searches that include the manufacturer, the product and the words "end of support." This will provide a date that the product is determined to end support.

View previous tips: *https://www.wipfli.com/30-tips*

WIPFLI

Tip #17: Mitigate threats from mobile devices

More than 95% of Americans have a mobile device now, and all those devices contain many forms of sensitive data. Hackers and spam phone calls are increasing the risk that cybercriminals can get sensitive banking information, usernames, passwords and other sensitive data.

More systems are creating apps and platforms that let workers accomplish tasks via mobile devices, opening the door for criminals to gain access to your company data.

Steps you can take

1. Set up a Virtual Private Network (VPN) that uses strong encryption for employees to connect to your internal environment from their mobile devices.
2. Draft policies for mobile device management that include an acceptable use policy for personal devices and other measures for corporate phones.
3. Train your team on how to recognize and handle spam phone calls.
4. Stay away from risky and unsecure Wi-Fi.
5. Train your team to be aware of people who might be looking over their shoulder.
6. Require multifactor authentication and use features such as fingerprint or SMS access codes.
7. Implement a mobile device management platform that requires strong passcodes/ biometric identification of the user and allows for corporate data to be wiped remotely if the mobile device is lost or stolen.
8. Instruct your employees to never leave their mobile devices unlocked.
9. Work with your employees to ensure they are updating to the latest mobile operating systems and apps.

View previous tips: https://www.wipfli.com/30-tips

WIPFLI

Tip #18: Don't forget about cloud security

Whether it was due to COVID-19 or workforce trends, many organizations moved their servers, files, email and all business to the cloud.

But that doesn't mean you don't have to think about maintaining all that infrastructure or security because "the cloud" is just another name for "someone else's computers."

Steps you can take

Your cloud provider is responsible for the security of their computers. They'll make sure the networking hardware that runs behind the scenes is updated, patched and capable of handling the workload. If you've contracted for it, they'll make sure that your data is kept in two different locations so it's safe from disasters.

But all that doesn't matter if your users keep using passwords like "Spring2020." It doesn't help if your users keep clicking phishing emails.

You have a shared responsibility with your cloud vendor.

You still need to keep your virtual machines in the cloud patched, the connections to the cloud secured, and your passwords to cloud services secure. You still need to implement security features like multifactor authentication, provide training for phishing attacks and do everything else you would have to do if you hosted your servers on premises.

View previous tips: https://www.wipfli.com/30-tips

WIPFLI

Tip #19: Don't use others' computers, Wi-Fi or printers

When you access your data or share your data on anyone else's system or hardware, you are only as safe as their security.

They may not have the same firewalls as you. In addition, you don't know what monitoring tools might have been installed.

Steps you can take

1. Avoid using public computers if possible: Though some are managed better than others, you just don't know the state of that computer, nor do you know how well it's protected .... It could have spyware installed that would capture all your passwords.
2. Think twice about even simply printing documents: If the document has sensitive information, is the hotel computer or printing/shipping computer the best one to use? Keep in mind that even loading a document on a computer and printing it can leave copies of that document on the computer, the print server and the printer itself.
3. Avoid public or unsecured Wi-Fi or connecting to an unfamiliar network via ethernet cable: If you have to get online, use a VPN provided by your employer.

View previous tips: https://www.wipfli.com/30-tips

WIPFLI

Tip #20: Subscribe to threat intelligence sources

Threat intelligence is critical to an organization's security posture. Threat intelligence and collaboration include processes to effectively discover, analyze and understand cyber threats, with the capability to share information internally and with appropriate third parties. This may be anonymous information shared with peer groups, or full reporting required by law or regulation.

Studies have shown that of companies researched that had a recent security breach that compromised the company's networks or enterprise systems, 80% believed if they had threat intelligence at the time of the breach, they could have prevented or minimized the consequences of the attack.

Steps you can take

Educate yourself.

Find respected organizations that can provide you with reliable information on threats. Some may require fee-based membership for full access or come as a part of a service.

One source of threat intelligence is the Multi-State Information Sharing & Analysis Center (MS-ISAC). MS-ISAC is the focal point for cyber threat prevention, protection, response and recovery for state, local, tribal and territorial (SLTT) governments. There is no cost to join the MS-ISAC; it is primarily supported by the U.S. Department of Homeland Security (DHS) to serve as the central cybersecurity resource for the nation's SLTT governments.

Other threat intelligence sources:

- General
  - SANS Institute
  - Internet Storm Center/DShield
  - MS-ISAC
  - US-CERT
- Financial
  - FS-ISAC
- Healthcare
  - Health-ISAC
  - HITRUST

These are just a few examples of sources. Whether you use one of these or find your own, it's important to have accurate information delivered to you as fast as possible.

View previous tips: https://www.wipfli.com/30-tips

WIPFLI

Tip #21: Have an aggressive plan

Despite education and antivirus programs, hackers still manage to find their way in.

That doesn't mean that a hack is inevitable, but it does mean the risk is high enough that you should have a plan in place that will help you identify the breach as soon as possible and respond immediately to minimize the damage.

Steps you can take

Implement a Managed Detection and Response (MDR) solution. The best MDR solutions combine the most advanced monitoring technologies with artificial intelligence and specially trained personnel.

A good MDR uses hundreds of threat sources that are integrated and used in real-time monitoring. Suspicious activity is analyzed by real experts to determine the validity before it ever reaches you. This removes false positives and saves you time while still keeping you informed.

A good MDR will also include a fast, clear response and recovery plan.

View previous tips: https://www.wipfli.com/30-tips

WIPFLI

Tip #22: Adopt zero trust security

You can increase the level of your security by adopting a zero trust architecture in your system.

Zero trust is a concept that organizations should not automatically trust anything inside or outside its perimeters. Instead, everything and everyone that tries to connect to your system requires verification.

If your current security protocols allow access, for example, from a company laptop or someone from your office's IP address, there's no way you can actually know who is sitting behind that keyboard. If someone stole a company laptop, you could inadvertently let them right in.

Zero trust security is increasingly important since many organizations have some systems in the cloud and many employees accessing applications from multiple devices from remote locations.

Once an attacker gets in, a zero trust security model will stop the hacker from moving laterally throughout your network, looking for the places to compromise to elevate their privilege and get at the systems or information you want to protect most.

Steps you can take

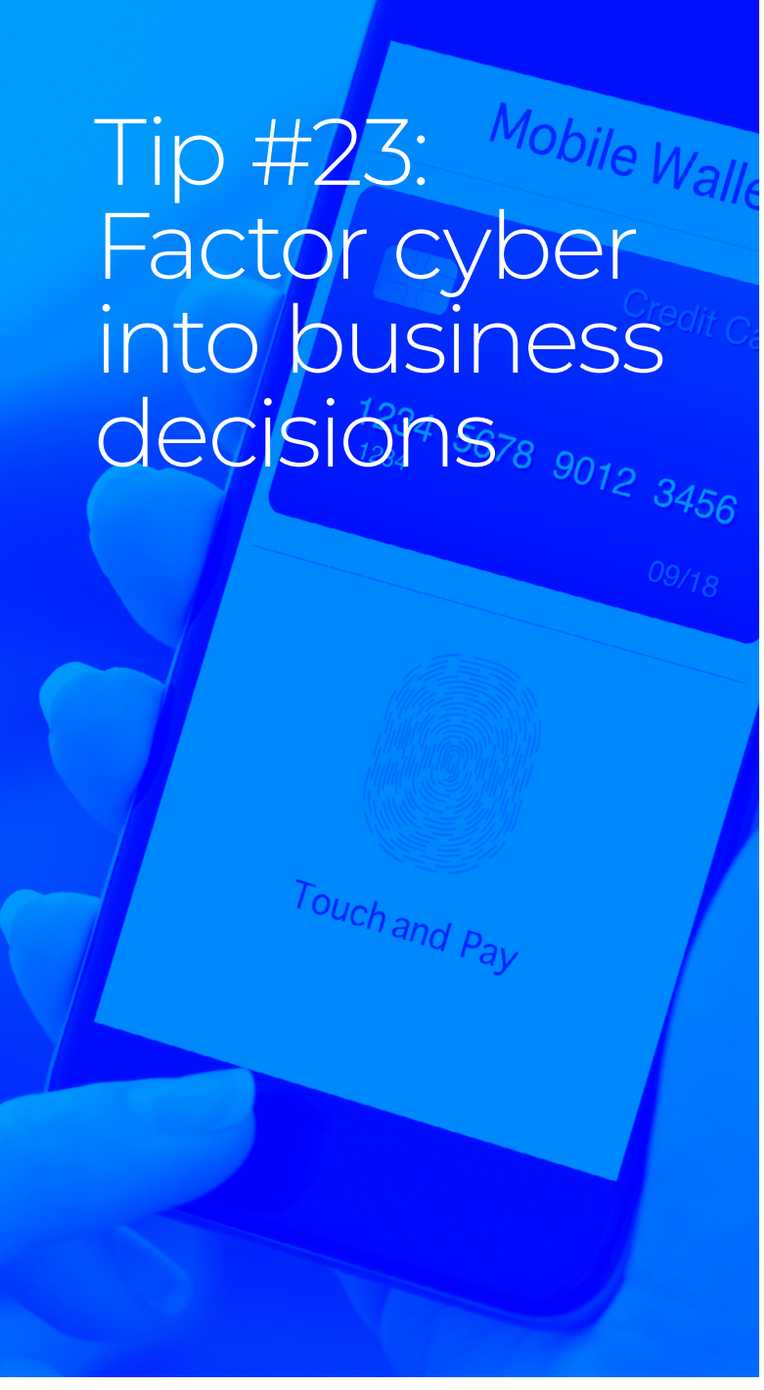
The big difference with zero trust security is that it assumes cybercriminals are already inside your system and focuses on limiting their movements — and damage. Traditional security models focus on keeping people out.

Implementing a zero trust architecture requires you to use micro-segmentation and perimeter enforcement using technologies such as multifactor authentication, biometric access, encryption, orchestration and identity access management. You'll also want to leverage advanced analytics systems so your team can see in real-time who is moving where in your network.

Once you segment your network, then you can establish what people, what devices and what applications you trust. Basically who, what, when and where you'll allow access to what data. In general, you also want to follow the principle of least privilege, meaning allowing users access to only the bare minimum they need.

A strong communication and training plan is another crucial element. Adopting zero trust security can lead to frustration among employees, as increased security measures often do. Without understanding the importance and rationale, your users may try to circumvent controls or waste time and energy worrying whether they can get their work done.

View previous tips: https://www.wipfli.com/30-tips



Tip #23: Factor cyber into business decisions

Good cybersecurity is more than an IT issue.

Many strategic choices about how to run the business have cybersecurity implications.

- How should we connect online with our customers?
- What data should we collect via our app?
- Should we use a vendor?

Good cybersecurity is based on understanding the business model and business processes of the organization, and that requires direction and consultation with executive management.

Without sufficient executive involvement or oversight for cybersecurity, an organization might be taking on more risk than it understands and could be more exposed to attack.

Or the opposite could happen, and IT could overspend on security and put in safeguards the business doesn't really need.

Steps you can take

Develop a culture of cybersecurity awareness at your organization to ensure it's at the top of mind during decisions and that the right teams are involved.

- As a business owner or executive for oversight of IT, make sure business functions/departments and IT have alignment on cybersecurity risks and what cyber risks the business should avoid, accept or mitigate/control. Perform a risk assessment.
- Make sure there is executive awareness of cybersecurity risks and an ability to engage on discussions on cybersecurity matters with IT leadership.
- Involve IT early on in strategic projects to help evaluate cybersecurity implications of new initiatives.

View previous tips: https://www.wipfli.com/30-tips

WIPFLI

Tip #24: Meet your legal obligations

Cybersecurity isn't just a technical issue. It's a legal one, too.

The regulatory landscape is constantly evolving, and different countries and even states are enacting their own cybersecurity and privacy laws.

Violations of cybersecurity regulations could carry hash fines or penalties.

It's important to understand what regulations apply to your organization so you can ensure compliance with these requirements.

Additionally, should there ever be a consumer complaint or investigation about violating a cybersecurity regulation, it's important that you have a defensible position and be able to articulate the steps you took to assess and meet your regulatory obligation. Lack of awareness could be interpreted as a neglectful management practice or ignorance — and that's never a good defense.

Steps you can take

If your in-house counsel has expertise in cybersecurity, start to involve them in your decisions. If not, find outside counsel that has that expertise.

1. Engage with counsel familiar with cybersecurity laws in your jurisdiction and places of commerce to understand what cybersecurity laws and consumer privacy laws apply to your organization.
2. Perform a current state assessment and identify gaps that prevent you from meeting the regulatory requirement. All too often, organizations tend to overstate their process capability, so it may make sense to engage a qualified consulting organization to help you through this assessment.
3. Develop a remediation plan to close any identified gaps.
4. Execute against that remediation plan and make sure your organization meets the compliance requirement and can prove compliance.

View previous tips: https://www.wipfli.com/30-tips

WIPFLI

Tip #25: Establish a communications protocol

Do you know who needs to be notified when you have a cybersecurity incident?

Figuring out a process during a crisis is never a good idea. Knowing who to notify and whom to escalate issues to could help minimize your risks by involving the right stakeholders at the right time.

Ultimately, cybersecurity breaches require effective coordination between executives, IT leadership, public relegations/corporate communications, legal counsel and potentially regulators and the FBI.

In addition, how you handle a communication that involves customer data can determine whether your weather the storm or go out of business. And the associates you need to keep your operations running need clear, targeted information so they know what to stop doing and what to start doing.

Steps you can take

Develop a communications protocol and communicate it with everyone on your team. To get started, you should:

- Identify internal and external stakeholders that need to be informed of cybersecurity incidents and data breaches.
- Build a communication plan in advance of an incident; if you don't have a corporate communications team, consider engaging a PR firm to help in the development of a plan.
- Identify a single source of truth for who is going to speak to employees, media and clients so there are not multiple or conflicting messages.
- Engage with counsel and understand your legal requirements for notification and communication to customers. This will vary by jurisdiction and the types of data you maintain.
- Understand in advance of a breach what law enforcement agencies you would work with in a criminal cybersecurity investigation.
- Consider all of the above and develop a communication plan that considers likely breach scenarios for your organization.

View previous tips: https://www.wipfli.com/30-tips

Tip #26: Get the right expertise

Executive-level cybersecurity resources are expensive and thrive in complex environments with continuous cybersecurity challenges.

Quite often in the mid-market, organizations don't have the budget or the constant cybersecurity challenges to keep top-tier talent fully engaged.

Additionally, while many smaller organizations may have "an IT person," they are usually busy managing the infrastructure and taking care of end-user issues and aren't focused on proactive protection of the business, much less in possession of the capabilities to respond to a cybersecurity incident and prevent a breach or evict attackers.

That means you need access to experts to validate management's representations and claims of cybersecurity effectiveness.

Steps you can take

Evaluate the current skill and knowledge level of your in-house team, and identify gaps.

1. Establish executive responsibility for cybersecurity. It should be someone at a high level of responsibility within the organization and who will have ultimate accountability.
2. If there is a board of directors, a committee — if not the general board — should have cybersecurity as a regular agenda topic.
3. Identify independent expertise that the executives or board can engage for cybersecurity advice and expertise.
4. Consider engaging expert consultants to fill critical roles, such as a virtual chief information security officer, so that you get access to necessary expertise and cyber risk management experience on a fractional basis.

View previous tips: https://www.wipfli.com/30-tips

WIPFLI

Tip #27: Keep your cryptocurrency safe

There are various ways to store your cryptocurrency, but some are safer than others in terms of security and exposure to theft.

In 2019, hackers breached 12 major cryptocurrency exchanges and stole more than $292 million worth of crypto.

Your crypto storage method should align with the intended use of that cryptocurrency.

Steps you can take

Not actively trading your cryptocurrency on an exchange? Then no need to hold your assets on an exchange-based, online wallet where your keys are held in the cloud.

You should move your crypto keys to a more secure wallet like desktop or mobile wallets. While these wallets are still considered hot wallets (meaning they are connected to the internet), they offer better security, don't require third-party trust and aren't subject to exchange hacks.

Want even more security? Move your keys to cold storage (meaning they are not connected to the internet) in a hardware wallet. Hardware wallets hold your keys on an offline device and connect to a computer via USB. If you're HODLing large amounts of crypto, then your best bet is cold, hardware storage.

View previous tips: https://www.wipfli.com/30-tips

WIPFLI

Tip #28: Sign up for SEC alerts

Broker dealers, investment advisors and investment companies are not immune to cybersecurity threats, yet many in the startup arena don't have dedicated resources to detect and respond.

That increases your risk that any cybersecurity incident like ransomware could be crippling to an organization, and you need to take measures to help maximize your resilience to such attacks.

Steps you can take

The SEC's Office of Compliance Inspections and Examinations can be a great resource for broker dealers and investment advisors.

The OCIE regularly shares information on trends they are seeing across registrants and provide guidance on how you can be more prepared.

For example, on June 10, 2020, the OCIE released a Risk Alert for ransomware. This alert contains practical guidance on procedures the OCIE has seen in place at registrants to help mitigate the risk of ransomware.

Regularly check the OCIE website to see if new risk alerts related to cybersecurity for SEC registrants have been posted; also consider signing up with the OCIE for email updates so you can be alerted to new risk alerts.

View previous tips: https://www.wipfli.com/30-tips

Tip #29: Follow DoD standards

With each passing month, more organizations are storing more controlled unclassified information (CUI) that could lead to business shut down or reputational risk.

The Department of Defense (DoD) has introduced new standards targeted at helping businesses protect CUI, which includes information that isn't classified but needs to be protected, like engineering drawings, financial information, research data or source codes.

The standards are part of a Cybersecurity Maturity Model Certification program that's required for defense contractors. But the standards offer insights into the evolution that all organizations can implement to improve their cybersecurity maturity.

Steps you can take

DoD standards contain some of the recommendations you'll see anywhere, such as establishing role-based access and limiting admin access.

Here are four elevated DoD guidelines that can help you up the level of your cybersecurity:

1. Monitoring and alerting: One aspect that has been expanded on in recent years is the use of security information and event monitoring, or SIEM. These systems gather logs from your servers, network devices and other sources to collect evidence that can be beneficial in re-creating the events that lead to compromise. In addition, alerts can be generated to trigger additional reviews of suspicious activity. While this can be done through other methods, a SIEM collects information into a single resource and protects information by restricting who can change or delete information.

2. Encrypt at rest and in transit: How we communicate with outside resources, such as cloud service providers, should be considered like a conversation in public. Information that is sensitive in nature should be protected. One way that information can be protected is through encryption. While it is a good practice to encrypt information where it is stored, it is also important that encryption (such as Transport Layer Security or TLS) is used to send and receive information. Note that while encryption is important, it's more important that you use current methods of encryption. Older types of encryption often have exposed flaws, which may not make them completely secure. Review any connection that uses encryption and make sure they are using a current encryption.
3. Limit removable storage: Protect information by treating it as sensitive as information you would lock in a safe. Just as you wouldn't leave a safe door open, you should not allow devices to copy and remove information. This recommendation goes beyond basic encryption by restricting access to what devices have access to copy information that is sensitive in nature.
4. Use advanced email protections: Protection against spam and malicious links in email has become more common place. Additional protections, such as SPF (Sender Policy Framework), DMARC (Domain-based Message Authentication Reporting & Conformance) and DKIM (DomainKeys Identified Mail) can be implemented to further protect email communications, which are one of the more targeted areas within an organization.

View previous tips: https://www.wipfli.com/30-tips

WIPFLI

Tip #30: Invest in B2B e-commerce security

Forecasters has estimated that global e-commerce will hit $34 trillion by 2024. And cyber criminals are quickly trying to find a way to steal a slice of that.

It's not just the dollars hackers are after. They also want to get credit card numbers and other sensitive client data.

Steps you can take

While your website has strong security, the devices consumers are using, plus risky Wi-Fi networks, often don't. As a result, 60% of all fraudulent transactions come from a mobile device.

Here are some security controls to explore for e-commerce sites:

1. Use risk-based transaction monitoring solutions: Security information and event monitoring (SIEM) and incident management (ATIM) systems and services scan huge volumes of data in real-time to collect evidence of possible security breaches. Integrated SIEM and ATIM systems can also deploy multistage tactics to respond to potential threats, such as adding an additional review of suspicious activity or locking accounts.
2. Use CAPTCHAs: Bad bots designed to look like real human users account for one-fifth of all e-commerce traffic. Those bad bots are a threat in terms of credit card fraud, theft of logins and price scraping. The easiest way to block them is to use CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart).
3. Protect against DDoS attacks: Distributed denial of service (DDoS) attacks can knock your website offline when hackers flood your servers with requests from thousands of untraceable IP addresses. You can reduce the threat by minimizing the possible points of attack by using load balancers, firewalls, access control lists and content distribution networks.
4. Block brute force attacks: Hackers will target your e-commerce admin panel in an attempt to figure out your password. They'll hit you repeatedly with programs that will try every combination of words and numbers to crack into your system. The solution is simple: Use a strong password and change it regularly.
5. Weigh risks with international sales: While e-commerce removes geographic barriers for many businesses, it can also increase your security risk. Experts say fraud on international channels is 2.5 times higher than domestic only. Use HTTPS: If you're still using outdated HTTP protocols, switch to HTTPS. In addition to lowering risk, many search engines will warn consumers your site is not safe if you don't.
6. Use HTTPS: If you're still using outdated HTTP protocols, switch to HTTPS. In addition to lowering risk, many search engines will warn consumers your site is not safe if you don't.
7. Don't store credit card numbers: While it's more convenient, storing credit card numbers in your database is a liability. If you do store numbers, use secure third-party payment processing systems.
8. Pick a secure e-commerce platform: Ensure you're building your site on a secure e-commerce platform that provides updates and high-level security.

View previous tips: https://www.wipfli.com/30-tips