Cybersecurity Risk Assessment

Organization: Kate's Insurance Inc.

Introduction

At its core, cybersecurity is all about identifying and managing risk. One of the most common mistakes made by small business owners is believing they are too small to be targeted by cyber threats. Kate's Insurance Inc., like most small insurance agencies, handles sensitive personal and financial information daily. This alone makes it an attractive target for cybercriminals, regardless of company size.

Kate's Insurance Inc. is a locally operated insurance brokerage with 12 employees, a small on-premises office, and a hybrid IT environment consisting of local workstations, a small file server, and several cloud-based applications. Because the insurance industry relies heavily on personally identifiable information (PII), payment data, and regulatory compliance, the potential impact of a cyber incident is significant.

This document outlines a first-time, organization-wide cybersecurity risk assessment for Kate's Insurance Inc. The purpose of this assessment is to identify, quantify, and prioritize cyber risks so appropriate security controls can be selected and implemented.

Key Risk Assessment Terms

Before conducting the assessment, the following terms are used throughout this document:

- **Risk:** The potential for a threat to exploit a vulnerability resulting in an impact on the organization
- **Threat:** An event that could jeopardize organizational assets
- **Vulnerability:** A weakness in an asset, system, or process
- **Exploit:** The method used to take advantage of a vulnerability
- **Payload:** What is executed after an exploit succeeds
- **Asset Value (AV):** The relative value of an asset to the organization
- **Probability:** The likelihood a threat will exploit a vulnerability
- **Impact:** The effect on the organization if the risk occurs
- **Control:** A process or safeguard used to reduce risk

The basic risk formula used is:

Risk = Probability × Impact

Risk Assessment Methodology

Kate's Insurance Inc. uses a **hybrid risk assessment approach**, combining both:

- **Quantitative analysis**, where financial estimates are possible
- **Qualitative analysis**, where expert judgment is required

This approach is appropriate for a small business that may not have complete historical incident data but still needs financially grounded decision-making.

Step 1: Determine Scope

This risk assessment covers the **entire technology environment** of Kate's Insurance Inc., including:

- Office network infrastructure
- Employee workstations and laptops
- On-premises file server
- Cloud-based insurance management software
- Email systems
- Customer data and internal business processes

All employees were notified in advance, and department heads were interviewed to ensure full visibility into daily operations and technology usage.

Step 2: Identify Assets

Key digital assets identified include:

- On-premises file server containing client policy documents
- Employee desktop and laptop computers
- Cloud-based insurance management platform
- Email system (Microsoft 365)
- Network firewall and Wi-Fi infrastructure
- Client PII (names, SSNs, addresses, policy numbers)
- Accounting and billing data

Step 3: Determine Asset Value (AV)

Asset values were estimated using purchase cost, replacement cost, and business impact:

Asset	Estimated AV
File Server (hardware + data)	$18,000
Cloud Insurance Platform Data	$25,000
Email System & Data	$12,000
Employee Workstations (12)	$24,000
Network Equipment	$6,000
Client PII (regulatory & reputational value)	$50,000

Step 4: Categorize Assets by Criticality

Assets were classified as follows:

- **Critical:** Client PII, file server data, insurance management platform
- **Major:** Email system, employee workstations
- **Minor:** Network peripherals, printers, non-sensitive applications

This process revealed that client data—rather than physical hardware—represents the highest business risk.

Step 5: Identify Threats & Vulnerabilities

Common Cyber Threats Facing Kate's Insurance Inc.

1. **Phishing Attacks**
    - Threat: Credential theft via deceptive emails
    - Vulnerability: Limited employee security training
    - Payload: Account takeover, data exfiltration
2. **Ransomware**
    - Threat: Malware encrypting internal systems
    - Vulnerability: Infrequent offline backups
    - Payload: Business disruption and ransom demand
3. **Unauthorized Access**
    - Threat: Stolen or weak passwords
    - Vulnerability: Lack of multi-factor authentication (MFA)
    - Payload: Data theft and fraud
4. **Insider Error**
    - Threat: Accidental data exposure
    - Vulnerability: No formal data handling policy
    - Payload: Compliance violations

5. **System Failure**
    - Threat: Hardware failure of file server
    - Vulnerability: Aging equipment
    - Payload: Data loss and downtime

Step 6: Quantify Risks (Example)

Example Risk: Ransomware Attack on File Server

- **Asset Value (AV):** $18,000
- **Exposure Factor (EF):** 0.5 (50% of data compromised)
- **Single Loss Expectancy (SLE):**
  $18,000 × 0.5 = **$9,000**
- **Annualized Rate of Occurrence (ARO):** 1.5
- **Annualized Loss Expectancy (ALE):**
  $9,000 × 1.5 = **$13,500**

This indicates ransomware is a high-priority risk.

Step 7: Assign Severity Levels

Kate's Insurance Inc. uses the following yardstick:

- **Low Risk:** <$1,000
- **Medium Risk:** $1,000–$5,000
- **High Risk:** >$5,000

Using this scale:

Risk	ALE	Severity
Ransomware	$13,500	High
Phishing	$6,000	High
Insider Error	$2,500	Medium
Hardware Failure	$1,200	Medium

Risk Matrix (Qualitative View)

Likelihood Scale: 1–5
Impact Scale: 1–5

- Ransomware: Likelihood 4, Impact 5
- Phishing: Likelihood 5, Impact 4
- Insider Error: Likelihood 3, Impact 3

These rankings reinforce the quantitative findings.

Step 8: Risk Register

All identified risks were documented in a risk register, including:

- Risk description
- Affected assets
- Severity
- Assigned owner
- Planned mitigation

The risk register is shared with management and IT stakeholders to guide remediation planning.

Step 9: Determine Appropriate Security Controls

Selected Risk Management Strategies

- **Risk Mitigation**
  - Implement MFA for email and cloud platforms
  - Deploy endpoint protection software
  - Conduct employee phishing awareness training
- **Risk Transference**
  - Purchase cyber insurance
  - Engage a managed IT security provider
- **Risk Acceptance**
  - Accept low-impact risks where mitigation cost exceeds benefit
- **Risk Avoidance**
  - Eliminate unnecessary local data storage where possible

Step 10: Monitor & Document Results

Security controls will be monitored continuously, with formal reassessments conducted:

- Annually
- After any cyber incident
- After major system or process changes

Risk assessment is treated as an ongoing process rather than a one-time task.

Conclusion

This risk assessment demonstrates that Kate’s Insurance Inc., like many small businesses, faces meaningful cybersecurity risks despite its size. By systematically identifying assets, threats, vulnerabilities, and impacts, the organization now has a clear roadmap for prioritizing security investments and reducing overall cyber risk.

A well-maintained risk assessment ensures that cybersecurity decisions remain aligned with business needs and evolving threats, helping protect both the company and its clients over time.