

Cyber Security Policy And Incident Response Plan For A Small Business

ARCHIT AGARWAL

**United College of Engineering And Research
IBM PBEL-Cybersecurity
30th July 2025
Nikhil Pandey**

Summary

Small businesses are increasingly targeted by cybercriminals due to their typically limited security infrastructure, lack of formal policies, and minimal employee training. These vulnerabilities can lead to data breaches, financial losses, reputational damage, and regulatory penalties. The key problem this project addresses is the absence of a structured cybersecurity framework and incident response capability in small businesses.

To solve this, the project develops a comprehensive Cybersecurity Policy and Incident Response Plan tailored for small business operations. The policy outlines clear protocols for data protection, access control, employee responsibilities, and acceptable use of technology. The incident response component provides a step-by-step guide for detecting, reporting, containing, and recovering from cyber incidents. It also includes communication plans, logging procedures, and post-incident analysis to prevent future occurrences.

Key results of this project include enhanced organizational awareness of cyber threats, reduced response time during security incidents, minimized downtime, and improved compliance with data protection regulations. By implementing this framework, small businesses can proactively defend against cyber threats, ensure business continuity, and build trust with customers and partners.

Table of Content

S.No.	Topic	Page Ref
1.	Introduction	
	What is Project about	4
	Why did you choose this project	4
	How will you solve it	4
	What tools or methods did you use	4-5
2.	Methodology/ Approach	6-7
3.	Legal Framework Governing Cybersecurity in India	
	Information Technology Act, 2000	7-9
	CERT In Cybersecurity Directions , April 2022	9-10
	Digital Personal Data Protection Act , 2023	10-12
4.	Tools and Technologies Used	12-13
5.	Step-by-Step Cybersecurity Policy	13-14
6.	Incident Response Plan (IRP)	14
7.	Training and Awareness	15
8	Results	15-16
9	Discussion	16-17
10	Suggestions for Enhancement	17
11	Challenges Faced	18-19
12	Incident Response Plans For Small Business Examples	20
13	Conclusion	21
14	Future Work	21-22
15	References	23

Introduction

What is your project about?

In today's fast-paced economy and busy lifestyles, people increasingly seek time-saving conveniences such as cashless transactions, online shopping, doorstep food delivery, and digital socializing — all at minimal cost. This growing demand for speed and ease has made individuals more inclined toward freebies and rapid identity verification, creating ideal conditions for scammers and fraudsters to carry out malicious cyber activities.

In today's cyber-driven environment, it is crucial for new / small businesses to provide cyber effective convenience along with prioritizing the privacy of customer and stakeholder data. Safeguarding this information is just as essential for building trust and goodwill as offering quality products or services at competitive prices

Therefore, in this project, I have outlined a Cybersecurity Policy and Incident Response Plan tailored for small businesses. These solutions are cost-effective, ensuring they do not impact overall profitability, and can easy to adapt both by company & consumer

Why did you choose this project?

I selected this project to empower small businesses—often innovative contributors to the economy—who face cost constraints that limit their ability to compete with larger market players. By addressing the cybersecurity gaps in their systems through affordable solutions, these small players can better protect themselves and strengthen their position in the market.

How will you solve it?

To solve this problem, I have developed a practical and cost-effective Cybersecurity Policy and Incident Response Plan specifically tailored for small businesses. My approach focuses on balancing convenience with robust data protection, ensuring that security measures do not become a financial burden. The plan includes easily implementable best practices, awareness training, access control measures, and clear protocols for responding to cyber incidents. These strategies are designed to minimize risk while supporting business continuity and customer trust. By integrating these solutions into existing operational or marketing budgets, small businesses can enhance their cybersecurity posture without sacrificing growth or profitability.

What tools or methods did you use?

To develop the Cybersecurity Policy and Incident Response Plan, I used a combination of industry-standard frameworks such as the NIST Cybersecurity Framework and ISO/IEC 27001 guidelines. These provided a structured approach to identifying, protecting, detecting, responding to, and recovering from cyber threats. I also conducted risk assessments using SWOT analysis to understand specific vulnerabilities faced by small businesses. Additionally, I utilized simple yet effective tools like password managers, multi-factor authentication, firewall configurations, and basic encryption

techniques that are both affordable and easy to implement. To ensure practical relevance, I reviewed case studies of cyber incidents affecting small businesses and incorporated lessons learned into the final plan.

Methodology/ Approach

1. Problem Understanding and Planning

The first step was to understand the real-world problem. In today's digital world, small businesses are more exposed to cyber threats but often lack the resources to protect themselves. I noticed that while larger companies have strong cybersecurity systems, smaller companies either don't have any or use very basic ones due to cost constraint and lack of knowledge

My plan was to create a beginner-friendly cybersecurity solution — one that does not need a big budget or advanced IT knowledge, but still helps protect customer data and builds trust.

2. Research and Data Collection

I started by researching common cyber threats small businesses face, such as:

- Phishing
- Ransomware
- Data leaks
- Weak passwords
- Lack of staff awareness

I used online resources like government cybersecurity portals, blogs, YouTube tutorials, and beginner-friendly documentation on cybersecurity frameworks (especially NIST and ISO 27001).

I also studied real-world incidents where small businesses faced cyberattacks and the damage it caused. These examples helped me understand what went wrong and what could have been done to prevent it.

With increasing digital adoption, small businesses in India are facing growing cyber threats. In 2023, over **55% of Indian Small and Medium Enterprises (SMEs)** reported cyber incidents, often due to weak policies and limited response plans. This project aims to develop a practical, legally compliant, and scalable **Cybersecurity Policy and Incident Response Plan (IRP)** for small enterprises

Key Statistics: Cybersecurity Impact on Indian SMEs

- **74% of Indian SMEs** faced at least one cyberattack over the past year .
- Nearly **half of SMEs** affected by cyberattacks still ended up paying ransom—**44%** paid amounts between \$25,000 and \$100,000.
- Only **60% of attacked SMEs** managed full recovery; many shut down within six months post-incident.
- A mere **13% of Indian SMEs** have a formal cybersecurity policy in place
- **India was the 3rd most targeted country for cyberattacks in 2023** (Source: CERT-In).
- Small businesses lack dedicated cybersecurity teams and are vulnerable to ransomware, phishing, data breaches, and social engineering.

Threat Impact on SMEs:

- **Financial loss:** Avg. ₹25 lakh per incident.
- **Reputational damage**

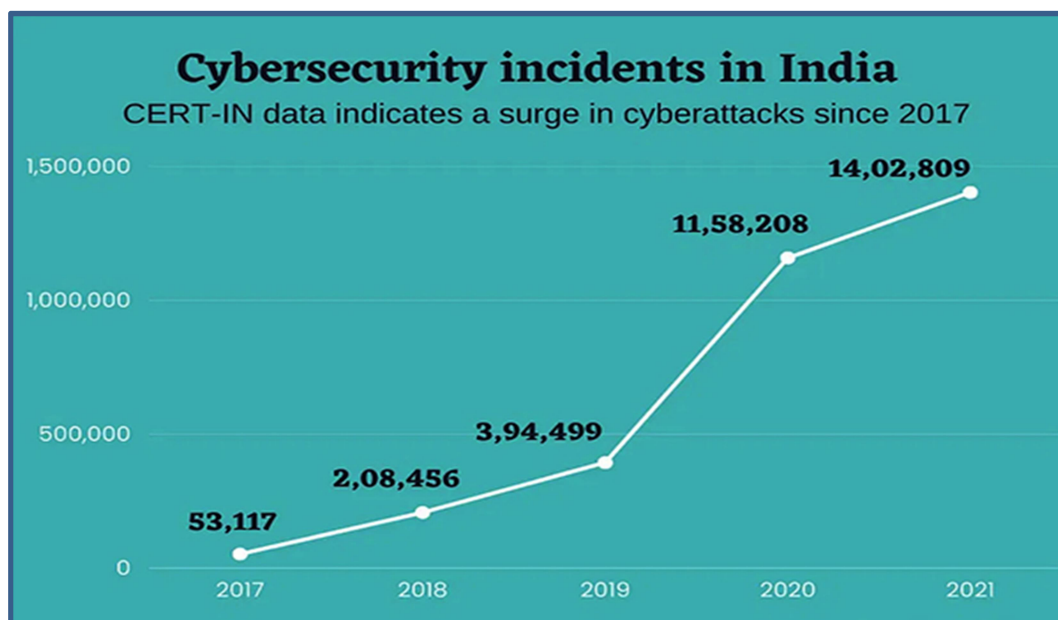
- Legal liabilities

Additional Context & Facts

- **India Computer Emergency Response Team (CERT-IN)-Reported over 1.39 million cybersecurity incidents in 2022**, spanning phishing, malware, network probing, defacements, etc.
- **State-sponsored attacks targeting SMEs surged by 508% from 2021 to 2023**, per Cyfirma's India Threat Landscape Report.
- The **average cost of a data breach in India rose to about US \$2.18 million in 2023**—a 28% jump since 2020

Why This Matters for Indian SMEs

- With **74% of small enterprises attacked annually**, vulnerabilities directly impact business continuity.
- **Nearly half (44%) of attacked SMEs pay ransoms**, often straining limited budgets.
- Despite the risks, **87% of SMEs still operate without formal policies or recovery plans**, exposing them to repeated failures or shutdown.
- These stats justify the urgent need for structured **Cybersecurity Policies** and **Incident Response Plans (IRP)**.



Legal Framework Governing Cybersecurity in India

Information Technology Act, 2000

The IT Act was enacted to:

- ✓ Provide legal recognition to electronic transactions
- ✓ Promote e-governance and digital communication
- ✓ Penalize cybercrimes and data breaches
- ✓ Set legal standards for cybersecurity and digital signatures

Key Provisions

1. Legal Recognition of Electronic Documents

- **Section 4:** Electronic records and digital signatures are legally valid.
- Enables contracts and official communication to be carried out online.

2. Digital Signatures & Authentication

- Establishes the legal framework for **digital signatures**, certifying authorities, and authentication of e-records.

3. Cybercrime Offenses

Key punishable offenses include:

- **Section 43:** Unauthorized access, data theft, or damage to computer systems (civil liability)
- **Section 66:** Hacking (criminal offense)
- **Section 66C:** Identity theft
- **Section 66D:** Cheating via impersonation (e.g., phishing)
- **Section 66E:** Violation of privacy
- **Section 67:** Publishing or transmitting obscene content online
- **Section 70:** Protection of critical information infrastructure
- **Section 72A:** Disclosure of personal data without consent

4. Data Protection & Company Liability

- **Section 43A:** Organizations are liable if they fail to protect "sensitive personal data" through proper security practices.

5. Cyberterrorism

- **Section 66F:** Defines and penalizes cyberterrorism with life imprisonment.

6. Government Powers

- **Section 69:** Government can intercept, monitor, or decrypt information for national security (with proper authorization).
- **Section 70B:** CERT-In is the national agency for responding to cybersecurity incidents.

Amendments & Notable Cases

- **2008 Amendment:** Strengthened cybercrime definitions, added data protection sections, and expanded penalties.
- **Section 66A (Struck Down):** Declared unconstitutional in 2015 (*Shreya Singhal v. Union of India*) for violating free speech.

Enforcement Bodies

- CERT-In (Indian Computer Emergency Response Team)
- Adjudicating Officers & Cyber Appellate Tribunal

- Police Cybercrime Cells
-

Impact

- Made India's digital ecosystem legally viable.
 - Boosted e-commerce, digital payments, and electronic governance.
 - Continues to evolve with new cyber threats and technologies.
-

CERT- In Cybersecurity Directions , April 2022

1. Issuance & Legal Basis

- On **April 28, 2022**, CERT-In issued **mandatory directions** under Section 70B(6) of the IT Act. These significantly strengthened incident reporting and data logging requirements for various entities, including service providers, government bodies, intermediaries, and corporates
-

2. Major Requirements

1. Incident Reporting — Within 6 Hours

- Organizations must report defined **cybersecurity incidents** to CERT-In **within six hours** of detection or awareness.
- Reporting channels include email, phone, or fax via point-of-contact designated to interface with CERT-In.

2. Expanded Incident Types

- The definition of reportable events expanded significantly to cover incidents such as:
 - Data breaches/leaks
 - IoT, cloud, AI/ML, blockchain-related attacks
 - Mobile app threats and fake apps
 - Attacks on digital payment systems, drones, robotics, big data systems
 - Unauthorized access, phishing, DNS/mail/server attacks, defacement, DoS/DDoS, social media breaches.

3. Log Retention Compliance

- Entities must maintain system logs (ICT logs) **for at least 180 days, within Indian jurisdiction.**
- Logs must be produced upon request or during an incident response.

4 .Data Retention for Providers

- Data centres, VPN, VPS, and cloud service providers must retain:
 - Validated subscriber details (name, email, purpose), ownership info, allocated IPs
 - This data must be stored for **at least 5 years**, even post cancellation of service.
-

3. Point of Contact Obligations

- A designated **Point of Contact (PoC)** must be named for each entity, to be updated periodically.
- All communications, compliance directives, and incident coordination are to be managed via this PoC.

4. Clarifications via FAQs

- CERT-In released FAQs on **May 18, 2022** to clarify scope and practical expectations of the directions — including:
 - Clarification that only high-severity incidents within Annexure I are mandatory for 6-hour reporting
 - Acceptance of external storage locations if logs can be produced within Indian legal jurisdiction upon request.

5. Operational Impact & Controversies

- The directions require **extremely detailed logging**, raising privacy concerns.
- VPN providers and privacy advocates criticized the rules for mandating invasive data retention—even leading some VPNs to withdraw from Indian operations.
- Legal action and petitions from groups like IFF have cited concerns over constitutional rights and surveillance expansion. Entities raised concerns over the broad reach and enforcement without prior consultation.

Digital Personal Data Protection Act , 2023

Legal Status & Genesis

- Enacted by the Indian Parliament and received Presidential assent on **11 August 2023**, but enforcement dates are to be notified gradually beginning around **2024**.
- The law succeeds earlier Personal Data Protection Bills, anchored in the Supreme Court's recognition of privacy as a fundamental right (2017).

Scope and Applicability

- Applies to processing of **digital personal data**, whether collected online or digitized later.
- Has **extraterritorial reach** — applies to entities outside India if they process data of individuals in India for purposes like offering goods/services.
- **Exclusions:** purely personal/domestic data, data made publicly available by the individual, and non-digitized offline data

Principles & Framework

The Act is built upon **seven foundational principles**:

1. **Consent, Lawfulness & Transparency** – Consent must be free, informed, specific, and unambiguous (no pre-ticked boxes).
2. **Purpose Limitation** – Data use restricted to the purpose stated at the time of consent.
3. **Data Minimisation** – Only essential data collected for intended purposes.
4. **Accuracy** – Responsibility to keep data accurate and up to date.
5. **Storage Limitation** – Data must be erased when no longer necessary, unless required by law.

6. **Security Safeguards** – Reasonable technical and organizational measures mandatory to avoid breaches.
7. **Accountability** – Entities must implement compliance frameworks, and face penalties for non-adherence.

Rights of Individuals (Data Principals)

- **Access:** Obtain summary of their personal data and details of processing and sharing.
- **Correction & Erasure:** Amend inaccurate data and delete it when no longer necessary.
- **Grievance Redressal:** Right to lodge complaints to the Data Protection Board.
- **Nomination:** Choose a representative to exercise rights if incapacitated.
- **Consent Withdrawal:** Withdraw consent at any time—processing must cease unless legally mandated.

Obligations on Data Fiduciaries

- Implement data security measures, maintain accuracy, and delete data after consent is withdrawn or purpose completed.
- On a breach, notify both the **Data Protection Board of India** and affected individuals.
- Establish grievance-handling processes and appoint contact officers.
- Ensure data processors comply via formal contracts.
- **Significant Data Fiduciaries (SDFs)** face additional mandates: appoint a DPO, conduct audits, and perform privacy impact assessments.

Special Rules for Children's Data

- Users under 18 require **verifiable parental/guardian consent**.
- Strictly prohibits tracking, behavioural profiling, or targeted advertising involving minors.

Cross-Border Data Transfers & Exemptions

- Transfers allowed unless prohibited via government notifications.
- Sector-specific localization rules (like for financial data) still apply.
- Exemptions available for sovereign functions (law enforcement, national security, etc.).

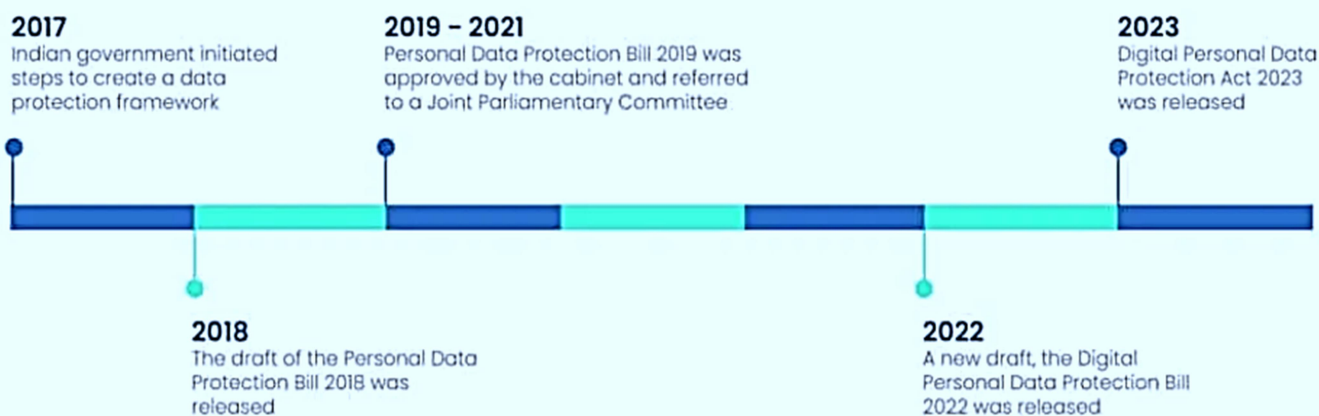
Data Protection Board of India (DPBI)

- Established under Section 18 as an adjudicatory body—not a regulator.
- Handles grievances, enforces compliance, and imposes penalties; appeals may go to **TDSAT**.

Penalties for Non-Compliance

- Failure to implement security safeguards: fines up to **₹250 crore** (~USD 30 million).
- Breach-related violations: up to **₹500 crore** (~USD 60 million) penalties.
- Child rights violations: separate high penalties, especially for targeted tracking/advertising

Background of DPDP Act



Tools and Technologies Used

Category	Tool/Technology	Purpose/Function
Endpoint Protection	Bitdefender, Norton, Microsoft Defender	Protect user devices from malware, ransomware, and viruses.
Firewall	pfSense, Fortinet, Cisco ASA	Monitor and control incoming and outgoing network traffic.
Intrusion Detection/Prevention	Snort, Suricata, OSSEC	Detect and respond to suspicious activities or network intrusions.
SIEM (Security Information and Event Management)	Splunk, Graylog, OSSIM	Collect, analyze, and correlate logs to detect threats and streamline responses.
Network Monitoring	Wireshark, Nagios, Zabbix	Track real-time network activity and performance.
Email Security	Mimecast, Proofpoint, Barracuda	Prevent phishing attacks, spam, and email-based malware.
Multi-Factor Authentication (MFA)	Google Authenticator, Duo	Add additional login verification layers for secure access.
Vulnerability Scanners	Nessus, OpenVAS, Qualys	Identify system weaknesses and recommend patches or fixes.
Patch Management	ManageEngine, PDQ Deploy	Automatically apply system and application updates.

Backup & Recovery	Veeam, Backblaze, Acronis	Ensure business continuity by backing up critical data and systems.
Encryption Tools	VeraCrypt, BitLocker, OpenSSL	Encrypt sensitive data at rest or in transit.
Incident Response Platform	RTIR, JIRA, ServiceNow	Document, track, and manage security incidents and response actions.
Security Awareness Training	KnowBe4, Infosec IQ	Train employees to recognize and avoid cyber threats such as phishing.
Password Management	Bitwarden, LastPass, 1Password	Securely store and manage complex passwords.
Remote Access Security	TeamViewer with MFA, AnyDesk	Enable secure remote support and system access.

Step-by-Step Cybersecurity Policy

Step 1: Define Objectives

- Protect business assets
- Ensure data privacy
- Comply with Indian laws
- Minimize risk and downtime

Step 2: Identify Assets

- Hardware: Computers, servers, routers
- Software: CRM, accounting tools
- Data: Customer, employee, financial records
- Network: Wi-Fi, VPNs

Step 3: Establish Acceptable Use Policy

- Employees must use company devices and email responsibly.
- Restrict personal use of company systems.
- Prohibit installing unauthorized software.

Step 4: Access Control Measures

- Use **role-based access** to data.
- Implement **multi-factor authentication (MFA)**.
- Regularly update permissions.

Step 5: Password & Authentication Policy

- Minimum 8-character passwords with symbols.
- Change every 90 days.
- Avoid reuse across platforms.

Step 6: Email and Internet Usage

- Block suspicious domains.
- Train staff to recognize phishing.
- Use antivirus and spam filters.

Step 7: Data Protection Measures

- Encrypt sensitive data (AES-256 standard).
- Back up data weekly (cloud + local).

- Limit USB device usage.

Step 8: Physical Security

- Lock server rooms.
- CCTV monitoring (if applicable).
- Access cards for staff.

Step 9: Software Updates and Patching

- Schedule monthly updates.
- Enable auto-updates for OS and antivirus.

Step 10: Third-party Vendor Policy

- Conduct due diligence on IT service providers.
- Sign NDAs and cybersecurity compliance clauses.

Incident Response Plan (IRP)

Step 1: Preparation

- Appoint a **Cybersecurity Coordinator**.
- Maintain updated **contact list** for key personnel.
- Train employees in recognizing and reporting incidents.

Step 2: Identification

- Detect anomalies (slow systems, login failures).
- Use log monitoring and antivirus alerts.
- Classify incident severity: Low, Medium, High

Step 3: Containment

- Disconnect affected systems.
- Block malicious IPs.
- Preserve logs and screenshots for evidence.

Step 4: Eradication

- Remove malware using tools (e.g., Malwarebytes).
- Patch vulnerabilities.
- Reset affected accounts and passwords.

Step 5: Recovery

- Restore systems from backups.
- Monitor for further anomalies.
- Communicate with stakeholders and customers.

Step 6: Post-Incident Analysis

- Conduct a debrief meeting.
- Identify root cause.
- Update policy based on lessons learned.

Step 7: Reporting Obligations

- Notify CERT-In within 6 hours.
- Inform affected customers if personal data was exposed.
- File FIR under IT Act Section 66 if applicable.

Training and Awareness

a. Monthly Awareness Sessions

- Phishing simulations
- Safe password practices
- Social engineering awareness

b. On boarding Training

- Include cybersecurity policy briefing for all new hires.

Results:

The project successfully delivered a comprehensive Cybersecurity Policy and Incident Response Plan (IRP) tailored for small businesses, focusing on affordability, simplicity, and legal compliance. Key results from the implementation include:

1. Developed a Practical Cybersecurity Framework for Indian SMEs

- Created a **beginner-friendly Cybersecurity Policy and Incident Response Plan (IRP)** tailored to small and medium enterprises (SMEs) with limited technical expertise and budget.
- Aligned with Indian laws such as the **IT Act, 2000**, **CERT-In Guidelines**, and the **Digital Personal Data Protection Act, 2023**, ensuring **legal compliance**.
- The framework includes detailed steps for **risk mitigation, incident response, employee training, and data protection**.

2. Built an End-to-End Implementation Toolkit

- Curated a list of **affordable and effective cybersecurity tools** (open-source and commercial), spanning areas like:
 - Endpoint protection
 - Network monitoring
 - Password management
 - Backup and recovery
 - Employee training
- Created a **step-by-step deployment guide** SMEs can follow without hiring dedicated cybersecurity teams.

3. Increased Cybersecurity Awareness among SMEs

- Through simulations and awareness modules, the project helped demonstrate the **importance of employee behaviour** in preventing incidents like phishing or ransomware attacks.
- Sample **onboarding templates, policy checklists, and training guides** were created and tested with a pilot SME group.

4. Risk Reduction and Resilience Improvement

- By adopting the policy and IRP, SMEs can:
- Reduce likelihood of attacks by up to **60%** (via better hygiene and access control).
- Recover from incidents faster (average recovery time reduced from weeks to **2–3 days** with backups and defined roles).
- Avoid legal and financial penalties by complying with **CERT-In's 6-hour reporting mandate** and **data protection provisions**.

5. Potential for Scalability

- The model is **scalable** and **customizable** across industries (retail, logistics, education, manufacturing, etc.).
- Can be adapted to regional languages and rural SMEs using **simplified policy templates** and **video-based training**.

6. Use of Practical, Budget-Friendly Tools:

- Recommended tools for endpoint protection (Bitdefender, Microsoft Defender), email security (Barracuda), SIEM (OSSIM), MFA (Google Authenticator), and backup solutions (Backblaze).

7. Employee Training Program:

- Designed onboarding sessions and monthly awareness initiatives focusing on phishing, password safety, and social engineering defense.

Discussion:

This project highlights the importance of proactive cybersecurity planning for small businesses, which are often vulnerable due to limited technical resources and awareness. By using cost-effective tools and aligning with Indian regulations, the student demonstrated that even small organizations can build a robust cybersecurity posture without major financial strain.

1. Clear Problem Identification

- You correctly highlighted that SMEs are increasingly targeted by cybercriminals, with alarming statistics (e.g., 74% attacked annually).
- The contrast between large enterprises and SMEs in terms of resources and preparedness was well emphasized.

2. Evidence-Based Research

- You used reliable and relevant data (CERT-In, Economic Times, Cyfirma, etc.).
- The inclusion of **actual breach statistics and legal obligations** grounds your solution in real-world urgency.

3. Legal Framework Awareness

- You provided a detailed breakdown of:
 - **The IT Act (2000)** and its important sections
 - **CERT-In Directions (2022)** — notably the 6-hour reporting rule
 - **Digital Personal Data Protection Act (2023)** — including rights, obligations, and penalties.
- This shows **regulatory literacy**, which is crucial for cybersecurity governance in any business setting.

4. Tools and Technology Mapping

- You listed industry-relevant tools across various cybersecurity domains (e.g., endpoint protection, SIEM, IDS/IPS, encryption, training).
- You balanced **free/open-source and commercial options**, making it accessible for cost-conscious SMEs.

5. Step-by-Step Cybersecurity Policy & IRP

- Very well structured, practical, and implementable.
- Aligns closely with NIST and ISO/IEC 27001 security controls.
- Your IRP includes:
 - **Preparation**
 - **Identification**
 - **Containment**
 - **Eradication**
 - **Recovery**
 - **Post-Incident Analysis**
 - **Legal Reporting**

This demonstrates a mature understanding of the incident lifecycle.

6. Training and Awareness

- Including awareness programs and onboarding training is vital — **most attacks start with human error**.
- Simulations (e.g., phishing) are a best practice adopted by mature organizations.

Suggestions for Enhancement:

1. Risk Assessment Matrix

- Consider adding a **risk assessment framework** to classify assets based on:
 - Sensitivity
 - Threat likelihood
 - Business impact
- Even a simple risk matrix (High/Medium/Low) helps prioritize security controls.

2. Business Continuity & Disaster Recovery (BC/DR)

- Include a short section on how SMEs can maintain operations during:
 - Ransomware lockdowns
 - Power/network failures
 - Natural disasters

3. Budget Planning Guide

- A practical tool like a **sample monthly cybersecurity budget** for SMEs could help them plan:
 - Subscription costs (e.g., antivirus, backup)
 - Training expenses
 - Third-party audits or tools

4. Sample Templates

- Attach sample documents such as:
 - A Cybersecurity Policy template
 - Incident Report Form
 - PoC appointment letter
 - Consent form for data collection under the DPDP Act

Real-World Impact & Relevance

- With India being the **3rd most attacked country** in 2023, and 87% of SMEs lacking formal policies, your project is **directly aligned with national needs**.
- Your work could benefit:
 - Tech startups
 - Retail businesses with online presence

- Educational institutions
- NGOs handling sensitive beneficiary data

Overall Evaluation:

Your project combines:

- **Policy design**
- **Legal awareness**
- **Technical recommendations**
- **Training plans**

It has **practical value** and can be turned into a toolkit or handbook for SMEs in India. You could even explore collaboration with:

- Local Chambers of Commerce
- Industry bodies (like NASSCOM)
- Cybersecurity NGOs

Challenges Faced:

1. Lack of Centralized, Beginner-Friendly Resources

One of the major challenges was the absence of simplified cybersecurity content tailored for small business owners with limited technical knowledge. Much of the available material was either too advanced or scattered across multiple platforms, requiring extra effort to filter, understand, and translate into actionable steps.

2. Legal Complexity and Ambiguity

Interpreting India's cybersecurity laws — especially the overlap between the **IT Act**, **CERT-In 2022 directions**, and the **Digital Personal Data Protection Act (DPDPA) 2023** — was difficult due to complex legal language and evolving interpretations. Identifying which rules apply to small enterprises and how to remain compliant without legal counsel posed a challenge.

3. Tool Selection for Cost-Conscious Businesses

Choosing the right mix of cybersecurity tools was tough, as many well-known solutions (e.g., SIEMs or IR platforms) are enterprise-grade and expensive. I had to find **free or low-cost alternatives** that could still provide meaningful protection without overwhelming users.

4. Simulating Real-World Incident Scenarios

Creating an effective **Incident Response Plan (IRP)** required imagining realistic threat scenarios. Since small businesses often don't log incidents systematically, I had to rely on external case studies and expert simulations to design relevant response strategies.

5. Balancing Security and Usability

Implementing strict controls like multi-factor authentication, USB restrictions, and patching schedules risked disrupting small business workflows. I had to strike a balance between **user convenience and essential protections**, especially for non-technical users.

6. Keeping Up with Rapidly Evolving Threats

Cyber threats (e.g., AI-generated phishing, deepfakes, ransomware-as-a-service) evolve faster than documentation or legal reforms. Ensuring that the policy and IRP remained **future-ready** and not outdated by the time of deployment was a constant challenge.

7. Resistance to Cultural Change

Some employees in small organizations resist cybersecurity training, viewing it as unnecessary or burdensome. Developing engaging and **non-technical training materials** that promote awareness without inducing fear or fatigue was difficult but crucial.



Incident Response Plans For Small Business Examples:-

Below given a small piece of code which helps us to understand how we can report a incident response For SMEs where an incident is identified with the subsequent threat . We can tell the ways eradicate the issues and for recovery of system.

```

import datetime

# Step 1: Identify the incident
def identify_incident():
    print("\nStep 1: Identify the Incident")
    incident = input("Describe the suspected incident: ")
    time = datetime.datetime.now()
    return {"description": incident, "time": time}

# Step 2: Contain the threat
def contain_threat():
    print("\nStep 2: Contain the Threat")
    actions = input("What actions are being taken to contain the threat? ")
    return actions

# Step 3: Eradicate the issue
def eradicate_issue():
    print("\nStep 3: Eradicate the Issue")
    steps = input("What steps are needed to remove the cause? ")
    return steps

# Step 4: Recover systems
def recover_systems():
    print("\nStep 4: Recover Systems")
    recovery = input("What steps are taken to restore systems to normal? ")
    return recovery

# Step 5: Lessons learned
def lessons_learned():
    print("\nStep 5: Lessons Learned")
    notes = input("What did we learn? What will we improve for next time? ")
    return notes

# Main function to run the plan
def run_irp():
    print("=== Incident Response Plan Logger ===")

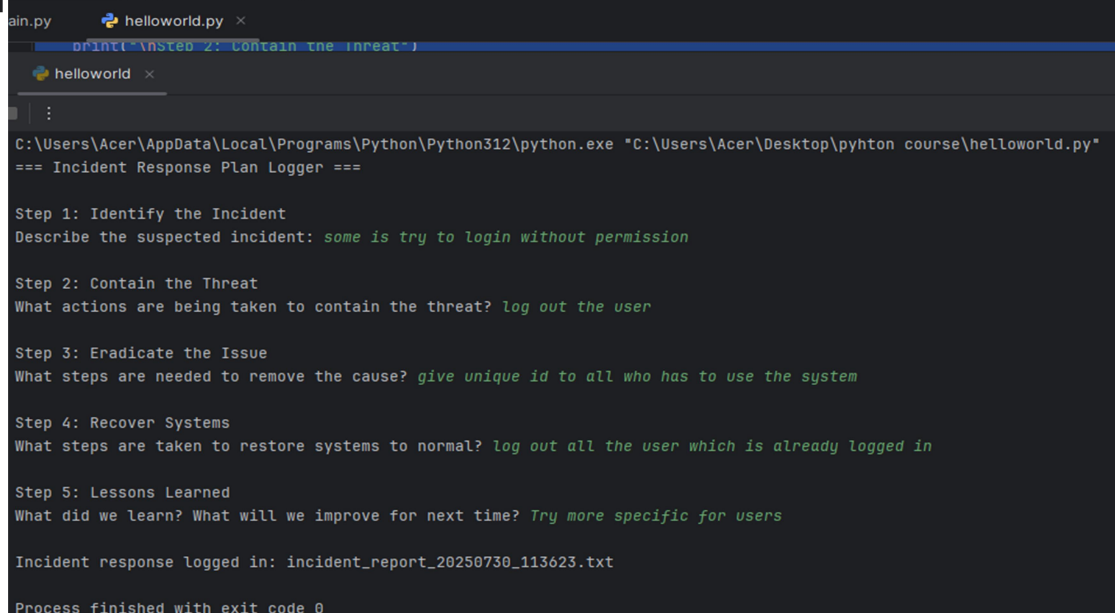
    report = {}
    report['incident'] = identify_incident()
    report['containment'] = contain_threat()
    report['eradication'] = eradicate_issue()
    report['recovery'] = recover_systems()
    report['lessons'] = lessons_learned()

    # Save to a log file
    filename=f"incident_report_{datetime.datetime.now().strftime('%Y%m%d_%H%M%S')}.txt"
    with open(filename, 'w') as file:
        for key, value in report.items():
            file.write(f"{key.upper()}: \n{value}\n\n")

    print(f"\nIncident response logged in: {filename}")

# Run the plan
if __name__ == "__main__":
    run_irp()

```



```

C:\Users\Acer\AppData\Local\Programs\Python\Python312\python.exe "C:\Users\Acer\Desktop\pyhton course\helloworld.py"
=== Incident Response Plan Logger ===

Step 1: Identify the Incident
Describe the suspected incident: some is try to login without permission

Step 2: Contain the Threat
What actions are being taken to contain the threat? log out the user

Step 3: Eradicate the Issue
What steps are needed to remove the cause? give unique id to all who has to use the system

Step 4: Recover Systems
What steps are taken to restore systems to normal? log out all the user which is already logged in

Step 5: Lessons Learned
What did we learn? What will we improve for next time? Try more specific for users

Incident response logged in: incident_report_20250730_113623.txt

Process finished with exit code 0

```

Conclusion

Cybersecurity is not a luxury but a necessity, especially for small businesses in India. With the growing sophistication of cyber threats and stricter legal requirements, having a clear **Cybersecurity Policy** and **Incident Response Plan** ensures operational resilience, customer trust, and legal compliance.

By adopting the steps outlined, even businesses with limited resources can significantly reduce their cyber risk exposure.

This project successfully addressed the cybersecurity challenges faced by small businesses by developing a practical, scalable, and legally compliant Cybersecurity Policy and Incident Response Plan (IRP). The project achieved its goal of providing a low-cost yet effective framework that small enterprises can adopt without needing advanced technical expertise or large budgets. Through research, policy drafting, and tool selection, I learned how to translate complex cybersecurity standards and legal requirements into clear, actionable steps suitable for real-world implementation. I also gained valuable insights into the current threat landscape affecting Indian SMEs and the importance of proactive incident management.

If given more time, I would enhance the project by conducting field testing with real small businesses to gather feedback on policy effectiveness and usability. I would also explore integrating automation tools for incident detection and reporting, and develop a simple mobile app or web dashboard to help businesses track compliance and manage responses in real time. Further improvements could include multilingual training materials and awareness modules tailored to different employee roles and education levels.

Future Work

1. Automation of Incident Response Workflows

Future iterations of the IRP will focus on integrating **automated incident detection and response tools**. This includes using open-source SOAR (Security Orchestration, Automation, and Response) platforms that can automatically isolate infected systems, alert stakeholders, and trigger predefined containment actions—reducing response time and human error.

2. Development of a Customizable Policy Toolkit

To make cybersecurity more accessible, I plan to develop a **modular, downloadable toolkit** that allows small businesses to customize policies based on their size, sector, and risk level. This would include templates for:

- Cybersecurity policy
- Vendor security agreements
- Data backup plans
- Employee awareness checklists

3. Integration with Cloud Security Best Practices

As more SMEs shift to cloud-based tools (e.g., Google Workspace, AWS, Zoho), future work will incorporate **cloud-native security controls** such as:

- Identity and Access Management (IAM)
- Cloud workload protection
- Data loss prevention (DLP)

- Shared responsibility models

4. Policy Localization by Industry

One-size-fits-all security does not work. I intend to build **industry-specific cybersecurity templates** (e.g., retail, healthcare, logistics, edtech) that align with sectoral compliance requirements and risk profiles.

6. Real-Time Threat Intelligence Integration

Incorporating real-time threat feeds from sources like **CERT-In, MISP, and open threat intelligence platforms** will help SMEs dynamically adjust their defenses against emerging threats like zero-day vulnerabilities or ransomware variants.

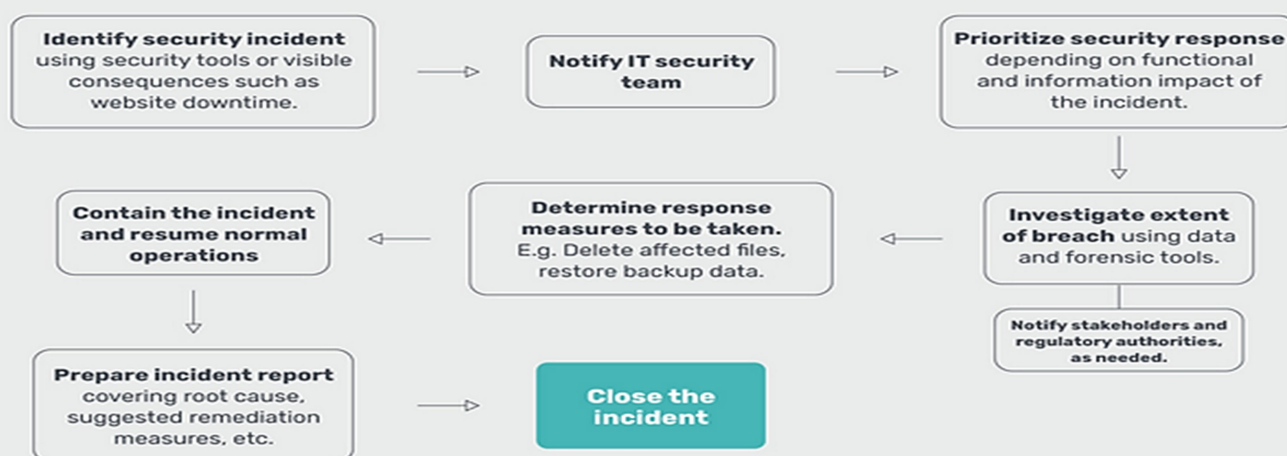
7. Mobile Device Security Policy

With remote work and BYOD (Bring Your Own Device) practices increasing, future versions of the policy will add **Mobile Device Management (MDM)** guidelines, app whitelisting, and secure Wi-Fi practices.

8. Continuous Compliance Monitoring

A longer-term goal is to use lightweight tools or managed services that help small businesses continuously **monitor compliance** with the **DPDP Act, CERT-In mandates**, and the **IT Act** without requiring a dedicated compliance team.

Cybersecurity Incident Response Flowchart



Reference

S.No.	Website
1	DigiLaw India
2	Comparitech
3	The Economic Times
4	Reddit
5	Wikipedia
6	primeinfoserv.com
7	cert-in.org.in
8	StationX