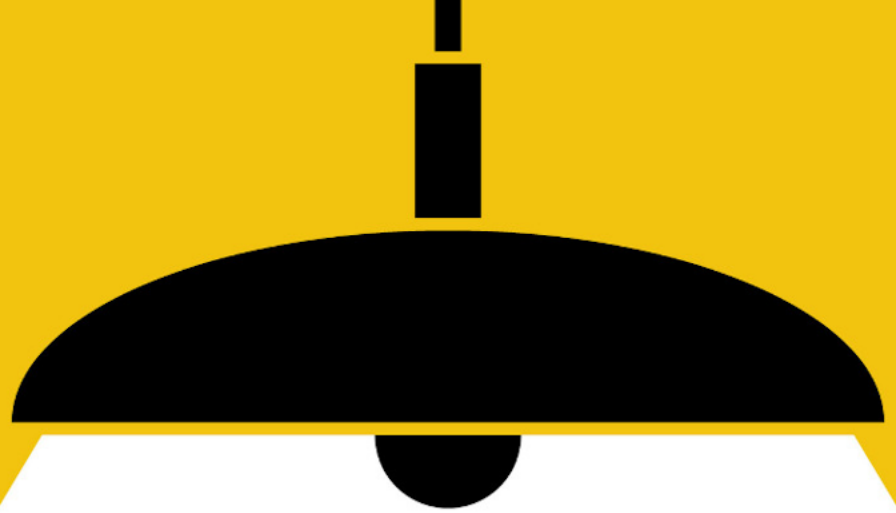


A Minimum Viable Security Program

Brian Myers

Brian Myers PhD, CISSP, CCSK

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

SMB: Small or Medium Business

Source	Definition (employee count)
Boston Fed	1-500
Cisco	250-499
McKinsey	1-999
Microsoft	25-299
Salesforce	1-200
Verizon	1-999

Cyber Reality for Small Businesses

CNBC Small Business Survey

August 2021

- 56% not concerned about an attack this year
- 59% confident they could quickly recover
- 28% have an incident response plan
- 26% carry cyber insurance

SMB Cybersecurity Research Report (2024)

Microsoft Security

VIKINGCLOUD®

VikingCloud's 2025 SMB Threat Landscape Report

In the past year alone, VikingCloud research revealed:

24%

Of SMBs were hit with malware.

19%

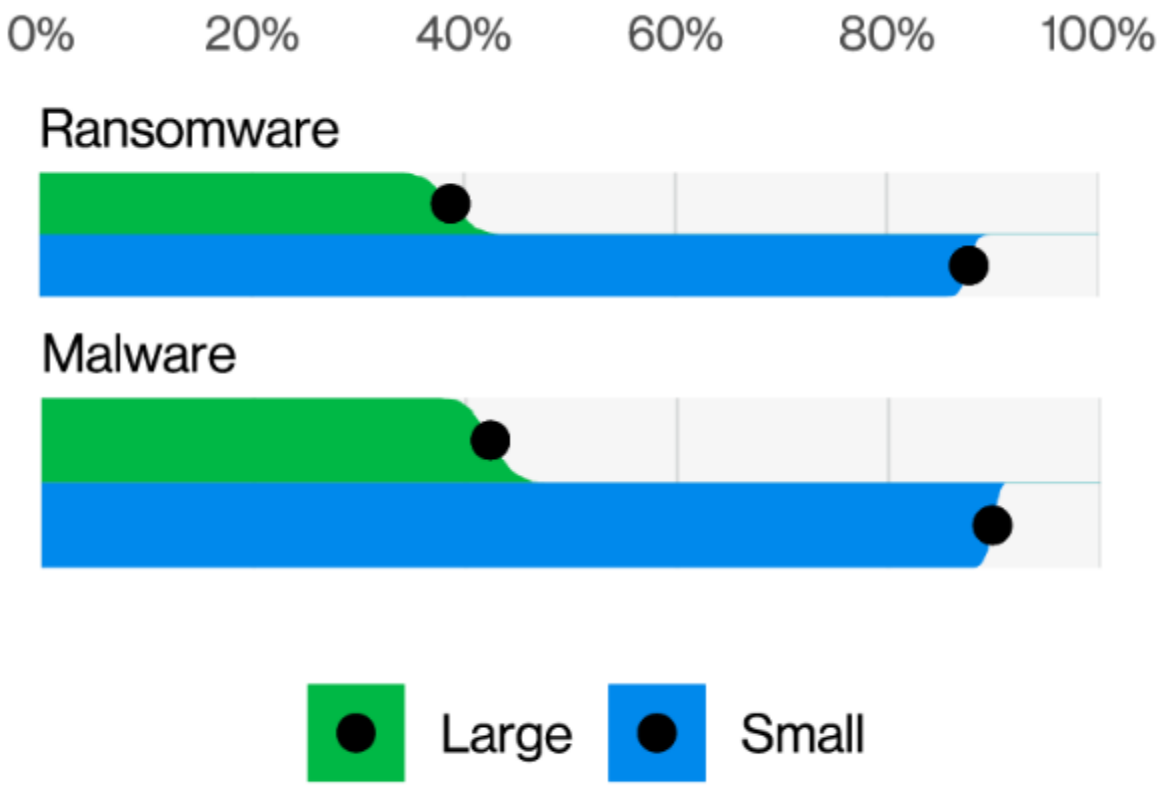
Faced a denial-of-service attack.

19%

Faced a deepfake scheme trying to access sensitive business accounts.

14%

Experienced a ransomware attack.



verizon business 2025

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.

mastercard

VIKINGCLOUD®

VikingCloud's 2025 SMB Threat Landscape Report

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.

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									
Endpoint protection									
Identity management & MFA									
Incident response									
Least privilege									
Logging & monitoring									
Network security									
Patch management									
Email/web filtering / anti-phish									
Encryption									
Policies & awareness training									
Secure config / hardening									
Secure remote access									
Asset inventory									
Business continuity & recovery									
Account lifecycle									
Mobile/BYOD									
Data classification									
Supply-chain risk mgmt									

Missing from the SMB Guidelines

Personnel	Screening, role training, remote work, sanctions, offboarding, culture…
Physical & Environmental	Secure areas, equipment and media disposal, environmental controls…
Supplier & Third-Party	Contract clauses, monitoring, supplier incident requirements…
System Development	Secure coding, SDLC, test data, encryption, development environments…
Technical Operations	Change management, capacity planning, clock sync, log analysis…
Information Transfer	Secure file sharing, confidentiality agreements, records management…
Compliance	Legal/regulatory requirements, privacy obligations, compliance audits
Management & Strategy	Org-wise risk strategy, capital planning, continuous monitoring, metrics…
AI Governance	Internal AI use; vendor AI drift; AI use transparency; licensing…

An Effort to Help

MVSP = Interim Risk Reduction

- Reduce exposure to the biggest security risks
- Establish a simple, sustainable security management process

Criteria for Brian's MVSP

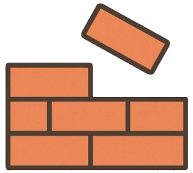
A "minimal" security program should include controls that are:

- Needed by most companies
- Directly address common threats
- Give good value for the cost
- Foundational for other best practices

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

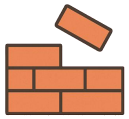
- Security starter kit
- Substantial risk reduction
- Digestible by a small org
- Foundation for growth

- Not a certification
- Not auditable
- Not a good final state



FOUNDATION	• Assets • Classifications
SAFEGUARDS	• Identity • User Devices • Infrastructure
OPERATIONS	• Resilience • Supply Chain • Governance

MVSP Main Points



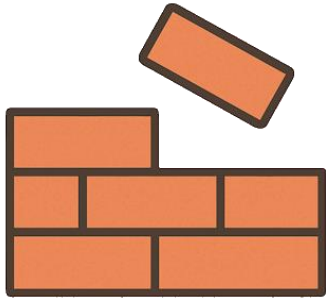
- Create asset inventories

- 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
- Assign a security leader
- Write a working agreement
- Train staff
- 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; purge unsubscribed entries

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

- 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

Safeguards: Infrastructure

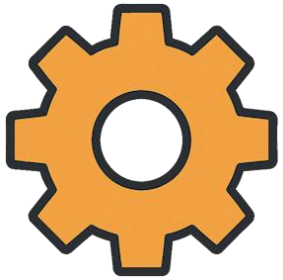
- Configure company email provider to filter spam
- Ensure company-managed networks:
  - Are securely configured
  - Are protected by a firewall
  - Require a secure connection for remote access
  - Require encryption for any supported Wi-Fi

Resources for Safeguards

Topic	Resource	Source
SSO	How to Implement Single Sign-On Office 356; Google Workspace	Security Senses Microsoft; Google
MFA	Multi-factor Authentication for Your Corporate Online Services Implementing Phishing-Resistant MFA	NCSC CISA
Passwords	Password Administration for System Owners Password Policy Recommendations for Microsoft 365	NCSC Microsoft
User devices	Device Security Guidance	NCSC
Network	Network Architectures Modern Approaches to Network Access Security	NCSC CISA
Remote Work	Home Working: Preparing Your Organization Bring Your Own Device (BYOD)	NCSC NCSC
Wi-Fi	Securing Wireless Networks	CISA

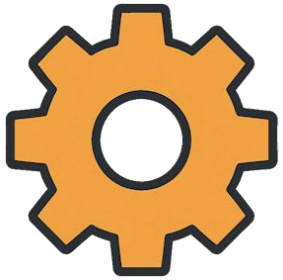
Operations: Resilience; Supply Chain

- Back up critical data.
- Configure systems to keep system event logs.
- Make plans for:
  - Recovering from disruptions.
  - Responding to security incidents.
- Evaluate vendors/partners.



Resources for Operations: Logging

Topic	Resource	Source
Logging & Monitoring	• Logging and Protective Monitoring • Best Practices for Event Logging and Threat Detection	NCSC (UK) ASD (AU)



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 communicate if email and chat are out?
- What steps do we follow to restore from a backup?
- Have we told customers our RPO/RTO goals?
- Who is authorized to talk to customers?

- 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

Business Continuity Plan

Last Reviewed: October 8, 2025

Purpose

This plan describes how MindPath will continue critical business functions and restore services after a disruption. The goals are to:

- Reduce downtime
- Meet customer expectations
- Protect the company's reputation

Roles

CTO	Owns this plan and oversees responses.
Disruption Response Team	Coordinates cross-team recovery efforts. The response team includes: • CTO • Lead Software Developer • IT Engineer • Customer Support Director
Executive team	Notified of significant disruptions and direct external communication (to customers, vendors, counsel…)
Employees	May be asked to help with response.

Risk Assessment

This section is about knowing what parts of our business we can't afford to lose, what might knock them out, and how fast we need them back. Writing them down helps clarify what must be restored first.

Critical Business Functions

- SaaS platform (Learning Management System) – product we sell
- Customer support and communications (email, helpdesk, status page)
- Development and deployment pipeline (GitHub, CI/CD, AWS environments)
- Financial functions (billing, payroll)

Possible Disruptions

- AWS service outage (regional or account-specific)
- Ransomware, malware, or data corruption
- Accidental deletion or misconfiguration
- Vendor outage (e.g., Transcribeo API down)
- Loss of Google Workspace access (email, identity, SSO)
- Office unavailability (natural disaster, power, connectivity)

Dependencies

- AWS (EC2, RDS, S3, IAM, CloudFront)
- Google Workspace (identity, email, Docs, Drive, Meet)
- Transcribeo API (video transcript integration, *service degradation if unavailable*)
- GitHub and CI/CD system (software delivery)
- Stripe (B2B invoicing and payments: ACH, credit card, reminders, reconciliation)

Recovery Objectives

- SaaS platform (LMS): Restore within **24 hours** (target RTO). Data loss should not exceed **4 hours** (RPO).
- Customer communications: Alternate method (status page, social media) within **2 hours** if Google Workspace (email) is unavailable.
- Development pipeline: Restore within **3 days** if lost.
- Financial functions: Restore within **5 days**.
- Customer SLA is 99.0%, but goal is **24/7 uptime with prompt notice of any outage**.

Alternate Work Location

- All staff can (and usually do) work from home.
- If the office is unavailable, business continues with laptops and cloud services.

Response & Recovery

This section is about responding to disruptions. It describes the process followed to assess severity, invoke a response team, and work through to a resolution while keeping stakeholders notified along the way.

1. Determine Disruption Severity

When disruptions are reported, the CTO determines the severity based on how many customers are affected, how long the issue is expected to last, and whether it risks breaching customer commitments.

Severity	Description	Examples	Required Actions
Minor	Small disruption with limited customer impact or lasting less than 1 hour.	Short delay in transcript delivery, small feature outage.	CTO directs a quick resolution without activating the plan.
Major	Disruption affecting many customers, or an outage expected to last more than 1 hour but not yet breaching SLA.	Partial LMS outage, Google Workspace email disruption.	CTO activates plan (proceed to steps below.)
Critical	Severe disruption breaching the SLA or preventing most customers from using the LMS.	Multi-hour SaaS outage, AWS regional failure.	CTO activates plan (proceed to steps below.)

2. Assemble the Disruption Response Team

The CTO notifies Response Team members and confirms the communication channel (Google Meet or phone).

If the event severity is not Minor, the CTO also notified executive staff who will direct external communication.

3. Assess & Prioritize

Development Lead and IT Engineer report on system status (AWS, Google, vendors).

Customer Support Director reports on customer-facing impact (tickets, complaints, accessibility issues).

Team compares situation against recovery objectives (RTO/RPO).

4. Stabilize

Development Lead begins recovery steps in AWS.

IT Engineer escalates to Google or other SaaS vendors as needed.

Customer Support Director drafts initial customer communication.

CTO assigns additional personnel if needed.

5. Communicate

Internal: CTO provides short updates to all staff so they know who is leading, current status, and how to handle customer inquiries.

External: Customer Support Director prepares draft updates; Executives approve before release. Updates may go to the status page, direct email, or social channels depending on impact.

Regular updates are shared until recovery is complete.

6. Recover & Monitor

Development Lead restores systems from backups or snapshots as required.

IT Engineer ensures internal tools (Google Workspace, identity, SSO) remain operational.

CTO monitors recovery progress and sets schedule for follow-up communication.

7. Close Out

CTO declares systems stable and operations restored.

Executives approve and release final customer update.

Response Team holds a short debrief to record what happened, what worked, and what needs improvement.

Procedures

The following procedures will assist in resolving some disruptions.

AWS
Restore from backups or snapshots using AWS Backup and RDS snapshots.

Google Workspace
Use Google Admin Console to reset accounts, revoke sessions, and restore access.

Transcribeo (Transcription Service)
If the Transcribeo API is down, video uploads are accepted but transcripts are delayed. If Transcribeo is down more than 48 hours, inform customers that transcripts will be delayed until the vendor recovers. No alternate vendor is currently in place. Executives will review whether to initiate an emergency vendor search.

Stripe (Billing Services)
If unavailable, invoices can be issued manually from Google Docs/Sheets and payments collected by bank transfer. Reconciliation with Stripe occurs once restored.

Appendix A: Personnel and Contact Info

Role	Name	Business Contact Info	Alternate Contact Info
Security Officer	Archie Tech	archie@mindpath.com	(503) 111-1111
Executive Leadership Team	Maxine Powers Archie Tech Mark Ketter Wynn Moore	max@mindpath.com archie@mindpath.com mark@mindpath.com wynn@mindpath.com	(503) 222-2222 (503) 333-3333 (503) 444-4444 (503) 555-5555
Customer Support Director	Will Fixit	will@mindpath.com	(503) 666-6666
IT Engineer	Grant X. Esse	grant@mindpath.com	(503) 777-7777
Lead Software Developer	Ruby Rails	ruby@mindpath.com	(503) 888-8888

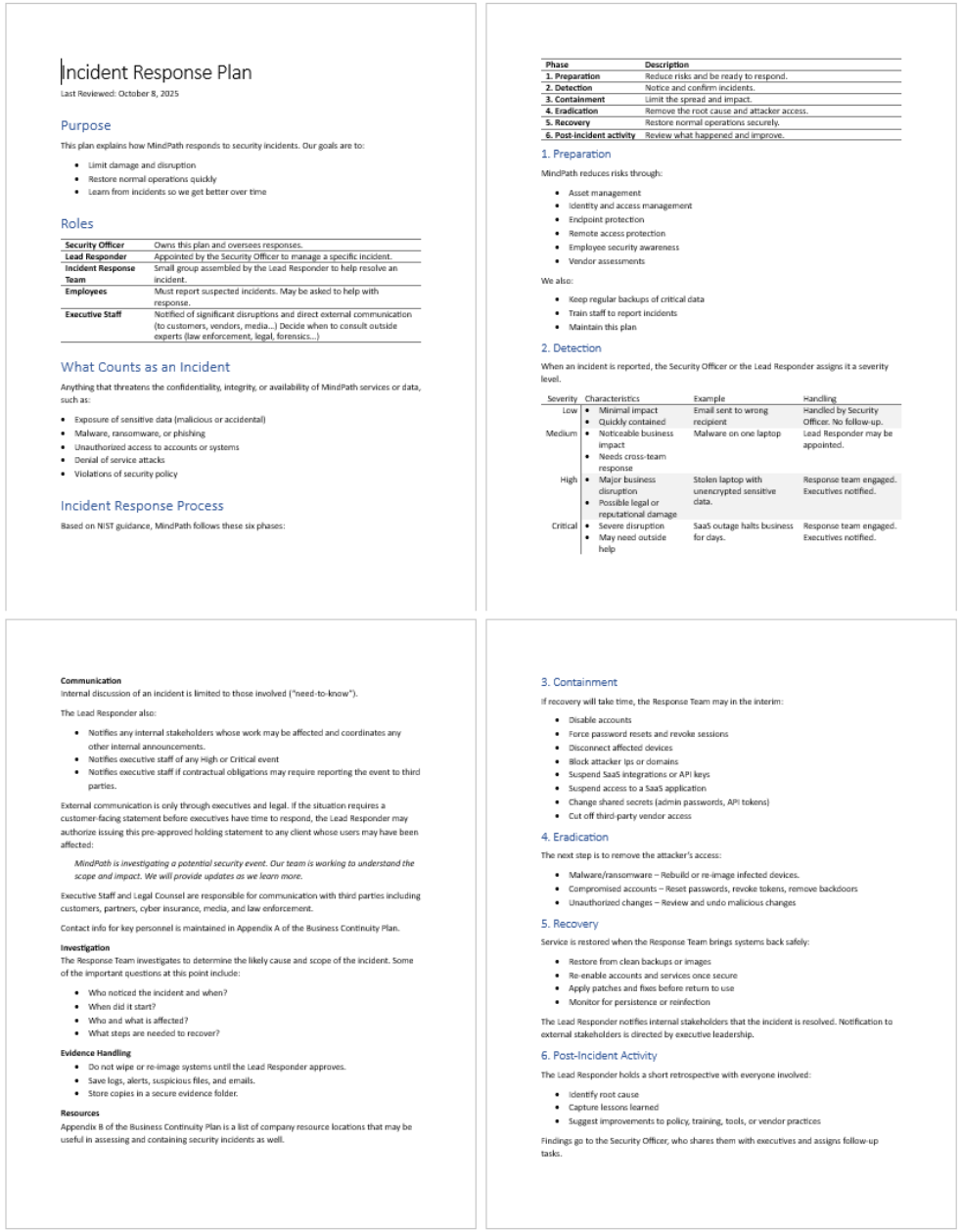
Appendix B: Response Resources

RESOURCE	URL / LOCATION	PURPOSE	OWNER
AWS CONSOLE	https://console.aws.amazon.com/	Access to AWS services (EC2, RDS, S3, IAM, Security Hub)	CTO / IT Engineer
AWS BACKUP	https://console.aws.amazon.com/backup/	Restore database and file snapshots	IT Engineer
AWS CLOUDTRAIL	https://console.aws.amazon.com/cloudtrail/	Review account activity logs	Security Officer
AWS GUARDDUTY	https://console.aws.amazon.com/guardduty/	Detect suspicious activity	Security Officer
AWS IAM	https://console.aws.amazon.com/iam/	Manage accounts, keys, MFA	CTO
GOOGLE ADMIN CONSOLE	https://admin.google.com/	Manage Workspace accounts, reset passwords, enforce SSO	IT Engineer
GOOGLE VAULT	https://vault.google.com/	Search Gmail/Drive content if needed	Security Officer
CONTRACT & POLICY FOLDER	Google Drive: /MindPath/Security/Contracts	Check for customer/vendor reporting requirements	CTO

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?

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



Incident Response Plan

Last Reviewed: October 8, 2025

Purpose

This plan explains how MindPath responds to security incidents. Our goals are to:

- Limit damage and disruption
- Restore normal operations quickly
- Learn from incidents so we get better over time

Roles

Security Officer	Owns this plan and oversees responses.
Lead Responder	Appointed by the Security Officer to manage a specific incident.
Incident Response Team	Small group assembled by the Lead Responder to help resolve an incident.
Employees	Must report suspected incidents. May be asked to help with response.
Executive Staff	Notified of significant disruptions and direct external communication (to customers, vendors, media…) Decide when to consult outside experts (law enforcement, legal, forensics…)

What Counts as an Incident

Anything that threatens the confidentiality, integrity, or availability of MindPath services or data, such as:

- Exposure of sensitive data (malicious or accidental)
- Malware, ransomware, or phishing
- Unauthorized access to accounts or systems
- Denial of service attacks
- Violations of security policy

Incident Response Process

Based on NIST guidance, MindPath follows these six phases:

Phase	Description
1. Preparation	Reduce risks and be ready to respond.
2. Detection	Notice and confirm incidents.
3. Containment	Limit the spread and impact.
4. Eradication	Remove the root cause and attacker access.
5. Recovery	Restore normal operations securely.
6. Post-incident activity	Review what happened and improve.

1. Preparation

MindPath reduces risks through:

- Asset management
- Identity and access management
- Endpoint protection
- Remote access protection
- Employee security awareness
- Vendor assessments

We also:

- Keep regular backups of critical data
- Train staff to report incidents
- Maintain this plan

2. Detection

When an incident is reported, the Security Officer or the Lead Responder assigns it a severity level.

Severity	Characteristics	Example	Handling
Low	• Minimal impact • Quickly contained	Email sent to wrong recipient	Handled by Security Officer. No follow-up.
Medium	• Noticeable business impact • Needs cross-team response	Malware on one laptop	Lead Responder may be appointed.
High	• Major business disruption • Possible legal or reputational damage	Stolen laptop with unencrypted sensitive data.	Response team engaged. Executives notified.
Critical	• Severe disruption • May need outside help	SaaS outage halts business for days.	Response team engaged. Executives notified.

Communication

Internal discussion of an incident is limited to those involved ("need-to-know").

The Lead Responder also:

- Notifies any internal stakeholders whose work may be affected and coordinates any other internal announcements.
- Notifies executive staff of any High or Critical event
- Notifies executive staff if contractual obligations may require reporting the event to third parties.

External communication is only through executives and legal. If the situation requires a customer-facing statement before executives have time to respond, the Lead Responder may authorize issuing this pre-approved holding statement to any client whose users may have been affected:

> *MindPath is investigating a potential security event. Our team is working to understand the scope and impact. We will provide updates as we learn more.*

Executive Staff and Legal Counsel are responsible for communication with third parties including customers, partners, cyber insurance, media, and law enforcement.

Contact info for key personnel is maintained in Appendix A of the Business Continuity Plan.

Investigation

The Response Team investigates to determine the likely cause and scope of the incident. Some of the important questions at this point include:

- Who noticed the incident and when?
- When did it start?
- Who and what is affected?
- What steps are needed to recover?

Evidence Handling

- Do not wipe or re-image systems until the Lead Responder approves.
- Save logs, alerts, suspicious files, and emails.
- Store copies in a secure evidence folder.

Resources

Appendix B of the Business Continuity Plan is a list of company resource locations that may be useful in assessing and containing security incidents as well.

3. Containment

If recovery will take time, the Response Team may in the interim:

- Disable accounts
- Force password resets and revoke sessions
- Disconnect affected devices
- Block attacker Ips or domains
- Suspend SaaS integrations or API keys
- Suspend access to a SaaS application
- Change shared secrets (admin passwords, API tokens)
- Cut off third-party vendor access

4. Eradication

The next step is to remove the attacker's access:

- Malware/ransomware – Rebuild or re-image infected devices.
- Compromised accounts – Reset passwords, revoke tokens, remove backdoors
- Unauthorized changes – Review and undo malicious changes

5. Recovery

Service is restored when the Response Team brings systems back safely:

- Restore from clean backups or images
- Re-enable accounts and services once secure
- Apply patches and fixes before return to use
- Monitor for persistence or reinfection

The Lead Responder notifies internal stakeholders that the incident is resolved. Notification to external stakeholders is directed by executive leadership.

6. Post-Incident Activity

The Lead Responder holds a short retrospective with everyone involved:

- Identify root cause
- Capture lessons learned
- Suggest improvements to policy, training, tools, or vendor practices

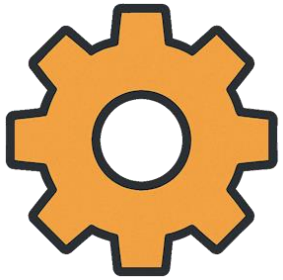
Findings go to the Security Officer, who shares them with executives and assigns follow-up tasks.

Questions to Ask Vendors

- Do they pay attention to security—or just say they do?
- How do they screen and train staff who will see your data?
- Do they vet their own vendors?
- If their system is breached, will they tell you?
- If their system goes down, how quickly will it come back?
- Does their AI train on your data?
- Can they prove any of this? Do you have to take their word?

Resources for Operations: Vendors

Topic	Resource	Source
Vendor Assessment	• CAIQ-Lite (Consensus Assessment Initiative Questionnaire)	CSA
Vendor Assessment	• Information and Communications Technology Supply Chain Risk…	CISA



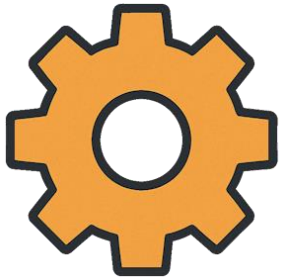
SCRM Template for SMBs

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

- Assign a leader to oversee company-wide security.
- Write down the security rules and choices the company has made.
- Make sure staff know their security responsibilities.
- Keep a list of security risks and go over it with leadership periodically.



Write down the security rules

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.

Write down the security rules

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

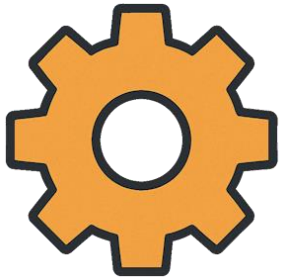
- Vendors shall be assessed for security and reliability before use.
- Vendors shall be reassessed when their contracts renew or their services change.

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.

Resources for Operations: Training

Topic	Resource	Source
Training	• Top Tips for Staff	NCSC (UK)



Tracking Risks

Risk	Description	Likelihood	Severity	Risk Level
Unmanaged AI Adoption	Well-meaning staff adopt AI tools without review and share data with them, introducing a new risk of data exposure along with others including AI hallucinations, data exposure, and loss of oversight.	High	Medium	High

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	Likelihooc	Severity	Risk Leve	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 cyclestrack 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.

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 * 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 * Publish list of approved tools * 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 * Implement payment verification procedures * 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 * Train staff on password hygiene * Encourage or require use of a password manager * Ensure customer requires MFA for access

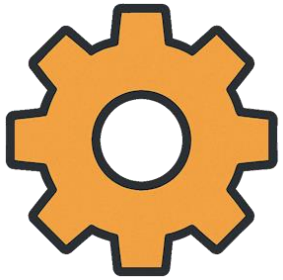
Rating Risks Consistently

Likelihood	Description	Practical Indicators
Very High	Expected to occur repeatedly (e.g., monthly or more). No controls or easy to exploit.	Happens frequently across the industry or internally. Example: automated login attacks, unpatched CVEs.
High	Likely to occur at least once per year. Common and credible threat.	Phishing, credential stuffing, minor misconfigurations.
Medium	Possible but not frequent. Could occur under	Insider mishandling, single-point supplier outage.
Low	Unlikely, but plausible under exceptional	Major ISP outage, targeted attack on a small firm.
Very Low	Extremely rare or hypothetical. Requires	Natural disasters, global pandemics.

Severity	Description	Observable Consequences
Very High	Severe, business-threatening loss or extended	Customer exodus, major data breach, executive/legal
High	Major disruption or loss, but survivable with	Days of downtime, serious data loss, regulator or
Medium	Noticeable impact requiring management action	Partial service outage, moderate financial loss, some
Low	Minor inconvenience with little or no customer	Brief downtime, small internal cost, no external
Very Low	Negligible impact, quickly reversible.	Momentary glitch, easily restored file.

Resources for Risk Assessment

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



The Story for Customers

- Critical assets are inventoried, protected, and backed up.
- Access is managed centrally with strong authentication.
- Devices are secured and updated.
- Vendors are reviewed for security and reliability.
- Incidents and recovery plans are in place.
- Risks are reviewed regularly.
- We’re ready to meet higher assurance standards as we grow.

brian@safetylight.dev

linkedin.com/in/bgmyers/

https://safetylight.dev/talks