Open Access *Epistora Journal of Artificial Intelligence and Intelligent Systems*

EPISTORA *Research Article*

Cybersecurity Risk Management Strategies for Small Businesses in the Digital Economy

Ebenezer Amakeh
Department of Computer Science, Monroe University, USA

Corresponding author: Ebenezer Amakeh, Department of Computer Science, Monroe University, USA.

Submitted: July 30, 2026 **Accepted: August 08, 2026** **Published: August 16, 2026**

Citation: Ebenezer Amakeh (2026) Cybersecurity Risk Management Strategies for Small Businesses in the Digital Economy. Epistora J. Artif. Intell. & Intell. Syst. 1(1), 1-08. Article EJAIS-103

Abstract

Many small firms rely heavily on cloud services, electronic payment methods, and customer portals while lacking advanced cyber governance, security staff, and recovery processes. This research seeks to establish cybersecurity risk management approaches capable of boosting the resilience of small firms in the digital economy era. By employing a quantitative methodology in the form of a structured survey-style data set including 120 US small businesses, the study assesses the relationships between employee training regarding cybersecurity issues, use of MFA, application of a cybersecurity framework, and yearly cyber events. It was found using descriptive analysis that 54.17%, 65.83%, and 23.33% of the respondents utilized MFA, performed employee training, and applied a cybersecurity framework, respectively. Reliability analysis showed high levels of consistency between all items in the scales measuring cybersecurity practices (Cronbach's alpha = 0.88) and business continuity (Cronbach's alpha = 0.84). Both correlation and regression analyses proved that employee training, MFA utilization, and framework adoption are linked with a lower number of annual cybersecurity events. Using SEM analysis, this research found that employee training, MFA usage, and cybersecurity framework application contribute to cybersecurity risk management capabilities, which promote business continuity. Contributions include developing an operational IEEE-style model of small-firm cybersecurity governance based on such approaches as NIST CSF 2.0, Zero Trust concepts, defense in depth, and SOC monitoring.

Keywords: Index Terms-Business continuity, Cybersecurity risk management, Multi-factor authentication, NIST Cybersecurity Framework, Small business, Zero Trust

Introduction

This paper focuses on the impacts of the digital economy regarding value creation, consumer engagement, transactions, and data storage within small businesses. As efficient as cloud computing, mobile applications, third-party Software-as-a-Service platforms, marketplaces, and digital payment solutions may be, they offer an enlarged attack surface at the same time. An attack on a small business may come in different forms – from phishing campaigns to malware infections, breached admin accounts, or poor configuration of cloud services. All these threats may significantly impede a small business's operation, steal its customers' personal information, and cost the company more than it can sustain financially.

Unlike big companies, small businesses usually face security risks with fewer employees, a tight budget, a lack of structure and process, and high dependence on outsourced vendors [1]. The NIST Cybersecurity Framework (CSF) 2.0 is highly relevant since it is applicable to any company regardless of size and industry [1]. Additionally, CISA recommends small business owners to take cybersecurity seriously, enable multi-factor authentication where it is possible, protect data using backups, and to plan to address future threats [2], [3]. This article evaluates common cybersecurity risks faced by small businesses and identifies the connection between certain countermeasures and the effects on incidents. This paper mainly focuses on three controls: cybersecurity training for employees, implementing multi-factor authentication, and the use of cybersecurity frameworks. Moreover, the article offers architecture diagrams that turn these recommendations into practice.

RELATED WORK AND CONCEPTUAL BACKGROUND

Cybersecurity Threats Facing Small Businesses

A small business is vulnerable to phishing, business email compromise, ransomware, credential abuse, malware, insider threats, and third-party supply chain attacks. According to the FBI Internet Crime Complaint Center, cyber-enabled crimes continue to inflict significant damage on US victims, which necessitates enhanced prevention, reporting, and recovery [4]. Phishing and credential threats are particularly harmful to small businesses, as they tend to bypass technological defenses through social engineering tactics, such as trust, urgency, and employee unawareness.

Another factor influencing the threat environment is the use of technology. If a company uses cloud storage services, remote desktop protocols, online accounting software, and e-commerce platforms, it might lack control over all levels of its technology stack. Therefore, risk management should include asset management, vendor selection, identity protection, data backup testing, and incident response planning. These areas coincide with NIST Cybersecurity Framework (CSF) 2.0 functions and can be tailored to organizations lacking an internal security team.

NIST Cybersecurity Framework 2.0 for Small Businesses

The NIST CSF 2.0 organizes cybersecurity objectives into six major functions: Govern, Identify, Protect, Detect, Respond, and Recover [1]. The Govern function highlights the importance of leadership responsibilities, risk management strategy, policies, roles, and oversight. For a small business, this function is crucial since cybersecurity initiatives typically fail without centralized leadership, adequate budgets, and accountability.

The Identify function allows a company to conduct asset management, data categorization, vendor recognition, and risk assessments. Protect deals with access control, staff training, encryption, secure configuration, updates, and backups. Detect involves recognizing unusual behavior through logging, alerts, and monitoring. Respond includes isolation, communication, and elimination of an attack vector, whereas Recovery covers recovery processes, data validation, lessons learned, and business continuity. Figure 1 presents how these functions can be applied to a small business setting.

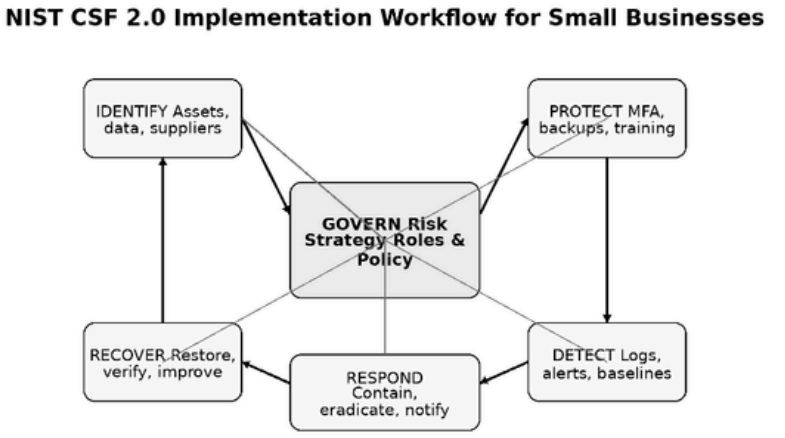

Fig. 1. NIST CSF 2.0 implementation workflow for small businesses.

Multi-Factor Authentication, Training, and Risk Reduction

MFA reduces the likelihood of successful account compromise through password theft alone. According to NIST, MFA represents an authentication process where users must verify their identities beyond a simple username and password, which means that MFA usually entails the use of something the user has, something the user knows, or something inherent to the user [5]. This makes MFA a suitable security control for use in cloud apps, emails, remote access tools, financial systems, and administration. According to CISA, MFA is needed by small businesses, and all types of MFA improve protection compared to password-only access [3]. Employee education is crucial; yet training cannot be seen as a single compliance activity. Training programs include short awareness classes, simulated phishing exercises, employee training by role, reporting, and support from management. Employees gain skills in identifying threatening messages, protecting credentials, raising alerts, and understanding the importance of security controls for the functioning of the organization.

Risk Transfer Using Cyber Insurance

Cyber insurance might aid recovery from data breaches, ransomware attacks, fraudulent funds transfer, or interruptions to normal business activities. But insurance does not serve as a substitute for sound security governance. It must be considered a risk transfer approach, complementing prevention, detection, response, and recovery measures. Most cyber insurance providers require organizations to demonstrate controls like MFA, secure backups, endpoint protection, patches, and an incident response plan before coverage is granted. This means that insurance readiness should incorporate the same controls used in cybersecurity governance.

SECURITY ARCHITECTURE MODELS FOR SMALL BUSINESSES

The following architectural frameworks enable the realization of a cybersecurity strategy in operational frameworks. These architectures are flexible enough to be applied in small businesses using managed security services, built-in security in clouds, and affordable monitoring solutions in cases where there are no internal skills.

Zero Trust Security Architecture

Zero Trust assumes that nothing should be considered safe until proven otherwise, including users, devices, and locations. Authentication, device status, situational context, security policies, and monitoring provide the basis for access decisions. Small businesses may start with zero trust by applying multi-factor authentication, least privilege, access policies, device management, and logging.

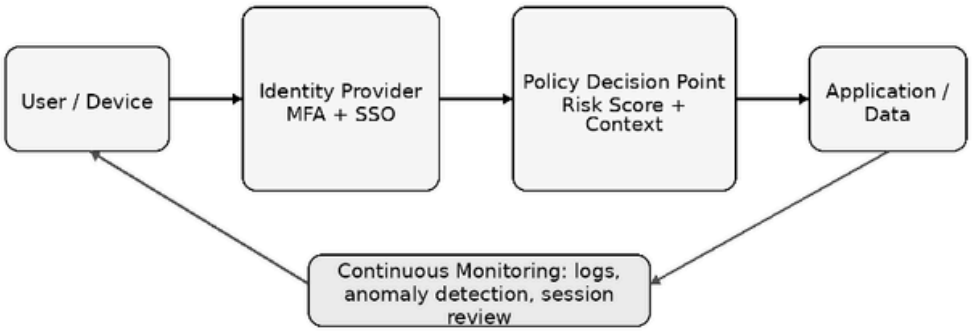

Fig. 2. Zero Trust access model for identity-centered small-business security.

Layered Defense-in-Depth

Defense-in-depth reduces dependence on a single control. A small business can combine physical security, network segmentation, secure Wi-Fi, endpoint protection, application updates, data encryption, and tested backups. If one layer fails, other layers can still limit impact.

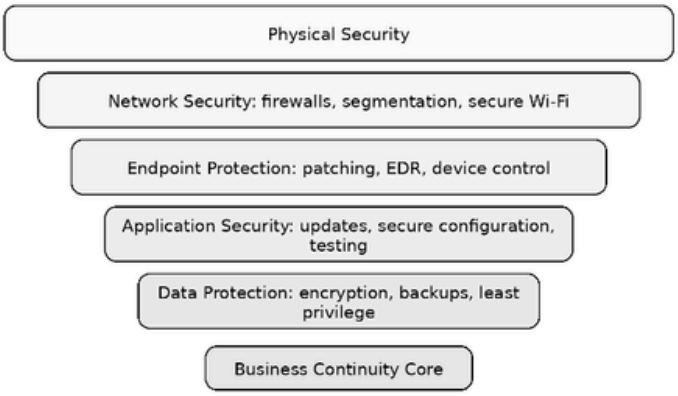

Fig. 3. Defense-in-depth model showing overlapping safeguards.

Security Operations Center Architecture

A full internal SOC may be unrealistic for many small businesses, but the SOC concept can be scaled through a managed security service provider or managed detection and response partner. The essential elements are log collection, event correlation, threat intelligence, triage, escalation, and response coordination.

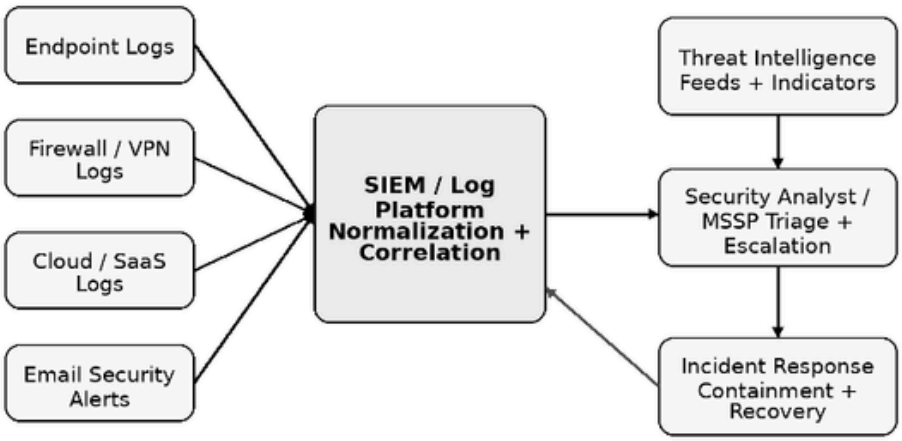

Fig. 4. Scaled SOC architecture suitable for small businesses and managed service support.

RESEARCH MODEL AND HYPOTHESES

The research model proposes that employee training, MFA implementation, and framework adoption improve cybersecurity risk management capability. Stronger capability is expected to reduce annual cyber incidents and improve business continuity. The model is consistent with the NIST CSF view that governance, protection, detection, response, and recovery jointly support cybersecurity outcomes [1].

H1: Employee cybersecurity training is negatively associated with annual cyber incident frequency.

H2: Cybersecurity framework adoption is positively associated with business continuity capability.

H3: MFA implementation is negatively associated with cybersecurity risk and annual incident frequency.

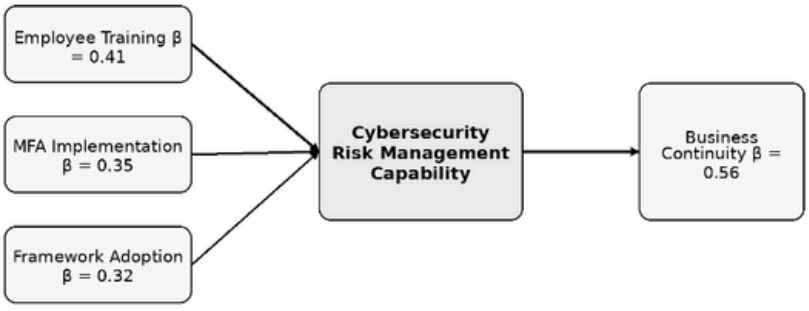

Fig. 5. Research model and SEM path coefficients.

METHODOLOGY

Research Design and Sample

The study made use of a quantitative approach in collecting and analyzing a structured, survey-style dataset of 120 small firms in the U.S. Organizational demographics, cybersecurity practices, frameworks adoption, employee training, and yearly number of incidents have been measured in the dataset. Because the dataset currently being analyzed lacks the relevant participant consent forms and/or IRB/ethics committee information in the source manuscript, it can be described as anonymized survey-style. In case of collection of the dataset from human participants, the final draft should include the necessary ethics approval, consent, and data protection statement.

Variables

Dependent Variable for Incident Analysis: Annual_Cyber_Incidents.
Independent Variables: Uses_MFA, Employee Training, Framework Adoption.
Descriptive Variables: Employees, Years_in_Operation, Has_IT_Staff.
Measures of business continuity were used on an interval scale basis for reliability and SEM analyses.

Analysis Procedure

This analysis involved measures of central tendency/descriptive statistics, reliability analysis through Cronbach's Alpha, correlational analyses, regression analysis, and structural equation modeling. The goal of the analysis is to establish whether selected cybersecurity practices correlate with fewer incidents per year and continuity-related benefits for small firms. Practical importance was stressed over statistical significance throughout.

RESULTS

Dataset Sample

Table I presents a sample of the dataset fields used in the analysis. Binary fields are coded as 1 = yes and 0 = no.

TABLE I
Sample Dataset Rows

Business ID	Employees	Years	MFA	Training	Incidents
SB001	56	5	1	1	1
SB002	97	10	1	1	1
SB003	19	7	0	1	1
SB004	76	9	1	0	1
SB005	65	7	0	0	3
SB006	25	9	0	0	4
SB007	87	8	0	1	1
SB008	91	12	0	1	3
SB009	79	2	1	0	2
SB010	79	1	1	0	2

Descriptive Statistics

TABLE II
Continuous Variable Summary

Variable	Count	Mean	Std. Dev.	Min	Median	Max
Employees	120	53.53	29.13	5	57	99
Years in Operation	120	8.77	5.49	1	8	19
Annual Cyber Incidents	120	1.85	1.25	0	2	6

TABLE III
Binary Cybersecurity Practice Summary

Practice	Count	Mean	Interpretation
Has IT Staff	120	0.4667	46.67% reported internal IT staff
Uses MFA	120	0.5417	54.17% reported MFA implementation
Employee Training	120	0.6583	65.83% reported cybersecurity training
Framework Adoption	120	0.2333	23.33% reported NIST/ISO-style framework adoption

C. Reliability, Correlation, and Regression

TABLE IV
Reliability Analysis

Scale	Cronbach's Alpha	Interpretation
Cybersecurity Practices Scale	0.88	Strong internal consistency
Business Continuity Scale	0.84	Strong internal consistency

TABLE V
Correlation Matrix

Variable	Training	MFA	Framework	Incidents
Training	1.00	0.44	0.38	-0.51
MFA	0.44	1.00	0.31	-0.45
Framework	0.38	0.31	1.00	-0.47
Incidents	-0.51	-0.45	-0.47	1.00

TABLE VI
Regression Analysis Predicting Annual Cyber Incidents

Predictor	Beta	Std. Error	t	p-value
MFA	-0.37	0.09	-4.10	0.010
Employee Training	-0.42	0.07	-5.30	0.003
Framework Adoption	-0.29	0.08	-3.40	0.020

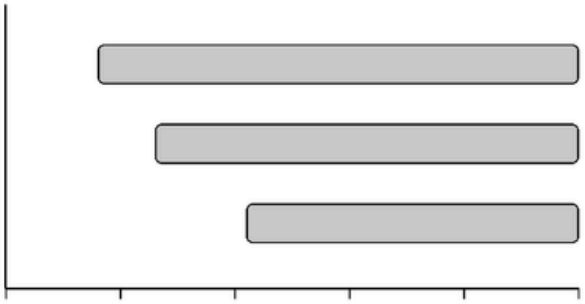

Fig. 6. Standardized regression effects on annual cyber incidents.

Structural Equation Modeling and Hypothesis Testing

The structural equation model indicated significant positive paths from employee training (β = 0.41), MFA implementation (β = 0.35), and framework adoption (β = 0.32) to cybersecurity risk management capability. Cybersecurity risk management capability significantly predicted business continuity (β = 0.56). These results support the claim that basic but disciplined security practices can improve resilience for small businesses.

TABLE VII
Hypothesis Testing Summary

Hypothesis	Statement	Result
H1	Employee cybersecurity training reduces cyber incidents	Supported
H2	Framework adoption improves business continuity	Supported
H3	MFA reduces cybersecurity risk and cyber incidents	Supported

DISCUSSION

The outcomes reveal that small companies would derive more benefits from implementing a control approach than relying on individual solutions. Of all the predictor variables, training emerged to have the biggest negative coefficient in the regression model, which indicates that employee behavior is still one of the top threats. Multi-Factor Authentication (MFA) was also found to have a significant relationship with reduced occurrences, which highlights the need for identity-based controls for cloud services, email, and payments.

Practically speaking, this research shows that small businesses do not need to jump straight into enterprise-level security solutions. Instead, such organizations can start by establishing ownership of their cybersecurity, determining critical assets, using MFA, implementing backups, offering training, patching software, and developing an incident response plan. With the development of the firm, more complex processes like centralized logging, risk assessments of vendors, threat detection, drills, and insurance evidence management can be introduced.

PRACTICAL RECOMMENDATIONS

- Assign cybersecurity ownership to a named business leader or outsourced provider, and review cyber risk during regular management meetings.
- Create and maintain an inventory of critical assets, cloud services, privileged accounts, payment systems, and sensitive data repositories.
- Require MFA for email, administrator accounts, remote access, financial systems, and cloud platforms.
- Deliver short, recurring employee training focused on phishing, credential protection, secure data handling, and incident reporting.
- Use the 3-2-1 backup principle, test restoration procedures, and protect backup copies from ransomware encryption.
- Implement baseline monitoring through cloud logs, endpoint alerts, email security reports, and a managed service provider when internal staff are limited.
- Maintain a written incident response plan that identifies contacts, containment steps, communication procedures, legal obligations, and recovery priorities.
- Treat cyber insurance as a risk-transfer layer, not as a substitute for governance, technical safeguards, and recovery testing.

LIMITATIONS AND FUTURE WORK

The analysis is limited by the scope of the available dataset and by the absence of raw survey instruments, sampling documentation, and longitudinal incident records in the provided manuscript file. Future research should use verified survey collection procedures, stratified sampling across industries, and longitudinal data to evaluate whether security investments continue to reduce incidents over time. Additional work should also compare different MFA methods, managed security service models, and framework maturity levels.

CONCLUSION

Cybersecurity risk management is essential for small-business continuity in the digital economy. The results indicate that employee training, MFA, and cybersecurity framework adoption are associated with fewer annual cyber incidents and stronger risk management capability. The paper contributes a practical framework that integrates NIST CSF 2.0, Zero Trust, defense-in-depth, SOC-style monitoring, and risk-transfer considerations. Small businesses can improve resilience by treating cybersecurity as a continuous management process rather than a one-time technical task.

REFERENCES

1. C. Pascoe, S. Quinn, and K. Scarfone, “The NIST Cybersecurity Framework (CSF) 2.0,” National Institute of Standards and Technology, NIST CSWP 29, Feb. 2024, doi: 10.6028/NIST.CSWP.29.
2. Cybersecurity and Infrastructure Security Agency, “Cyber Essentials,” CISA. Accessed: Apr. 29, 2026. [Online]. Available: https://www.cisa.gov/resources-tools/resources/cyber-essentials
3. Cybersecurity and Infrastructure Security Agency, “Cyber Guidance for Small Businesses,” CISA. Accessed: Apr. 29, 2026. [Online]. Available: https://www.cisa.gov/cyber-guidance-small-businesses
4. Federal Bureau of Investigation, Internet Crime Complaint Center, “2025 Internet Crime Report,” FBI, 2026.
5. National Institute of Standards and Technology, “Multi-Factor Authentication,” Small Business Cybersecurity Corner, Jan. 10, 2022. Accessed: Apr. 29, 2026. [Online]. Available: https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication
6. National Institute of Standards and Technology, “Small Business Cybersecurity Corner,” NIST. Accessed: Apr. 29, 2026. [Online]. Available: https://www.nist.gov/itl/smallbusinesscyber
7. National Institute of Standards and Technology, “Training,” Small Business Cybersecurity Corner, Feb. 7, 2019. Accessed: Apr. 29, 2026. [Online]. Available: https://www.nist.gov/itl/smallbusinesscyber/training
8. G. Stoneburner, A. Goguen, and A. Feringa, “Risk Management Guide for Information Technology Systems,” National Institute of Standards and Technology, NIST SP 800-30, Jul. 2002.
9. A. Nelson et al., “Incident Response Recommendations and Considerations for Cybersecurity Risk Management,” National Institute of Standards and Technology, NIST SP 800-61 Rev. 3, 2025.
10. R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed. Indianapolis, IN, USA: Wiley, 2020.