Right Sized Cybersecurity Controls

Essential strategies to protect business digital assets

Secure Your Business

Practical Cybersecurity Focus

Cybersecurity is a practical business concern, emphasizing realistic, affordable controls achievable quickly.

Prioritization of Safeguards

Focus on safeguards that deliver the most risk reduction with limited resources and time.

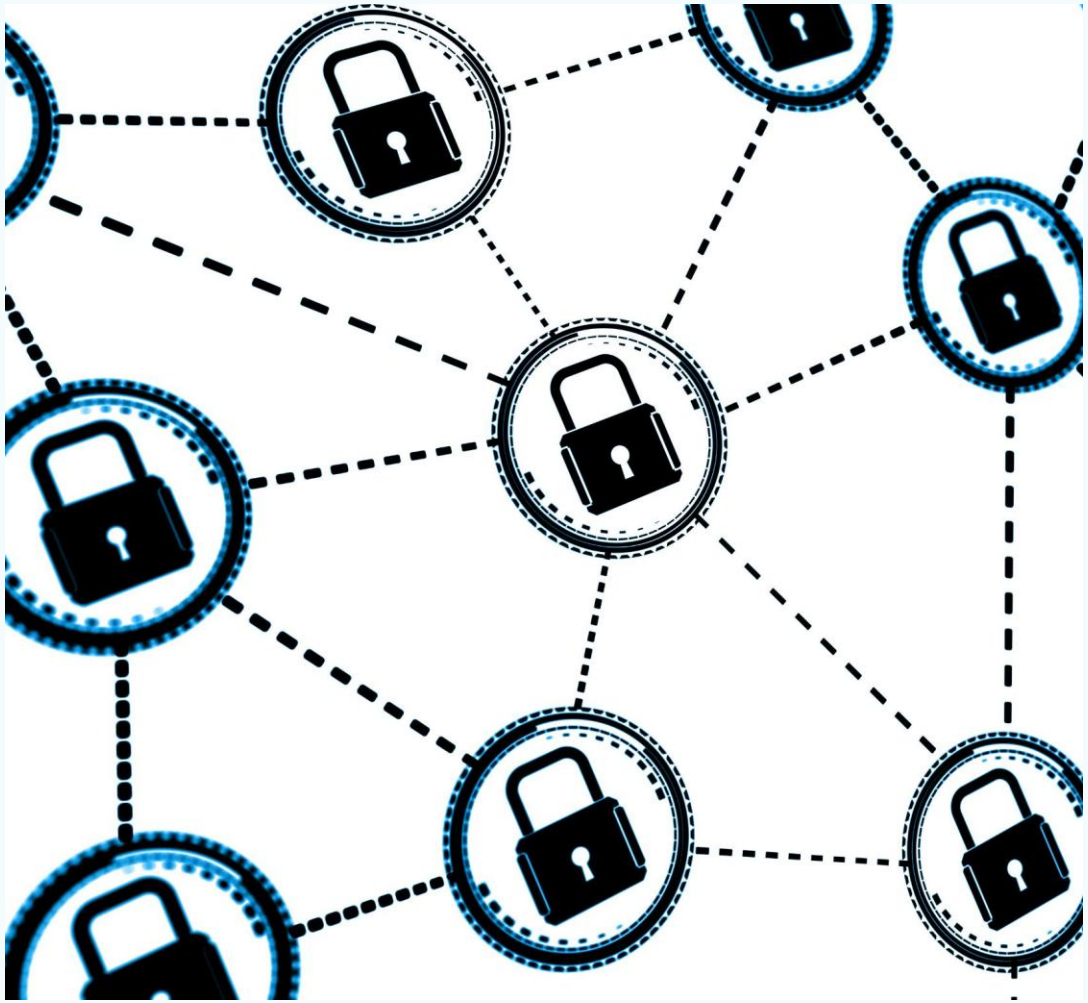
Guidance for Decision-Makers

Designed for leaders without dedicated security teams who handle sensitive data and systems.

Security as a Journey

Cybersecurity maturity is a process starting with small, consistent, documented actions.

Why Cybersecurity Matters for You



You are a target

Smaller firms are frequent targets of cybercriminals due to often weaker cybersecurity defenses.

Consequences of Cyber Incidents

Cyber incidents cause operational downtime, revenue loss, reputational harm, and legal issues for small businesses.

Supply Chain Vulnerabilities

Attackers use smaller suppliers as gateways to larger organizations, making cybersecurity a shared responsibility.

Leadership and Cyber Risk

Cybersecurity is a business risk requiring leadership involvement and investment in protective controls.

Federal Legal Stakes for Small Businesses

Cyber incidents are legal and regulatory events

No single U.S. cybersecurity law – small businesses face a patchwork of federal and state rules.

Applies to nearly everyone:

- FTC Act Section 5 – requires "reasonable" data security and honest privacy/security promises.
- CAN-SPAM – sets rules for commercial email (truth subject lines, clear opt-outs)
- Extra rules if you are in a regulated bucket –
  - GLBA Safeguards Rule – financial services and some non-bank "financial institutions" (lenders, finance, tax prep, etc.)
  - HIPPA / HITECH – health plans, providers, and their vendors handling Protected Health Information (PHI)
  - COPPA / FERPA/ SEC / federal contracts / CIRCIA – specialized obligations for children's services, education, public companies, federal contractors. And critical infrastructure.

Guiding Principles

Simplicity and Repeatability

Simplicity and repeatability ensure cybersecurity controls are maintainable and less prone to failure in smaller settings.

Focus on Critical Assets

Prioritize protection of customer data, financial systems, and mission-critical applications to maximize security impact.

Incident Detection and Recovery

Plan for incident detection and recovery, accepting that breaches can happen despite prevention efforts.

Documentation and Continuity

Maintain thorough documentation of ownership, procedures, and contacts to ensure continuity during stress or staff changes.

Guiding Principles are a Regulator's Playbook

Regulators look for "was your security reasonable"

Risk-based, not perfection

FTC, GLBA, HIPPA use a "reasonable security " standard tied to your size, data, and risk profile.

Written security program:

Regulators expect written policies, roles, and procedures, mot just "tribal knowledge".

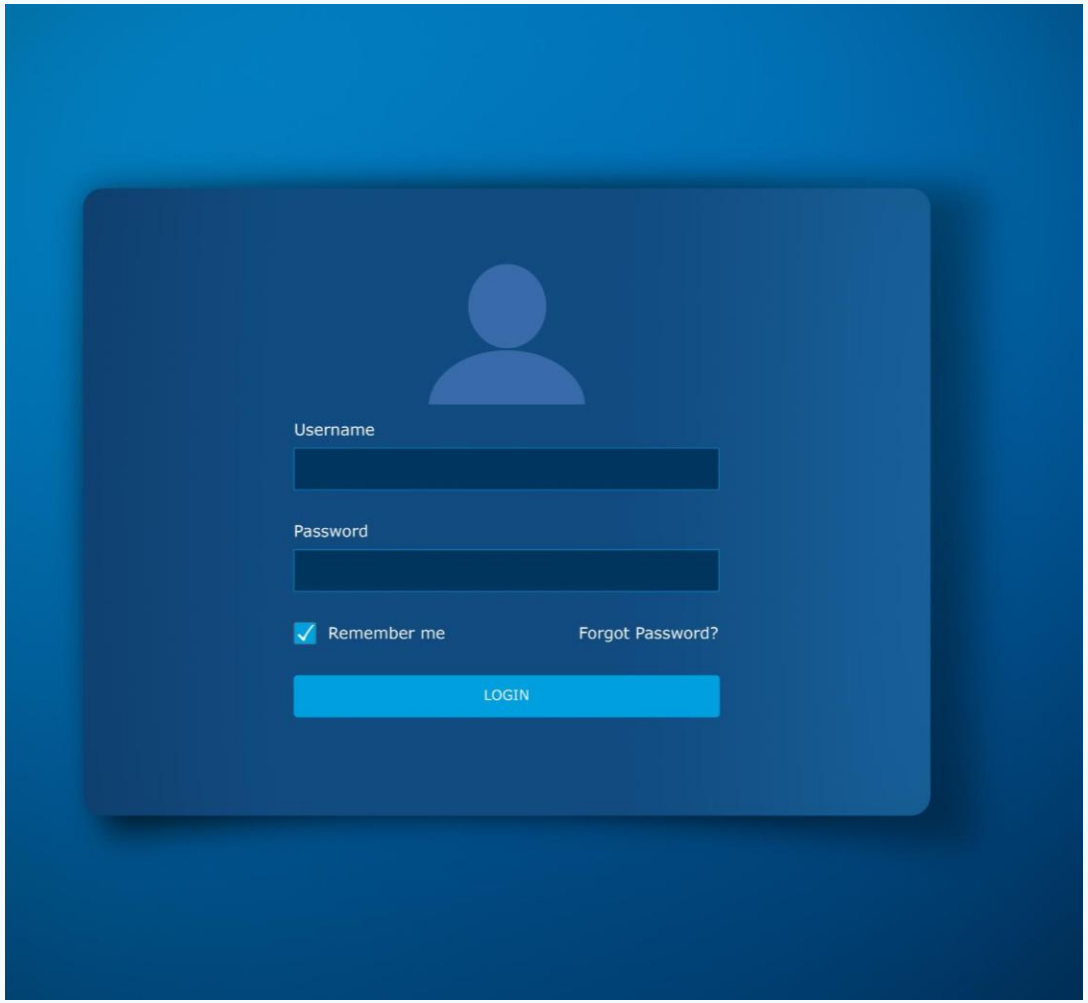
People, technology, vendors:

Training, technical safeguards, and vendor security clauses are all part of "reasonable" security.

Plan for incidents and learn from them:

Incident response, breach assessment, notification decisions, and "lessons learned" are core expectations.

Identity & Access Controls



Multi-Factor Authentication

Enforce multi-factor authentication on critical systems to enhance login security and reduce unauthorized access risks.

Password Management

Use password managers to create long, unique passwords without increasing user frustration or complexity.

Administrative Privileges Control

Limit administrative rights, avoid shared accounts, and use separate admin credentials to minimize access risks.

Access Removal Process

Promptly remove user access during role changes or departures through an efficient joiner, mover, and leaver process.

Endpoint & Patch Management

Standardizing Devices

Using company-managed devices reduces risks associated with unmanaged personal hardware.

Automatic Updates

Enabling automatic OS and browser updates addresses vulnerabilities quickly and efficiently.

Endpoint Protection Tools

Deploying endpoint detection and response tools helps detect and stop malicious activity.

Asset Inventory Management

Maintaining an accurate asset inventory supports incident response and lifecycle management.

Email & Phishing Protection

Email as Cyberattack Vector

Email is still the most common entry point for cyberattacks targeting businesses.

Use Business-Grade Email Protection

Employing business-grade email platforms with built-in spam and phishing protections reduces risk significantly.

Block High-Risk Content

Blocking high-risk attachments and links helps minimize exposure to phishing threats effectively.

Phishing Awareness Training

Regular, short training sessions help employees identify and avoid phishing attempts confidently.

Easy Phishing Reporting

Providing a simple way for staff to report suspicious emails speeds detection and response times.

Comply with CAN-SPAM for marketing emails

Use honest subject lines, identify marketing where required, and provide easy unsubscribe options to avoid FTC enforcement.

Data Protection & Backups

Identify Critical Data

Focus on protecting essential business data like customer records, financial information, and intellectual property.

Consolidate Data Systems

Store critical data in a few secured systems instead of scattered file shares for better security and management.

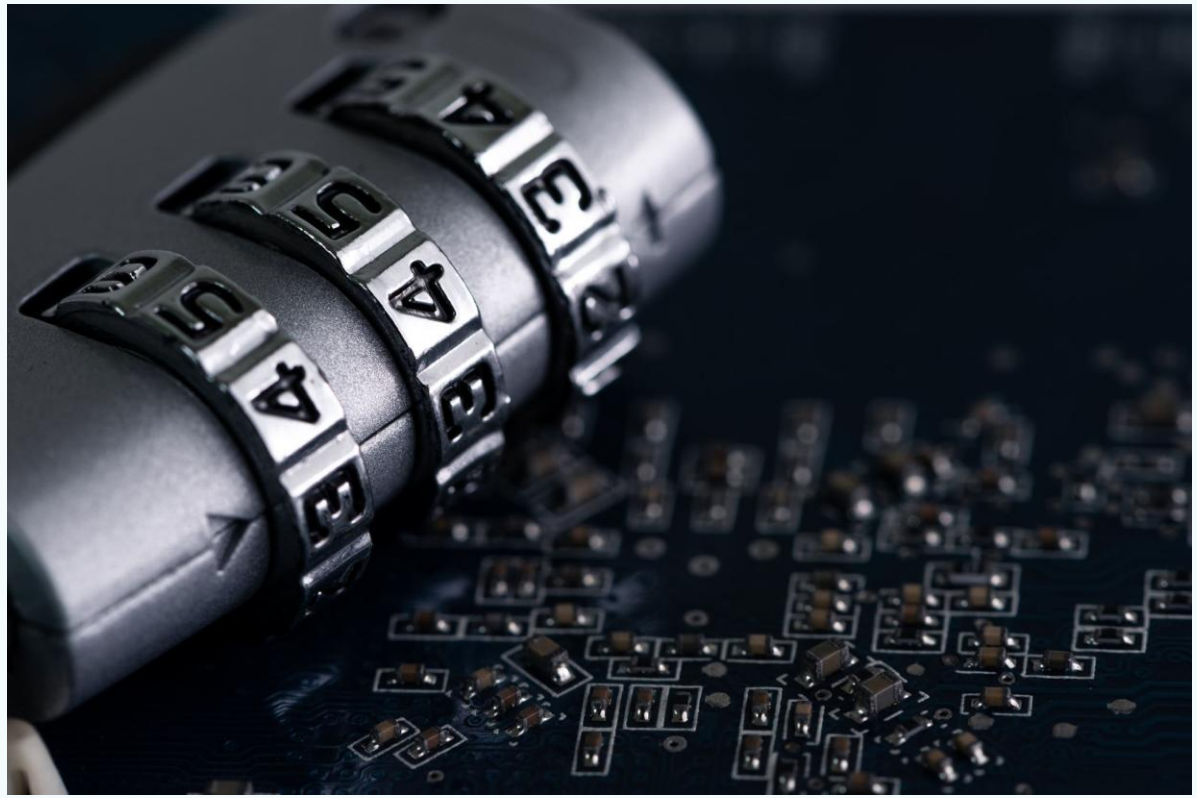
Regular Automated Backups

Perform regular automated backups and keep at least one offline or immutable copy to protect from ransomware.

Test Data Restoration

Periodically test data restoration to ensure backup usability and support business recovery efforts.

Federal Rules that Care About Your Data Security



Certain data protection and access controls are not option “nice-to-haves”.

If you store customer or consumer data

FTC Act – expects “reasonable safeguards and truthful statements about your security and privacy practices. Example regulators expect: risk assessment, patching, MFA on sensitive systems, training, vendor oversight.

If you’re a financial institution (broadly defined – e.g., lenders, finance companies, tax preparers, some advisors)

GLBA Safeguard Rule – requires a written information security program with access controls, encryption, secure disposal, testing/monitoring, training, vendor oversight, and board reporting.

If you handle data as Personal Health Information (PHI)

HIPPA Security & Breach Rules – require specific safeguards for electronic PHI and breach notification to individuals and regulators.

- Identify & Access Control (MFA, least privilege, joiner/mover/leaver) supports access control expectations under FTC/GLBA/HIPPA.
- Endpoint & Patch Management and Network & Remote Access, map to “technical safeguards’ mentioned in enforcement actions and guidance.

Network & Remote Access

Network Perimeter Protection

Modern firewalls or routers with automatic updates safeguard the network perimeter against threats.

Remote Access Controls

Disable unused remote access paths and enforce VPN with multi-factor authentication for admin tasks.

Network Segmentation

Separating guest Wi-Fi from internal networks is an effective control to protect business resources.

Cloud Access Review

Regularly review cloud and SaaS access settings to limit administrative portal exposure by IP range.

Vendors & Cloud Services

Vendor Risk Management

Maintain an updated list of key vendors including email, CRM, payment, and IT services to manage risks effectively.

Security Features Preference

Prefer vendors that offer multi-factor authentication, logging, and recognized security certifications for enhanced protection.

Access Control and Review

Limit vendor access to only necessary resources and review access periodically to minimize vulnerabilities.

Vendor Exit Planning

Plan for vendor exit including data retrieval and account closure to avoid hidden risks after termination.

Reflect Your Legal Duties in Vendor Contracts

If you're under GLBA, HIPPA, or federal contract rules, you're expected to push security requirements and breach-notification duties into vendor agreements (e.g., Safeguard Rule service-provider oversight, HIPPA business associate agreements).

Incident Response Basics

Define Security Incidents

Clearly define what constitutes a security incident like ransomware or lost devices for effective response.

Incident Response Playbook

Create a concise playbook detailing contacts, information capture, and decision-making authority.

External Support Identification

Identify external resources like legal counsel, insurers, and managed service providers beforehand.

Lessons Learned and Updates

Capture lessons learned post-incident and update controls to improve future response and security.

Legal Duties When an Incident Happens

What you must do depends on who you are:

- GLBA financial institutions – Must notify the FTC within 30 days of discovering certain breaches involving >500 customers' encrypted customer information, under the updated Safeguard Rules.
- HIPPA entities/business associates – Must notify affected individuals, HHS, and sometimes media, following specific timelines and thresholds.
- Critical infrastructure – Will have to report certain incidents to the Cybersecurity and Infrastructure Security Agency (CISA) under CIRCIA once regulations are fully implemented.
- Public companies – Must disclose material cyber risks and incidents under SEC rules.

Cross-cutting expectations, even outside those regimes:

- Involve legal counsel early to assess notification duties and preserve privilege.
- Preserve logs and evidence; avoid destroying anything potentially relevant.
- Keep customer and public communications accurate and consistent to avoid "deception" issues under the FTC or securities law.

Training, Policies, and Culture

Employee as Defense

Employees serve as both the first and last line of cybersecurity defense, requiring constant awareness training.

Clear Security Policies

Simple, readable policies guide acceptable use and remote work to ensure consistent security practices.

No-Blame Reporting Culture

A no-blame culture encourages employees to report mistakes and concerns for better detection and prevention.

Security Integration

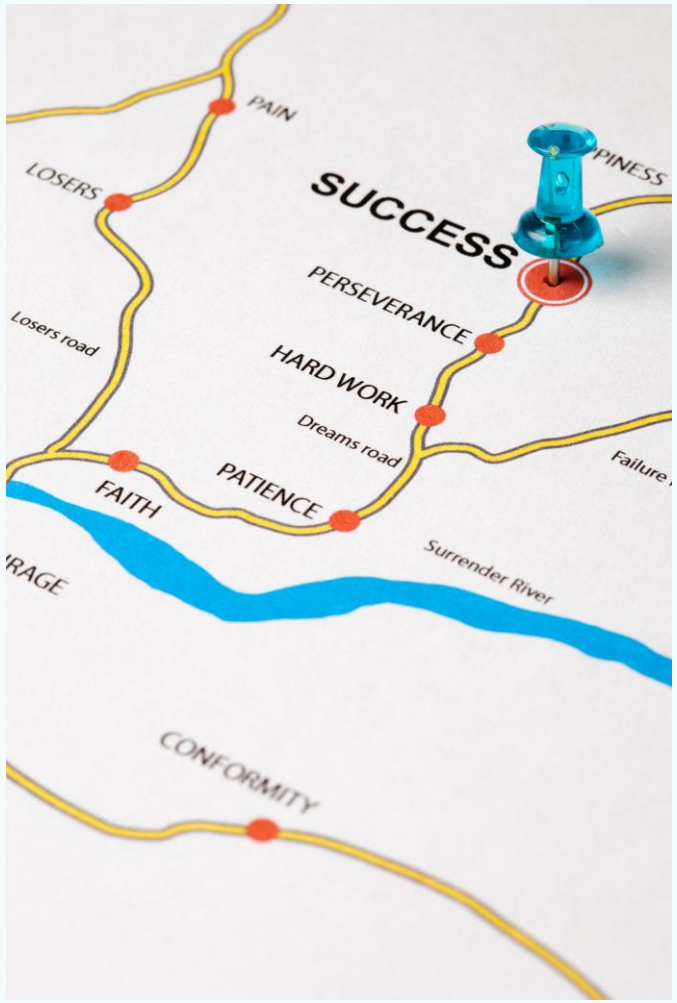
Embedding security in onboarding, vendor setup, and purchasing promotes consistent secure behavior.

AI Etiquette

Be careful what you put into AI, educate users on the risk of downloading AI tools. Reflect in acceptable use policies.

*Note that having documented policies, training, and a no-blame reporting culture is often cited positively in enforcement matters and can demonstrate that your program was reasonable and taken seriously by leadership.

90-Day Action Plan and Wrap-Up



Initial 30-Day Phase

Begin with enabling multi-factor authentication, confirming backups, and building a comprehensive asset list to secure the foundation.

Mid 31-60 Day Phase

Standardize devices, deploy endpoint protection, and document access processes to improve system consistency and security.

Final 61-90 Day Phase

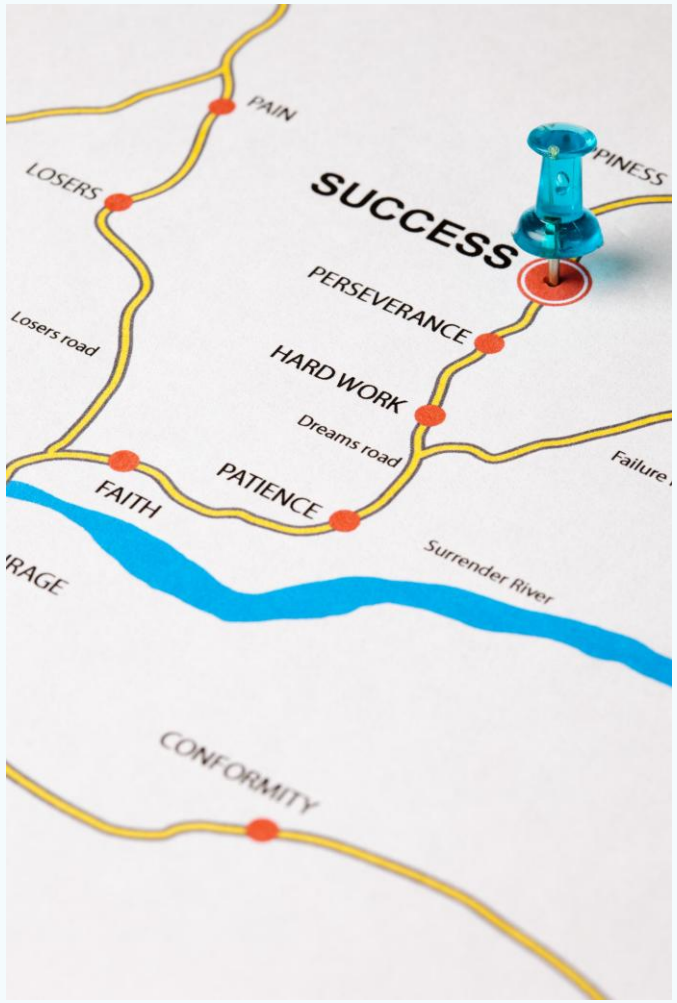
Finalize incident response playbook, review key vendors, and schedule ongoing cybersecurity training for preparedness.

Strategic Wrap-Up

Reinforce cybersecurity as a core business risk, not just an IT issue.

A small set of controls can reduce the risk of many common attacks.

Legal Takeaway: Three-Step Triage



1. Know your sector and customers

- Financial like activities? (lending, financial advice, tax preparation, servicing) – GLBA Safeguards Rule likely applies.
- Health-related services or vendor handling Personal Health Information (PHI) – HIPPA/HITECH applies.
- Services targeted at kids under 13, schools, or EdTech? – COPA and or FERPA applies.
- Publicly listed, or in heavily regulated critical infrastructure or defense supply chains? – SEC cyber rules, CIRCIA, DFARs/NIST, etc. applies.

2. Confirm baseline expectation regardless of sector

- Treat FTC Section 5 and basic data-security principles as always applicable.
- Implement Mike's controls as your "reasonable security" starter set.

3. Use your contracts as a forcing function

- Large enterprise customers will increasingly require evidence of controls (often mapped to NIST or other framework) and incident-response clarity, meeting those expectations also help demonstrate regulatory compliance.

References (any IT/Security changes should be made by a qualified professional to avoid outages)

- Cybersecurity budget: https://www.crowdstrike.com/en-us/cybersecurity-101/small-business/how-to-create-a-cybersecurity-budget/
- Free user phishing test: https://phishingquiz.withgoogle.com/
- https://www.phishingbox.com/phishing-test
- Cyber Readiness Playbook: https://cyberreadinessinstitute.org/resource/the-cyber-readiness-playbook/
- Ransomware protection Windows and Windows services https://support.microsoft.com/en-us/windows/protect-your-pc-from-ransomware-08ed68a7-939f-726c-7e84-a72ba92c01c3
- CIS Benchmarks: https://learn.cisecurity.org/benchmarks
- CMMC 2.0 Level 1 Practical Guide: https://omadaidentity.com/resources/blog/cmmc-2-0-practical-guide/
- AI policy Guidelines: https://www.thecorporategovernanceinstitute.com/insights/guides/creating-an-ai-policy/
- MFA Guidelines: https://cheatsheetseries.owasp.org/cheatsheets/Multifactor_Authentication_Cheat_Sheet.html (Advanced)
  - https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication (just starting out)
- What is Reasonable Data Security - https://www.theclm.org/Magazine/articles/what-is-reasonable-data-security-according-to-the-ftc/930
- Safeguards Rule notification requirements - https://www.ftc.gov/business-guidance/blog/2024/05/safeguards-rule-notification-requirement-now-effect
- A Legal Guide to Privacy and Data Security 2025 – https://www.lathropgpm.com/wp-content/uploads/2025/01/A-Legal-Guide-To-Privacy-and-Data-Security-2025-Final.pdf