Cybersecurity Implementation Plan

William Batts

February 22, 2025

**1.0 Introduction**

The Merger & Acquisition (M&A) team conducted a Gap Analysis of PBI-FS’s network infrastructure and reviewed the financial industries’ legal and regulatory requirements. The gap analysis also outlined network security risks, laws, regulations, and standards PBI-FS will need to incorporate into its operating procedures. Additionally, the M&A team proposed a Cybersecurity Strategy, Plan of Action (CSPA), and a summary of recommendations to ensure the CSPA fulfills legal and IT security control requirements. Finally, the M&A team reviewed Island Banking Service’s hardware, software, and licenses. As a result of the CSPA and Island Banking Service’s hardware and software review, a Cybersecurity Management Plan will be developed to address and rectify security risks and vulnerabilities in PBI-FS’s network infrastructure.

The Cybersecurity Management Plan (CMP) will address PBI-FS’s critical cybersecurity gaps and priorities and make specific recommendations to strengthen the organization’s cybersecurity posture. The CMP will outline recommendations for security controls that comply with U.S. banking laws, regulations, and standards and the replacement of outdated hardware and software that will reduce threats to PBI-FS’s network infrastructure.

**2.0 Goals and Objectives**

The CMP will outline PBI-FS’s goals and objectives in two categories:

* Business goals and objectives: Business goals and objectives will identify expectations PBI-FS wants to accomplish in the following months to achieve long-term goals that propel the business forward.
* Project goals and objectives: Project goals and objectives will outline goals PBI-FS will execute to implement the CMP and strengthen the organization’s cybersecurity posture and ensure the organization abides by U.S. and Fiji laws and regulations.

**2.1 Business Goals and Objectives**

The following are PBI-FS’s Business Goals and Objectives:

1. Assesses the current network infrastructure. This plan aims to identify the current state of PBI-FS’s network infrastructure; this will identify potential threats and vulnerabilities to the IT infrastructure. Also, the supervision of cybersecurity risks and the management of internal and external threats to the information security program.
2. To apply policies and security controls that abide by U.S. and Fiji laws and regulations. This plan will outline the policies, regulations, and controls PBI-FS must incorporate to ensure the business will not break any national laws that PBI-FS conducts business.
3. PBI-FS will ensure the security and confidentiality of its customers, including names, addresses, and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers (FTC, 2006). PBI-FS will develop policies and controls to ensure that client information and organizational data are secure from unauthorized access from threat actors.
4. Will ensure the confidentiality, integrity, and availability of PBI-FS’s resources and customer data. This plan aims to ensure customers have constant access to PBI-FS’s resources and authorized data without having to worry that their data is secure from unauthorized access or modification from cybercriminals.

**2.2 Project Goals and Objectives**

The following are PBI-FS’s Project Goals and Objectives:

1. Establish User Security Controls. This document will identify actions PBI-FS will take to limit access to organizational assets only to authorized individuals, entities, or devices. An Access Control Policy will which users should be granted access to systems, applications, and databases based on their job responsibilities.
2. Establish Threat and Vulnerability Management. This document will establish requirements that maintain policies, procedures, and technologies to detect and identify threats and vulnerabilities to the IT infrastructure.
3. Establish Information Sharing and Communications. This document will establish requirements that initiate and maintain relationships with external and internal entities that collect information on threats and vulnerabilities against Information Technology security.
4. Event and Incident Response Planning. This document will establish requirements that will outline what constitutes an event or incident when an event or incident happens, who is tasked with specific duties, how the incident should be handled, and reporting the incident or event.
5. Employee Cyber Awareness Training. This document will establish requirements to create a training program for employees that focus on log-in requirements, password guidelines, and recent cyber threats targeted against financial institutes.

**3.0 Scope**

The project scope includes the operations of the financial institute Padgett-Beale acquired that will be known as Padgett-Beale, Inc - Financial Services (PBI-FS). Padgett-Beale will move PBI-FS’s data center and IT support to a Padgett-Beale property located within the continental United States. However, PBI-FS will have a call center located in Figi, and this means PBI-FS will need to adhere to U.S. and Fiji federal laws and regulations. The project will identify potential internal and external threats and vulnerabilities to the IT infrastructure, create a secure network infrastructure, and upgrade network hardware and software.

**4.0 Assumption**

The following are the assumptions that will be made when conducting the Cybersecurity Management Plan:

* The criminal charges against Island Banking Services’ upper management will negatively impact PBI-FS’s reputation. PBI-FS’s future and present customers and investors have lost trust in the business (RSI Security, 2020), and PBI-FS will have to reassure its investors and customers that the network infrastructure is secure and safe; and PBI-FS has taken measures to reduce insider threats in the future. For example, access controls have been implemented to restrict employees from accessing unauthorized information. Also, a monitoring and analysis tool has been implemented to alert security personnel in identifying cybersecurity events.
* Threat actors will target PBI-FS in the future. An IBM study found that “53% of data breaches are financially motivated, which explains why financial institutions are constantly on the cybercrime radar” (Buzz Staff, 2021).
* PBI-FS’s network is most likely to be compromised by an insider threat. Insider threats can come in many forms; for example, a negligent employee, malicious employee, contractor, or third-party vendor can be insider threats; 25 percent of all security incidents involve insiders (Proofpoint, 2021).
* Outdated hardware and software will need to be replaced to reduce the risk of IT security incidents. Experts consider five years to be a maximum machine’s lifespan (Kill, 2017). Outdate machines may run slower and cannot support new operating systems, which could result in the inability to receive updated patches leaving the device open to malicious attacks.

**5.0 Constraints**

The following are the projected constraints in the project:

* Time will be a constraint in the project. Implementing new security policies, procedures, and controls in conjunction with replacing hardware and software will take a considerable amount of time. Due to the complexity of the project and unknown issues, meeting time frames will be an issue.
* Replacing old hardware and software with updated devices and operating systems will be challenging. The IT team will need to ensure the new hardware and software is compatible with existing systems and operations and will not hinder PBI-FS from accomplishing its business goals.
* Implementing the correct policies and regulations that abide by U.S. and Fiji laws will also be a constraint in the project. Ensuring policies that address The Bank Secrecy Act (BSA) 31 USC 5311, the Foreign Assets Control Regulations (OFAC) 31 CFR 500, Title 31 of the Code of Federal Regulations, Payment Card Industry Data Security Standard (PCI-DSS), and International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001 may be challenging without a proper audit.

**6.0 Project Management Plan**

**6.1 People**

**6.1.1** **Policy**

Individuals can be a severe threat to the cybersecurity of an organization’s network infrastructure, from intentionally or unintentionally downloading malicious software to disclosing sensitive information. Incorporating access controls and cyber security training into the network security platform can reduce insider threats. Access Controls can prevent unauthorized individuals or software from accessing information or computer systems they are not allowed to access. Access Controls will hinder individuals from making unauthorized administrative changes to the system configurations or changing or deleting documents or files. In addition, cyber awareness and training are the first-line defense against network attacks. “According to the 2017 Data Security Incident Response Report from BakerHostetler, employee actions and mistakes were the cause of 32 percent of security incidents, second only to phishing, hacking, and malware at 43 percent” (Dgulling, 2018). Incorporating employee awareness and training will ensure employees know PBI-FS’s policies and procedures on network and software use and diminish the likelihood they fall victim to email phishing scams or social engineering.

**6.1.2 Access Controls**

Employees, contractors, and third-party vendors will only be permitted access to data and software required to complete their daily duties. PBI-FS will implement Role-Based Access Control into the network security posture, and individuals or entities will only have access to information or data that their employee role is authorized. System managers must remember to place employees into the proper role corresponding to their job position, and failure to put employees into the correct role could prevent them from completing their daily duties.

**6.1.3 Employee Security Awareness Training**

Employees, contractors, and third-party vendors must complete an approved Security Awareness Training annually. The security awareness training will inform employees and other entities on PBI-FS’s policies and what is and is not acceptable when using PBI-FS’s hardware and network. Additionally, the security awareness training will provide employees with a basic understanding of information security, users’ responsibilities to maintain security, and how to respond to security incidents.

**6.1.4 Authentication**

PBI-FS will require employees, contractors, and third-party vendors to use multi-factor authentication to access the organization’s hardware or network. Individuals will be required to have a strong password (minimum of 10 characters, use of two numbers, and two special characters) and a smart card assigned to every employee to access PBI-FS’s network. Multi-factor authentication will provide additional security because if one of the credentials becomes compromised, unauthorized users will need the other credential to access the hardware or network.

**6.1.5 Point of Contact**

PBI-FS does not have a permanent CISO. However, Padgett-Beale’s CISO will act as the intern CISO for PBI-FS. Employees, contractors, and third-party vendors should contact the intern CISO for any network security-related questions or concerns.

**6.2 Processes**

**6.2.1 Transactions**

To prevent fraudulent transactions such as the actions conducted by the officers and managers of Island Banking Services. PBI-FS will implement a dual authorization control into the transaction process. Dual authorization will require two authorized personnel to be present and validate that all financial transactions between PBI-FS and other businesses are legitimate.

**6.3 Technologies**

**6.3.1 Firewalls**

A firewall is a network security tool that monitors incoming and outgoing network traffic. The firewall determines what traffic gain access to the organization’s operating system and blocks the traffic that does not meet the predefined security rules. By scanning the network and preventing unauthorized access, firewalls help reduce the threat of malicious actors and software that could threaten PBI-FS’s users, applications, and data.

**6.3.2 Virtual Private Network**

PBI-FS has multiple divisions that operate at different locations; as a result, the information transmitted over the internet is at risk of interception by threat actors during the data exchange. PBI-FS will need to implement a Remote Access VPN on the routers that connect to the modem to help mitigate the risk of stolen or altered sensitive information. Remote Access VPNs provide a secure private network that encrypts data using a Transport Layer Security (TLS) protocol, allowing PBI-FS employees to transmit data over the internet safely.

**6.3.3 Anti-malware Software**

PBI-FS can sustain significant damage to its network if malicious software (viruses, worms, Trojan Horses, Rootkits, and Ransomware) gains entry into the network infrastructure. Antimalware will detect, remove, and block known malicious software and reduce the risk of causing damage to the daily operation of the company.

**6.3.4 Intrusion Prevention System**

An Intrusion Prevention System (IPS) scans and examines network traffic to detect possible threats or risks to the network. Once the IPS detects an anomaly or danger to the network, the program will rectify the situation; for example, send an alarm to the administrator, drop the malicious packets, block traffic from the source address, or reset the connection.

**7.0 Strategy Implementation**

**7.1 Security Controls**

Security controls are essential in protecting PBI-FS’s network infrastructure from potential threats and vulnerabilities and will ensure the organization abides by U.S. and Fiji federal laws and regulations. The security controls recommended below will address the vulnerabilities and threats that will threaten PBI-FS’s daily operations while simultaneously ensuring the organization abides by national laws.

**7.1.1 Baseline (Mandatory Controls)**

**7.1.1.1 Access Rights**

PBI-FS will implement access rights that are in accordance with the organization’s access control policy. Employees that have unlimited access rights to the organization’s database and software can pose a severe threat to the confidentiality and integrity of the network. Contractors’ and third-party vendors’ access can intentionally or unintentionally have their access rights exploited and used to cause damage to the organization. As a result, PBI-FS should implement the Principle of Least Privilege (PoLP), which would give employees, contractors, and third-party vendors access to necessary information and network resources to complete their job necessities. The IT department will need to define users’ profiles and align their job descriptions to the users’ profiles to create a user access program.

**7.1.1.2 Data Back-Ups**

PBI-FS will need to incorporate data backup procedures into the business continuity plan to ensure business operations can fully function in a security disaster. PBI-FS will backup employee files, billing records, and financial transactions once a day and a complete network backup once a week on a cloud storage platform.

**7.1.2 Compensatory Controls**

**7.1.2.1 Audit Log Reviews**

PBI-FS will incorporate segregation of duties (SoD) to prevent errors or fraudulent activities in financial transactions. Errors and fraud could cause significant damage to the organization’s data and reputation. An SoD will ensure no one employee has complete control over a financial tasking to mitigate the risk. However, implementing SoD could be challenging due to the limited personnel employed at PBI-FS; a compensatory control PBI-FS could incorporate are monthly log reviews of all critical information systems. Log reviews will show a timestamp of historical events and will assist IT personnel in identifying unusual events in the IT system.

**7.1.2.2 Encrypted Cloud Storage**

PBI-FS handles and stores financial records and customers’ personal information, making the stored data valuable for cybercriminals. Encrypting the entire data system can be difficult and expensive; however, PBI-FS could use an encrypted cloud storage service when backing up data to ensure PBI-FS’s data is secure even if Cybercriminals breach the network. Encrypted cloud storage ensures files and stored data are incomprehensible to unauthorized users, and only authorized users will possess the decryption key to convert the data into readable plaintext.

**7.2 System Development Life Cycle**

The System Development Life Cycle is a project management model that provides a detailed outline of each phase of the project that brings it from its initial concept to becoming fully operational and later enters the maintenance phase that ensures policies, protocols, and procedures are implemented keep the network secure. PBI-FS will use planning, requirements, design, development, testing, deployment, and maintenance for the seven System Development Life Cycle phases. The following will outline how PBI-FS will implement the seven phases:

* **Planning**: Define the project’s scope, schedule, and any problems that may arise. Also, estimate funding and resources that are needed to complete the project.
* **Requirements:** Determine the needs of end-users and specify the software, hardware, network requirements, and IT policies to ensure employees of PBI-FS can perform their duties.
* **Design:** Outline in specific the location and function of hardware, software, user interfaces, software interfaces, data closets, and the materials needed to bring these locations to fully operational. Also, the design will outline the specific IT Policies required to ensure PBI-FS abide by national laws and the security of the network infrastructure.
* **Development:** Develop PBI-FS network infrastructure, policies, and regulations to ensure the confidentiality, integrity, and availability of the hardware, software, and data.
* **Testing:** Going over the network infrastructure to determine if the requirements of the end-users and software interface can be met while ensuring the confidentiality, integrity, and availability of the hardware, software, and data.
* **Deployment:** Once the network testing phase has been completed and it has been determined that adequate security protocols and procedures have been implemented, PBI-FS will bring the network online and allow full operation of services to customers and employees.
* **Maintenance:** During the maintenance phase, the IT department will monitor network traffic, unauthorized software, and unauthorized users daily; also conduct software patches. Semiannually internal IT audits will be performed, and an external IT audit will be conducted annually.

**7.3 Milestones**

Project managers use milestones to track progress in The System Development Life Cycle. Project milestones show forward movement and progress in the project, and it also shows the project manager areas that are lagging behind schedule so management can implement the best course of action to rectify the situation (Harrin, 2018). PBI-FS will use the following milestones in the System Development Life Cycle model:

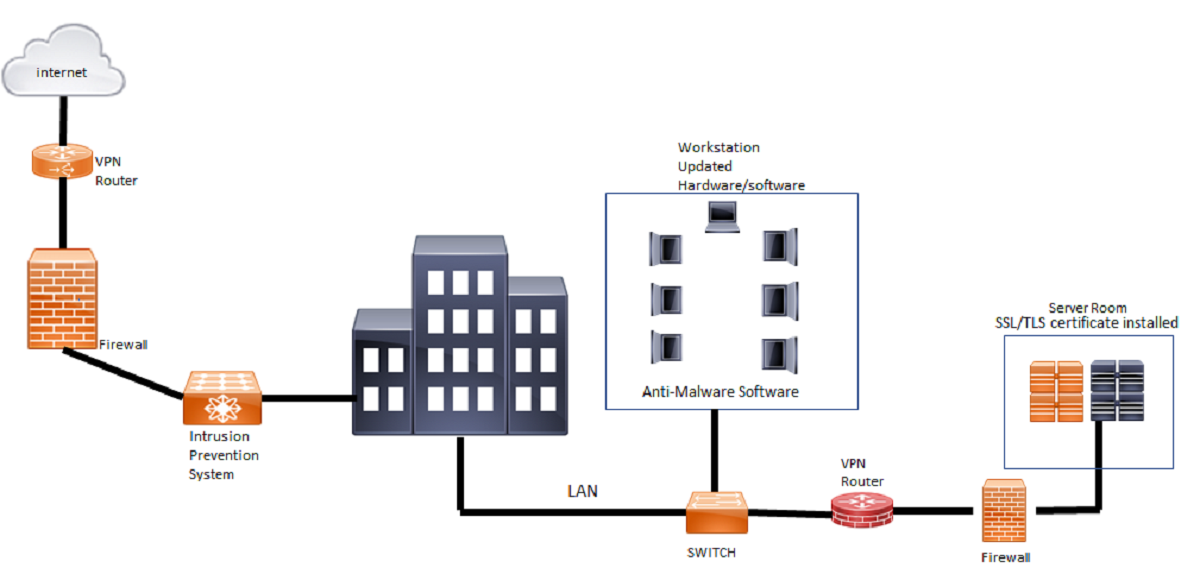
* **Planning:** Project Funding estimated
* **Requirements:** Identified Software, hardware, and network requirements for the project
* **Design:** The project manager decided the exact location of the hardware and software
* **Development:** PBI-FS’s network is operational
* **Testing:** Network security protocols pass Internal Audit
* **Deployment:** PBI-FS network is fully operational
* **Maintenance:** On-going

**7.4 Resource Requirements**

Resource requirements are the personnel and items needed in The System Development Life Cycle. An itemized list of the personnel and items needed will ensure the project has the resources necessary to complete the project on time and within the planned budget. PBI-FS will need the following personnel and items to develop a secure network infrastructure:

* **Personnel:** CISO and Upper Management will plan the project schedule, define the project’s scope, and correct any problems during the project. Internal Auditor will perform an internal audit during the testing and maintenance phase, and an External auditor will perform an external audit during the maintenance phase. Also, a finance manager will ensure the project stays within the budget of PBI-FS, and a legal advisor will ensure policies and regulations abide by national laws.
* **Items:** To ensure the PBI-FS network is secure, the purchase of firewalls, a virtual private network, and malware software is required in the network infrastructure. In addition, the project will replace outdated hardware and OS with new and updated devices and software.

**8.0 Enterprise IT Architecture**



Figure

**8.1 Hardware**

PBI-FS acquired computer workstations that are more than five years old and running on Windows 8.1. To ensure network security and proficiency, PBI-FS will purchase new workstations. Also, Cisco ASA 5500 will be to be purchased to upload an Intrusion Prevention System (Mondal, 2017).

**8.2 Software**

PBI-FS will purchase VPN software and install it on the router; the IT department will install Windows 10 operating system on all PBI-FS workstation computers and update and license anti-malware.

**8.3 Network Infrastructure**

PBI-FS’s network infrastructure is encapsulated in a private network that secures outgoing network traffic by encrypting data traffic. Also, the webserver has the SSL/TLS certificate installed on it that will encode sensitive information submitted on PBI-FS’s website.

**8.4 Cybersecurity Defense**

PBI-FS can implement the following policies and procedures to reduce cybersecurity threats against the organization’s network, customers, and clients.

* **Virtual Private Network (VPN)**: A VPN will encrypt all outbound traffic from PBI-FS; encrypting the data will ensure that even if Cybercriminals successfully intercept data, they will not be able to decrypt it, leaving the data useless and invaluable.
* **Firewalls:** Firewalls are the first line of defense in network security. Firewalls monitor organizational network traffic, and network managers can set specific rules and filter to protect the business’s network.
* **Intrusion Prevention System (IPS**): If cybercriminals or malicious software successfully bypass the firewall, a Cisco ASA 5500 Intrusion Prevention System will be in place to scan and examine network traffic to detect possible threats or risks to PBI-FS’s network. Once the IPS detects an anomaly or danger to the network, the program will rectify the situation.
* **Anti-Malware Software:** Employees can download malicious software, plugin an infected thumb-drive, open a malicious email, or visit an unauthorized website; these are a few ways malware can infect a network. To reduce the damage malware can cause, anti-malware will detect, remove, and block known malicious software and reduce the damage to the daily operation of PBI-FS.
* **Employee Security Awareness Training:** Employees play a significant role in cybersecurity breaches. According to research conducted by Stanford University, 88 percent of cybersecurity breaches are caused by employee negligence (M, 2021). Employee Security Awareness Training will inform employees and other entities on PBI-FS’s policies and what is and is not acceptable when using PBI-FS’s hardware and network. Additionally, the security awareness training will provide employees with a basic understanding of information security, users’ responsibilities to maintain security, and how to respond to security incidents.