# A Minimum Viable Security Program

Brian Myers

# Brian Myers PhD, CISSP, CCSK

SafetyLight LLC

Experience

- 20 years in software development
- 10 years in information security

Past Positions

- Director of InfoSec, WebMD Health Services
- Senior AppSec Architect, WorkBoard
- Senior Risk Advisor, Leviathan Security

Current Work

- Independent Information Security Consultant

Volunteer

- Western Oregon University CS Advisory Board
- OWASP AppSec Days PNW  (2021-2024)
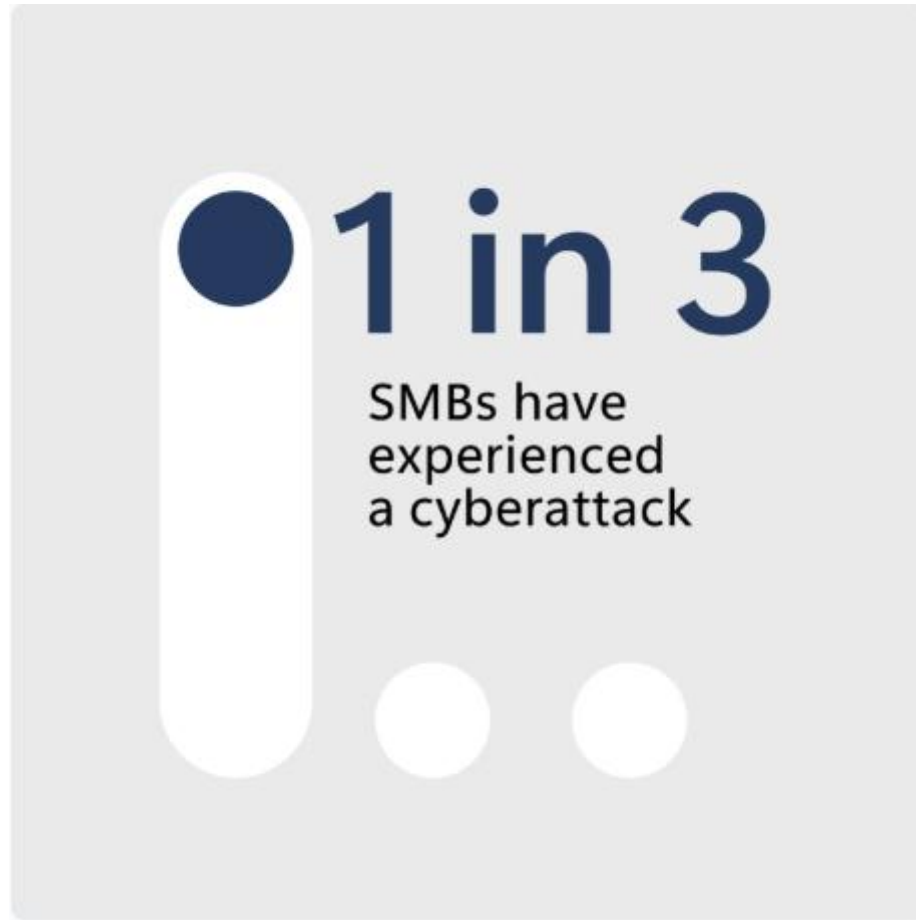
# Getting the Slides

safetylight.dev/talks

# Cyber Reality for Small Businesses

# SMB Cybersecurity Research Report (2024)



1 in 3 SMBs have experienced a cyberattack

Microsoft Security

# Real Incidents, Real Costs

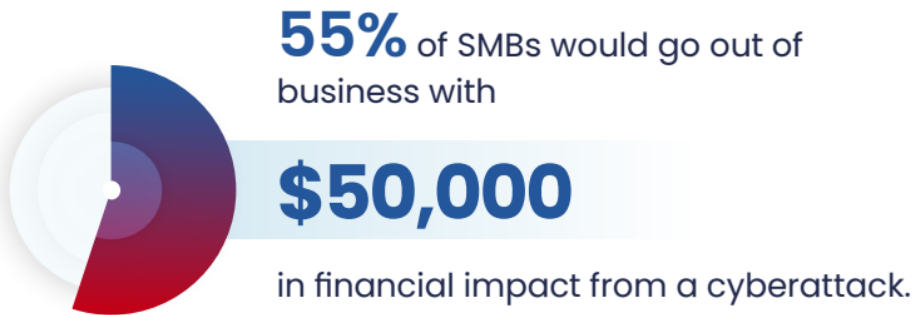| | |
|---|---|
| **Construction firm** | Ransomware found an open remote-desktop port. Every project file was lost. |
| **Dental clinic** | An employee clicked a phishing email. Patient data leaked. Weeks of rebuilding trust. |
| **Retailer** | An email looked like it came from the owner. Three months of salaries gone. |
| **Law Firm** | No one applied Microsoft's Exchange patch. Data on 100,000 patients stolen. Legal fines: $200,000. |
| **Property management** | Laptop stolen from employee car. Data on 620 residents exposed. $15,000 in fines. Ordered to comply with its own written security program. |

# Average and high end of cyberattack costs:

|  | Average costs | High end of costs |
|---|---|---|
| Investigation and recovery | $77,957 | $3,930,000 |
| Fines | $20,623 | $655,000 |
| Cost to reputation | $73,393 | $1,310,000 |
| Missed opportunities | $23,806 | $6,550,000 |
| Other costs | $58,666 | $3,275,000 |

Microsoft Security

SMBs have to run a tight ship on tight margins. It's no surprise that VikingCloud data shows **a successful cyberattack could put nearly**

## 1 in 5 SMBs out of business.

**The ramifications of an SMB cyberattack can be crippling:**

**55%** of SMBs would go out of business with

**$50,000**

in financial impact from a cyberattack.

For **32%,** it would take less than

**$10,000**

or less than a day of downtime.

**VIKING**CLOUD®

**VikingCloud's 2025 SMB Threat Landscape Report**

# What Guidance do SMBs Get?

# SOC 2 or ISO 27001

| Effort Dimension | Typical Range |
|---|---|
| Total time for first audit | 3-12 months |
| Cost of first audit | $15,000 - $60,000 |
| Annual staff hours | Hundreds of hours |
| Annual audit | $8,000 - $40,000 |

# Standards and Guidelines for SMBs

| Australia | Essential Eight |
|-----------|-----------------|
| Canada | Baseline Cyber Security Controls for Small and Medium Organizations |
| CIS | Critical Security Controls: Implementation Group 1 (IG1) |
| CISA | Cyber Essentials |
| ENISA | 12 Steps to Securing Your Business |
| FTC | Cybersecurity for Small Business |
| Mastercard | Small Business Cybersecurity "Quick Wins" |
| NCSC (UK) | Cyber Essentials |
| NIST | Cybersecurity Framework (CSF) 2.0 Small Business Quick-Start Guide |

| Control Area | AU Essential 8 | Canada Baseline | CIS IG1 | CISA Cyber Essentials | ENISA | FTC Small Biz | Master-card | NIST CSF (SB Quick Start) | UK Cyber Essentials |
|---|---|---|---|---|---|---|---|---|---|
| Backups | Green | Green | Green | Green | Green | Green | Green | Green | Green |
| Endpoint protection | Green | Green | Green | Green | Green | Green | Green | Green | Green |
| Identity management & MFA | Green | Green | Green | Green | Green | Green | Green | Green | Green |
| Incident response | Green | Green | Green | Green | Green | Green | Green | Green | Green |
| Least privilege | Green | Green | Green | Green | Green | Green | Green | Green | Green |
| Logging & monitoring | Green | Green | Green | Green | Green | Green | Green | Green | Green |
| Network security | Green | Green | Green | Green | Green | Green | Green | Green | Green |
| Patch management | Green | Green | Green | Green | Green | Green | Green | Green | Green |
| Email/web filtering / anti-phish | Yellow | Green | Green | Green | Green | Green | Green | Green | Green |
| Encryption | Yellow | Green | Green | Green | Green | Green | Green | Green | Green |
| Policies & awareness training | Yellow | Green | Green | Green | Green | Green | Green | Green | Green |
| Secure config / hardening | Green | Green | Green | Yellow | Green | Green | Green | Green | Green |
| Secure remote access | Yellow | Green | Green | Green | Green | Green | Green | Green | Green |
| Asset inventory | Yellow | Green | Green | Green | Green | Green | Green | Green | Yellow |
| Business continuity & recovery | Yellow | Green | Green | Green | Green | Green | Green | Green | Yellow |
| Account lifecycle | Yellow | Green | Green | Green | Yellow | Green | Yellow | Green | Green |
| Mobile/BYOD | Yellow | Green | Green | Green | Green | Green | Yellow | Green | Yellow |
| Data classification | Yellow | Green | Green | Yellow | Green | Green | Yellow | Green | Yellow |
| Supply-chain risk mgmt | Red | Green | Green | Green | Green | Green | Yellow | Green | Yellow |

Unmanaged assets
Sensitive data exposure
Unowned security gaps
Unauthorized access
Malware infection
Network intrusion
Exploited vulnerabilities
Data loss
Slow incident response
Third-party breach
Business disruption
Human error
Undetected issues
Software flaws
Uncontrolled changes
Key compromise
Physical damage
System overload
Missing audit evidence
Access approval gaps
Privilege misuse
Excess data retention
Weak contracts
Poor system design
Regulatory failure
No performance metrics
Portable device leakage
Unmonitored code changes

## SMB Guidelines

## Risk Universe

| Maturity | Data Backup | Patch Management |
|---|---|---|
|  | • Make backups regularly. | • Apply vendor patches ad hoc. |
|  | • Keep backups offsite.<br>• Test ability to restore. | • Set a patching cadence.<br>• Expedite critical patches. |
|  | • Document RPO/RTO.<br>• Run restore drills often. | • Automate scanning.<br>• Report on patch status. |

- Security starter kit
- Substantial risk reduction
- Digestible by a small org
- Foundation for growth

- Not a fully mature state

# Defining a Minimum Viable Security Program
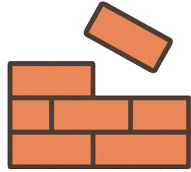
# MVSP Main Points

- Create asset inventories
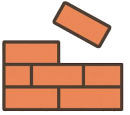
- Centralize identities
- Require MFA
- Grant minimum permissions
- Protect user devices
- Filter spam
- Secure network access
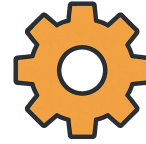
- Back up data
- Retain system logs
- Plan for incidents
- Assess vendors
- Train staff

- Write a working agreement
- Review risks periodically

# Foundation: Assets and Classification

- Create inventories of all:
  - hardware assets
  - software assets
  - data assets

- Create a data classification scheme
  - Include rules for handling data in each classification
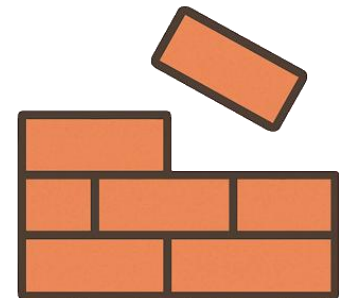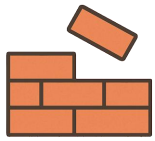
# *Create asset inventories*

| Asset Type | Owner | Data Sensitivity | Serial # or ID | Lifecycle | Vendor/Provider | Notes |
|---|---|---|---|---|---|---|
| Hardware | IT Manager | Confidential | SN-LAP101 | Active | Dell | Encrypted, under warranty until 2026 |
| Hardware | IT Manager | Internal | SN-LAP102 | Active | Apple | Encrypted, auto-updates enabled |
| Hardware | IT Manager | Internal | SN-LAP103 | Retired | HP | Awaiting disposal |
| Software | Ops Manager | Confidential | - | Active | Google | Covers email, docs, storage |
| Software | Ops Manager | Internal | - | Active | Slack Technologies | Collaboration and messaging |
| Software | Finance Lead | Confidential | - | Active | Intuit | Accounting and payroll |
| Data | CTO | Restricted | - | Active | Salesforce | Holds customer accounts and contracts |
| Data | HR Lead | Restricted | - | Active | Workday | Personnel files, benefits |
| Data | Marketing Director | Confidential | - | Active | HubSpot | Collected leads |
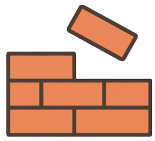
# Create a data classification scheme

| Classification | Description | Examples | Access |
|---|---|---|---|
| Public | Intended for people outside the company | Website, press releases… | Anyone |
| Internal | Routine business info not meant for public | Policies, internal emails… | All staff |
| Confidential | Sensitive business information | Contracts, personnel reviews… | Authorized staff |
| Restricted | Regulated data or security secrets | PII, encryption keys… | Execs or sysadmins only |

# Safeguards: Identity and Access

## IDENTITY AND ACCESS

- Require passwords be unique, strong, and not shared.
- Manage all staff identities in one place.
- Configure everything you can to use SSO.
- Require MFA.
- Assign users minimum necessary permissions.

# Safeguards

## USER DEVICES

- Ensure all user devices:
  - Require login
  - Use the primary identity provider
  - Are configured securely
  - Have anti-virus protection
  - Get updates regularly

- Configure company email provider to filter spam

## INFRASTRUCTURE

- Ensure company-managed networks:
  - Are securely configured
  - Are protected by a firewall
  - Require a secure connection for remote access
  - Require encryption for any supported Wi-Fi

# Resources for Safeguards

| Topic | Resource | Source |
|---|---|---|
| SSO | How to Implement Single Sign-On<br>Office 365; Google Workspace | Security Senses<br>Microsoft; Google |
| MFA | Multi-factor Authentication for Your Corporate Online Services<br>Implementing Phishing-Resistant MFA | NCSC<br>CISA |
| Passwords | Password Administration for System Owners<br>Password Policy Recommendations for Microsoft 365 | NCSC<br>Microsoft |
| User devices | Device Security Guidance | NCSC |
| Network | Network Architectures<br>Modern Approaches to Network Access Security | NCSC<br>CISA |
| Remote Work | Home Working: Preparing Your Organization<br>Bring Your Own Device (BYOD) | NCSC<br>NCSC |
| Wi-Fi | Securing Wireless Networks | CISA |

# Operations: Resilience; Supply Chain

- Back up critical data.
- Configure systems to keep system event logs.
- Make plans for:
    - Recovering from disruptions.
    - Responding to security incidents.
- Evaluate vendors/partners.
- Make sure staff know their security responsibilities.
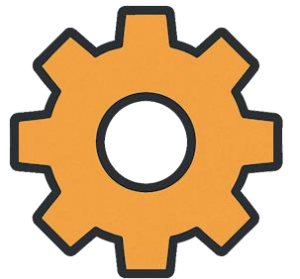
# Resources for Operations
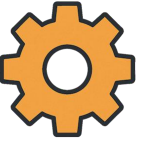
| Topic | Resource | Source |
|---|---|---|
| Logging & Monitoring | <ul><li>Logging and Protective Monitoring</li><li>Best Practices for Event Logging and Threat Detection</li></ul> | NCSC (UK) ASD (AU) |
| Vendor Assessment | <ul><li>CAIQ-Lite (Consensus Assessment Initiative Questionnaire)</li><li>Information and Communications Technology Supply Chain Risk Management Template for SMBs  [*spreadsheet*]</li></ul> | CSA<br><br>CISA |
| Training | <ul><li>Top Tips for Staff</li><li>Hook Minute (phishing test)</li></ul> | NCSC (UK) Hook Security |

- Risk Assessment
- Response and Recovery
  1. Determine Severity
  2. Assemble Response Team
  3. Assess and Prioritize
  4. Stabilize
  5. Communicate
  6. Recover
  7. Close Out
- Procedures
- Appendix A: Contact Info
- Appendix B: Resources

# Questions to Address in the BC/DR Plan

- If something goes wrong, who decides what to do first?
- Which systems are business critical?
- How will we take payments if the eCommerce vendor is down?
- How will we communicate if email and chat are out?
- What steps do we follow to restore backups?
- Who is authorized to talk to customers about outages?

- # What is an Incident?
- # Response Process
  1. Preparation
  2. Detection
  3. Containment
  4. Eradication
  5. Recovery
  6. Close Out

# Questions to Address in the IR Plan

- If something goes wrong, who's in charge?
- If we see malware, how do we keep it from spreading?
- Who decides if it's OK to shut down our systems?
- How do I contact legal / insurance / key vendors?
- Do we tell customers about this? When?
- Who is authorized to talk to media or law enforcement?
- What evidence do we need to preserve and how?

# SCRM Template for SMBs

*Supply Chain Risk Management from CISA*

| Use Case | Question Sets |
|---|---|
| Access Controls | • Acquirer/Supplier/Integrator |
| Cloud Hosted Solution | • Acquirer |
| | • Integrator |
| Vetting MSPs | • Acquirer |

| AI Use & Disclosure | 1.1 Do you currently use AI or machine learning in your product or service, or do you have plans to use it? |
| | 1.2 Do you notify customers before introducing or changing AI features? |
| | 1.3 Can customers opt out of AI-assisted processing involving their data or content? |
| | |
| Data Use & Protection | 2.1 Does any of your AI processing involve our data? If yes, describe the purpose and safeguards. |
| | 2.2 Is customer data ever used to train, fine-tune, or improve AI models? |
| | 2.3 Are AI features isolated from sensitive or regulated data (e.g., PII, PHI, payment info)? |
| | |
| Third-Party and Supply Chain | 3.1 Do you use any third-party AI services within in your product? If yes, identify them and your contractual relationship (e.g., API use, business license, enterprise contract). |
| | 3.2 Do you assess and monitor those third-party AI providers for security and compliance? If so, how? |
| | |
| Governance & Oversight | 4.1 Is someone responsible for approving AI adoption and ensuring compliance with security and privacy obligations? |
| | 4/2 Do you have documented policies for evaluating and managing AI risk? |
| | |
| Reliability & Transparency | 5.1 Do you monitor and secure AI components against threats (e.g., data leakage, prompt injection, model vulnerabilities)? |
| | 5.2 Do you maintain documentation or logs of AI-driven decisions or outputs affecting customer data or services? |
| | 5.3 Do you have processes to detect, correct, and communicate AI errors, bias, or unintended behavior? |

# Operations: Governance

- Write down the security rules and choices the company has made.

- Keep a list of security risks and go over it with leadership periodically.
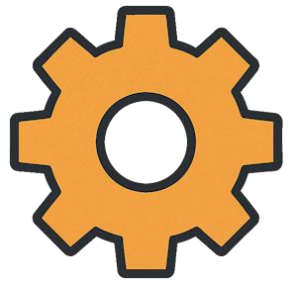
- Foundation
  - Assets
  - Classifications
- Safeguards
  - Identity and Access
  - User Devices
  - Infrastructure
- Operations
  - Resilience
  - Supply Chain
  - Governance

## Security Working Agreement

*Last updated: Oct 8, 2025*

This document establishes the security practices [Company] has adopted to protect data, systems, and services. It provides a single reference for the rules we follow and the responsibilities we have agreed on.

### Foundation

These foundational measures establish what must be protected.

#### Assets

- The IT team shall maintain an inventory of all hardware and software assets.
- The Security Officer shall maintain an inventory of the company's sensitive data assets.

#### Classifications

- The Security Officer shall create a data classification scheme defining categories of sensitivity and handling requirements for company data.

### Safeguards

These safeguards protect [Company]'s assets.

#### Identity and Access

- All persons with access to sensitive company systems shall authenticate through the same central identity provider (e.g. Active Directory, Google Workspace).
- Passwords must be unique and strong, and they must not be shared.
- Where practical, systems and services shall be configured to authenticate using single sign-on (SSO) from the central identity provider.
- Multi-factor authentication (MFA) shall be required for all sensitive company systems, including the central identity provider.
- Personnel shall be granted the minimum permissions required to perform their jobs.
- User access shall be revoked promptly when staff change roles or leave.

#### User Devices

- The IT department shall ensure that user devices with access to company systems:
  - Require authentication for use of the device.
  - Authenticate through the company's primary identity provider.
  - Are configured with security protections, including full-disk encryption.
  - Run defensive software (AV/EDR) to mitigate malware risks.
  - Stay current with security updates, using automatic updates where supported.
  - Are approved by IT before use. Personal devices may be approved only if they meet these same requirements.

#### Infrastructure

- The IT department shall ensure:
  - Company networks are securely configured and protected by a firewall.
  - Company Wi-Fi requires authentication using WPA2 or stronger.
  - All traffic to company systems is encrypted in transit (e.g., HTTPS or TLS).
  - Sensitive information is encrypted at rest.
  - Remote access uses secure methods (e.g., VPN or ZTNA) with MFA.
  - Company email is protected by spam and phishing filtering.

### Operations

These measures ensure resilience and reliability.

#### Resilience

- The IT department shall ensure:
  - Critical business information is backed up securely and off site.
  - Critical systems generate and retain logs of security-related events.
  - System logs are reviewed regularly for signs of security issues.
- Sensitive company information shall not be shared with AI tools or services without prior approval from the Security Officer.
- The Security Officer shall maintain and test plans for restoring disrupted services.
- The Security Officer shall maintain and test plans for responding to security incidents.

#### Supply Chain

- Vendors shall be assessed for security and reliability before use.
- Vendors shall be reassessed when their contracts renew or their services change.

#### Governance

- Executive leadership shall appoint a Security Officer to oversee security.
- The Security Officer shall:
  - Maintain this working agreement to share with staff.
  - Ensure employees receive security awareness training.
  - Ensure staff understand their security responsibilities.
  - Promote a constructive security culture.
  - Maintain a list of security risks and review it with leadership periodically.

https://safetylight.dev/talks

# Security Working Agreement

*Last updated: Oct 8, 2025*

This document establishes the security practices [Company] has adopted to protect data, systems, and services. It provides a single reference for the rules we follow and the responsibilities we have agreed on.

## Foundation

These foundational measures establish what must be protected.

### Assets

- The IT team shall maintain an inventory of all hardware and software assets.
- The Security Officer shall maintain an inventory of the company's sensitive data assets.

### Classifications

- The Security Officer shall create a data classification scheme defining categories of sensitivity and handling requirements for company data.

# Prioritizing Risks

| Risk | Description | Likelihood | Severity | Risk Level | Possible Mitigations |
|------|-------------|------------|----------|------------|----------------------|
| Patch & Update Gaps | Failure to apply operating system, application, or device patches in a timely manner. | High | Very High | 20 | * Enable automatic updates where possible<br>* Schedule patch cyclestrack and verify patch status |
| Shadow IT | Employees adopt unapproved SaaS tools (file-sharing, GenAI, productivity apps) outside official controls. | High | High | 16 | * Educate staff<br>* Publish list of approved tools<br>* Use SSO to limit access to sanctioned apps |
| Business Email Compromise | Attackers impersonate executives or vendors via email to trick staff into transferring money or sensitive data. | Moderate | Very High | 15 | * Train staff on BEC<br>* Implement payment verification procedures<br>* Enable email authentication (DMARC, SPF, DKIM) |
| Compromised customer credentials | Attacker acquires credentials to a customer account in our product (phishing, social engineering...) | Low | Very High | 10 | * Require password hygiene in policies<br>* Train staff on password hygiene<br>* Encourage or require use of a password manager<br>* Ensure customer requires MFA for access |

# Prioritizing Risks

Shadow IT

Weak Authentication

Patch & Update Gaps

Over-Privileged SaaS Integrations

Natural Disaster

Inadequate Security Expertise

Unverified Backups & Recovery

Business Email Compromise

Regulatory compliance drift

Remote work security gaps

Compromised network connection

Privilege creep

Untrained staff

…

| Risk ID | Category | Risk | Description | Potential Impact | Likelihood | Severity | Risk Level | Possible Mitigations |
|---|---|---|---|---|---|---|---|---|
| RSK-039 | Cloud & SaaS | Shadow IT | Employees adopt unapproved SaaS tools (file-sharing, GenAI, productivity apps) outside official controls. | * Data stored in uncontrolled locations * Compliance violations * Increased attack surface | High | High | 16 | * Educate staff * Publish list of approved tools * Use SSO to limit access to sanctioned apps |
| RSK-038 | Identity & Access | Weak Authentication | Lack of multi-factor authentication (MFA) or inconsistent enforcement across systems. | * Account compromise * Unauthorized access to sensitive systems * Business disruption | High | Very High | 20 | * Enforce MFA on all business accounts * Disable legacy authentication * Monitor for non-compliant accounts. |
| RSK-037 | Operations & Resilience | Patch & Update Gaps | Failure to apply operating system, application, or device patches in a timely manner. | * Exploitation of known vulnerabilities * Malware/ransomware infection * Regulatory or contractual noncompliance | High | Very High | 20 | * Enable automatic updates where possible * Schedule patch cycles/track and verify patch status |
| RSK-036 | Cloud & SaaS | Over-Privileged SaaS Integrations | Third-party SaaS integrations (e.g., CRM add-ons, automation tools) granted excessive permissions. | * Data exfiltration if integration is compromised * Lateral movement into core systems | Moderate | High | 12 | * Review app permissions before approval * Use least-privilege access * Audit integrations regularly |
| RSK-035 | Physical & Environmental | Natural Disaster | An earthquake or storm could damage the AWS zone where all our servers and data are hosted. | * Loss of AWS resources--servers, backups, buckets, etc. * Loss of data * Business operations halted | Low | High | 8 | * Purchase AWS resources in an alternate zone for backup and redundancy * Use physical media to store backups somewhere secure |
| RSK-034 | Operations & Resilience | Monitoring & Logging Gaps | Lack of central logging or monitoring makes security incidents go undetected. | * Extended attacker dwell time * Larger breaches before discovery * Increased regulatory/insurance exposure | Moderate | High | 12 | * Enable logging on critical systems * Use centralized log collection * Review alerts regularly |
| RSK-033 | Human Factors | Inadequate Security Expertise | Organization lacks in-house security knowledge to assess risks, configure controls, or evaluate vendors effectively. | * Misconfigured systems and controls * Inability to detect/respond to incidents * Poor vendor or contract decisions * Elevated residual risk across all areas | Moderate | High | 12 | * Engage external advisors or MSPs * Provide role-appropriate training * Adopt lightweight frameworks for structure |
| RSK-032 | Human Factors | Email & Collaboration Tool Misuse | Sensitive data shared insecurely via email, chat, or file-sharing platforms without safeguards. | * Accidental data exposure * Loss of customer trust * Regulatory fines | Moderate | High | 12 | * Provide secure file-sharing alternatives * Train staff on safe use of collaboration tools * Monitor outbound sharing |
| RSK-031 | Operations & Resilience | Unverified Backups & Recovery | Backups exist but are not regularly tested or isolated. Recovery after ransomware or outage may fail. | * Extended downtime * Permanent data loss * Business disruption | Moderate | Very High | 15 | * Test backups regularly * Keep offline/immutable copies * Include recovery in continuity planning |
| RSK-030 | Data Management | Poor Data Retention & Shadow Data | Sensitive data retained longer than necessary or stored in uncontrolled locations (personal devices, unapproved apps). | * Regulatory fines * Increased breach impact * Harder to secure and manage | Moderate | High | 12 | Define retention rules * Regularly clean up old data * Educate staff to avoid unapproved storage. |
| RSK-029 | Fraud | Business Email Compromise | Attackers impersonate executives or vendors via email to trick staff into transferring money or sensitive data. | * Financial loss * Legal liability * Customer/vendor relationship damage | Moderate | Very High | 15 | * Train staff on BEC * Implement payment verification procedures * Enable email authentication (DMARC, SPF, DKIM) |
| RSK-028 | Operations & Resilience | Pandemic/Disaster | A pandemic or natural disaster could make unavailable portions of our staff (or vendor/partner staff.) | * Reduced productivity * Customer service delays * Supply chain disruptions | Low | Low | 4 | * Document key tasks and train backup personnel |
| RSK-027 | Regulations | Regulatory compliance drift | New regulations, or changes to existing regulations such as GDPR, could affect <company> | * Compliance failure * Chance of increased regulatory fines * Increased compliance cost * Loss of customer trust | Moderate | Low | 6 | * Subscribe to regulatory update services * Engage with industry associations and compliance communities * Arrange compliance reviews with external experts * Establish relationships with specialized healthcare attorneys |
| RSK-026 | Human Factors | Remote work security gaps | Home network vulnerabilities, family members accessing work devices, unsecured video calls discussing sensitive matters. | * Data exposure from accessible - internal systems - cloud platform | Moderate | High | 12 | * Train users on safe home usage * Systematically audit laptops for evidence of shared usage. * Require dedicated workspaces with physical controls * Inspect home office environments for suitability (could be done by webcam.) * Create home office security checklists and require periodic self-assessment |
| RSK-025 | Endpoints & Devices | Compromised network connection | Data transmitted could be intercepted if not properly encrypted. | * Data exposure from accessible - internal systems - cloud platform | Moderate | High | 12 | * Train users to consider reliability of unknown wifi providers. * Train users to manage home routers safely. * Require VPN for connecting to secure systems. * Provide staff with company-issued phones that provide hotspots. * Use encrypted protocols such as HTTPS for all connections |
| RSK-024 | Identity & Access | Privilege creep | A staff member may be granted access permissions over time and, particularly when changing roles, gradually accumulate more privileges than needed for the current role. | * Increased exposure if the privilege user's credentials are hacked * Increased potential for more damaging insider attack | High | Moderate | 12 | * Establish standard workflow(s) with approval(s) for granting access privileges to anyone * When users change roles, always review existing privileges to see what can be removed. (RBAC facilitates this: delete all existing access privileges and then assign those RBAC roles associated with the user's new position. |
| RSK-023 | Identity & Access | Unapproved access | A staff member may be granted new access permissions without a legitimate business need, violating the principle of least privilege. | * Increased exposure if the privilege user's credentials are hacked * Increased potential for more damaging insider attack | Moderate | Moderate | 9 | * Establish standard workflow(s) with approval(s) for granting access privileges to anyone * Ensure that no request is granted without adequate confirmation that it meets a legitimate business need. * Ensure that all access requests and grants are logged immutably. |
| RSK-022 | Human Factors | Untrained staff | A staff member who has not received company training but has been granted access to sensitive data may handle the data improperly, inadvertently creating a security incident. | * Data exposure from accessible - internal systems - cloud platform - customer systems (ePHI) * Compliance failure * Increased legal and regulatory liability | Moderate | Moderate | 9 | * Establish standard workflow(s) with approval(s) for granting access privileges to anyone * Confirm that training has been delivered and acknowledged before approving any request for access to sensitive systems. |

# Resources for Risk Assessment

| Resource | Source |
|---|---|
| Minimum Viable Risk Management Program | Rachael Lininger |
| Binary Risk Analysis [readme] [app] | Ben Sapiro |
| FAIR: A Framework for Revolutionizing Your Risk Analysis | CIS |

# What Have We Accomplished?

# The Story for Customers

- Critical assets are inventoried, protected, and backed up.
- Access is managed centrally with strong authentication.
- Devices are secured and kept up to date.
- Vendors are reviewed for reliability and security.
- Incident and recovery plans are in place.
- Risks are reviewed regularly.
- The company is ready to meet higher assurance standards as it grows.

brian@safetylight.dev

linkedin.com/in/bgmyers/

https://safetylight.dev/talks