PARTNER COLORADO
CREDIT UNION

Cyber security

Cyber security is a constantly evolving threat, with cybercriminals using increasingly sophisticated tactics to exploit vulnerabilities. Without proper safeguards, your business could face data breaches, financial losses, and reputational damage.

This checklist outlines key measures to help you strengthen your defenses, protect sensitive information, and reduce the risk of cyber threats.

✓ Back up and secure your data

- □ Backup critical business and customer data
- □ Automate and schedule regular backups
- □ Securely store backups in multiple locations
- □ Enhance cloud security with authentication and monitoring
- □ Monitor security alerts and respond quickly

✓ Keep systems updated and monitored

- □ Use supported devices and software
- □ Enable automatic system and software updates
- □ Monitor failed login attempts and password changes
- □ Track and respond to security alerts
- □ Make sure IT providers apply updates promptly

✓ Control access

- □ Limit data collection and storage
- □ Encrypt any data in transit
- □ Encrypt any data at rest
- □ Restrict employee access based on roles
- □ Secure applications and devices

✓ Secure communication channels

- □ Monitor and protect email activity
- □ Strengthen email authentication with DNS records
- □ Establish a fraud escalation process
- □ Setup applications to enforce MFA on logins
- □ Set-up each employee with MFA access

✓ Write a security policy

- □ Create a security policy document
- □ Plan for responding to a cyber security attack
- □ Include password and data policy
- □ Define employee cyber security responsibility
- □ Set guidelines for third-party access

✓ Onboarding and exit processes

- □ Add security training to employee on-boarding
- □ Educate staff about the security policy
- □ Systemize removal of access when employees leave
- □ Record items to be returned when employees leave
- □ Limit access until fully trained

Cyber security

Back up and secure your data

Backup critical business and customer data

Customer records, employee data, and essential business documents are invaluable assets. Regularly backing them up means that accidental deletions, cyberattacks, or hardware failures don't result in permanent loss.

Use secure, encrypted storage solutions such as cloud services or protected on-premise servers. Implement strict access controls with strong passwords and multi-factor authentication (MFA) to prevent unauthorized access.

Automate and schedule regular backups

Manually backing up data is prone to errors and delays. Automating the process means backups happen consistently, reducing the risk of missing important updates. Schedule backups based on business needs, e.g. real-time for high-volume data or daily/weekly for lower activity levels.

Use reliable backup solutions that encrypt data and store copies in multiple locations. Regularly test your backup recovery process to confirm files are intact and can be restored quickly when needed.

Securely store backups in multiple locations

Storing backups in a single location increases the risk of losing data due to theft, natural disasters, or system failures. Maintain multiple copies, including cloud-based and offsite physical backups, to protect against unforeseen events.

Cloud storage should be encrypted and secured with strong authentication, while physical backups should be kept in a fireproof, waterproof, and access-controlled facility. Review storage practices periodically to make sure of accessibility without compromising security.

Enhance cloud security with authentication

Not all cloud services automatically back up data, and security breaches can put sensitive information at risk. Review your provider's backup policies and consider additional backups to independent cloud storage or local devices.

Enable Two-Factor Authentication (2FA) for all cloud accounts to prevent unauthorized access. Use authentication apps instead of SMS-based verification to reduce vulnerability to attacks like SIM swapping.

Monitor security alerts and respond quickly

Cyber threats often start with unauthorized access attempts or suspicious activity. Enable security notifications from your cloud provider to receive real-time alerts on breaches, failed login attempts, or other security concerns.

Regularly review security logs and establish a response plan for handling breaches. Train employees on recognizing security threats and make sure they follow best practices for maintaining data integrity.

Keep systems updated and monitored

Use supported devices and software

Devices and software that are no longer supported by manufacturers stop receiving security updates, making them vulnerable to cyber threats. Unsupported systems are prime targets for hackers looking to exploit outdated technology.

Regularly review all business devices and software to make sure they are within their support lifecycle. Replace outdated hardware and upgrade software to current, secure versions. Encourage employees using personal devices for work to follow the same security standards.

Enable automatic system and software updates

Keeping operating systems, applications, and security software updated is one of the easiest ways to protect against cyber threats. Security patches fix vulnerabilities that attackers may exploit. Automating updates means critical fixes are applied without delay.

Enable automatic updates for all business devices, including desktops, laptops, and mobile phones. For software that requires manual updates, set a clear update schedule and make sure employees follow security best practices to keep systems protected.

Monitor failed login attempts and password changes

Repeated failed logins can indicate a brute-force attack or an unauthorized access attempt. Monitoring password changes helps detect if an attacker has taken control of an account.

Set up alerts for multiple failed login attempts, especially from unknown locations, and temporarily block access after repeated failures. Enable logging for password

Cyber security

changes and notify users when their credentials are updated to prevent unauthorized modifications.

Track and respond to security alerts

Security software, including anti-malware and firewall systems, provides real-time alerts about potential threats. However, these alerts are only effective if they are actively monitored and acted upon.

Make sure anti-malware software is always running and up to date. Configure automated notifications to alert IT staff or management of suspicious activity, quarantined files, or failed security updates. Regularly review logs to detect potential security breaches.

Make sure IT providers apply updates promptly

Delayed updates leave your business at risk, as cybercriminals exploit known vulnerabilities. Updates should be installed within weeks of release to minimize exposure.

If your business relies on an IT provider, confirm they have a process to deploy updates quickly. Request regular reports or logs to verify updates are applied on time and conduct periodic reviews to make sure all critical patches are installed.

Control access

Limit data collection and storage

Only collect and store customer information that is essential for business operations to minimize the risk of data breaches. Retaining unnecessary data increases exposure if a cyberattack occurs.

Regularly review data retention policies and securely delete outdated or unnecessary information to maintain compliance with privacy regulations.

Encrypt any data in transit

Data in transit, which is information being sent over the internet, through emails, or between systems, is vulnerable to interception by cybercriminals. Encrypting data while it's being transmitted means that even if hackers intercept it, they cannot read or use it without the correct decryption key.

Use secure communication protocols like HTTPS, TLS, and VPNs to protect sensitive information. Educate employees on secure file-sharing practices and make sure that confidential data, such as customer records and financial details, is never sent over unsecured channels.

Encrypt any data at rest

Data at rest refers to stored information on servers, databases, or devices that is not actively being transmitted. Encrypting stored data adds an extra layer of security, making it unreadable to unauthorized users, even if they gain access to the storage system.

Make sure encryption is enabled for all sensitive files, including customer records, financial data, and employee details. Use strong encryption standards and store encryption keys securely, separate from the encrypted data.

Restrict employee access based on roles

Not all employees need access to all data. Role-based access controls (RBAC) limit exposure by making sure staff can only view or modify the information necessary for their job.

Assign system permissions, regularly review access levels, and enable multi-factor authentication (MFA) to verify user identities before granting access to sensitive data.

Secure applications and devices

Unsecured apps and outdated software create vulnerabilities that cybercriminals can exploit. Employees should only use approved, up-to-date applications for work-related tasks.

Implement policies that block access to business networks from devices running insecure apps. Use endpoint security tools to detect and prevent high-risk applications from being installed or used.

Secure communication channels

Monitor and protect email activity

Cybercriminals use compromised email accounts for phishing and fraud. Monitoring email traffic helps detect suspicious login attempts, spoofing, or unauthorized messages before they cause harm.

Use an email security service to track threats, flag unusual activity, and send real-time alerts. Regularly review email logs and update security settings to prevent breaches.

Cyber security

Strengthen email authentication

Properly configured DNS records protect your domain from email spoofing and phishing attacks. Authentication protocols like SPF, DKIM, and DMARC mean only authorized servers can send emails on your behalf.

Regularly review and update these records, especially if using third-party email services. If unsure, consult an expert to maintain secure, trusted email communication.

Establish a fraud escalation process

Fraudulent transactions, invoice scams, or unauthorized payment requests can result in financial losses. A clear escalation process ensures employees know how to respond to suspicious activity.

Require verification for unusual payment requests, such as confirming supplier bank detail changes through a separate communication channel. Train employees to spot fraud tactics and assign a dedicated team to handle suspicious transactions.

Setup applications to enforce MFA on logins

To maximize security, configure business applications and systems to require MFA for logins. This means that all users must verify their identity before accessing sensitive information.

Many software platforms, including email services, cloud storage, and financial applications, offer built-in MFA options. Enable these settings across all critical business applications and regularly review access logs to monitor for any suspicious login attempts.

Set-up each employee with MFA access

MFA is most effective when applied consistently across all employees and devices. Setting up MFA for each employee means that everyone follows the same security protocols, minimizing the risk of security gaps in your network.

Provide training on how to use MFA effectively, including best practices for managing authentication apps or backup codes. Regularly audit MFA usage to confirm that all employees have it enabled and address any issues that arise to maintain a secure working environment.

Write a security policy

Create a security policy document

This provides clear guidelines for protecting your business's data, systems, and networks. It sets expectations for employees and provides consistency in security practices across the organization.

Include details on system access controls, acceptable use of company devices, procedures for handling sensitive information, and incident response protocols. Regularly review and update the policy to address new threats and make sure you're compliant with industry standards and regulations.

Plan for responding to a cyber security attack

A strong incident response plan should outline roles and responsibilities, communication procedures, and steps for containing and recovering from an attack.

Include guidelines for reporting security breaches, isolating affected systems, restoring data from backups, and notifying customers or stakeholders if necessary. Conduct regular drills or simulations to make sure employees understand their role in the event of a cyber incident.

Include password and data policy

A security policy should clearly define how passwords and sensitive data are managed to prevent data breaches. Outline requirements for password complexity, expiration timelines, and multi-factor authentication enforcement.

Additionally, specify how customer and business data should be stored, accessed, and shared. Include protocols for encrypting sensitive information, restricting access to authorized personnel, and securely disposing of outdated data. Regularly review these policies so that they align with best practices and emerging threats.

Define employee cyber security responsibility

A strong security policy outlines the specific cybersecurity responsibilities for employees at all levels. Clear expectations help prevent human errors that lead to data breaches and security incidents.

Cyber security

Specify guidelines for handling sensitive information, using company devices, and accessing business systems remotely. Regularly train employees on best practices, phishing awareness, and how to report security concerns.

Set guidelines for third-party access

Vendors, contractors, and partners with access to your systems can introduce security risks. Your policy should establish strict controls for granting, managing, and revoking third-party access.

Require third parties to follow your security standards, use secure login methods (such as MFA), and undergo regular access reviews. Limit access to only necessary data and disable credentials immediately when they are no longer needed.

Onboarding and exit processes

Add security training to employee on-boarding

New employees need to be introduced to your company's security policies as part of their onboarding process. This means they understand the importance of data protection, the potential threats to your business, and how to mitigate those risks from day one.

Provide training on safe internet practices, recognizing phishing attempts, handling sensitive information, and securing company devices. Reinforce the importance of following security protocols, and offer regular refresher training so that security remains a priority throughout their employment.

Educate staff about the security policy

Your security policy should be well-known and understood by all employees to prevent breaches caused by ignorance or negligence. Make sure every employee has access to the security policy and comprehends their role in maintaining a secure working environment.

Schedule regular security briefings and make sure that the policy is clear and easy to understand. Encourage staff to ask questions about security procedures and use real-world examples to illustrate the potential impact of breaches, reinforcing the importance of adherence.

Systemize removal of access when employees leave

When an employee leaves the company, their access to company systems and data must be promptly and securely revoked. This includes deactivating accounts, changing passwords, and making sure any shared access or permissions are removed.

Create a clear process for employee exits that includes steps to remove access from all systems, applications, and company devices. Maintain a checklist that can be followed each time an employee departs so that no access is overlooked and assign responsibility for completing these tasks.

Record items to be returned when employees leave

It's essential to recover all company-owned equipment and materials, including laptops, phones, keys, and ID cards. Having a detailed list of items that need to be returned means nothing is forgotten and helps maintain accountability.

Establish a checklist of company assets assigned to each employee at the start of their employment, and make sure it's completed upon their departure. This process should include verifying the return of all items and checking the condition of devices to make sure they are securely wiped of any sensitive company data.

Limit access until fully trained

New employees may not be familiar with cybersecurity risks, making it essential to restrict access to sensitive systems until they complete security training. Gradually increasing access means they understand best practices before handling critical data.

Set role-based access controls (RBAC) that limit new hires to only the tools and information they need. Require employees to complete security training and acknowledge the company's cybersecurity policy before granting full system access. Regularly review access permissions as employees take on new responsibilities.

Cyber security

Notes

Note
This is a guide only and should neither replace competent advice, nor be taken or relied upon as financial or professional advice. Seek professional advice before making any decision that could affect your business.