**AI Hackcathon 2025**

**Case Title:** **Cybersecurity Solutions for SMEs in Bangladesh**

**Team Name:** idk what

**Category:** Tech

**Team Lead Full Name:** Shruti Khisa

**Team Lead Email:** shrutikhisa.edu@gmail.com

**Team Lead Contact Number:** 01608909258

**Member 2 Name:** Farhan Tanvir

**Member 3 Name:** Shaira Akhter Diba

**Member 4 Name (if applicable):** Fazli Rabbi Noor

**Date of Submission:** 18/08/2025

## 

Table of Contents

[Problem Summary 3](#_Toc190809746)

[High Vulnerability to Cyber Threats 3](#_Toc190809747)

[Lack of Awareness 3](#_Toc190809748)

[Limited Reporting and Response 3](#_Toc190809749)

[Potential Impact 4](#_Toc190809750)

[Solution 5](#_Toc190809751)

[Proposed Solution 5](#_Toc190809752)

[How It Works 6](#_Toc190809753)

[Key Assumptions & Resources Required 6](#_Toc190809754)

[Risk Management 6](#_Toc190809755)

[Ethical Considerations 7](#_Toc190809756)

[Timeline 8](#_Toc190809757)

[Budget 9](#_Toc190809758)

[Cost Breakdown 9](#_Toc190809759)

[Potential Impact 10](#_Toc190809760)

[Support & Assumptions 11](#_Toc190809761)

**[Executive Summary](#_Toc190809762)****[11](#_Toc190809762)**

[Appendix: 12](#_Toc190809763)

[1. Cybersecurity Awareness Among MSMEs 12](#_Toc190809764)

[13](#_Toc190809765)

[2. Impact of Cybercrime on SMEs 13](#_Toc190809766)

[13](#_Toc190809767)

[3. Survey Results on Cybersecurity Preparedness 13](#_Toc190809768)

[14](#_Toc190809769)

[4. Recommendations from Studies 14](#_Toc190809770)

**[Conclusion](#_Toc190809771)** [15](#_Toc190809771)

## Problem Summary

### High Vulnerability to Cyber Threats

SMEs in Bangladesh are particularly susceptible to cyberattacks, with a staggering 55% of ransomware attacks targeting businesses with fewer than 100 employees [1]. Common threats include fraud, data breaches, and phishing scams, which have become prevalent as more entrepreneurs engage in digital commerce (Cybersecurity Annual Report, 2022). The lack of proper security infrastructure exposes SMEs to significant financial and reputational risks.

### Lack of Awareness

A study revealed that over 92% of micro, small, and medium entrepreneurs are unaware of cybersecurity issues, despite nearly 40% having been victims of cyberattacks [2]. Only 7.7% could identify potential cyber threats, highlighting a critical gap in knowledge that leaves these businesses vulnerable (Inspira Advisory and Consulting Ltd, 2022). Without proper awareness, SMEs fail to adopt even basic cybersecurity measures, making them easy targets for cybercriminals.

### Limited Reporting and Response

Among those who experience cybercrime, only 21.43% report incidents to law enforcement due to a lack of understanding about how to file complaints. This underreporting further complicates the landscape, making it difficult to gauge the full extent of cyber threats facing SMEs (Cybersecurity: A National Priority for Bangladesh, 2021). Additionally, the lack of a centralized incident response system prevents quick mitigation and recovery from cyberattacks. [4]

### **Potential Impact**

Enhancing cybersecurity for SMEs can improve business resilience, reduce financial losses, and increase trust in digital platforms. SMEs contribute 23% of Bangladesh’s GDP, and securing their digital assets will bolster economic stability and job creation. A well-implemented cybersecurity strategy could reduce cyber fraud cases by at least 30% in the first three years of implementation (Cybersecurity Annual Report, 2022). [3]

**Stakeholder Analysis**

A stakeholder analysis of the cybersecurity crisis facing SMEs in Bangladesh reveals several key groups with distinct roles and concerns:

|  |  |  |  |
| --- | --- | --- | --- |
| Group Name | Interest | Influence | Potential Role |
| MSME Owners | Lack cybersecurity knowledge, vulnerable to threats | High | Adopt cybersecurity measures to protect business assets |
| Employees of MSMEs | Targeted in phishing and cyber threats | Medium | Follow cybersecurity best practices |
| Policymakers and Advisors | Address regulatory and policy challenges | High | Develop laws supporting SME cybersecurity |
| Development Partners | Boost cybersecurity practices through advocacy | High | Support initiatives like SARDI to enhance awareness |
| Private Sector Stakeholders | Work with MSMEs in digital sectors | Medium | Provide cybersecurity services and consultation |
| Law Enforcement Agencies | Handle cybercrime reports and enforcement | Medium | Strengthen response systems for reported incidents |
| Cybersecurity Professionals | Improve SMEs' cybersecurity hygiene | High | Offer training and technical support |
| Bangladeshi University Students | Potential contributors to cybersecurity awareness | Medium | Promote knowledge-sharing and advocacy |
| Government Officials | Equip MSMEs with cybersecurity knowledge | High | Implement nationwide cybersecurity education programs |

**Key Considerations:**

* Customized Cybersecurity Awareness Programs: Tailored training programs are necessary to educate SME owners and employees on identifying and mitigating cyber threats effectively.
* Affordable & Scalable Solutions: Implementing cost-effective cybersecurity tools that SMEs can afford and scale as their business grows will increase adoption.
* Strong Policy and Regulatory Support: Effective collaboration between policymakers, industry leaders, and law enforcement is required to enforce cybersecurity standards and streamline reporting procedures.
* Continuous Monitoring & Threat Intelligence: SMEs need continuous risk assessments, security audits, and real-time cyber threat intelligence to stay ahead of evolving threats.
* Public-Private Partnerships for Sustainability: Sustainable cybersecurity initiatives require cooperation between government bodies, private sector stakeholders, and development agencies to provide resources, training, and incentives..

## ****Solution****

### **Proposed Solution**

Our proposed solution, **CyberShield for SMEs**, is a comprehensive, technology-driven cybersecurity framework that enhances security practices for SMEs in Bangladesh. It consists of three core components:

* **Cybersecurity Awareness & Training:** Leveraging insights from initiatives like "Bebshay Digital Shurokkha" (USAID) [4], this component offers online and offline cybersecurity training for SME owners and employees to promote digital hygiene and secure online practices.
* **Affordable Security Suite:** A low-cost software package offering endpoint protection, firewalls, phishing detection, and automated security updates to protect SMEs from evolving cyber threats.
* **SME Cybersecurity Helpline:** A dedicated real-time assistance service that offers SMEs support in responding to cyber incidents, securing their digital assets, and improving cybersecurity posture.

### **How It Works**

* **Training Modules:** Interactive workshops, gamified learning (e.g., "Snakes and Ladders" cybersecurity games), and knowledge tests to assess awareness improvements.
* **Security Suite Implementation:** Lightweight, cloud-based security solutions tailored for SMEs with limited IT resources.
* **24/7 Cyber Helpline:** Instant access to cybersecurity experts for real-time troubleshooting and guidance.

### **Key Assumptions & Resources Required**

* SMEs will be willing to adopt cybersecurity practices if they are affordable and easy to implement.
* Government and private sector stakeholders will support policy improvements and funding.
* Digital transformation among SMEs will continue to grow, necessitating better cybersecurity solutions.
* Resources required include cloud infrastructure, training materials, cybersecurity professionals, and funding from development partners.

## ****Risk Management****

**Identified Risks & Mitigation Strategies**

| **Risk (Describe the risk and who can be impacted)** | **Mitigation (Steps before, during, or after implementation)** | **Who can help with mitigation?** |
| --- | --- | --- |
| **Low Adoption by SMEs** – Many SMEs lack awareness and perceive cybersecurity as unnecessary. | Implement targeted awareness campaigns, offer financial incentives, and create simplified security solutions tailored for SMEs. | Government, Banks, Cybersecurity Firms |
| **High Implementation Costs** – SMEs may struggle with affordability for robust cybersecurity solutions. | Develop cost-effective, scalable solutions with potential subsidies from the government and financial institutions. | Private cybersecurity firms, Government, NGOs |
| **Lack of Technical Expertise** – SMEs often lack in-house IT teams to manage cybersecurity tools. | Offer training programs, deploy easy-to-use security tools, and establish dedicated SME cybersecurity support hubs. | Universities, IT Consultants, Government Initiatives |
| **Phishing & Malware Attacks** – SMEs frequently fall victim to phishing and malware attacks, leading to financial and data losses. | Implement security awareness training, enforce email security protocols, and deploy anti-malware solutions. | Cybersecurity Professionals, Private Security Providers |
| **Data Breaches & Unauthorized Access** – Customer and business data could be compromised, leading to financial and reputational harm. | Use multi-factor authentication (MFA), strong encryption, and conduct regular security audits. | IT Security Firms, Government Agencies |
| **Regulatory Non-Compliance** – SMEs may fail to meet legal and regulatory cybersecurity requirements. | Provide compliance checklists, legal advisory services, and regular audits to ensure SMEs meet standards. | Legal Experts, Government Regulators |
| **Incident Response & Recovery** – SMEs often lack structured plans for responding to cyber incidents, leading to extended downtimes. | Develop incident response frameworks, create helpline support for SMEs, and establish recovery assistance programs. | Government, Cybersecurity Firms, Industry Associations |

### **Ethical Considerations**

* **· Loss of Data Control:** Outsourcing IT services, including cybersecurity, leads to a loss of data control, impacting confidentiality, integrity, and availability.
  + Mitigation: Implement robust Service Level Agreements (SLAs) that specify data management, security, and privacy criteria.
* **Transparency and Communication:** Ensuring transparent reporting and clear communication is essential for SMEs outsourcing cybersecurity services.
  + Mitigation: Establish clear communication channels and reporting standards within the SLA to maintain transparency.
* **Dependency and Loss of Internal Competence:** SMEs relying on outsourced cybersecurity providers may lose technical skills internally.
  + Mitigation: Retain some internal cybersecurity expertise to oversee outsourced operations and ensure ethical security practices.
* **SLA Compliance and Trust:** Without well-defined SLAs, outsourced providers may fail to meet security standards, leading to increased vulnerabilities.
  + Mitigation: Ensure SLAs include agreements on reliability, uptime, performance metrics, and response times to uphold accountability.
* **Inconsistent Turnaround Times:** Cybersecurity providers managing multiple clients may prioritize larger clients, delaying responses to SME security issues.
  + Mitigation: Negotiate SLAs that prioritize response times and ensure providers allocate sufficient resources for SMEs.

## Timeline

**Project Phases & Key Milestones**

| **Phase** | **Milestone** | **Expected Completion Date** |
| --- | --- | --- |
| **Phase 1: Research & Planning** | **Conduct cybersecurity risk assessment for SMEs** | **Month 1** |
| **Phase 2: Awareness Program** | **Develop and launch SME-focused cybersecurity training** | **Month 2-3** |
| **Phase 3: Security Implementation** | **Deploy cost-effective cybersecurity tools for SMEs** | **Month 4-5** |
| **Phase 4: Incident Response Setup** | **Establish SME cybersecurity helpline** | **Month 6** |
| **Phase 5: Monitoring & Optimization** | **Conduct regular audits and performance reviews** | **Month 7-9** |
| **Phase 6: Scaling & Sustainability** | **Expand program reach and partnerships** | **Month 10-12** |

## ****Budget****

### **Cost Breakdown**

| **Expense Category** | **Details** | **Estimated Cost (BDT)** |
| --- | --- | --- |
| **Software Development** | Security tools, mobile apps, backend systems | 5,00,000 |
| **Training & Awareness** | Workshops, online modules, training materials | 3,00,000 |
| **Incident Response Setup** | SME cybersecurity helpline infrastructure | 2,50,000 |
| **Marketing & Outreach** | Campaigns, social media, partnerships | 1,50,000 |
| **Personnel & Support** | Hiring cybersecurity trainers, consultants | 4,00,000 |
| **Compliance & Audits** | Regular security audits, compliance checks | 1,50,000 |
| **Maintenance & Updates** | Continuous system upgrades, security patches | 2,00,000 |
| **Total Estimated Cost** | **Overall budget requirement** | **14,50,000** |

**Assumptions:**

* Training will be conducted in collaboration with government agencies and NGOs to minimize costs.
* Open-source cybersecurity tools will be utilized where possible.
* Cloud infrastructure will be leveraged to reduce hosting and maintenance expenses.

### **Potential Impact**

Cybersecurity implementation in SMEs will have significant positive impacts across multiple areas:

* **Business Continuity & Economic Stability**: By reducing cyber threats, SMEs can avoid operational disruptions, ensuring stable revenue and contributing to Bangladesh’s economy. Since SMEs make up 99% of private sector manufacturing, cybersecurity protection can prevent economic downturns caused by business closures due to cyberattacks.
* **Customer Trust & Reputation**: Enhanced cybersecurity will improve customer confidence in digital transactions, allowing SMEs to grow their online presence while protecting customer data from breaches.
* **Reduced Financial Losses**: SMEs often struggle to recover from cyberattacks due to limited resources. Implementing security measures will lower risks of fraud and extortion, reducing the financial burden of cyber incidents.
* **Regulatory Compliance & Legal Protection**: Compliance with cybersecurity standards will shield SMEs from legal liabilities and penalties, helping them align with national and international data protection regulations.
* **Innovation & Digital Growth**: Secure IT infrastructure will allow SMEs to embrace new technologies such as e-commerce platforms and digital payment systems without fear of cyber threats.
* **Workforce Skill Development**: Through cybersecurity training, SME employees will enhance their digital literacy, reducing human error as a leading cause of cyber incidents.

### **Support & Assumptions**

* **Government & Private Sector Support**: Policies such as the SARDI Cybersecurity Awareness Campaign highlight the importance of collaborative cybersecurity initiatives.
* **Growing Digital Adoption**: SMEs are increasingly shifting towards digital platforms, making cybersecurity essential for sustainable growth.
* **High Financial Impact of Cyber Incidents**: Reports show that SMEs spend between $826 and $653,587 annually recovering from cyber incidents, making proactive security solutions cost-effective.

# Executive Summary

| Item | Description |
| --- | --- |
| Problem Summary | SMEs in Bangladesh are highly vulnerable to cyberattacks, with 55% of ransomware attacks targeting businesses with fewer than 100 employees. Lack of awareness, insufficient security infrastructure, and underreporting of incidents expose SMEs to financial losses and reputational damage. |
| Potential Impact | Implementing cybersecurity solutions will enhance business resilience, reduce financial losses, and increase trust in digital transactions. It will ensure regulatory compliance, support digital innovation, and improve workforce skills. Cyber fraud cases could reduce by 30% within three years. |
| Stakeholder Analysis | Key stakeholders include SME owners, employees, policymakers, development partners, private sector stakeholders, law enforcement, cybersecurity professionals, university students, and government officials. Their roles range from policy-making to technical training and incident response. |
| Solution | CyberShield for SMEs includes cybersecurity awareness training, an affordable security suite with endpoint protection and firewalls, and a 24/7 SME cybersecurity helpline to assist with incident response and digital security. |
| Risk Management | Risks include low adoption rates, high implementation costs, lack of technical expertise, and phishing/malware threats. Mitigation strategies include awareness campaigns, financial incentives, training, encryption, and compliance support. |
| Timeline | The project follows a 12-month structured rollout, covering risk assessments, training programs, security tool deployment, helpline setup, monitoring, and scaling. |
| Budget | Estimated total cost: BDT 14,50,000, covering software development, training, incident response, marketing, personnel, compliance audits, and maintenance. |
| Impact | Cybersecurity implementation will prevent financial losses, improve customer trust, ensure regulatory compliance, and promote digital transformation, ensuring long-term SME growth and resilience. |

## ****Appendix:****

This appendix includes data and findings that support the potential success of CyberShield for SMEs in Bangladesh, focusing on the current cybersecurity landscape and the need for effective solutions.

### **1. Cybersecurity Awareness Among MSMEs**

A recent study highlights that **92% of micro, small, and medium enterprises (MSMEs) in Bangladesh are unaware of cybersecurity**. This lack of awareness is alarming, especially as around **40% of these entrepreneurs have been victims of cyberattacks**. The study indicates that only **7.7% can identify cyber threats**, emphasizing the urgent need for educational initiatives in this sector. [1][2]

**Table 1: Cybersecurity Awareness Among MSMEs**

| **Awareness Metric** | **Percentage** |
| --- | --- |
| Unaware of Cybersecurity | 92% |
| Experienced Cyberattack | 40% |
| Can Identify Cyber Threats | 7.7% |
| Believe Cybersecurity is Relevant | 18% |
| Reported Cyber Incidents to Authorities | 21.43% |

### **Sardi-2**

### **2. Impact of Cybercrime on SMEs**

The financial implications of cybercrime on SMEs are significant. The following table summarizes the average costs associated with cyber incidents reported by SMEs:

**Table 2: Financial Impact of Cybercrime on SMEs**

| **Metric** | **Value (BDT)** |
| --- | --- |
| Average Cost per Cyberattack | 250,000 |
| Average Downtime per Attack (Hours) | 48 |
| Average Data Breach Cost | 400,000 |
| Total Annual Loss (Estimated) | 5,00,00,000 |

### **enisa_07072021**

### **3. Survey Results on Cybersecurity Preparedness**

An assessment conducted among MSME owners indicates a critical gap in cybersecurity preparedness: [5]

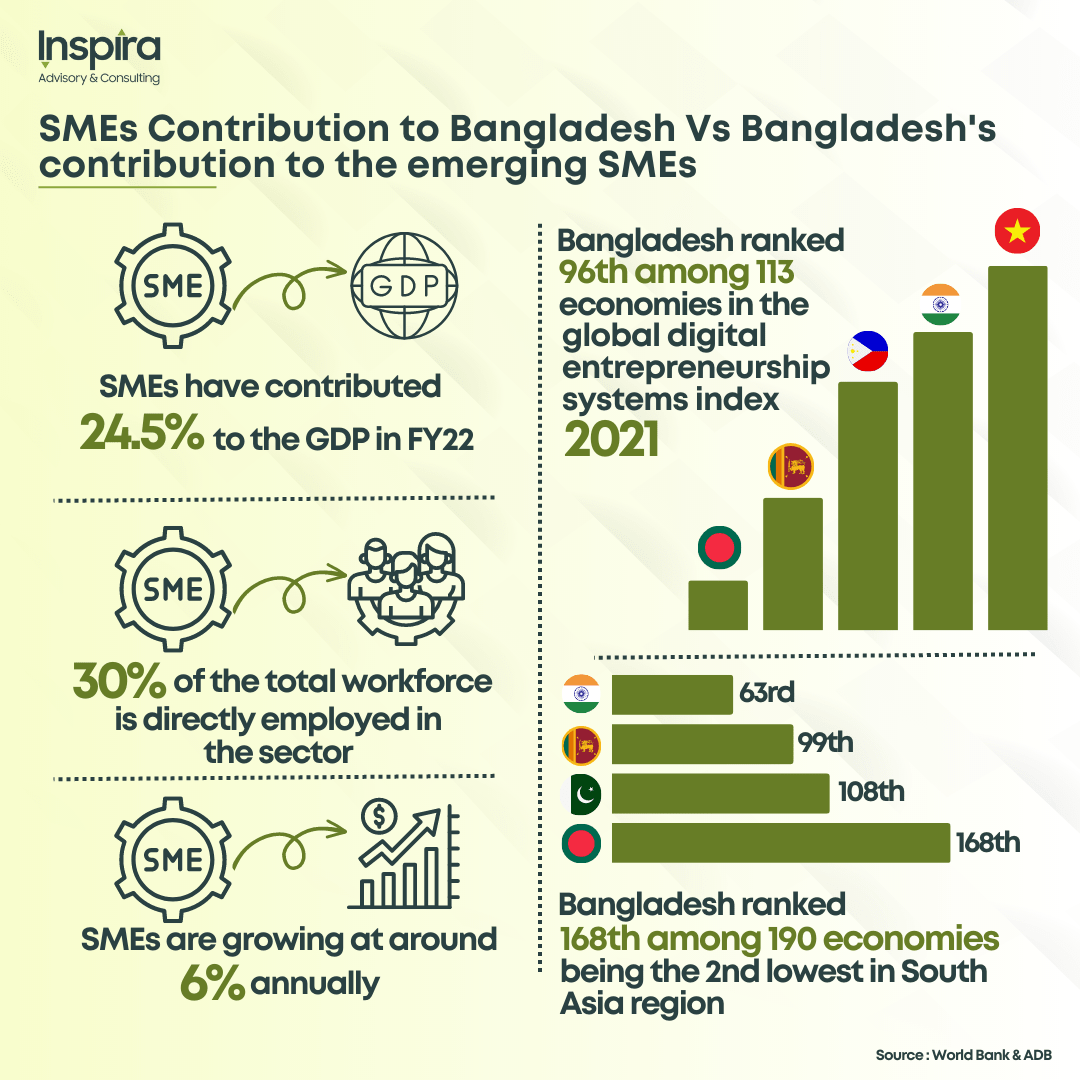
**Table 3: Survey Results on Cybersecurity Preparedness**

| **Preparedness Metric** | **Percentage** |
| --- | --- |
| Use Digital Tools for Business | 47% |
| Familiarity with Cybersecurity Measures | 31% |
| Implemented Basic Security Measures | 15% |

### **bangladesh-cybersecurity-market-size-image-1735473881546**

### **4. Recommendations from Studies**

The studies recommend launching comprehensive awareness campaigns targeting MSMEs to address the gaps in knowledge and practices regarding cybersecurity. Such campaigns could significantly enhance the understanding and implementation of cybersecurity measures among entrepreneurs .



### **Conclusion**

The data presented underscores a pressing need for effective cybersecurity solutions tailored for SMEs in Bangladesh. The overwhelming lack of awareness and high incidence of cybercrime indicate that initiatives like CyberShield can play a crucial role in safeguarding these businesses against growing cyber threats.

**Referencing:**

1. “SARDI Cybersecurity Awareness Campaign for MSMEs in Bangladesh | Inspira Advisory and Consulting Ltd.,” *Inspira Advisory and Consulting Ltd.*, Sep. 18, 2023. <https://inspira-bd.com/case-studies/sardi-cybersecurity-awareness-campaign-for-msmes-in-bangladesh/>
2. T. Report, “92% MSME entrepreneurs unaware of cyber security: Study,” *The Business Standard*, Oct. 26, 2022. [Online]. Available: <https://www.tbsnews.net/bangladesh/92-msme-entrepreneurs-unaware-cyber-security-study-520674>
3. Awal, M. (2022, June 27). What is the impact of cybercrime on SMEs? The Business &

Financial Times. <https://thebftonline.com/2022/06/27/what-is-the-impact-of-cybercrime-on-smes>

1. *Cyber crime trend in Bangladesh, an analysis and ways out to combat the threat | IEEE*

*Conference Publication | IEEE Xplore*. (n.d.). Ieeexplore.ieee.org. Retrieved November

27, 2023, from <https://ieeexplore.ieee.org/document/8323800>

1. [4] Digital Frontiers, "Final Report on SARDI SME Cybersecurity Awareness Campaign," 2023. [Online]. Available: https://files.digitalfrontiersdai.com/media/documents/Revised\_Campaign\_Final\_Report\_SARDI\_SME\_Cybersecurity\_Awareness\_Campaign.pdf. [Accessed: 18-Aug-2025].