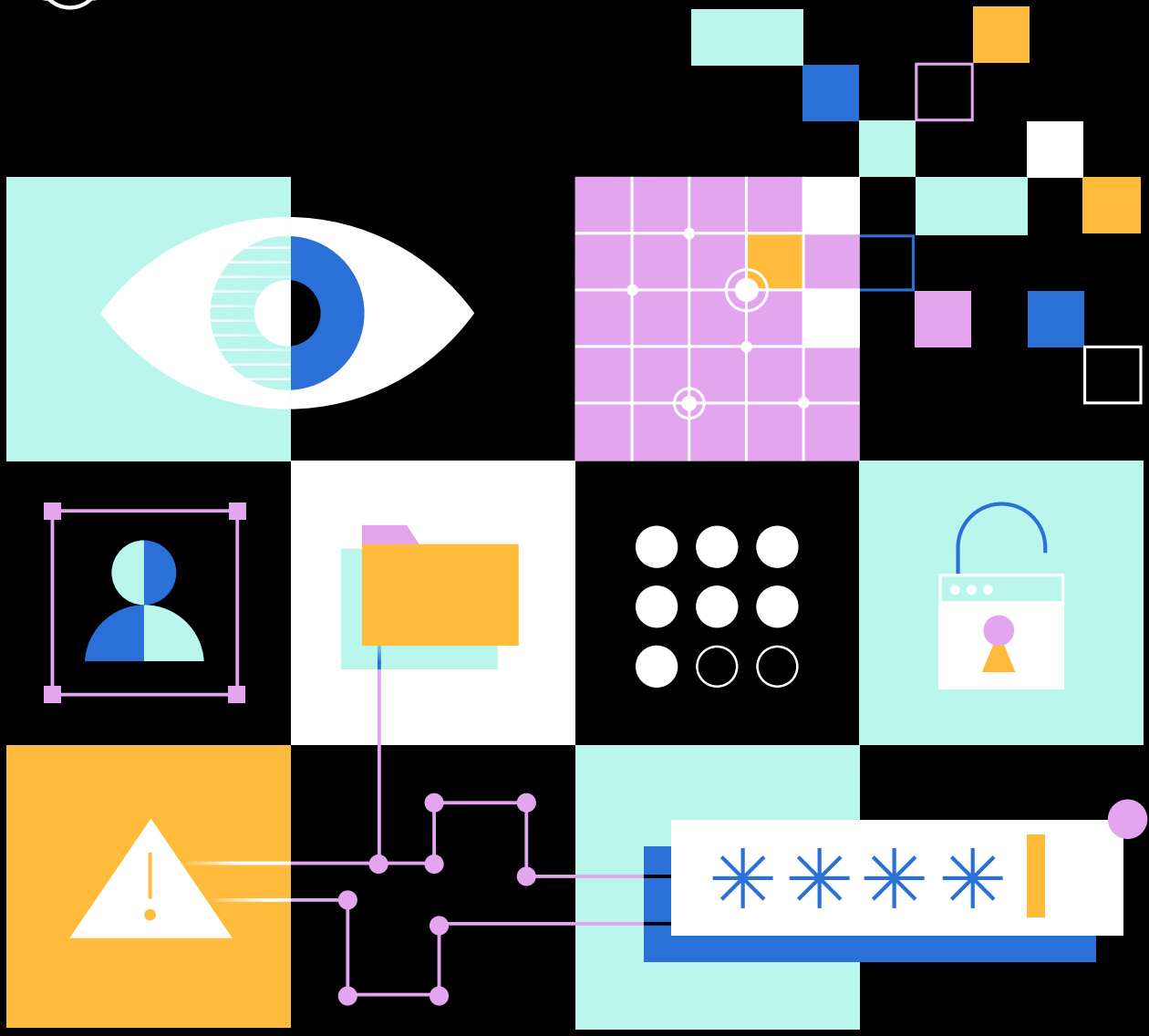
Coalition®



Small Business Cybersecurity Guide

coalitioninc.com

SMALL BUSINESS

Cybersecurity Guide

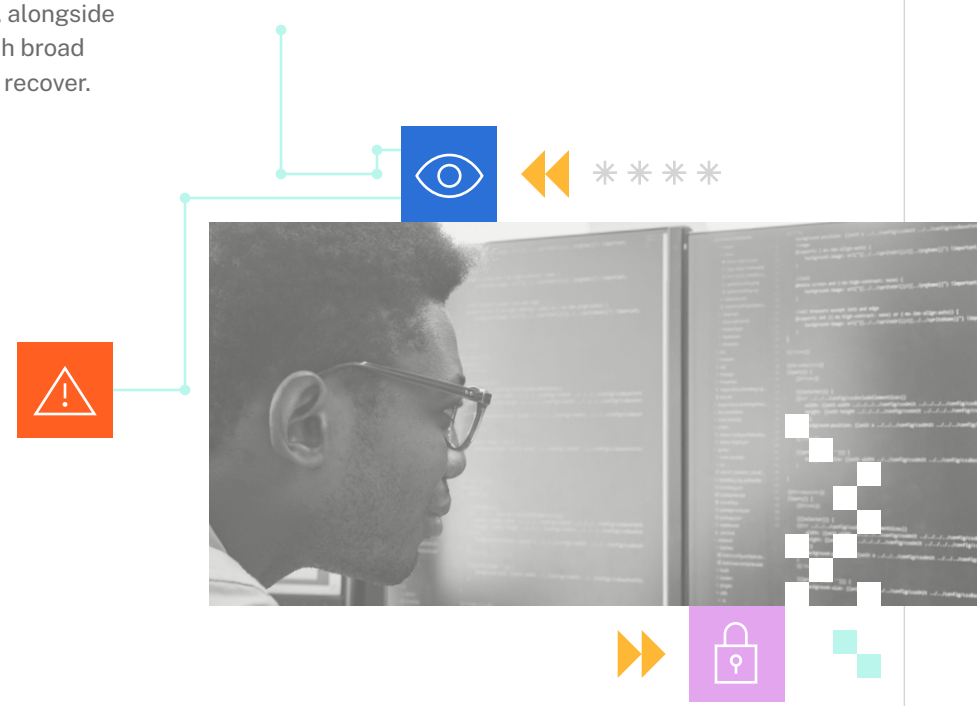
Introduction

Organizations are more connected than ever and rely on technology across all aspects of their business. This comes with new exposures, and every business must take the right steps to proactively manage risk. According to the Global Cyber Alliance, more than 43% of cyber attacks target small businesses, which often lack the security and technical expertise of larger organizations.

Cyber criminals exploit these digital risks. They target organizations of all sizes and industries for financial gain, and many organizations are unprepared to withstand an incident. Coalition built a new approach to risk management — what we call Active Insurance — to help our customers be resilient to digital risk. We provide active monitoring and alerting to prevent risk before it escalates, alongside in-house claims and incident response with broad insurance coverage to help our customers recover.

When combined with cybersecurity best practices and tools, this provides comprehensive protection for your organization. This guide gives businesses specific recommendations to improve their cybersecurity program and create a layered defense. While there is no such thing as a silver bullet in cybersecurity, these actionable steps can help prevent (or at least minimize) cyber threats.

Addressing these areas of security will help to mitigate cyber risk, but they can't guarantee an organization won't be targeted. If you're looking for more detailed cybersecurity advice, please reach out to our team, and they will be happy to assist.



Common cybersecurity terminology

Phishing

A social engineering attack where threat actors send fraudulent emails that appear to be from legitimate institutions in an attempt to trick users into providing sensitive information. Phishing can also happen via text (smishing).

Ransomware and malware attacks

A threat actor encrypts and disables access to business-critical systems and data until a ransom payment is made. Data may also be exfiltrated and exposed if the ransom isn't paid.

Business email compromise

Email intrusion resulting from spoofing, phishing, or spear phishing that can result in a data breach or funds transfer loss.

Funds transfer fraud (FTF)

A threat actor uses social engineering, sometimes in concert with phishing attacks and business email compromise, to cause funds to be sent to the attacker instead of the proper recipient.

Data breaches

A security incident that exposes confidential or protected information. Data breaches can be accidental due to a security failure or intentionally instigated by threat actors. Even if an external party has a data breach, if user credentials, such as usernames and passwords, were exposed, your company and customers could suffer account takeovers.

Legal and regulatory issues

Violation of a legal or regulatory framework, such as HIPAA, PIPEDA, GDPR, or CCPA.

Web application compromise

Direct compromise of a web-based technology, such as an e-commerce platform, as a result of a broad or targeted attack.

Technology Errors & Omissions (E&O)

A failure in the technology product or services results in business interruption or loss on behalf of your customers.

Table of contents

Increase email security

Email compromise could take down more than just your inbox. Lose access to your email, and you might lose everything. For many tools, email and calendar functions are tightly coupled. Keep your organization running smoothly by securing your email functionality.

For many businesses, email is an essential method of communication and organization. Unfortunately, email is also one of the most vulnerable business tools, and every organization should use caution when sending or verifying sensitive information by email.

Email compromise can take many forms. Threat actors use phishing emails to impersonate legitimate institutions and trick the recipient into performing an action — such as downloading an attachment or clicking a malicious link. Often, phishing or direct social engineering campaigns can evolve into a business email compromise (BEC), wherein a threat actor gains control of your email box. Once a threat actor has access to your business mailbox, they can manipulate your contacts and modify payment instructions, sometimes without even triggering any security alerts.

Things to consider

- BEC attacks can often result in funds transfer fraud (FTF) losses.
- Like ransomware, FTF losses have surged in recent years, and successfully clawing back payments depends on the timeliness of reporting the attack.
- It is significantly more difficult to clawback funds from FTF losses if one or both of the banks is international.

How to combat FTF

The primary defense against funds transfer fraud is a defined process for how your organization processes new requests and changes payment requests.

- Call the requesting party on a known, good number to confirm the demand — never use the contact information provided in an email as these are often manipulated via phishing.
- Develop a defined, two-party approval process for transfers and required reviews for payment change details.
- Check to see if a threat actor has introduced forwarding rules in the mailbox. Threat actors use forwarding rules to minimize the number of times they need to access the inbox.
- Threat actors often search for keywords such as “invoice” or “wire transfer” so they can attempt to redirect funds once they know a payment or wire transfer is scheduled.

Implement free email security settings

Sender Policy Framework (SPF)

SPF is a record you can add to your domain name system (DNS) settings that specifies what mail servers are allowed to send email on your domain's behalf. SPF helps to ensure that someone cannot create an email server and send it from your domain unless you have authorized them to do so in your DNS records.

- To implement SPF, you must publish a valid SPF record. We recommend carefully reviewing and testing SPF records before applying them.
- Utilize an SPF checker to validate your SPF record for your domain.

DomainKeys Identified Mail (DKIM)

DKIM ensures that emails sent to and from your mail server haven't been altered in transit. DKIM is configured through your mail provider and is free.

- To enable DKIM, you need to generate encryption keys and place them in your DNS. Your mail service provider will have precise instructions on how to do that.

Domain-based Message Authentication, Reporting and Conformance (DMARC)

DMARC ties SPF and DKIM together with another simple DNS record that provides a policy for how SPF and DKIM operate. DMARC also specifies an email address where delivery and forensic reports can be sent for analysis.

- To enable DMARC, you need to add a DNS TXT record with the name `_dmarc` and the content set to appropriate values for your organization. Learn more about enabling DMARC.

Multi-factor Authentication (MFA)

According to Verizon's Data Breach Investigations Report (DBIR), approximately 80% of breaches can be attributed to stolen credentials such as usernames and passwords. One of the most effective methods to mitigate the risk of an email-based cybersecurity incident is to enable Multi-factor Authentication (see next chapter).

Monitoring your mailbox is important. Threat actors will often redirect emails into the junk or trash folder. Periodically review your email folders for anything suspicious and also pay attention to any rules that forward or redirect messages.

Implement Multi-factor Authentication (MFA)

In addition to MFA, implement a company-wide password policy that requires strong passwords that are never reused or shared.

MFA immediately increases your account security by requiring multiple forms of identity verification when signing into an application. The second factor can be something you know, something you are, or something you have. With MFA, users must provide a digital token or code provided by a secondary device the user physically possesses to gain access to their account.

We recommend using MFA on all online accounts. In the event of a breach, MFA adds an additional level of protection to your accounts to prevent a threat actor from accessing your sensitive information.

Google Suite MFA Tips

Note: to set up MFA for Google Suite you must have admin privileges:

- Communicate to your users that MFA will be required to retain access to their Google account.
- Allow users to set up MFA. Text-based authentication is possible, but authentication apps are recommended.
- Google provides the option to turn on MFA enforcement.
- Google Advanced Protect safeguards user accounts from spoofs by third party 0auth trusts, among other scenarios.
- Consult Google Suite support documentation for additional questions.

Microsoft 365 MFA Tips

Note: to set up MFA for Microsoft 365, you must have global admin privileges.

- Microsoft 365 supports conditional access.
- Legacy users will have to follow additional steps.
- Subscribers who purchased 365 before 2017 will have to turn on Modern authentication.
- Consult Microsoft 365 support documentation for additional questions.

Selected vendors or existing services

- Select an MFA solution that works with your existing tools and devices, and figure out which services you currently use that have MFA settings you can enable.
- Deploy MFA to your organization with customizable posters, emails, and other training materials.

Recommended Vendors

BEC prevention

- Armorblox COALITION PARTNER

Authentication app

Provides a token for a software/service that already has MFA enabled.

- Google Authenticator
- Authy from Twilio
- Microsoft Authenticator
- 1Password
- Authentication solution — Enables you to configure MFA natively for any software
- Duo Security
- Okta COALITION PARTNER

Maintain good data backups

Ransomware is a criminal business model whereby threat actors gain access to a victim's data or network, encrypt it, and hold it hostage in exchange for ransom. As ransomware exploded in frequency and severity, it seemed there was no limit to what threat actors would demand. However, increased awareness of ransomware and prevention measures such as maintaining offline backups have helped mitigate the threat.

A good data backup can mean the difference between a complete loss or a full recovery after a ransomware attack. To best protect your organization, you'll need to develop a strategy tailored to your organization and regularly test your backups to ensure you can complete a full restoration. Maintaining data backups may also be a recommendation for your cyber insurance policy, depending on your organization's data.

Things to consider

- Maintain backups both on and off-site for critical business data. We recommend using offline backups to store essential data completely separate from the primary network.
- Cloud backups with a username and password combination not associated with an organization's domain are another alternative.
- You must test your backups by trying a full recovery. It is extremely common for organizations to only test their backups when they need them, and restoration failures are extremely high in those situations.
- If you choose to restore your data, applications, and operating system after an adverse event, keep in mind that a vulnerability in the system could have led to the compromise in the first place. Immediately patch all software and the operating system.

Regularly test your data backups to ensure you can successfully complete a full restoration of all critical business data.

Developing a backup strategy

- What data should be backed up, and where it should be stored?
- How frequently should data backups occur?
- How quickly could you restore your data from that system in the event of an incident and at different times (right now and years down the line)?
- How can you test and iterate on your backup solution to ensure it's working as intended and accommodates changing business needs?
  - Comply with legal requirements.
  - Implement a retention policy, as accumulating data without a plan to age it off could be a legal liability (discoverable in legal proceedings).

Recommended Vendors

- Acronis
- Backblaze
- Carbonite
- CrashPlan
- Datto
- IDrive
- Veeam Cloud

Enable secure remote access

Supporting remote work is the new standard for many organizations. To protect your business data, layer the appropriate tools and controls to ensure employees safely access, and are only provisioned, the resources they need to perform their jobs.

As more organizations now support remote and hybrid work models, employees are no longer in environments controlled or directly secured by their companies. Instead, employees access their organization's resources from outside corporate networks, known as remote access.

Without the proper security controls, remote connections can be a gateway for cyber criminals to access your devices and sensitive data.

Things to consider

- Remote access protocols (especially Remote Desktop Protocol or RDP) are features that enable employees to log into their corporate computers from home remotely. However, RDP can also pose a significant risk. Threat actors often target this technology and exploit known vulnerabilities.
- Consider implementing a perimeter-less remote access capability, such as Cloudflare Teams, that will add security to the authentication process and eliminate the external network exposures that threat actors continue to target.
- Place remote access protocols behind a virtual private network (VPN) or Zero Trust solution, which will establish a secure connection over the public internet. We also suggest logging and reviewing access weekly or bimonthly.

How to safely offer remote access

- When possible, utilize an authentication proxy or identity and access management solution for all remote access.
- Make sure the remote access is encrypted (SSL, IPSec, etc).
- Set up strong authentication for remote access (MFA).
- Set an organization-wide policy for strong passwords for remote access and encourage good password hygiene — never reuse passwords.
- If possible, require remote users to use company-provided hardware that has been secured to your company standards.
- Be sure to limit authorization to those with critical business needs.
- Review authorizations for remote access regularly to make sure unwanted personnel cannot gain access.
- Develop onboarding and offboarding procedures to ensure employees are granted and removed from access in a timely manner.

Technology recommendations

- Authentication Proxies with Twingate and Cloudflare Teams
  COALITION PARTNERS
- VPNs (Supported by firewalls such as Cisco, PaloAlto, Checkpoint)

Update your software

Secure your software and accounts; limit the number of service accounts to only those needed by your IT or security team, and implement a plan to offboard and update these accounts.

Threat actors are continuously looking to gain unauthorized access, and they often use old, out-of-date software as a means of ingress. To combat this risk, your organization should implement a process of regularly patching all connected devices: including laptops, workstations, tablets, and mobile devices with access to business data.

Manufacturers and app developers routinely release software updates as long as their product remains supported. These updates may contain new features or fixes for bugs and vulnerabilities. Examples of patch programs include Microsoft, which releases security patches on the second Tuesday of the month, informally called Patch Tuesday.

While most users think of patches and software updates in terms of the computer's operating system, every device that accesses business data requires updates. If your organization uses messaging apps such as Slack or Teams for communication, users should routinely update these apps and their mobile device operating systems. Any software exposed to the internet can pose a significant risk.

Should threat actors gain access to your network via old, outdated software, they can steal data, encrypt your files, or prevent your device from working.

Things to consider

- Be cautious with automatic updates; they can only occur if the device is connected to both Wi-Fi and plugged in.
- Some updates may require users to restart their devices.
- It is always a good idea to backup your critical data before rolling out a major update or patch.
- Users may decline or delay updates — look into how you can confirm compliance with critical updates or even force users who are out-of-date to update their devices.
- Communicate your organization's policies and procedures regarding device updates to your users.

Best practices for local software updates

Make sure that updates are applied regularly, including:

- OperatingSystem (Windows/OSX)
- Microsoft 365 and other desktop applications, such as Adobe Reader
- Web browsers and plugins
- Third-party applications
- Mobile devices and their applications
- Review updates on an ongoing basis

Vendor recommendations for internet software

- **Coalition Control:** Coalition's platform provides continuous scanning and automated security alerts, for free.
- Tenable, or other vulnerability scanners, can be used to scan internal network assets. This can help prevent an adversary from moving deeper into the network or exploiting other internal servers.

Use a password manager

The passwords your employees set for their business-related accounts and devices matter. Passwords grant access to the most private information your company deems critical. The reality is hackers have mastered the art of stealing password credentials using brute force attacks, where they automate every combination possible until they get it right, or through phishing attempts, where cybercriminals trick people into entering their information under false pretenses (using social engineering). Exposed passwords are also used to gain access to other accounts, potentially increasing the extent of the damage.

While it may feel daunting to worry about the length, strength, and update-frequency of your company passwords — it's necessary. Passwords need to be unique and never reused. To create strong passwords, use a mix of letters, numbers, and symbols, and regularly update passwords. We advise you to codify password requirements in a company-wide password policy and enforce this policy by forcing a logout, requiring users to update their passwords upon logging back into the network.

Password managers help keep track of multiple passwords and generate new ones at random, using a mix of factors to strengthen the passwords. They are essentially an encrypted vault for storing passwords that are protected by one master password.

Password managers and MFA

Even the most secure passwords aren't 100% secure — they may be lost in a third-party breach that you can't control. We recommend using MFA in conjunction with a password manager as the most secure approach to managing your logins. Check out our MFA section for vendor recommendations.

Things to consider

- Make sure your password manager supports each device platform your employees use.
- Find a password manager with browser extensions and full mobile support.
- Some password managers let your employees securely share passwords, and some automate password changes regularly.

How to implement a password manager

- Select a password manager solution that meets your budgetary and usage needs.
- Work with your IT team to vet and distribute the software.
- Host a company-wide training to introduce the new tool and make sure to include it in future new employee onboarding.
- Create a password policy in writing that employees can easily access at any time.

Recommended Vendors

- 1Password
- Dashlane
- Keeper
- LastPass (free with limited use)

Weak and reused passwords are a very pervasive threat vector, which adversaries routinely leverage to attack networks. Never share or reuse passwords — even between your personal and work accounts.

Scan for malicious software

While valuable, traditional antivirus software cannot detect all forms of malware, some of which are designed to evade its scans. End Detection and Response (EDR) provides more in-depth scanning containment and alerting if a threat actor compromises your network.

Work has been transformed over the last few years, with employees accessing company resources from multiple devices and locations. But as organizations continue to support an increasingly agile and hybrid work model, they open themselves up to new risks. Every device — phones, laptops, tablets — connected to your business network is an endpoint. Without endpoint protection in place, your organization is vulnerable to threat actors seeking to gain unauthorized access.

EDR collects and analyzes information from endpoints to respond to suspicious activity, including zero-day viruses or malware that antivirus cannot yet detect and polymorphic threats. Typically EDR solutions consist of the following features: Endpoint Protection Platform (EPP), which performs passive threat prevention, threat intelligence, a centralized management console, and active threat prevention.

EDR's active threat prevention allows it to identify and stop threats before a human administrator can respond to them. Once an EDR solution has identified a problem, it takes steps to quarantine and remove the malware. Unlike traditional antivirus, where the detection is only as good as its signature library, which must be regularly updated, EDR relies on behavioral analysis to detect and remediate threats based on their observed activity on the endpoint.

Best practices for implementing EDR

- Require that EDR be installed and active 100% of the time.
- Make sure the EDR tech pushes notifications to you rather than forcing you to request updates from the software provider.
- Review periodically to verify EDR is installed and updated.
- Set a schedule to review EDR detections (weekly, monthly, etc.)

Antivirus vendors

- Crowdstrike COALITION PARTNER
- Emsisoft
- ESET
- Malwarebytes COALITION PARTNER
- Webroot
- Windows Defender

EDR vendors

- Crowdstrike Falcon Insights COALITION PARTNER
- JAMF Protect
- Carbon Black
- Comodo COALITION PARTNER
- Endgame
- SentinelOne COALITION PARTNER

Encrypt your data

IBM defines data encryption as a way of translating data from plaintext (unencrypted) to ciphertext (encrypted). It's important to note that while users can still access their data, encryption helps to protect it from threat actors, and enhances the security of communication between client apps and servers.

If you lose a device and your organization's data is protected, the expense is limited to replacing the device, not the information on it — assuming the data is backed up. If your data is not encrypted and you lose a device, your organization may face a data breach and all of the legal, regulatory, and notification costs that come with it. Physical damage and loss are far cheaper than the loss of sensitive data.

We recommend checking applicable privacy statutes (or federal statutes) to ensure that your encryption meets the relevant standard. Individual locales and other regulatory bodies may require a base level of encryption. NIST currently recommends the Advanced Encryption Standard (AES) as the algorithm of choice to protect electronic data.

If you have a different device, or the encryption process has been updated for your device, check with your provider. Visit our website for more information about device encryption.

Things to consider

Your organization may be subject to additional compliance requirements based on the data you store.

Mobile phone encryption best practices

- Require a passcode or biometric identifiers to unlock the phone.
- Require entering a passcode after a set number of minutes inactive.
- Require mobile phones to leverage encryption when possible.
- On all mobile platforms, keep your operating system software up to date from authorized vendors (e.g., Apple, Google, Android).

Unprotected sensitive data traversing the public internet has the potential to result in identity theft, fraud, fines, compliance issues, reputational harm, and theft of financial resources from employees and customers.

Implement a security awareness training program

Create a culture where employees are aware of the risks of phishing and report report any suspicious activity immediately.

If you ask any IT security professional who is responsible for cybersecurity in their organization, they will probably say everyone — from the C-suite to contract workers and third-party vendors. Properly mitigating cyber risk isn't accomplished by one small team. It requires a deliberate culture of cyber risk awareness that holds every individual accountable.

Cyber criminals, targeting small and large businesses alike, aren't taking advantage of obscure technology. They rely on the manipulation of busy employees to gain access to your company's networks and devices. Through security awareness training programs, every employee gains the knowledge they need to stay vigilant and avoid becoming the victim of a phishing attack.

Cybersecurity tips for employees

- Do not click links or open any attachments you are not expecting. If you are not expecting a specific attachment, do not open it for review. Additionally, do not click links within emails if you are not expecting them. Follow up with a phone call to the sender directly; it's better to be safe than sorry.
- Use proper email security. Always verify that the emails you receive are from legitimate and trusted sources. Inspect the **From** addresses closely, and be wary of downloading any files that you're not anticipating, especially if they have an unusual file format such as .dmg or .exe files that indicate an executable file that will run on your computer.
- Use proper web security. Only download files from known and trusted websites. Verify that the URL is not intentionally misspelled to confuse you into downloading malware from a malicious website.
- Stay vigilant. Hackers rely on people letting their guard down and taking action without thinking. It only takes one mistake for malware to get installed and spread through a company.

Possible training options

- Curricula COALITION PARTNER
- Proofpoint
- Global Cyber Alliance

CYBER READINESS 201

Advanced tools and techniques

These tools and techniques are meant to advise organizations with a mature security program. If your organization does not have a dedicated IT or security staff this section may not be applicable.

No single technology, product, or service can achieve the goal of being 100% secure. Instead, solving cyber risk is an ongoing process of understanding your organization's risk, mitigating vulnerabilities as they are found, and responding to potential incidents promptly.

A key component of cybersecurity is having a documented incident response plan. Incident response plans define the responsibilities of your organization's security and IT teams involved in managing the breach. This can include the steps to address the incident, how it will be investigated and communicated to your customer base, and any potential notification requirements based on your industry.

This section details more advanced authentication and security measures that can be layered with the solutions and services previously discussed.

Single sign-on (SSO)

Like MFA, single sign-on (SSO) falls under the identity and access management (IAM) framework. IAM is a framework of policies and technologies that layer together to ensure the users have the appropriate access to the technology and resources they need to perform their job duties.

MFA and SSO layer together to support Zero Trust authentication. Foundational to Zero Trust is the concept of least-privileged access or only giving users access to the resources necessary to perform their job duties.

Zero Trust

In 2021, Cybersecurity and Infrastructure Security Agency CISA released a draft Zero Trust Maturity model. Zero Trust grants employees only the level of access that is absolutely necessary, treating all devices and traffic as potential threats. According to the U.S. General Services Administration (GSA), Zero Trust Architecture (ZTA) layers technologies that perform the following functions:

- Authenticate, monitor, and validate user identities and trustworthiness.
- Identify, monitor, and manage devices and other endpoints on a network.

Things to consider

- SSO and ZTA can be costly solutions to implement.
- SSO and ZTA are part of a mature security model and will require a dedicated staff to roll out properly.
- Support for SSO and ZTA are related to the rapid changes in work and the digital economy brought about by the COVID-19 pandemic.

Recommended vendors

- Okta COALITION PARTNER
- Auth0
- Twingate COALITION PARTNER
- Tailscale
- ZScaler

Cyber insurance: Coverage for when all else fails

Technology is the cornerstone of today's digital economy; it has changed how we work, shop, and interact. Unfortunately, this transformation has also accelerated the pace of digital risks.

At Coalition, we believe that all businesses should be able to embrace technology and thrive in the digital economy. That's why we've created a new way to mitigate digital risk with Active Insurance. Active Insurance combines the power of technology and insurance to provide coverage that is built for modern organizations. Active Insurance stands in stark contrast to traditional insurance, which wasn't built for the speed and amorphous nature of digital risks and leaves many organizations unprepared.

Active Insurance from Coalition brings together in-depth technology, cybersecurity, and insurance expertise to help organizations assess, prevent, and respond to an emerging set of digital risks. We support brokers and policyholders before, during, and after an incident occurs, taking a holistic approach to supporting our customers.

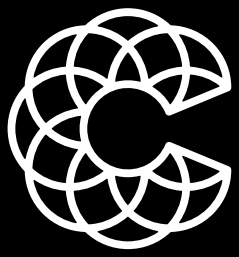
Coalition's Active Risk Platform analyzes complex sets of public data, threat intelligence, and proprietary claims information to create personalized risk assessments and threat monitoring that goes far beyond traditional insurance. Coalition helps to protect our customers with Active Cyber, Active Executive Risks, and P&C policies.

Coalition's Active Protection and Response provides a holistic risk management solution for your organization, including:

- Attack surface monitoring and third-party risk management in Coalition Control — valued at over $10k and included with your policy
- In-house claims and incident response support
- Cybersecurity education resources and discounted cybersecurity solutions

Protect your business with Active Cyber Insurance from Coalition

- Contact your broker to get a quote. If you don't have one, contact us and we can provide a list of recommended brokers in your area.
- Sign up for Coalition Control and get your free Coalition Risk Assessment to understand your specific risks.



Coalition®

coalitioninc.com

44 MONTGOMERY STREET, SUITE 4210
SAN FRANCISCO, CA 94104