Bachelor's thesis

Information and Communications Technology

2025

Jacob Mdaki

A Hybrid Cybersecurity Framework for Small Businesses

- Integrating NIST CSF, ISO 27001, and CEO Engagement

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Bachelor’s Thesis | Abstract

Turku University of Applied Sciences

Information and Communications Technology

2025 | 22

Jacob Mdaki

A Hybrid Cybersecurity Framework for Small Businesses

- Integrating NIST CSF, ISO 27001, and CEO Engagement

Small businesses face escalating cyber threats but often lack the resources to implement robust defenses. This thesis proposes a hybrid cybersecurity framework integrating NIST CSF, ISO 27001, and CEO proactive culture to address business vulnerabilities. Through a literature review the study identifies and recommends a framework that prioritizes cost effective controls such as multifactor authentication, regular audits and leadership engagement to foster a proactive security culture. These findings suggest that small businesses can significantly mitigate risks by adopting a phased approach combining NIST’s flexibility with ISO 27001’s structured governance. The thesis concludes with actionable steps for implementation and continuous improvement, offering a scalable model for small businesses.

Keywords:

Cybersecurity, Hybrid framework, ISO 27001, NIST CSF, Small business

Contents

Figures

Tables

List of abbreviations

CIS	Center for Internet Security
CISA	Cybersecurity Infrastructure Security Agency
CSF	Cybersecurity Framework
IEC	International Electrotechnical Commission
IRP	Incidence Response Plan
ISMS	Information Security Management Systems
ISO	International Organization for Standardization
MFA	Multifactor Authentication
NIST	National Institute of Standards and Technology
SME’S	Small and Medium Enterprises
SIEM	Security Information and Event Management

1 Introduction

This thesis explores the best possible cybersecurity framework for small businesses. The topic was selected based on a small ICT business company need for a framework. As technology advances, small businesses are targeted with various cyberattacks as most of these businesses have no or low experiences in these fields. Recent industry research reveals a 60% failure rate among small businesses within six months of experiencing a data breach (Verizon, 2024), underscoring the critical need for robust cybersecurity frameworks.

Therefore, this thesis provides a framework that could protect and guide a small business onto a safer and precautious path while avoiding the negative impacts of cyber-attacks. The goal is to explore various updated cybersecurity information sharing platforms and pick out critical resources that could be used by the business to navigate through a modern age cyber business world with low or no consequences.

This thesis aims to answer the question of how small businesses can leverage a hybrid framework to mitigate cyber risks. The content begins with statistics collected from a Verizon Report 2024, followed by National Institute of Standards and Technology Cybersecurity Framework (NIST), International Organization for Standardization (ISO) 27001, CEO proactive culture from Cybersecurity Infrastructure Security Agency (CISA)and concludes with a recommended framework. A small business can be defined as any business with limited resources, personnel and experience.

2 Statistical Analysis

To contextualize the critical cybersecurity challenges facing small businesses, statistical evidence reveals alarming trends in cyber-attacks. These demand immediate action from small businesses. Ransomware attacks have increased by 32% since 2018, Figure 1 establishes this by showing attacking methods used over time in cyber systems.

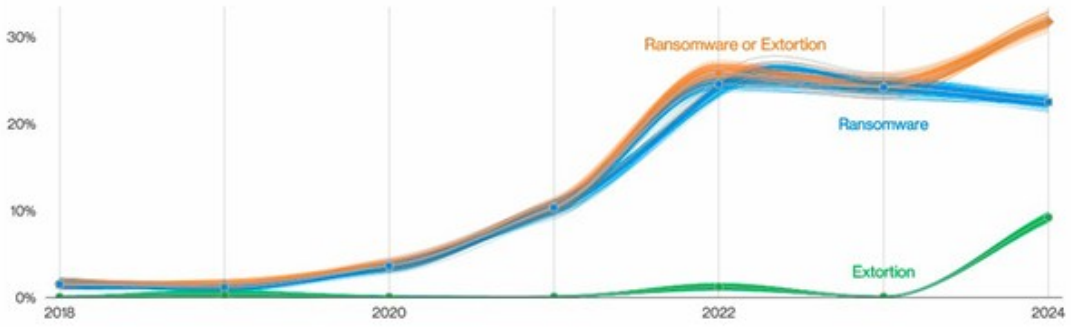

Figure 1. Ransomware and extortion breaches over time (Verizon, 2024, p.7).

Recent cybersecurity research reveals that human factors constitute the most significant vulnerability in any organizational defences, leading to 68% of all breaches (Verizon, 2024, p.8). This statistic highlights three critical implications for small business security frameworks:

1. Workforce Training Imperative: The dominance of human related breaches demonstrates that technical controls alone are insufficient without comprehensive employee cybersecurity awareness programs.
2. Framework integration: Effective security frameworks should be incorporated behavioural elements, such as mandatory phishing simulations and role-based access controls to mitigate human error.
- Continuous reinforcement: As cyberattacks technology evolves, for-example, AI-enhanced social engineering. Periodic training updates become essential rather than optional.

Before detailing our framework, Figure 2 establishes statistical evidence of the critical significance of the human element in cyber security.

Figure 2. Key breach components (Verizon, 2024, p.8).

3 Internal Business Cross-sections with NIST

Understanding how business channels are connected is required in establishing a cybersecurity framework for a business. According to NIST (Burkhardt, n.d. p.4), there are 5 steps which can be taken to achieve this which include identifying organizational context, analysing and prioritizing risks, conducting workforce assessments, identifying and planning workforce responses, implementing, evaluating and adjusting responses.

3.1 Identifying organizational context

The first step towards establishing a working framework is that the business should take time and effort to obtain a shared understanding of each of the business branches operating within it, meaning their roles, responsibilities and internal processes (Burkhardt, n.d. p.5).

If any documentation exists on hiring and training employees, it should be collected and reviewed. All other current cybersecurity documents can be included in this review to establish a clear understanding of the organization context.

3.2 Analyzing and prioritizing risks

The second step will be analyzing different threat levels and potential risks that could occur to the business. After reviewing the cybersecurity documentations and practices, a clear picture of them will help prioritize the risks (Burkhardt, n.d. p.6).

3.3 Conducting workforce assessment

Conducting which different employees in their respective work areas will be accountable for managing cybersecurity risks is crucial. It’s important to know

the risk owner and risk action owner to establish a proper and timely response (Burkhardt, n.d. p.7).

3.4 Identifying and planning workforce responses

After getting a clear picture of the cybersecurity workforce need, the business can begin reshaping its workforce to operate efficiently by setting clear response plans and competent workers in the correct field. This can be incorporated in the hiring and training stages as well (Burkhardt, n.d. p.8).

3.5 Implementing, evaluating and adjusting responses

When adjustments have been made, the workforce can begin to successfully implement them, this promotes a safer and efficient working environment where-by every organizational member is accounted and a clear plan functional. Regular updates and training should be conducted to keep the framework efficient (Burkhardt, n.d. p.9).

An illustration of NIST Cybersecurity Framework's figure 3 outlining a cyclic process comprising six core functions: Govern, identify, protect, detect, respond and recover. This model aligns with ISO 27001's plan-do-check-act cycle, and standard making sure of a continuous adaptation to emerging threats.

Figure 3. NIST CSF Core Functions. (NIST Cybersecurity Framework 2.0, 2023)

4 ISO 27001 in Business

ISO 27001 is a standard for information management systems. It provides companies guidance for establishing, implementing, managing and updating on an information security management system (ISMS). It was developed by the international organization for standardization (ISO) and the international electrotechnical commission (IEC) to help such companies protect their information in a systematic and cost-effective way (ISO, 2022).

This standard offers valuable key resources to our framework that could be incorporated. Benefits mentioned in the ISO 2022 standard include:

- Resilience to cyber-attacks
- Preparedness for new threats
- Data integrity, confidentiality and availability
- Security across all supports
- Organization-wide protection
- Cost saving

4.1 Resilience to cyberattacks

ISO 27001 provides structured guidance to help businesses build robust security controls. These controls enhance the business ability to detect, respond to, and recover from cyberattacks, reducing the risk of operational and financial losses (ISMS. online, 2018).

4.2 Preparedness for new threats

Cyberthreats continuously evolve, requiring businesses to adopt proactive security measures. ISO standards promote regular risk assessments, continuous improvement, and adaptability to emerging threats, ensuring that a

business's cybersecurity position remains resilient in the face of new threats (ISO, 2022).

4.3 Data integrity, confidentiality and availability

ISO 27001 standard promote business protection by having integrity safeguards to prevent unauthorized alterations to data, confidentiality controls which restrict access to sensitive information, and availability measures that make sure data is accessible when needed. This minimizes disruptions in business operations.

4.4 Security across all supports

This means to have a comprehensive protection across various digital and physical assets, including networks, devices, applications and employees. ISO 27001 standards emphasize the importance of securing all layers of an organization's IT infrastructure to prevent vulnerabilities across different platforms and operational environments (ISO, 2022).

4.5 Organization-wide protection

ISO 27001 standard promote a holistic security approach by integrating cybersecurity practices across all departments, from IT to finance to human resources. This ensures that security is not limited to technical teams but is embedded in the business policies, procedures, and employee awareness programs (ISO, 2022).

4.6 Cost saving

Implementing ISO 27001 standard can lead to long-term financial benefits by preventing costly security breaches, business disruptions and optimizing resource allocation through efficient security management practices.

Compliance with ISO guidelines al minimizes regulatory fines and ensures adherence to legal requirements (ISO, 2022).

According to IT Governance (2025) ISO 27001 standard is achieved by following almost similar steps to the previous NIST framework.

- Context of the organization
- Leadership
- Plan
- Support
- Operation
- Performance evaluation
- Improvement

4.7 Context of the organization

It is important to understand the business and its context, what the needs and expectations of interested parties. This will be beneficial in determining how wide a framework needs to be to cover the business (IT Governance, 2025).

4.8 Leadership

Having a clear picture of the leadership structure and responsibilities can help set better policies and procedures for a good framework. Knowing each employee role creates accountability in the case of tracking and managing cyber-attack incidents (IT Governance, 2025).

4.9 Plan

This involves actions that are set to counter risks and opportunities. What are the steps taken by each member when an incident occurs. This is a critical area in developing a good framework (IT Governance, 2025).

4.10 Support

Having a reliable support system can help a small business avoid a catastrophic scenario and save both time and money. Support could include a variety of things from previously documented data to just having competent people. All these small things have massive consequences when dealing with cyber-attacks (IT Governance, 2025).

4.11 Operation

This includes the planning stage mentioned above, meaning that accessing security risks and risks treatment. Having prioritization plans for severe risk to low levels of risks can help the business cyber security team handle cases in more efficient ways than randomly jumping from one case to another. Establishing how each case should be handled and whether to investigate at the time of discovery (IT Governance, 2025).

4.12 Performance evaluation

By monitoring and conducting analysis of how day-to-day business activities are conducted and handled particularly the ones that are done online, it can benefit in preventing future cyber-attacks by reducing the errors observed. Therefore, internal audits should be conducted regularly to establish a good framework (IT Governance, 2025).

4.13 Improvement

Adding to the previously mentioned step, continuous improvement to the established framework is necessary to keep up with the newly discovered risks especially with the ongoing development in technology. Cyber-attacks always find newer ways to exploit vulnerabilities; therefore it is essential for the business to keep updating their systems and educating their personnel on these

potential vulnerabilities. A more proactive culture in the business can save it (IT Governance, 2025).

NIST CSF provides the most scalable entry point for SMEs, while ISO 27001 remains optimal for regulated industries. Table 1 compares these frameworks.

Table 1. Comparison table between three main frameworks.

Framework	Cost	Flexibility	Key Focus	Certification	Best For	Implementation Time	Resources
NIST CSF	Free	High	Risk management	No certification	Adaptable guidance	3-6 months	CSF 2.0 Quick Start Guides | NIST
ISO 27001	3k-15k+	low	Comprehensive ISMS (Annex A controls)	Mandatory certification (10k-50k)	Regulated industries (GDPR, HIPAA)	6-12+ months	What is ISO/IEC 27001? | Implement, Certify & Comply
CIS controls	Free	medium	18 prioritized technical controls	Optional assessment	Resource constrained organizations	1-3 months	CIS Critical Security Controls SME Companion Guide for v7.1

5 Roles of the CEO

Small businesses owner's often think that only the IT team is responsible for cybersecurity. These mistakes may lead to a compromised business that could have been avoided. According to CISA, (2024) here are some critical roles played by a proactive CEO:

- Creating a cybersecurity culture
- Appointing a clear cybersecurity program manager
- Evaluating and approving all incident response plans
- Getting involved in incident drills
- Supporting the cybersecurity management leadership team.

5.1 Creating a cybersecurity culture

To bring in a cybersecurity culture, businesses should prioritize information sharing with the employees on cybersecurity reports and security programs that are ongoing. The leadership should set goals to improve authentication systems through multifactor authentication (MFA), backups and patches (CISA, 2024).

5.2 Appointing a clear cybersecurity program manager

The CEO roles in selecting a qualified cybersecurity manager that will oversee the implementation of all important cybersecurity measures. The appointed manager will report on progress and setbacks to the CEO and other senior employees often (CISA, 2024).

5.3 Evaluating and approving all incident response plans

After the appointed manager creates an IRP, it is then thoroughly reviewed by the CEO. It is given enough attention and other senior leaders across the

business are involved during this step, not only the security and IT team (CISA, 2024).

5.4 Becoming involved in incident drills

The CEO should participate in cyberattacks simulations that are prepared by the security manager. This will help the CEO and team develop good cybersecurity mitigation re-flexes for potential cases (CISA, 2024).

5.5 Supporting the cybersecurity management leadership team

Having a strong collaboration with the cybersecurity team will create a good and secure culture for the business. Further incidents can be prevented by implementing the proposed security changes (CISA, 2024).

6 Recommended framework

This thesis proposes a hybrid cybersecurity framework for a small business. This means integrating NIST CSF, ISO 27001, and CEO proactive culture. Considering insights from industry reports (Verizon DBIR, 2024), CISA recommendation for small businesses and academic studies (Peltonen, 2024), this model balances cost efficiency with comprehensive risk mitigation specific for small businesses.

6.1 Pillars of the framework

The proposed framework includes four interdependent pillars, designed to address technical, organizational, and cultural security gaps. They are grounded in NIST CSF's core functions, ISO 27001's Annex A controls (Edwards, 2022) and operationalize CISA's 2023 recommendations for a small business while prioritizing scalability and affordability.

6.1.1 Risk identification and prioritization

Understanding an organization's unique risk profile is an effective cybersecurity measure. This pillar mandates systematic mapping of digital assets and threat landscapes. By conducting an ISO 27001-compliant risk assessment (Clause 6.1.2), businesses can prioritize vulnerabilities with the highest financial and operational impacts, as evidenced by a 58% reduction in breaches among SMEs adopting this approach (Verizon, 2024). Key steps include:

- Mapping business processes and the business digital assets.
- Conducting a risk assessment to know the threat levels and their impacts.

6.1.2 Leadership and workforce engagement

Human factors account for 68% of cybersecurity breaches (Verizon, 2024), underscoring the need for leadership driven culture change. This pillar integrated CISA's 2023 guidelines for CEO accountability and workforce training, leading to a security first mindset. Critical actions include:

- Assigning a cybersecurity program manager according to CISA guidelines.
- Training employees in incident reporting, MFA and phishing at-tacks.

6.1.3 Implementation of controls by prioritizing low cost and high impact controls

This pillar prioritizes low-cost, high-impact controls validated by (CIS, 2024) and (Wazuh, 2024) to maximize limited resources. By adopting ISO 27001's Annex A.8 (Access Control) alongside CIS Control 8 (Malware Defenses), SMEs achieve 80% threat coverage with minimal investment, as demonstrated in recent case studies (IT Governance UK, 2023). Core components include:

- Access control (MFA, least privilege).
- Patch management (regular software updates).
- Backup and recovery (3-2-1 backup rule).

6.1.4 Continuous improvement

This pillar embeds ISO 27001's plan-do-check-act cycle (Clause 4.4), requiring quarterly incident drills and annual framework reviews. Cybersecurity is not a onetime project (Peltonen, S. 2024 p.10). Key activities include:

- Conducting quarterly incident drills.
- Reviewing the framework annually.

6.2 Implementation roadmap

Table 2 outlines a 12-month phased implementation strategy, synthesizing NIST CSF's Quick Start Guide 2023, CIS Small Business Guide and ISO 27001's templates. Designed to for a resource constrained environment, this roadmap prioritizes CIS controls deployment while building toward long term goals like ISO certification. A tool such as Wazuh is integrated for cost effective monitoring, ensuring alignment with the framework's four pillars.

Table 2 Implementation roadmap for hybrid cybersecurity framework.

Phase	Action	Resources
1-3 months	Asset inventory and risk assessment	NIST CSF Quick Start Guide
4-6 months	Deploy CIS controls (MFA, backups)	CIS Small Business Guide
7-12 months	ISO 27001 -match policies	IT Governances Free ISO 27001 Templates

7 Conclusion

This thesis proposes that small businesses can significantly enhance their cybersecurity posture based on well-established standards and frameworks by adopting a hybrid framework that integrates the flexibility of NIST CSF'S risk-based approach, ISO 27001's guiding structure and proactive CEO leadership.

The framework's foundation in NIST CSF's Identify-Protect-Detect-Respond-Recover model ensures a more systematic risk management plan. Prioritizing key controls mitigate the most common threats (Verizon ,2024, p.18).

ISO 27001 compliance will meet global standards and reduce legal and reputational risks. Studies confirm ISO 27001's efficacy for risk reduction.

The proposed framework model will strengthen current practices and emphasize more workforce training, prioritizing controls and iterative improvements. For future developments, it is recommended that a business monitors this framework efficiently for the next 12 months, tracking metrics such as incident response time and employee compliance rates. Small businesses owners should consider the use of automation tools for example SIEM for small businesses to reduce manual efforts. An example of an open source SIEM option is Wazuh which can work for small businesses. Small businesses should expand their work-force training like quarterly phishing simulations to measure progress, explore cyber insurance to lower premiums and mitigate financial risks.

Cybersecurity is an ongoing journey. By adding this framework into the business day-to-day operations and mitigating evolving threats, the business can transform from a reactive to a proactive, resilient organization. As cyber-attacks grow in sophistication, a business commitment to the proposed framework will aid protection and give a strategic advantage in an increasingly digital marketplace.

References

Burkhardt, C. (2025). NIST Cybersecurity Framework 2.0: Cybersecurity, Enterprise Risk Management, and Workforce Management Quick Start Guide. [online] U.S. Department of Commerce. Available at: https://doi.org/10.6028/NIST.SP.1308.ipd [Accessed 15 April. 2024].

Center for Internet Security (CIS) (2024) CIS Controls Implementation Guide for Small Businesses. [online] Available at: https://www.cisecurity.org/controls [Accessed 15 April. 2024].

Cybersecurity and Infrastructure Security Agency (CISA) (2023) Cyber Guidance for Small Businesses. [online] Available at: https://www.cisa.gov/cyber-guidance-small-businesses [Accessed 16 April. 2024].

Edwards, M. (2022). ISO 27001: 2022 Annex A Controls. [online] ISMS. online. Available at: https://www.isms.online/ISO-27001/annex-a Accessed 10 May. 2024].

International Organization for Standardization (ISO) (2022) ISO/IEC 27001:2022 - Information Security Management Systems. [Online] Available at: https://www.ISO.org/standard/82875.html [Accessed 16 April. 2024].

ISMS. online (2018). Annex A.8 Asset Management. [online] ISMS. online. Available at: https://www.isms.online/ISO-27001/annex-a-8-asset-management/ [Accessed 16 April. 2024].

IT Governance UK (2025) What is ISO 27001? An Easy-to-understand Explanation. [Online] Available at: https://www.itgovernance.co.uk/ISO27001 [Accessed 16 April. 2024].

National Institute of Standards and Technology (NIST) (2023) NIST Cybersecurity Framework 2.0: Quick start guide. [Online] Available at: https://www.nist.gov/cyberframework [Accessed 16 April. 2024].

Peltonen, S. (2024) ISO27000 Implementation Handbook. Bachelor's thesis. Turku University of Applied Sciences. [Online] Available at: https://www.theseus.fi/bitstream/handle/10024/852451/Peltonen_Sebastian.pdf [Accessed 16 April. 2024].

Verizon (2024) 2024 Data Breach Investigations Report (DBIR). [Online] Available at: https://www.verizon.com/business/resources/reports/dbir/ [Accessed 16 April. 2024].

Wazuh (2024) Open-source Security Monitoring. [Online] Available at: https://wazuh.com/. [Accessed 16 April. 2024].