SUCCESS

Security Democratized

Secure Universal Creative Cost-saving Efficient Standards for Small Businesses

Table of Contents

Introduction

Security standards can be complex and costly to implement, posing challenges for small businesses with limited resources. This paper addresses these challenges by investigating the effectiveness of current security standards and proposing a novel framework tailored to the needs of Small and Medium-sized Businesses (SMBs). We present the Security Standards for Small Business (SUCCESS) framework, developed through a rigorous research methodology involving surveys, interviews, and field tests with SMBs. SUCCESS stands for **S**ecure **U**niversal **C**reative **C**ost-saving **E**fficient **S**tandards for **S**mall Businesses.

Scope

The Security Standards for Small Business (SUCCESS) framework is designed to provide a streamlined and practical security standard tailored specifically to the unique operational environment and resource constraints of Small and Medium-sized Businesses (SMBs). This framework aims to address the complexities and financial burdens associated with conventional security standards, enabling SMBs to establish and maintain robust security practices effectively.

Intended Audience

The intended audience for the standards aimed at small businesses encompasses owners, operators, and stakeholders of small-scale enterprises. This includes entrepreneurs, managers, and decision-makers who oversee the day-to-day operations and strategic direction of these businesses. Additionally, it extends to employees who play a role in implementing and adhering to the prescribed security measures. These standards are tailored to meet the specific needs, resources, and operational scope of small businesses, recognizing their distinct challenges and constraints. By addressing this audience, the standards aim to provide practical and accessible guidance to enhance security measures and protect sensitive information within the context of small business operations.

SUCCESS Overview

SUCCESS Standards - High-Level Overview

GOVERNANCE	Leadership should provide support for security, including budget allocation
	Information Security Policy should be developed and implemented
ACCESS CONTROL	Strong password policies should be implemented along with Mult-factor authentication
	Access should be granted based on roles and responsibilities to adhere to the principle of least privilege
ASSET MANAGEMENT	Inventory of data should be compiled and maintained
	Data classification based on sensitivity should be performed
DATA SECURITY	Sensitive data should be encrypted
	Data leakage prevention should be ensured
HUMAN RESOURCES	Criminal Background checks for all employees and contractors should be performed
	Job-specific training that addresses the unique security challenges shall be done annually
SOFTWARE SECURITY	Security should be integrated into every stage of the software development lifecycle
	Secure coding practices and code reviews should be implemented
INCIDENT RESPONSE	Develop a comprehensive incident response plan and test it
	Establish clear roles and protocols for reporting and escalating security incidents
VULNERABILITY MANAGEMENT	A patch management process to handle critical patches should be implemented
	Vulnerability risks should be identified and remediated
RISK MANAGEMENT	Potential risks should be identified and assessed for various assets
	Plans should be developed to mitigate those risks
PHYSICAL SECURITY	Security measures to restrict physical access to sensitive areas should be implemented
	Comprehensive physical security policies should be developed to guide personnel and equipment protection
TEAM	An employee shall be designated as the Head of Security and Compliance

Detailed Requirements and Testing Procedure

Requirements and Testing Procedure		Guidance
Main Guideline	**Defined Testing Procedure**	**Purpose:** Support from leadership helps motivate all to care about security **Best Practices:** Allocate and document budget for security. **Examples:** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed.
1-Leadership should provide support for security, including budget allocation.	1A-Interview personnel responsible for performing activities in Requirement 1 to verify that roles and responsibilities are assigned as documented and understood.	
	1B-Review budgetary allocation.	

Requirements and Testing Procedure		Guidance
Main Guideline	**Defined Testing Procedure**	**Purpose:** A documented Information Security Policy helps focus on a set of security priorities specific to the business. **Best Practices:**
2-Information Security Policy should be developed and implemented.	2A-Review the Information Security Policy	

	2B-Interview a randomly selected employee about their understanding of the Information Security Policy.	Do as you say, Say as you do. **Examples:** A template shall be shared at success4biz.info.

Requirements and Testing Procedure		Guidance
Main Guideline	**Defined Testing Procedure**	**Purpose:** Strong passwords help prevent unauthorized access. **Best Practices:** Use a two-factor app like Duo. **Examples:** Duo is an example of a two-factor tool and app.
3-Strong password policies should be implemented along with Multi-factor authentication.	3A-Verify the existence of Two-factor access for all admins.	
	3B-Verify the adoption of two factors among randomly selected employees.	

Requirements and Testing Procedure		Guidance
Main Guideline	**Defined Testing Procedure**	**Purpose:** Support from leadership helps motivate all to care about security **Best Practices:** Allocate and document budget for security. **Examples:** A
4-Access should be granted based on roles and responsibilities to adhere to the principle of least privilege	4A Interview personnel responsible for performing activities in Requirement 1 to verify that roles and responsibilities are assigned as documented and understood.	
	4B Review budgetary allocation.	

Requirements and Testing Procedure		Guidance
Main Guideline	**Defined Testing Procedure**	**Purpose:** Support from leadership helps motivate all to care about security **Best Practices:** Allocate and document budget for security. **Examples:** A
5-Inventory of data should be compiled and maintained.	5A Interview personnel responsible for performing activities in Requirement 1 to verify that roles and responsibilities are assigned as documented and understood.	

Requirements and Testing Procedure		Guidance
Main Guideline	**Defined Testing Procedure**	**Purpose:** Proper data classification helps prioritize the security of highly sensitive data. **Best Practices:** Encrypt the highly sensitive data. **Examples:** A
6-Data classification based on sensitivity should be performed	6A Review Data Classification document	
	6B Review actual Data Classification	

Requirements and Testing Procedure		Guidance
Main Guideline	**Defined Testing Procedure**	**Purpose:** Encrypted data mitigates the risk of data theft in case of unauthorized access **Best Practices:** Allocate and document budget for security. **Examples:** A
7-Sensitive data should be encrypted	7A Verify encryption	

Requirements and Testing Procedure		Guidance
Main Guideline	**Defined Testing Procedure**	**Purpose:** This reduces the risk of data loss and helps with legal compliance **Best Practices:** Allocate and document budget for security. **Examples:** A
8-Data leakage prevention should be ensured	8A Interview personnel responsible for the implementation of Data Leakage prevention	

Requirements and Testing Procedure		Guidance

Main Guideline	Defined Testing Procedure	
9 Criminal Background checks for all employees and contractors should be performed	9A Review one randomly selected background check	**Purpose:** Promotes safe workplace and helps meet contractual obligations **Best Practices:** Allocate and document budget for security. **Examples:** A list of background check providers shall be shared at success4biz.info
	9B Review the secure way of storing of the background check information.	

Requirements and Testing Procedure		Guidance
Main Guideline	**Defined Testing Procedure**	**Purpose:** Training helps reduce human errors and social engineering attacks **Best Practices:** Allocate and document budget for security. **Examples:** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed.
10 Job-specific training that addresses the unique security challenges shall be done annually.	10A Review employee training evidence	

Limitations

1. **Resource Constraints**: Small businesses typically have limited budgets and may not be able to allocate significant resources to implement and maintain robust security measures.
2. **Limited Expertise**: Small businesses may not have dedicated IT or security teams. As a result, employees with other responsibilities may be tasked with managing security, potentially leading to gaps in knowledge and expertise.
3. **Scalability Issues**: Some security standards may be designed with larger organizations in mind. Adapting these standards to fit the scale and scope of a small business can be challenging.

4. **Compliance Complexity**: Meeting certain security standards may require navigating complex compliance frameworks and legal requirements. Staying updated and compliant with evolving regulations can be difficult for small businesses with limited resources.
5. **Vendor and Supply Chain Risks**: Small businesses often rely on vendors and third-party services. Ensuring that these entities also adhere to security standards can be difficult, potentially exposing vulnerabilities.
6. **Balancing Usability and Security**: Implementing strict security measures can sometimes hinder user experience and productivity. Striking the right balance between security and usability is a challenge for businesses of all sizes.
7. **Limited Data Protection Resources**: Small businesses may not have the capacity to invest in advanced data protection technologies, potentially leaving them vulnerable to cyber threats.
8. **Target for Cyber Attacks**: Small businesses are not immune to cyber threats, but they might not have the same level of security infrastructure as larger enterprises. This can make them attractive targets for cybercriminals.
9. **Training and Awareness**: Ensuring all employees understand and follow security protocols can be challenging in a small business setting. Limited resources may hinder the ability to provide comprehensive training programs.

Contacts

Since this work is part of ongoing research and is under consideration for publication; the actual contact information is anonymized for now. You can reach us at admin@success4biz.info or at (303) SUCCESS.

References

TBD