Cybersecurity Policy and Incident Response Plan for a Small Business

Name: Ashutosh Kumar

Institution: United College of Engineering and Research

Course Name: IBM Cybersecurity Summer Training

Date: 31 July 2025

Supervisor's Name: Ayush Kumar

Abstract

Small businesses often become targets of cyberattacks due to their limited security measures and lack of dedicated IT staff. This project explores the development of a practical and accessible cybersecurity policy along with a step-by-step incident response plan tailored for small enterprises. Drawing upon globally recognized frameworks such as NIST, CIS Controls, and ISO/IEC 27001, the report distills complex technical requirements into clear, manageable policies. The core aim is to enable small businesses to protect sensitive information and maintain operational continuity in the face of cyber threats. This project provides not only a framework but also actionable guidelines that businesses can implement immediately.

What sets this project apart is its emphasis on **simplicity, scalability, and practicality**. It doesn't rely on expensive software or high-level certifications but instead focuses on empowering small businesses with awareness, basic tools, and structured procedures. Through this project, small business owners gain a ready-to-implement cybersecurity framework that helps them reduce risk, respond effectively to incidents, and foster a security-aware culture within their organization.

In conclusion, this project bridges the gap between technical cybersecurity knowledge and everyday business practices, making cybersecurity achievable for small enterprises. By adopting the strategies outlined in this policy and response plan, small businesses can enhance their resilience against cyber threats and ensure the safety and integrity of their digital operations.

Table of Contents

1. Introduction
2. Literature Review
3. Methodology
4. Results
5. Challenges
6. Conclusion
7. Recommendations
8. References
9. Appendices

Introduction

In an era where nearly every business transaction, communication, and data exchange occurs online, **cybersecurity has become a foundational aspect of organizational resilience and trustworthiness**. While headlines often focus on massive breaches impacting multinational corporations, **small businesses are increasingly finding themselves in the crosshairs of cybercriminals**. According to recent reports by cybersecurity firms and government agencies, over 60% of small businesses have faced a cyberattack in the past year, and many were unable to fully recover from the incident.

The reason is simple: **small businesses often lack the resources, infrastructure, and expertise** to build robust cybersecurity defenses. They may rely on outdated hardware, unpatched software, and generic security settings. More critically, they may not have any **formal policies or plans** in place to address information security, making them soft targets for cybercriminals employing automated attacks, phishing campaigns, or malware injections. Unfortunately, the impact of such breaches is often devastating—leading to **financial loss, data theft, regulatory penalties, reputational damage**, and in severe cases, **permanent closure**.

Despite this growing threat, most small businesses still believe that cybersecurity is either **too technical**, **too expensive**, or **not relevant** to their scale of operations. This assumption is dangerous and outdated. In reality, **even basic cybersecurity measures—if formalized and consistently followed—can drastically reduce risk**. That is the core motivation behind this project.

The primary objective of this project is to **design a practical, affordable, and understandable cybersecurity policy and incident response plan tailored for small businesses**. The goal is not to overwhelm business owners with technical jargon or enterprise-grade solutions, but to empower them with **simple, actionable guidelines** that can be implemented with minimal resources. The policy aims to define the **rules and responsibilities** for protecting information assets, managing risks, and educating employees on safe digital practices. Meanwhile, the incident response plan acts as a structured guide that outlines **how to detect, respond to, and recover from a cybersecurity event**.

This report draws upon **well-established industry standards and frameworks**, including the **NIST Cybersecurity Framework**, **CIS Critical Security Controls**, and **ISO/IEC 27001**. However, it deliberately avoids the complexity of these frameworks, instead focusing on translating them into **plain-language policies** and

step-by-step procedures suited to small-scale operations. Key components of the cybersecurity policy include:

- Data Protection Measures (e.g., encryption, backups)
- Acceptable Use and Access Control Policies
- Password Management Best Practices
- Email and Internet Usage Guidelines
- Remote Work and Bring Your Own Device (BYOD) Security
- Physical Security of Systems
- Employee Awareness and Training Initiatives

The **Incident Response Plan** is designed around six phases: **Preparation**, **Detection**, **Containment**, **Eradication**, **Recovery**, and **Lessons Learned**. Each phase is described in detail, with examples and low-cost tools that businesses can use to identify and manage threats, limit damage, and resume operations safely.

What makes this project unique is its **accessibility and focus on real-world application**. Instead of proposing costly software or advanced monitoring systems, it emphasizes **practical steps** like using strong passwords, conducting regular backups, educating employees, and documenting response protocols. This approach ensures that even the smallest companies—without a dedicated IT department—can build a strong foundation for cybersecurity.

In summary, this project serves as both a **protective shield and a recovery roadmap** for small businesses in the digital world. By implementing the cybersecurity policy and incident response plan provided herein, small businesses can take a major leap toward safeguarding their digital assets, maintaining customer trust, and ensuring long-term business continuity in the face of evolving cyber threats.

Literature Review

Several frameworks and standards guide cybersecurity practices worldwide. The National Institute of Standards and Technology (NIST) provides a well-structured cybersecurity framework focusing on five core functions: Identify, Protect, Detect, Respond, and Recover. The Center for Internet Security (CIS) offers 18 Critical Security Controls that provide prioritized defensive actions. ISO/IEC 27001 is another globally recognized standard that sets requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). This project references these frameworks and adapts their core principles into a format that small business owners can easily understand and implement.

The frameworks and tools reviewed in this section provide a robust foundation for understanding and managing cybersecurity risks. However, their complexity often limits their application in smaller organizations. By distilling and integrating the key ideas from NIST, CIS, ISO, and educational resources, this project aims to offer a **simple, clear, and effective** cybersecurity policy and response plan suitable for small businesses. The following sections describe how these distilled principles were practically applied in the development of this project.

Methodology

The methodology adopted for this project combines **research-driven insights**, **industry best practices**, and **practical simplification strategies** to develop a cybersecurity policy and incident response plan specifically tailored for small businesses. The goal was to strike a balance between effectiveness and simplicity, ensuring that even organizations with no dedicated IT personnel could understand and implement the framework.

This section outlines the steps followed in developing the policy and response plan, the tools and resources used, and the structure adopted to ensure clarity, usability, and compliance with cybersecurity standards.

1. Research and Framework Analysis

The first step in this project involved an in-depth review of prominent cybersecurity standards and frameworks including:

- **NIST Cybersecurity Framework**
- **CIS Critical Security Controls (especially Implementation Group 1 - IG1)**
- **ISO/IEC 27001**
- **SANS Incident Response Lifecycle**
- Government and industry guidelines (e.g., CISA, CERT-IN, IBM SkillsBuild)

These frameworks were selected for their global recognition and practical guidance. However, instead of applying them directly—which may be complex for small businesses—each was **analyzed, simplified, and restructured** into practical components that align with the operational realities of small-scale enterprises.

2. Identification of Key Cybersecurity Areas

Based on the frameworks and real-world risks faced by small businesses, the following **key domains** were identified as essential for a basic cybersecurity policy:

- **Data Protection and Backups**
- **Acceptable Use Policy**
- **Password and Access Management**
- **Email and Internet Safety**
- **Remote Work and BYOD (Bring Your Own Device) Policy**
- **Physical Security of Systems and Offices**

- **Employee Cybersecurity Awareness and Training**

Each domain was carefully reviewed to determine the **minimum essential controls** needed to provide effective protection against common threats like phishing, malware, data breaches, and unauthorized access.

3. Policy Development Process

The cybersecurity policy was drafted with the following core objectives:

- **Clarity** – Use of non-technical language so all employees, regardless of their role or expertise, can understand the rules.
- **Simplicity** – Focus on practical, cost-effective measures that don't require specialized tools.
- **Relevance** – Address real-world challenges like remote access, password reuse, and device misuse.
- **Modularity** – Each section stands on its own so businesses can adopt the whole policy or individual components based on their maturity.

Each section of the policy includes:

- A **brief rationale** for the control.
- A **list of dos and don'ts**.
- **Examples or scenarios** to improve comprehension.
- **Checklist format** options for easy implementation.

This modular design also makes the policy easily adaptable for different types of small businesses (e.g., retail, education, consulting, etc.).

4. Designing the Incident Response Plan

Once the policy was created, the **Incident Response Plan (IRP)** was developed based on the widely accepted **SANS/NIST IR lifecycle**, which includes six core phases:

1. **Preparation** – Establish roles, tools, contact points, and backups.
2. **Identification** – Recognize an incident through alerts, reports, or signs.
3. **Containment** – Isolate the threat before it spreads further.
4. **Eradication** – Remove the cause of the breach or infection.
5. **Recovery** – Restore systems from backup and resume operations.

6. **Lessons Learned** – Analyze the incident to improve future responses.

Each phase was broken down into simple, actionable steps using a **step-by-step guide** format with examples such as:

- What to do if a phishing email is opened.
- How to respond if ransomware encrypts business files.
- What steps to take if a device is lost or stolen.

A printable **"incident checklist"** was also created to help small businesses act quickly during a real-world crisis.

5. Tools and Resources Used

To develop the project and supporting materials, the following tools and resources were used:

- **Microsoft Word & Canva** – For drafting, formatting, and visualizing policies and plans.
- **Online platforms like IBM SkillsBuild and Cybrary** – For security awareness guidelines.
- **Government resources from CISA, CERT-IN, and local law enforcement** – For localized cybersecurity advisory.
- **Community feedback from small business forums and Reddit's r/sysadmin and r/smallbusiness** – To understand real challenges faced in the field.

No paid tools or enterprise-level software were used, ensuring that the final solution can be adopted without cost barriers.

6. Review and Iteration

Once the initial drafts of the policy and IRP were completed, they were reviewed for:

- **Language simplicity**
- **Logical flow**
- **Practicality for day-to-day operations**
- **Coverage of essential threats**

Improvements were made to reduce technical jargon, clarify processes, and introduce examples wherever possible. The aim was to create a living document that can evolve with the business and its environment.

This methodology demonstrates a **research-driven, user-centric approach** to solving one of the biggest cybersecurity challenges faced by small businesses: lack of awareness and structure. By building upon recognized standards and adapting them for real-world simplicity, this project provides not just a policy, but a **practical framework for daily security and incident readiness**—a necessary foundation in today's digital-first world.

Results

The finalized cybersecurity policy and incident response plan are detailed below.

Cybersecurity Policy Overview

The cybersecurity policy is divided into the following sections:

1. Data Protection
2. Acceptable Use Policy
3. Email and Internet Usage
4. Password Management
5. Remote Work
6. Physical Security
7. Employee Training

Each section includes specific actions, recommendations, and tips for enforcement. The goal is to ensure policies are easy to follow yet comprehensive enough to mitigate threats.

Incident Response Plan

The incident response plan follows six essential phases:

1. Preparation - Establish policies, assign roles, and educate staff.
2. Detection - Use antivirus, firewalls, or staff reports to detect incidents.
3. Containment - Isolate affected systems to prevent spread.
4. Eradication - Remove the threat through antivirus tools or reconfiguration.
5. Recovery - Restore systems using verified backups.
6. Lessons Learned - Review what happened and update the plan accordingly.

The completed project provides **immediate value** to small businesses by equipping them with a ready-to-use cybersecurity toolkit. Rather than focusing on theoretical security concepts, this project delivers **practical, resource-light solutions** that address the actual pain points of real-world small business operations. The documents are easy to distribute, explain, and enforce, making cybersecurity more of a habit than a burden.

The result is a framework that not only strengthens a company's defense against digital threats but also cultivates a **culture of cyber awareness and readiness** among employees—a major step toward resilience in the digital age.

Challenges

During the course of this project, several challenges emerged:

- Translating complex cybersecurity concepts into plain language.
- Designing procedures that require minimal technical resources.
- Addressing human factors like employee negligence or lack of awareness.
- Ensuring the policy is scalable and adaptable to different business types.
- Integrating low-cost or free tools in the security and response processes.

Developing a cybersecurity policy and incident response plan for small businesses presented several notable challenges, particularly due to the constraints of limited technical knowledge, financial resources, and workforce capacity. These challenges shaped the way the content was designed, ensuring that it remained practical, lightweight, and easily adoptable.

1. Simplifying Technical Concepts:
Cybersecurity frameworks like NIST, CIS, and ISO/IEC 27001 are comprehensive but technically dense. Translating these into easy-to-understand policies for business owners and employees with no IT background was a major challenge. It required rewriting complex principles into plain language while still preserving the core intent of each security measure.

2. Resource Limitations:
Small businesses often lack advanced security infrastructure such as firewalls, endpoint detection systems, or IT support staff. This limited the feasibility of many traditional recommendations. The challenge was to suggest **cost-effective and low-tech solutions**—such as password managers, free VPNs, and simple backup routines—that could still offer meaningful protection.

3. Human Behavior and Awareness:
Employee actions are often the root cause of security breaches, such as falling for phishing emails or using weak passwords. Designing policies that encourage good behavior and integrating easy-to-digest awareness training materials was crucial. However, getting employees to engage with and follow cybersecurity guidelines remains a practical challenge.

4. Ensuring Flexibility and Adoption:
Every small business is different in terms of size, digital exposure, and data sensitivity. A one-size-fits-all policy wouldn't work. The policy needed to be modular—allowing businesses to adopt key components first and scale up over time. Ensuring that the document was not only written but actually implemented and reviewed regularly was a key hurdle.

5. Designing a Usable Incident Response Plan:
Traditional incident response plans assume technical knowledge and tools. Adapting the

standard six-phase lifecycle into a format that could be followed during real-time stress (e.g., ransomware attack or lost device) using basic tools like printed checklists or simple communication trees was a significant design challenge.

Despite these obstacles, the final outcome of the project reflects the success of overcoming each barrier through **research, simplification, iteration, and user-centric design**. These challenges not only shaped the content of the cybersecurity policy and response plan but also strengthened the relevance and usability of the final deliverables. The lessons learned during these stages were instrumental in developing a truly functional and accessible security framework for small businesses.

Conclusion

The project provides a practical and accessible cybersecurity policy and response plan for small businesses. It demonstrates that, with proper guidance, even non-technical businesses can implement robust cybersecurity practices. The framework not only safeguards sensitive data but also ensures business continuity in the face of cyber threats. Adopting this plan can significantly reduce the risk and impact of cyber incidents for small enterprises.

In an increasingly digital and interconnected world, cybersecurity is no longer optional—even for small businesses. This project aimed to address the pressing need for a practical and accessible **cybersecurity policy and incident response plan** tailored to the specific challenges small businesses face. Unlike large enterprises, small organizations typically operate with limited resources, minimal IT support, and low cybersecurity awareness, making them easy targets for cybercriminals.

Through in-depth research and adaptation of global cybersecurity standards—such as the **NIST Cybersecurity Framework**, **CIS Controls**, and **ISO/IEC 27001**—this project has successfully distilled essential security practices into **plain, actionable language**. The final deliverables include a modular cybersecurity policy and a step-by-step incident response plan that are realistic, cost-effective, and easy to implement without specialized knowledge or software.

The policy addresses key areas like data protection, acceptable use, password hygiene, remote work practices, and employee awareness. The incident response plan provides a structured approach to recognizing, managing, and recovering from security incidents, even under stressful and high-risk conditions.

Ultimately, this project empowers small businesses to take control of their digital security posture, reduce risk, and create a culture of cybersecurity awareness. While no system is ever 100% secure, having a **clear policy and defined response strategy** significantly improves resilience and readiness. The framework created here is designed not just as a static document, but as a **living guide** that can grow and evolve as the business matures and cyber threats change.

References

1. **National Institute of Standards and Technology (NIST)**.
   Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).
   Available at: https://www.nist.gov/cyberframework

2. **Center for Internet Security (CIS)**.
   CIS Critical Security Controls v8 – Implementation Group 1 (IG1).
   Available at: https://www.cisecurity.org/controls

3. **ISO/IEC 27001:2022** – Information Security, Cybersecurity and Privacy Protection.
   International Organization for Standardization (ISO).
   Overview at: https://www.iso.org/isoiec-27001-information-security.html

4. **Cybersecurity and Infrastructure Security Agency (CISA)**.
   Cyber Essentials for Small Businesses.
   Available at: https://www.cisa.gov

5. **IBM SkillsBuild for Cybersecurity**.
   Cybersecurity Foundation Training Modules.
   Available at: https://skillsbuild.org

6. **Google Cybersecurity Certificate**.
   Google Career Certificates – IT Support & Cybersecurity.
   Available at: https://grow.google/certificates/cybersecurity/

7. **SANS Institute**.
   Incident Handler's Handbook & Incident Response Lifecycle.
   Available at: https://www.sans.org/white-papers/incident-handler/

8. **Bitwarden** – Password Manager (Open Source).
   Available at: https://bitwarden.com

9. **VeraCrypt** – Open-source Encryption Software.
   Available at: https://www.veracrypt.fr

10. **OpenDNS / Cisco Umbrella** – Internet Filtering for Businesses.
    Available at: https://www.opendns.com

Appendices

This section includes supplementary materials that support the main content of the report. These resources are provided to enhance understanding, assist in implementation, and serve as templates or references for small business use.

Appendix A – Sample Cybersecurity Policy Template

A complete, editable version of the cybersecurity policy containing:

- Employee Acceptable Use Policy
- Password Management Policy
- Data Backup Schedule Template
- Internet & Email Usage Guidelines
- Remote Work Security Checklist
- Policy Acknowledgment Form (for employee signatures)

Purpose: Can be printed, signed, and circulated to all employees within the organization.

Appendix B – Incident Response Plan Checklist

A printable guide summarizing each of the six IR phases:

1. **Preparation** – Contact lists, backup routine verification
2. **Identification** – How to detect and report suspicious activity
3. **Containment** – Step-by-step isolation instructions
4. **Eradication** – Threat removal methods (e.g., antivirus tools)
5. **Recovery** – Backup restoration checklist
6. **Lessons Learned** – Documentation format for post-incident review

Purpose: Keep this physical copy accessible for emergency response even when systems are down.

Appendix C – Cybersecurity Awareness Training Topics

Suggested outline for monthly training sessions:

- Phishing detection with real email examples
- Safe internet practices and risky website indicators

- Password creation and management tips
- Social engineering tactics and how to avoid them
- Importance of software updates and patches

Purpose: Helps create a culture of cybersecurity awareness within the company.