FITLSDOG

FITLSDOG

The Financial Information Technology Leader’s Strategy Development and Operations Guide

Anthony Scarola

Security Connect LLC

For permission requests, email the publisher, Security Connect LLC, at info@securityconnect.us with the subject line “Attention: Permissions Coordinator.”

First Edition, 2024

ISBN: 979-8-874-21644-3

Library of Congress Control Number: 2024906187

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties concerning the accuracy or completeness of the contents of this book and expressly disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Further, readers should be aware that websites listed in this work may have changed or disappeared between when it was written and when it was read. Neither the publisher nor the authors shall be liable for any loss of profit or other commercial damages, including but not limited to special, incidental, consequential, or other damages.

If you believe you have found a mistake in this book, please bring it to our attention by emailing us at info@securityconnect.us.

Cover design: OpenAI DALL-E

Printed in the United States of America

Appendix C – Sample Documents

IT Strategic Plan Outline

The following is an outline with examples that can be used to develop an IT or IS Strategic Plan. This outline represents a comprehensive approach to creating an IT strategic plan, ensuring that IT initiatives are directly aligned with the business's strategic objectives.

IT Strategic Plan

1. Executive Summary

- *Overview of the IT strategic plan's purpose, key IT initiatives, and expected outcomes in alignment with the business strategy.*

2. Business Goals and Objectives Alignment

- *A brief description of the financial institution's business goals and objectives.*
- *An overview of how IT initiatives align with and support these goals.*

3. IT Vision and Mission

- *Statement of the IT department's vision and mission, reflecting how IT contributes to its success.*

4. Strategic IT Objectives

- **Digital Transformation for Enhanced Customer Experience**: Implement digital banking solutions to improve customer access and satisfaction.
- **Operational Efficiency Through Technology**: Leverage automation and advanced analytics to streamline operations and reduce costs.
- **Robust IT Security and Risk Management**: Strengthen cybersecurity frameworks to protect against evolving threats and ensure compliance with regulatory standards.
- **Innovation and Emerging Technologies**: Explore and integrate innovative technologies to create new business opportunities and improve service offerings.

5. IT Initiatives and Projects

- **Digital Banking Platform Upgrade**: Develop and deploy a new digital banking platform to provide customers with enhanced online and mobile banking experiences.
- **Data Analytics for Personalized Banking Services**: Utilize data analytics to gain insights into customer behavior and preferences, enabling the development of personalized products and services.
- **Cybersecurity Enhancement Program**: Implement a comprehensive cybersecurity enhancement program, including employee training, advanced threat detection systems, and regular security audits.
- **Cloud Infrastructure Migration**: Migrate key IT systems and applications to a cloud-based infrastructure to improve scalability, flexibility, and disaster recovery capabilities.

6. Governance and Compliance

- *Outline the governance structure for managing IT initiatives, including roles, responsibilities, and decision-making processes.*
- *Describe the approach to ensuring all IT initiatives comply with relevant laws, regulations, and standards.*

7. IT Resource Management

- *Detail the human, financial, and technological resources required to execute the IT strategic plan.*
- *Plan for developing and retaining IT talent, including training and career advancement opportunities.*

8. Performance Measurement and Continuous Improvement

- *Define key performance indicators (KPIs) for IT initiatives to measure their impact on business goals.*
- *Establish a process for regularly reviewing and adapting the IT strategic plan based on performance data and changing business needs.*

9. Implementation Roadmap

- *Provide a high-level timeline for executing IT initiatives, including significant milestones and dependencies.*

10. Risk Management and Contingency Planning

- *Identify potential risks to the IT strategic plan's success and outline contingency measures.*

Conclusion

The conclusion should reiterate the strategic alignment between IT initiatives and business goals, emphasizing the IT department's role in driving the organization's success.

Cybersecurity Tool Implementation

I wrote a proposal for a fictitious employer (Advanced Research Co.) in 2014, as an educational project, to purchase Tenable Nessus and Metasploit tools to identify security vulnerabilities for remediation. The "institution" had a mix of Windows and Linux servers and approximately 2,200 workstation endpoints. Here is that proposal:

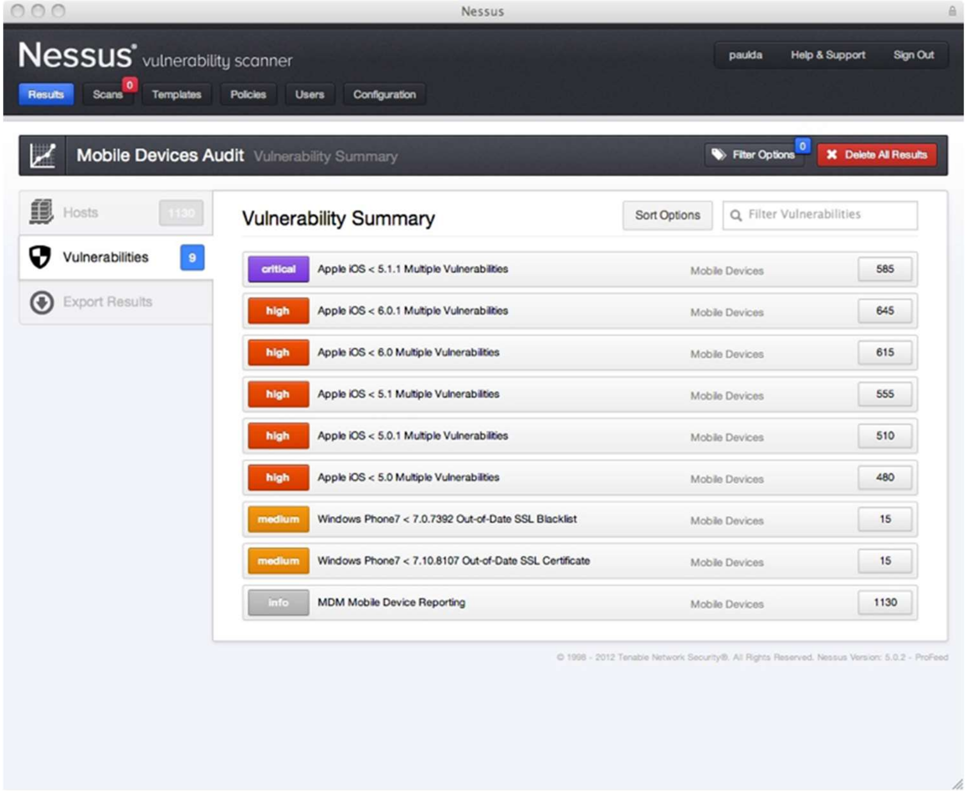
Executive Proposal: Nessus/Metasploit for Advanced Research Co., Security Test Software Project

Considering that evil has existed in the world since the dawn of man and property theft is not going away anytime soon, it is wise for those with valuable items to protect them as well as others with similar items. Direct currency is probably the most valuable target for a criminal, and the second is that which can be turned into currency quickly: sensitive information. In the physical world, if money cannot be directly pilfered, criminals will seek high-value items such as jewelry, weapons, or electronics that can be quickly converted to currency. A stroll through the neighborhood pawnshop confirms this to be true. Confidential or sensitive information is desirable in the cyber world because it can quickly turn into currency in underground markets. For example, Dockterman (2013) reports that an individual's identity costs approximately five US dollars on the black market. Multiply that by thousands of records, and you can see how quickly money can add up. Considering this and the harm and reputation damage from a stolen identity, companies storing, transmitting, or processing such valuable electronic information should protect it using industry-standard, best-practice control methodologies and procedures and frequently test those controls.

The study of Information Security provides knowledge regarding cyber threats, vulnerabilities, tools, and other measures for businesses to protect their valuable data from cyber criminals and the threats to the confidentiality, integrity, and availability of such information and underlying systems. It is understood that software, computer systems, and underlying network components come pre-packaged with bugs and vulnerabilities, some known and others unknown. Each vulnerability poses varying levels of risk to an organization, and that risk must be managed. Organizations must employ layered security controls, policies, procedures, employee awareness training, and other industry best practices to control the risk of exploiting such vulnerabilities. In order to apply security controls and measures appropriately, organizations must first understand the value of their information and also perform frequent Information Security Risk Assessments on some frequency. The outcome will give senior management an understanding of their risk and areas requiring enhancement to manage risk. Cyber liability insurance may also be acquired to limit costs due to security breaches; however, in my opinion, insurance, like other individual security control components, should only be considered single layers in an overall layered approach to securing the enterprise. As a security professional for Advanced Research Co., you employ and empower me to remain educated on the threats, vulnerabilities, security controls, and methodologies to protect our organization, and this proposal offers one such solution to manage our overall risk better.

As we grow larger and become more of a target, we must expand our cyber security toolsets to identify, assess, and address vulnerabilities in our environment to protect our information from criminals and competitors and better manage related risks more quickly. Vulnerabilities come in many different shapes and sizes and have varying risk levels. Individually, low-risk "informational" vulnerabilities pose minimal risk to our organization; however, larger numbers may pose greater risk overall. High-risk vulnerabilities may allow criminals to access confidential information directly or easily and exfiltrate it for direct or indirect financial profit. For example, Heggesteun (2013) reports that vulnerabilities in Target's [2013] point-of-sale systems allowed the breach of over 40 million credit and debit cards. High-risk vulnerabilities known to be exploitable by cybercriminals pose a greater risk than those not. Exploitable vulnerabilities with no known ‘patch’ or fix are considered ‘zero-day’ or “0-day” and may pose an extreme risk. As our current security tools do not allow us to determine the risk of individual vulnerabilities, our business currently spends significant time, resources, and costs attempting to resolve them as though they are all the same, high risk. We are estimated to spend two times more than we should to complete this process today. New tools should be implemented, allowing us to better understand the risk of our vulnerabilities, manage our time and resources, and save significant money for our organization.

Nessus, a product by Tenable Network Security, is a software vulnerability scanner that finds vulnerabilities, allowing cybercriminals to gain remote access to our systems for storing, processing, or transmitting sensitive information. See **Figure 1** for a screenshot. Nessus will help to find misconfigurations and missing patches in workstations, servers, routers, and other devices, which may allow cyber criminals to escalate their access to computers or the network. Nessus will help to find default, weak, or missing passwords, allowing criminals easy access to systems or underlying information. Nessus will help to determine Denial of Service (DoS) vulnerabilities which may allow criminals to disrupt operations. According to *Ethical Hacking and Countermeasures, Linux, Macintosh, and Mobile Systems* (2010), Nessus works to detect vulnerabilities in Microsoft Windows and *NIX systems and can detect Distributed Denial of Service (DDoS) zombies and Trojans. Nessus will also allow us to scan our public-facing website frequently and allow us to mitigate discovered DDoS-related vulnerabilities before they become availability issues. Last, Nessus will help our organization prepare for forthcoming Health Insurance Portability and Accountability Act (HIPAA) based audits. Overall, Nessus will work to identify vulnerabilities in our organization and risk-rank them for resolution, help keep our customers’ data safe, and keep our intellectual property out of the hands of our competitors.



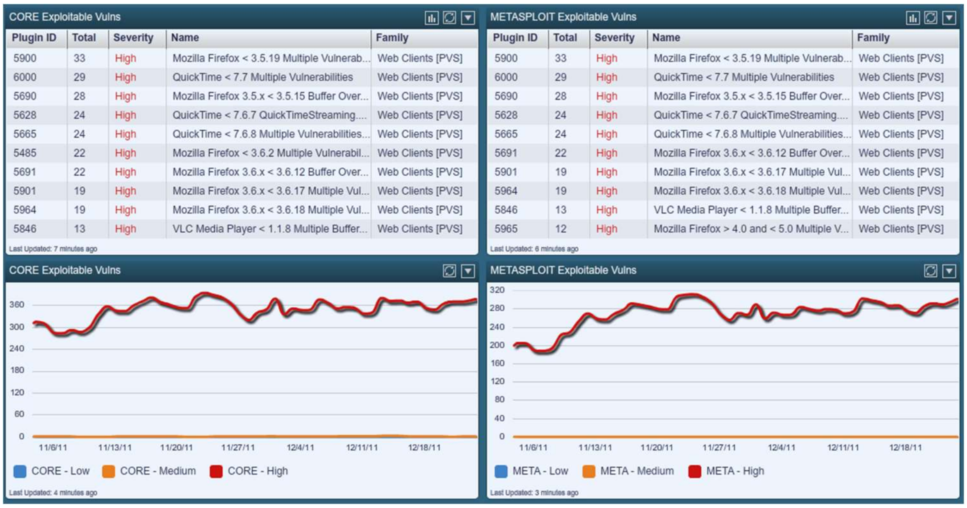
Vulnerability Summary

critical	Apple iOS < 5.1.1 Multiple Vulnerabilities	Mobile Devices	585
high	Apple iOS < 6.0.1 Multiple Vulnerabilities	Mobile Devices	645
high	Apple iOS < 6.0 Multiple Vulnerabilities	Mobile Devices	615
high	Apple iOS < 5.1 Multiple Vulnerabilities	Mobile Devices	555
high	Apple iOS < 5.0.1 Multiple Vulnerabilities	Mobile Devices	510
high	Apple iOS < 5.0 Multiple Vulnerabilities	Mobile Devices	480
medium	Windows Phone7 < 7.0.7392 Out-of-Date SSL Blacklist	Mobile Devices	15
medium	Windows Phone7 < 7.10.8107 Out-of-Date SSL Certificate	Mobile Devices	15
info	MDM Mobile Device Reporting	Mobile Devices	1130

© 1998 - 2012 Tenable Network Security®. All Rights Reserved. Nessus Version: 5.0.2 - ProFeed

Figure 1: Tennable Nessus Vulnerability Scanner

Metasploit, a product developed by Rapid7 LLC, provides ‘exploitability’ information for vulnerabilities, allowing our organization to assess risk further. See **Figure 2** for a screenshot. Metasploit is used to test systems, check for the installation of patches, and perform regression testing (*Ethical Hacking and Countermeasures, Web Applications and Data Servers,* 2010). As described above, not all vulnerabilities have known exploits in the wild. It is unknown if criminals have used discovered vulnerabilities to hack or breach a network. Although this fact does not make vulnerabilities any less exploitable, without a known exploit, the vulnerability will be less risky overall to our organization. A Nessus plug-in module, called the Metasploit Exploit Framework, will allow us to use the Metasploit framework as described here. Once the Nessus scanning utility identifies a vulnerability, Metasploit will allow us to test the vulnerability with known exploit code to determine if the vulnerability will allow criminals to actively use it to gain access to our information or underlying computer systems.



CORE Exploitable Vulns

Plugin ID	Total	Severity	Name	Family
5900	33	High	Mozilla Firefox < 3.5.19 Multiple Vulnerab...	Web Clients [PVS]
6000	29	High	QuickTime < 7.7 Multiple Vulnerabilities	Web Clients [PVS]
5690	28	High	Mozilla Firefox 3.5.x < 3.5.15 Buffer Over...	Web Clients [PVS]
5628	24	High	QuickTime < 7.6.7 QuickTimeStreaming....	Web Clients [PVS]
5665	24	High	QuickTime < 7.6.8 Multiple Vulnerabilities...	Web Clients [PVS]
5485	22	High	Mozilla Firefox < 3.6.2 Multiple Vulnerabil...	Web Clients [PVS]
5691	22	High	Mozilla Firefox 3.6.x < 3.6.12 Buffer Over...	Web Clients [PVS]
5901	19	High	Mozilla Firefox 3.6.x < 3.6.17 Multiple Vul...	Web Clients [PVS]
5964	19	High	Mozilla Firefox 3.6.x < 3.6.18 Multiple Vul...	Web Clients [PVS]
5846	13	High	VLC Media Player < 1.1.8 Multiple Buffer...	Web Clients [PVS]

Last Updated: 7 minutes ago

METASPLOIT Exploitable Vulns

Plugin ID	Total	Severity	Name	Family
5900	33	High	Mozilla Firefox < 3.5.19 Multiple Vulnerab...	Web Clients [PVS]
6000	29	High	QuickTime < 7.7 Multiple Vulnerabilities	Web Clients [PVS]
5690	28	High	Mozilla Firefox 3.5.x < 3.5.15 Buffer Over...	Web Clients [PVS]
5628	24	High	QuickTime < 7.6.7 QuickTimeStreaming....	Web Clients [PVS]
5665	24	High	QuickTime < 7.6.8 Multiple Vulnerabilities...	Web Clients [PVS]
5691	22	High	Mozilla Firefox 3.6.x < 3.6.12 Buffer Over...	Web Clients [PVS]
5901	19	High	Mozilla Firefox 3.6.x < 3.6.17 Multiple Vul...	Web Clients [PVS]
5964	19	High	Mozilla Firefox 3.6.x < 3.6.18 Multiple Vul...	Web Clients [PVS]
5846	13	High	VLC Media Player < 1.1.8 Multiple Buffer...	Web Clients [PVS]
5965	12	High	Mozilla Firefox > 4.0 and < 5.0 Multiple V...	Web Clients [PVS]

Last Updated: 6 minutes ago

CORE Exploitable Vulns

Last Updated: 4 minutes ago

METASPLOIT Exploitable Vulns

Last Updated: 3 minutes ago

Figure 2: Metasploit Framework Modules

In a case study, Rapid7 (n.d.) claims that the company Bitbrains, an IT solutions provider, reduced the time spent scanning their network from approximately one week to around 24 hours by implementing the Tenable Nessus vulnerability scanning solution. In another case study, Tenable Network Security (n.d.) claims that Essentia Health reduced its risk by more than 98% while adding five hospitals and implementing Nessus and Metasploit. From my hands-on testing and experience using both solutions, I confirm that the time required for testing, risk assessment, and mitigation of discovered vulnerabilities has been significantly reduced, if not divided in half.

The total cost for Nessus and Metasploit will be $14,000 plus tax for software and hardware and $6,000 for installation services by a third-party vendor – a total cost of approximately $20,000. Going forward, costs will be approximately $10,000 annually for licenses. It will take our team one month total for training and complete implementation. We are expected to make up this cost, due to the increased capabilities and reduced resource requirements, between 12 to 18 months. These solutions, in combination, will help us potentially save hundreds of thousands, if not millions of dollars as experienced by our competitors, on the recovery costs of stolen research data. Once implemented, all vulnerability testing will be performed after working hours (between 8:00 PM and 6:00 AM) to minimize any impact the testing has on the production systems. All DDoS testing, required to mitigate the risk of criminals bringing down our public Apache and IIS-based web servers, will be performed on Sunday mornings between 1:00 AM and 3:00 AM to mitigate the risk of impact to production-based websites as such tests may negatively impact our website and require servers to be restarted after.

In conclusion, the combination of Tenable Nessus and Metasploit will allow us to detect known software and system vulnerabilities on our current and future servers, computer workstations, web servers, databases, network devices, and all applicable services including file transfer, email, name resolution, dynamic IP addressing, and remote access VPN. With minimal costs, by implementing these solutions, we can mitigate the risk associated with threats related to the confidentiality, integrity, or availability of our customer and business proprietary data. This, in turn, will minimize the costs associated with breaches and regulatory fines, offering direct savings to our bottom line for the foreseeable future.

Security Policy Framework

I developed the following Security Policy Framework for an educational project based on NIST (2014), using JPMorgan Chase bank as the target institution (this is not an actual policy document):

MISSION

JPMorgan Chase & Co. is an American bank and financial services holding company. It is the largest bank in the United States with combined total assets of US$2.6 trillion and is the world's fourth-largest public company based on a compound ranking. The banks owned by JPMorgan Chase have a combined 5,111 branches and offices in the United States and abroad, and as of July 2022, they employ nearly 250K+ employees. The purpose of this document is to outline a methodology by which the company can use to secure its architecture and computer assets. The framework will outline ten 'enterprise areas' as documented by Bacik (2008) and NIST (2014) that will provide the institution a solid approach to securing their confidential information and assets per Federal and state laws and regulatory requirements by which they must abide.

GENERAL POLICY

a. Policy Statement

JPMorgan Chase is responsible for maintaining the confidentiality, integrity, and availability ("CIA Triad") of the information contained within their computer systems to uphold the law, meet the requirements of their customers, and continue business operations. JPMorgan Chase will implement a policy to instruct employees on requirements to secure and protect the institution's assets, information, and underlying systems. Besides ensuring that the information and assets are secured from unauthorized access, alteration, and downtime, the policy will also help to minimize fees associated with breaches.

b. Roles and Responsibilities

Overall responsibility to develop, implement, and maintain this policy falls to the Chief Information Officer (CIO). Functional responsibilities include the regional Chief Information Security Officers (CISO), the regional and local Chief Technology Officers (CTO), and underlying IT Security Managers. All JPMorgan Chase employees, including vendors and subcontractors, have a role in implementing and complying with this policy.

SECURITY POLICIES (NIST, 2014)

1.0 Risk Assessment Policy

a. Identify and document internal and external threats

b. Identify potential business impact related to threats

2.0 Asset Management Policy

a. Identify physical devices and systems within the JPMorgan Chase organization

b. Inventory all applications and software platforms

3.0 Access Control Policy

a. Incorporate the principle of least privilege

b. Incorporate separation of duties

4.0 Security Awareness and Training Policy

a. Train all employees

b. Employees acknowledge they have received and understand the policy

5.0 Information Protection Policy

a. Backups are routinely conducted

b. Data is destroyed according to policy

6.0 Technology Security Policy

a. Audit/log records are implemented, documented, and reviewed according to policy

b. Removable media is protected, and its use is restricted according to policy

7.0 Data Security Policy

a. Data is protected to ensure its availability

b. Protections against data leaks are implemented

8.0 Network Security Policy

a. Network is monitored to detect potential cyber security events

b. Monitoring for unauthorized personnel, connections, devices, and software is performed

9.0 Communication Policy

a. Personnel know their roles when a response is needed

b. Information is shared consistent with response plans

10.0 Disaster Recovery Policy

a. Incidents are contained

b. Critical business processes are restored promptly

Internet Policy

I developed the following Organizational Internet Policy for an educational project outlining the necessary security controls for consumer data protection.

Organizational Internet Policy

Security Controls and Consumer Data Protection

Policy

It is the duty and responsibility of the bank and its employees to protect consumer data per State and Federal law and treat protected data responsibly. To ensure the institution consistently meets this obligation, its IT department will implement security mechanisms and controls designed to mitigate risks associated with connecting to malicious Internet websites. For example, the department may implement automated and integrated Internet website filtering controls to limit employee access to potentially harmful, adult-related, legal liability or other websites that harbor malware such as viruses or trojans. The company's employees must use such automated security controls whenever connecting to and browsing the Internet from any company computer system. These security controls must not be circumvented, tampered with, disabled, bypassed, or otherwise rendered ineffective by any company employee at any time for any reason.

Governance

This policy follows Federal law as outlined by the Bureau of Consumer Financial Protection (2013) Part 1016 (Regulation P), the Gramm-Leach-Bliley Act (2014) for financial institutions, the Health Insurance Portability and Accountability Act (2014) for healthcare organizations, and Virginia law (2014) § 18.2-186.6 (breach of personal information notification) for all other private business entities.

Policy Effects

This policy will help the organization by mitigating risks associated with connecting to known-bad Internet websites. Such websites have a high potential for harboring malicious content, such as viruses and trojans, which could steal, modify, or destroy consumer information or the systems on which this data resides. This, in turn, mitigates the risk such breaches have on the consumer, such as Identity Theft and the loss of funds due to unauthorized access to financial accounts. Furthermore, this policy mitigates the risk and expenses such breaches have on the company due to consumer notification requirements, legal battles, fines, and reputational impacts.

Policy Consequences

At a high level, the positive consequence of this policy is diminished and manageable risk for both the consumer and the company. This translates into increased trust and enhanced relationships between consumer and company, financial safety, earning potential, and overall business continuity. In addition, as other company employees will not see fellow employees browsing adult-rated websites, no conflict will exist between what these employees know to be the company's duty and the actual browsing activity. Therefore, the probability of employee lawsuits based on such unethical browsing of peers is relatively low.

One negative consequence or side effect of this policy is that automated Internet security controls could be better and may cause sporadic business challenges. For example, some Internet filtering mechanisms may incorrectly block valid business-related websites. This is known as a "false positive," which may be caused by improper security control configuration. Regardless of the cause, inadvertent blocking results in increased Information Technology (IT) helpdesk calls, increased resource requirements, and diminished business. One solution to this challenge is to ensure adequate time and findings exist during the product research phase and that state-of-the-art Internet security control technologies are purchased and implemented adequately. This should not be considered an overnight process.

Policy Conflicts

One conflict between organizational and personal beliefs that this policy may impose on individuals is that employees may assume they have a right to privacy. By filtering Internet access, the company's management will most likely have access to employees' Internet browsing activity records. Therefore, privacy may be limited, as it is with many private organizations. Such employee privacy stipulations should be clearly defined within organizational policy documentation, such as within employee computer login banners and the employee handbook, and be readily available to all employees to ensure any confusion is dispelled.

Organizational Commitment

This policy is one in a series of organizational policies, alongside the employee handbook, which demonstrates the company's commitment to ethical and professional employee conduct, due care, and due diligence concerning the protection of consumer information. The Corporate Information Security Office has developed this policy. It is reviewed and approved by the company's Board of Directors annually or as needed for impromptu revisions. As Reynolds (2011, p. 65) stipulates, the audit committee and related employees ensure that IT organization and employees comply with this policy.

Failure to Comply

The consequences for not following this policy include but are not limited to, fines, termination of employment, or imprisonment as applicable. Specifically, intentional behavior against this policy will be grounds for penalties, termination of employment, and possibly imprisonment as justified by business type. Behavior proven to be unintentional will be carefully reviewed by a team of Human Resources, Compliance, Internal Audit, Legal, and external third-party experts to determine the proper course of action.

Data Center Password Policy

I developed the following Data Center Password Policy for an educational project using JPMorgan Chase bank as the fictitious target institution (this is not an actual policy document):

JPMorgan Chase IT Local Access Policy

Tier 1 Data Center Staff Password Policy

1. Overview

Title:	UNION COUNTY NEW JERSEY DATA CENTER, TIER 1 STAFF PASSWORD POLICY				
Part Number:	JPMCPOL002	Revision:	1	Effective:	20150129
Owner:	Anthony Scarola, Data Center Manager			Last Review:	20150129
This document supersedes all previous electronic and printed documents or oral statements regarding this policy.					
All company policies are subject to change at the sole discretion of JPMorgan Chase.					

2. Scope

This policy applies to all JPMorgan Chase Bergen County New Jersey Data Centers, Tier 1 Staff (including system support staff with access to privileged administrative passwords), contractual third parties, and agents accessing the data center information and information systems.

3. Definition

Access control rules and procedures are required to regulate who can access valuable information resources or systems (assets) and the associated access privileges. This policy requires that standards be developed for creating strong passwords, protecting passwords, and overall password use. This policy always applies and must be adhered to whenever accessing information in any format or computing device.

4. Policy

Information and information systems are critical and vital to JPMorgan Chase's mission and objectives. JPMorgan Chase has a fiduciary duty to protect, limit risk, preserve, improve, and always account for JPMorgan Chase's information. JPMorgan Chase employees must appropriately safeguard their information from dangers and threats. JPMorgan Chase's information must be protected commensurate with its sensitivity, value, and criticality. Security measures must be employed regardless of the media on which information is stored, the systems that process it, or the methods by which it is moved. Such protection includes restricting access to information based on the need to know. JPMorgan Chase staff must devote sufficient time and resources to ensure that information is adequately protected and properly protect and manage this property. Management reserves the right to audit, monitor, and log all data these systems store or transmit.

Strong passwords and user IDs work to establish a method of authentication for computer systems. Passwords also help maintain confidentiality, integrity, and availability (the CIA Triad) of information and information systems by ensuring access is granted only to authorized individuals. Weak passwords can be brute force attacked, potentially leading to unauthorized access to confidential JPMorgan Chase business, customer information, or related information systems. This, in turn, could lead to misuse of customer ID (ID Theft) and even the theft of funds due to unauthorized wire or ACH transactions via the online banking channel. As the Internet Crime Complaint Center (IC3, n.d.) outlined, this is defined as Corporate Account Take Over (ATO) fraud and was first identified in 2006.

JPMorgan Chase employee passwords should be between 12 and 14 characters in length if permitted by the system. Use fewer characters only if the target system disallows 12 to 14 characters in length (NIST, 2009, p. 3-6). If using passphrases (e.g., "ILuv2PlyB@dm1nt()n!!" for "I love to play badminton!"), 20 to 30 characters are strongly suggested if they meet the requirements outlined below. Passwords should consist of lowercase and uppercase alphabetic characters, numbers, and symbols if permitted (use lowercase and uppercase alphabetic characters and digits only if symbols are not allowed). Employees should generate passwords using automatic random creation (NIST, 2009, p. 3-8) or dictionary-based attacks to alleviate password guessing (NIST, 2009, p. 3-4). When developing passwords, employees should avoid character repetition, keyboard patterns, dictionary words, letter or number sequences, usernames, relative or pet names, romantic links (current or past), and biographical information (e.g., ID numbers, ancestor's names, or dates of birth). In addition, employees should avoid using information that is or might become publicly associated with the employee or the account, information that the employee's colleagues and acquaintances might know to be associated with the employee and avoid passwords that consist entirely of any simple combination of the weak elements.

Once passwords are created, JPMorgan Chase employees should not share passwords/passphrases with anyone else, including the IT department, auditors, co-workers, assistants, family members, or anyone else. It is recommended that employees who require many passwords use an IT-approved password manager to store passwords, as this will mitigate the risk of written passwords being discovered by unauthorized parties. As NIST (2009, p. 3-1) outlines, password managers must be encrypted. As a last resort, if you must write your password down, store it in a safe place far away from your computer workstation, server, or other device requiring the password. Last, employees must change passwords at least every 45 days. Lost or stolen passwords must be changed immediately. Employees must refrain from using the same password within three password changes. And the same passwords should not be used across varying systems or Internet sites.

By following this policy, creating strong passwords, and keeping them secure, JPMorgan Chase employees will actively apply the policy and do their part to mitigate the exploitation of related threats and overall risk to the organization.

5. Responsibilities

Information Security	Will perform regular risk and compliance reviews against JPMorgan Chase information and coordinate any information incidents.

Information Technology	Will maintain the technology required for information assurance.
Management	Must ensure that information is protected in a manner that is at least as secure as other organizations in the same industry handling the same type of information and as required by law. Must further develop and enforce this password policy.
Tier 1 Data Center Staff	They must have sufficient training and supporting reference materials to adequately protect and otherwise manage JPMorgan Chase's information. They must also review and abide by the password policy developed by JPMorgan Chase Management and report any password-related incidents (e.g., lost or stolen passwords) to JPMorgan Chase Management and Security.

6. Violations

If any user is found to have breached this policy, they may be subject to JPMorgan Chase's disciplinary procedure. If a criminal offense is considered to have been committed, further action may be taken to assist in prosecuting the offender(s).

If you need help understanding the implications of this policy or how it may apply to you, seek advice from the JPMorgan Chase Compliance Department.

7. Approvals

Sponsor Approval	Name	Date
Approved	Supervisor Landreville	January 22, 2015

8. Revision History

Revision Date	Reviser	Previous Version	Description of Revision
January 22, 2015	Anthony Scarola	N/A	Initial (version 1) policy development.

Vulnerability Assessment Matrix and Policy

I developed the following Vulnerability Assessment Matrix and Policy for an educational project using JPMorgan Chase bank as the fictitious target institution (this is not an actual policy document):

Vulnerability Assessment Matrix and Policy For JPMorgan Chase, Insider Threat

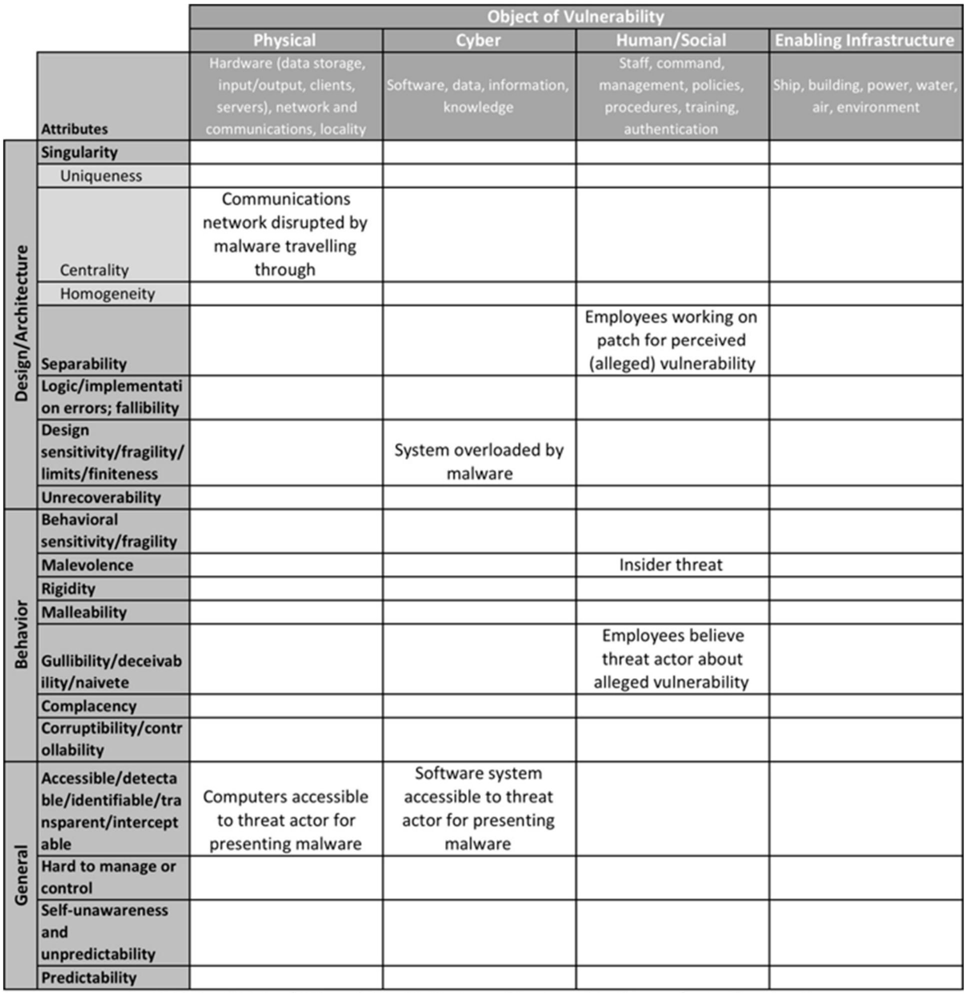
Policy is required to mitigate the risk of insider threats to JPMorgan Chase. The process outlined by Antón, P. S., Anderson, R. H., Mesic, R., & Scheiern, M. (2003) is valuable in assessing vulnerabilities and determining solutions. The process utilizes the Vulnerability Assessment and Mitigation (VAM) methodology. This top-down approach begins with identifying an organization's essential information functions and ends with testing the robustness and actual feasibilities under threat. As part of the six-step process, in step three, the organization must work to identify threats and vulnerabilities in an Assessment Matrix. The next step is to identify pertinent security techniques to mitigate the identified vulnerabilities, implement those techniques, and test to ensure the plan is successful. By following this methodology, JPMorgan Chase can identify vulnerabilities and solutions to mitigate the risk associated with the insider threat. This document runs through the process for the threat and produces a policy for JPMorgan Chase to implement to reduce this threat.

Insider Threat Scenario

The scenario for this threat is that of a malevolent insider. The insider created malware and disrupted all network traffic flowing through the system, creating a Denial of Service (DoS) attack. Before the attack, the insider persuaded employees that a vulnerability existed in a system, and they moved quickly to create a patch to address it. At the same time, the unrelated malware does its damage.

Identification of Threats and Vulnerabilities

Table 1 depicts the matrix by Antón et al. (2003, p. 27), which outlines the vulnerability attributes and system object types for the scenario described above. If not adequately planned for, insider threats, as depicted in the above scenario, can result in many problems, including deception of other employees and system and personnel resource constraints. This combination of problems may lead to a complete network failure due to overloaded circuitry.



		Object of Vulnerability			
		Physical	Cyber	Human/Social	Enabling Infrastructure
	Attributes	Hardware (data storage, input/output, clients, servers), network and communications, locality	Software, data, information, knowledge	Staff, command, management, policies, procedures, training, authentication	Ship, building, power, water, air, environment
Design/Architecture	Singularity				
	Uniqueness				
	Centrality	Communications network disrupted by malware travelling through			
	Homogeneity				
	Separability			Employees working on patch for perceived (alleged) vulnerability	
	Logic/implementation errors; fallibility				
	Design sensitivity/fragility/ limits/finiteness		System overloaded by malware		
	Unrecoverability				
Behavior	Behavioral sensitivity/fragility				
	Malevolence			Insider threat	
	Rigidity				
	Malleability				
	Gullibility/deceivability/naivete			Employees believe threat actor about alleged vulnerability	
	Complacency				
	Corruptibility/controllability				
General	Accessible/detectable/identifiable/transparent/interceptable	Computers accessible to threat actor for presenting malware	Software system accessible to threat actor for presenting malware		
	Hard to manage or control				
	Self-unawareness and unpredictability				
	Predictability				

Table 1 - Matrix of Vulnerability Attributes and System Object Types for Insider Threat

Identification of Issues, Resolutions, and Solutions

Table 2 identifies the insider threat scenario's issues, resolutions, and solutions. As the table shows, insider threats and their results can be mitigated by combining general management practices (before the event), including intelligence operations, policies, system hardening, network segmentation, employee awareness and threat knowledge, monitoring, and assessments.

Additional measures can be used during the threat, including rapid detection and response to the malicious event and ensuring adequate staff would be readily available and not distracted or led astray by alleged and potentially non-existent vulnerabilities.

Typical behaviors or triggers that could be indicators that insider threats may or could occur include (Lockheardt, 2012):

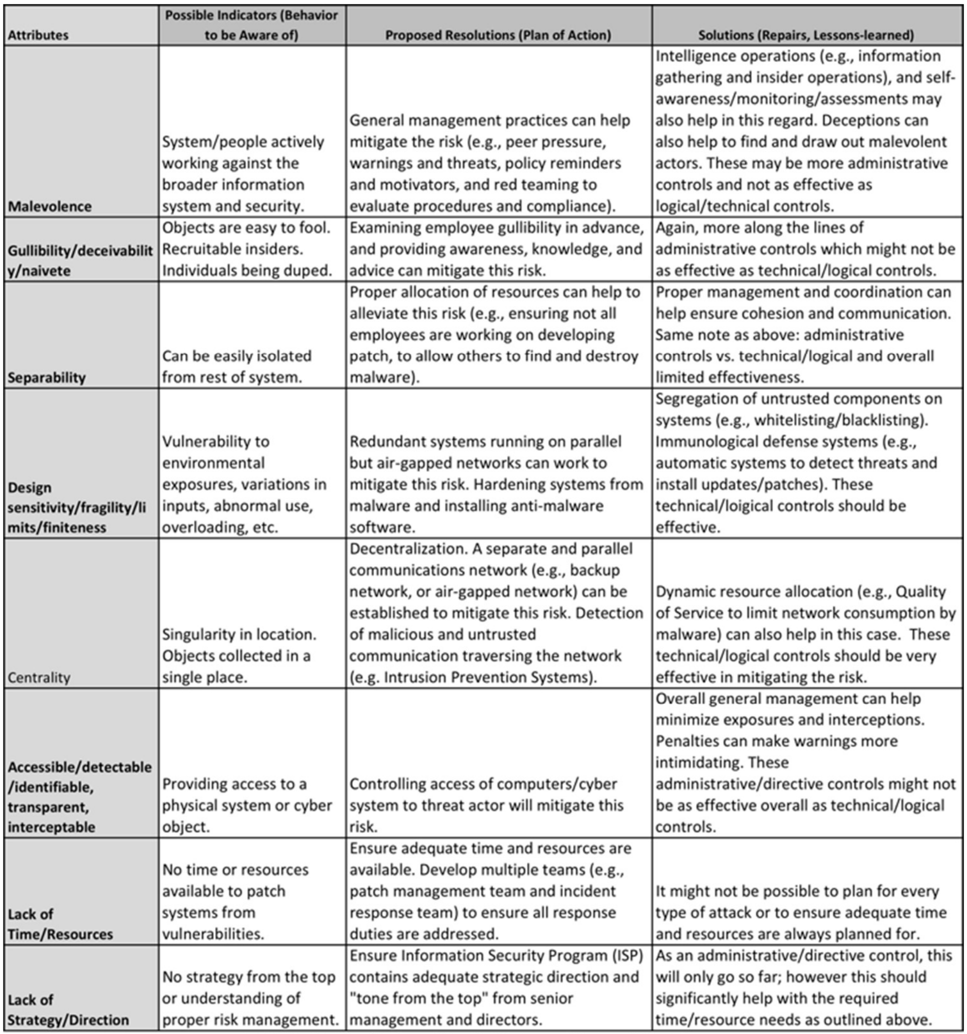
- Employee's use of removable media, printers, or copiers far from the office;
- Employees logging onto the computer system in a building despite not being signed in at that building;

Gelles, M. G., Mahoutchian, T., & Deloitte Consulting (2012) outline that such employees might also have the following characteristics:

> A history of managing crises ineffectively; a pattern of disappointment, frustration, and a sense of inadequacy; seeks validation; an aggrandized view of their abilities and achievements; a strong sense of entitlement; views self above the rules; actions seek immediate gratification, validation, and satisfaction.

Considering these characteristics and triggers, monitoring the JPMorgan Chase enterprise employees and reporting any such activity would make sense. Discussing employee behavior with Human Resources on some frequency would also help to mitigate the overall insider threat and potential high risk they might incur.

Table 3 is a table of analysis based on the attributes outlined, which provides the characteristics, identification of potential indicators (behaviors to be aware of), proposed solutions (plans of action), and solutions (repairs, lessons learned, etc.) JPMorgan Chase should use this information, solutions, and plans as the policy to address the insider threat.



Attributes	Possible Indicators (Behavior to be Aware of)	Proposed Resolutions (Plan of Action)	Solutions (Repairs, Lessons-learned)
Malevolence	System/people actively working against the broader information system and security.	General management practices can help mitigate the risk (e.g., peer pressure, warnings and threats, policy reminders and motivators, and red teaming to evaluate procedures and compliance).	Intelligence operations (e.g., information gathering and insider operations), and self-awareness/monitoring/assessments may also help in this regard. Deceptions can also help to find and draw out malevolent actors. These may be more administrative controls and not as effective as logical/technical controls.
Gullibility/deceivability/naivete	Objects are easy to fool. Recruitable insiders. Individuals being duped.	Examining employee gullibility in advance, and providing awareness, knowledge, and advice can mitigate this risk.	Again, more along the lines of administrative controls which might not be as effective as technical/logical controls.
Separability	Can be easily isolated from rest of system.	Proper allocation of resources can help to alleviate this risk (e.g., ensuring not all employees are working on developing patch, to allow others to find and destroy malware).	Proper management and coordination can help ensure cohesion and communication. Same note as above: administrative controls vs. technical/logical and overall limited effectiveness.
Design sensitivity/fragility/limits/finiteness	Vulnerability to environmental exposures, variations in inputs, abnormal use, overloading, etc.	Redundant systems running on parallel but air-gapped networks can work to mitigate this risk. Hardening systems from malware and installing anti-malware software.	Segregation of untrusted components on systems (e.g., whitelisting/blacklisting). Immunological defense systems (e.g., automatic systems to detect threats and install updates/patches). These technical/loigical controls should be effective.
Centrality	Singularity in location. Objects collected in a single place.	Decentralization. A separate and parallel communications network (e.g., backup network, or air-gapped network) can be established to mitigate this risk. Detection of malicious and untrusted communication traversing the network (e.g. Intrusion Prevention Systems).	Dynamic resource allocation (e.g., Quality of Service to limit network consumption by malware) can also help in this case. These technical/logical controls should be very effective in mitigating the risk.
Accessible/detectable/identifiable, transparent, interceptable	Providing access to a physical system or cyber object.	Controlling access of computers/cyber system to threat actor will mitigate this risk.	Overall general management can help minimize exposures and interceptions. Penalties can make warnings more intimidating. These administrative/directive controls might not be as effective overall as technical/logical controls.
Lack of Time/Resources	No time or resources available to patch systems from vulnerabilities.	Ensure adequate time and resources are available. Develop multiple teams (e.g., patch management team and incident response team) to ensure all response duties are addressed.	It might not be possible to plan for every type of attack or to ensure adequate time and resources are always planned for.
Lack of Strategy/Direction	No strategy from the top or understanding of proper risk management.	Ensure Information Security Program (ISP) contains adequate strategic direction and "tone from the top" from senior management and directors.	As an administrative/directive control, this will only go so far; however this should significantly help with the required time/resource needs as outlined above.

Table 3 - Matrix of Vulnerability Attributes and System Object Types

In summary, the process outlined by Antón et al. (2003) should be used to assess vulnerabilities and determine plans and solutions to address the insider threat. JPMorgan Chase should follow this methodology for vulnerabilities and solutions to mitigate the risk associated with the insider threat.

Cloud Computing Security Policy

I developed the following Cloud Computing Security Policy for an educational project for the fictitious company "SNPO-MC, Inc.":

Cloud Computing Security Policy

For SNPO-MC, Inc. by USA Management Consulting, Inc.

I. Purpose

The purpose of this draft policy is to provide industry best-practice guidance to the managers, executives, and cloud computing service providers of the SNPO-MC, Inc. organization, headquartered in Boston, MA, on the acquisition, management, and cessation of cloud computing environments, considering related threats and overall risk. As part of the development of this policy, issues outlined by SNPO-MC, Inc. executives and managers during preliminary brainstorming sessions were thoroughly considered and included herein, along with risk-based solutions. Once approved, this draft policy will supersede the existing SNPO-MC, Inc. Enterprise IT Security Policy, which works to address the security requirements for organizational assets and equipment, including database servers, web and email servers, file and print servers, remote access servers, and workstations to include desktops and laptops as well as all related and integrated software applications as related to cloud computing environments.

II. Definitions

Cloud computing, as defined by Mohanty, Pattnaik & Mund (2014), "[…] is an emerging field in the era of internet where information and physical resources can be provided to cloud users according to their needs in pay-per-go basis" to include, "[…] public cloud, private cloud, hybrid cloud, and community cloud" (p. 261).

According to Choudhary & Vithayathil (2013, p. 69), cloud computing has been characterized by three primary elements to include *infrastructure as a service* (IaaS), *platform as a service* (PaaS), and *software as a service* (SaaS). At the most basic level of cloud computing, *IaaS* includes the necessary physical and environmental elements, such as physical storage (e.g., the building, the rooms, and the server racks), HVAC, power, and Internet connectivity. Building upon this, *PaaS* may include virtualized server operating systems (e.g., the hypervisor). *SaaS* contains everything mentioned above, including the application (e.g., PeopleSoft human resource management system). Depending on the cloud-computing vendor, additional functionality and services may be appended to these three core elements to complete the solution.

SNPO-MC, Inc. refers to its employees as *employees*. *Staff members* include all executives and other employees on loan' from the Fortune 500 organizations SNPO-

MC, Inc. does business with. Last, SNPO-MC, Inc. refers to *volunteers* as those staff employees who generally telework from their homes once or twice weekly to perform volunteer work for the organization. All SNPO-MC, Inc. employees, staff members, volunteers, and 3rd party cloud computing service providers must agree to familiarize themselves with and abide by this policy.

Inherent risk is the risk that exists fundamentally before the organization implements security controls or control measures. Controls are the administrative, technical/logical, and physical elements or methodologies implemented by an organization to lower inherent risk (e.g., this policy document, firewalls, Intrusion Prevention Systems, access controls, and authentication systems). *Residual risk* is the risk that exists after controls are implemented. Reference the SNPO-MC, Inc. Corporate Information Security Risk Management Framework policy and methodology for details on these elements.

Confidential information includes information with sensitivity levels identified and classified as *low*, *moderate*, and *high*, excluding all known-public information, as outlined within the SNPO-MC, Inc. Corporate Information Security Program policy and also highlighted below:

Sensitivity Level:	**Low**	**Moderate**	**High**
Examples:	Administrative organizational data includes any general information about the organization or its customers that is required to continue business operations. This might consist of customer demographic data or general transactional details.	Confidential institution data to include business and financial transactions of the organization or its employees. This is considered need-to-know information only. This would consist of business financial transactions without public knowledge or customer names not associated with other identifiers.	Regulated information includes customer-sensitive information, personally identifiable information (PII), non-public information (NPI), protected health information (PHI), financial records, and customer payment information (e.g., credit card data). This would include customer names and identifiers such as social security numbers or account credentials (e.g., usernames and passwords).
Handling:	Information in these categories may be provided to		Information in this category

	3rd party cloud services hosting providers to be used for organization business only. Information may be hosted in environments shared at the equipment (IaaS) and operating system (PaaS) level; however, not at the SaaS level unless encryption is in use. Such information can only be shared with 3rd party cloud hosting service providers with an active and valid non-disclosure agreement (NDA). Information at this or higher sensitivity levels is to be transmitted to the 3rd party cloud hosting provider via approved encryption methods as defined by the organization or in-person for physical delivery. Information must be backed up in encrypted form to multiple backup facilities. Information must be destroyed when it is past its usable life per organizational data retention policies using organization-approved methods only. All information will be labeled "sensitive: low" or "sensitive: moderate" as applicable.	may not be provided to third-party cloud services hosting providers unless it is explicitly hosted on servers dedicated to the organization and not shared with other cloud hosting service provider customers. Such information can only be shared with third-party cloud hosting service providers with an active and valid non-disclosure agreement (NDA). The information must be encrypted at rest, in motion, or processed by the cloud hosting service provider or the user. All information in this category will be labeled "sensitive: high."

Please refer to the SNPO-MC, Inc. Corporate Information Security Program policy for a complete description of confidential information and proper handling procedures for compliance.

III. Scope

Once this draft policy is approved, it will cover all employees, staff members, and volunteers of the SNPO-MC, Inc. organization, headquartered in Boston, MA, to include all remote teleworker employees operating out of the New Orleans, LA, and San Francisco, CA, facilities. The policy outlines controls to manage threats against the confidentiality, integrity, and availability (CIA Triad) of SNPO-MC, Inc. confidential information and related applications and systems as outlined within the SNPO-MC, Inc. Corporate Information Security Program policy and related risk assessment. The policy will cover all organizational and personal equipment used for SNPO-MC, Inc. business, including the equipment and systems acquired or 'on lease' from cloud service providers.

IV. Policy Statement

1. Overview

The definition of cloud computing, as defined by Mell & Grance (2011) in the *NIST Definition of Cloud Computing*, "[… It] is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider configuration" (p. 2). See also the definitions outlined in Section II above. Within this policy, the cloud computing environments being addressed are those at the infrastructure (IaaS), platform (PaaS), and application (SaaS) levels, and either only those services defined as "cloud services" by applicable 3rd party solution providers or services matching the descriptions as described within this policy.

Considering that cloud computing environments are generally designed, developed, operated, and maintained by 3rd party vendors (outsourced providers), that typically such environments are shared between multiple customers of those vendors, that such environments are relatively quick and easy to deploy, and that such environments are generally accessible to the Internet where they are susceptible to attack and breaches, significant inherent risk exists. With the known threats and high levels of inherent risk of cloud services, controls must be implemented for the acquisition, management, and disbanding of such environments to mitigate that risk to acceptable levels. These controls are outlined by the SNPO-MC, Inc. confidential information classification and handling guidelines addressed in the Corporate Information Security Program policy document and the additional, more specific policy elements.

2. Applicability

As outlined in Section II above, this policy applies to all SNPO-MC, Inc. employees, staff members, volunteers, and applicable 3rd party cloud computing service providers acquiring, implementing, using, managing, servicing, operating, monitoring, testing, or disbanding cloud computing services owned, leased, or licensed. In addition, this policy applies to all SNPO-MC, Inc. confidential information as defined in Section II above, including any low, moderate, and high sensitivity level data. Last, this policy covers all computing devices configured to access the cloud computing environment and confidential information retained as defined herein, including all SNPO-MC, Inc. purchased equipment and any employee personally owned equipment.

3. Acquisition

Cloud computing solutions may only be purchased by SNPO-MC, Inc. after a full security review by the IT Security Officer, contract review by the Vendor Management department, and approval by the Chief Information Officer (CIO). Cloud computing solutions may only be acquired via a purchase order from the SNPO-MC, Inc. Accounting department. They must not be purchased using company credit cards, checks, or other payment methods. Last, individual SNPO-MC, Inc. employees, staff members, volunteers, or 3rd party cloud computing service providers must not purchase cloud computing services. Before acquisition, cloud computing service contracts must be reviewed and approved by the applicable SNPO-MC, Inc. line of business manager and the Vendor Management contract review team. The final contract, including all prior changes, must be submitted with signatures by the line of business manager and the Vendor Management contract review manager to the Chief Information Officer (CIO), along with the IT Security team review and signature. Please refer to applicable policies for the Vendor Management department, contract review, and financial review for further details.

4. Compliance Reviews and Attestation

Annually, the applicable SNPO-MC, Inc. line of business manager will review the cloud services contract to include the financials, legality, and security controls (e.g., SOC reports) in place to protect SNPO-MC, Inc. confidential information per regulatory requirements. Resources from the Legal, IT Security Manager, Vendor Management, and Credit Review/Accounting departments may be utilized as required. The SNPO-

MC, Inc. Vendor Management department will schedule and coordinate reviews. Attestation of compliance reviews will be submitted to the Chief Information Officer (CIO) with all applicable signatures. Throughout the year, the appropriate line of business manager will be ultimately responsible for all contracted service level agreement (SLA) monitoring and management. Significant SLA issues and challenges will be reported quarterly to the IT Steering Committee or the CIO if more immediate reporting is necessary.

5. Content Ownership

All information stored, hosted, transacted with, transmitted to, received by, or otherwise processed by the applicable cloud-hosted service provider by way of the system, application, or program outlined by the contracted service will be owned solely by SNPO-MC, Inc. unless otherwise agreed upon by the SNPO-MC, Inc. Chief Executive Officer (CEO). This applies to all information, not only information deemed confidential. SNPO-MC, Inc. will own all such information until it has reached its useful life as outlined by the SNPO-MC, Inc. Retention Policy. After that, the data must be securely deleted per SNPO-MC, Inc. IT Security policy and procedures.

6. Privacy and Confidentiality

All SNPO-MC, Inc. confidential information stored, processed, transmitted, or received by the cloud services solution provider must be kept private and secure from unauthorized access per the SNPO-MC, Inc. Corporate Information Security Program policy. In addition, any confidential information classified with a high sensitivity level must only be hosted on dedicated equipment and not shared with other provider customers per SNPO-MC, Inc. policy, as such information is further protected by applicable state and federal law and related regulations. All breaches of confidentiality must be reported immediately (within 24 hours or less) by the 3rd party cloud services provider to the SNPO-MC, Inc. Privacy Officer. Once breaches are reported, notice will be provided to the SNPO-MC, Inc. Regulatory Compliance Officer for further action as required by SNPO-MC, Inc. Corporate Incident Response Program policy, applicable state and

Federal laws, and regulations. Please also refer to the ISO 27018 standard, which, as Kean et al. write, "[…] addresses the [privacy] controls required for PII" (2012, p. 18).

7. Departmental Use

Any department of SNPO-MC, Inc. may use cloud computing services without restriction, including Sales and Marketing, Customer Service / Outreach, Public Relations and Corporate Communications, Advertising and e-commerce, or Teleworkers. Regardless of the department, note that all departments and employees must adhere to this policy while SNPO-MC, Inc. company confidential information is stored, hosted, or processed by the 3rd party cloud services hosting provider. Last, every department or employee must refrain from bypassing any security controls or control measures implemented to mitigate the risk associated with cloud services environments.

8. Content and Services Monitoring Tools

All information (content) sent to or received from the cloud services hosting provider must be monitored by the IT Security Officer for compliance with the handling elements (e.g., encryption) of this policy, as outlined in Section II above. All encrypted elements will be decrypted and inspected for compliance with the SNPO-MC, Inc. Corporate Information Security Program policy, confidential information classifications, and handling requirements. In addition, all cloud services systems will be monitored for adherence to contracted Service Level Agreements (SLAs) by the applicable line of business manager and the IT department. Services falling outside the contracted SLAs will be reported as documented in Section IV, item 4 above.

9. Penalties for Violations of Policy

Any parties violating this policy may be immediately terminated from employment with SNPO-MC, Inc. If violations occur with the 3rd party cloud services solution provider (vendor), applicable contracts may be immediately removed. It is ultimately the responsibility of the SNPO-MC, Inc. Chief Executive Officer (CEO) to determine employee or contract fault and decide the outcome.

V. Review Entity(ies) and Review Cycle

Once approved, IT Management, the Information Security Officer, and the Chief Information Officer (CIO) will review this draft policy annually. See section XII below concerning the details and methodologies of revision.

VI. Approval Date

This draft policy has yet to be approved. Once approved, the approval date will be added to this document at this location.

VII. Effective Date

This draft policy will become effective upon approval. Once approved, the Chief Information Officer (CIO) will declare the 'effective date' and add it to this document at this location.

VIII. Executive Sponsor(s)

Executive sponsors include the SNPO-MC, Inc. cloud computing grant overseers. Once the grant overseers approve this draft policy, the individual names and titles of these individuals will be added to this document in this location.

IX. Policy Manager(s)

This draft policy, once approved, will be managed and maintained by the office of the Chief Information Officer (CIO) of SNPO-MC, Inc., monitored and enforced by IT and IT Security management.

X. Responsible Office(s)

The office of the Chief Information Officer (CIO) is responsible for monitoring and managing this policy to ensure compliance with laws and regulations applicable to SNPO-MC, Inc. As section XIII below outlines, the Human Resources and Vendor Management departments are responsible for distributing this policy.

XI. Supersedes

This policy replaces the existing SNPO-MC, Inc. Enterprise IT Security Policy; however, any elements contained in the SNPO-MC, Inc. Enterprise IT Security Policy not directly replaced by this Cloud Computing Security Policy (e.g., any internal information, systems, or assets not covered by cloud computing) will still be covered by the existing policy until such elements are captured within this document.

XII. Revision

SNPO-MC, Inc. may revise the information contained within this policy as deemed necessary to meet business objectives. All revision suggestions (proposed changes) will be submitted to the Chief Information Officer (CIO) annually for final review and approval.

XIII. Distribution

Once this draft policy is approved, it will be distributed by the Chief Information Officer (CIO) to the Human Resources department for further distribution, review, and acknowledgment by all other SNPO-MC, Inc. employees, including staff and volunteers. In addition, the Vendor Management Manager will provide the policy to all existing 3rd party cloud hosting service providers for review and acknowledgment. All acknowledgments must be captured within 30 days of distribution by either the Human Resources department (for employees/staff/volunteers) or the Vendor Management Manager (for 3rd party cloud hosting service providers) and delivered to the office of the Chief Information Officer (CIO).

Disaster Recovery / Business Continuity Program Assessment

Here is an assessment paper I developed in 2017 as an educational project for a fictitious company, “WeSecure, Inc.” of another fictitious company “Bank Solutions”:

Abstract

The purpose of this paper is to examine the referenced case study, *Bank Solutions Disaster Recovery and Business Continuity* (Camara, Crossler, Midha, & Wallace, 2011), to determine information technology/security gaps and provide a security strategy that includes addressing issues relating to confidentiality, integrity, and availability (CIA), and including the key elements relative to people, process, and technology. This paper will cover five specific steps: 1) a description of the key issues/challenges/risks; 2) a description and documentation of the recommended security strategy to mitigate the issues/challenges identified; 3) a description of the proposed security solutions and relationship to the case study; 4) a detailed, proposed

timeline for addressing each element of the identified strategy along with necessary resources and estimates including the rationale for implementing the strategy; and, 5) a high-level recommendation regarding the next steps required to mitigate the identified risks.

Keywords: case study, disaster recovery, business continuity, incident handling

Bank Solutions Disaster Recovery and Business Continuity

Introduction

Bank Solutions is a mid-sized company that provides item processing solutions for approximately 345 financial institutions. In 2011, our company, WeSecure, Inc., was hired to perform a security assessment of the business continuity, disaster recovery, and incident response programs, policies, controls, and procedures to prepare the company for a potential buyout. Federal regulatory compliance, industry standards, and information security best practices were considered as part of this assessment. WeSecure, Inc. has prepared this assessment report to identify the risks discovered and potential solutions to mitigate them. It is highly recommended that Bank Solutions take the suggested next steps to address compliance and industry information security standards. Failure to do so may increase the risk associated with a network intrusion or a failure of one or more Bank Solutions processing centers and ultimately cause reputational harm and/or financial loss.

Key Issues, Challenges, and Risks

People

Bank regulators expect financial institutions to have practices in place to plan for and protect against disasters adequately. The Federal Financial Institutions Examination Council (FFIEC) requires explicitly that institutions have adequate personnel who are sufficiently trained on business continuity plans and procedures, as outlined within the *IT Examination HandBook InfoBase*, *Business Continuity Planning* booklet, *Appendix G* (FFIEC, n.d.) During the information assessment risk assessment, it was discovered that Bank Solutions has not adequately trained critical plan participants to use the Disaster Recovery Business Continuity Plans (DRBCPs). In addition, these participants have not received the latest copies of the plans, which are currently stored on the network. In the case of a disaster, such network plans would likely not be accessible. Without adequate training, key plan individuals would not know what to do or who to call to ensure proper recovery procedures are taking place.

Process

Although the current Bank Solutions DRBCP contains sections covering emergency/crisis response procedures, business recovery procedures, “return to normal” procedures, and various appendices, it fails to document other critical sections addressing personnel matters, communication protocols, facilities, electronic payment systems, liquidity concerns, financial disbursement, or manual operations, as required by the FFIEC (n.d.). In addition, the Bank Solutions DRBCP does not contain key information such as Recovery Time Objectives (RTO) or Recovery Point Objectives (RPO). RPOs, as defined by Singh (2008), are “[…] the interval of time that might pass during a disruption before the quantity of data lost during that period exceeds the Business Continuity Plan’s maximum allowable threshold or ‘tolerance’”. RTOs, as defined by Isaacson (2005), are “the point in time when you must have at least the critical aspects of your business operational again.” The RTO and RPO elements must be identified as part of the Business Impact Analysis (BIA) process, in which the Bank identifies its assets and prioritizes them for recovery purposes. Some of the information required for this process is outlined in the current DRBCP appendices.

The most recent DRBCP test occurred four years ago and was conceptual (table-top). In addition, only engineers and data center managers—only those very familiar with the sites and technology—were included in the exercises. Item processing facility testing has not taken place. DRBCP testing is insufficient, does not cover all facilities, and does not include all required personnel. Should a disaster occur, recovery efforts will likely fail.

Today, disasters come in all shapes and sizes. As our organizations rely heavily on technological systems and the information stored and processed on them about our customers, technology-based disasters—such as network intrusions and distributed denial of service attacks—must be considered for business continuity planning purposes. Bank Solutions does not currently account for such technological disasters in its DRBCP, which, like physical disasters, can impact the availability of the network, the financial institution's computing systems, and, ultimately, its customers.

The confidentiality and integrity of server event log data, tightly controlled access, and segregation of duties must be maintained in a network environment, especially in those where financial transactions take place and sensitive customer data reside. Failure to do so could lead to successful insider attacks or failure to detect and provide the data on such attacks after the fact for legal and prosecution purposes. Although Bank Solutions does an excellent job logging privileged server activity, power users can overwrite their logs.

Technology

It is vital that complex financial institutions have adequate backup and recovery strategies and technology in place and that these backup strategies function properly and are tested routinely. Bank Solutions fully backs up critical data files, software programs, and configurations once a week, with incremental backups daily (Monday through Friday) at all locations. In addition, daily transaction details and item image files from the current day's processing operations are uploaded from each item processing facility to their regional data center (see Appendix A). Finally, electronic vaulting has been established whereby all e-mail, file, and application servers and databases at the data center are continuously backed up to the other data center via dual dedicated fiber optic lines. Although this strategy seems sound, there are a few key flaws. First, replication will surely fail if the dual dedicated fiber optic lines get cut, without adequate network routing and backup connectivity (preferably via alternate circuit types). Second, if time allows, Bank Solutions should perform full [versus incremental] backups daily to lessen recovery time should these backups be required. Last, at least one processing facility backup job is failing due to unknown causes, with reliance on the replication process. Should this item processing facility require a complete restoration, it may be nearly impossible without the critical system files necessary for recovery.

Recommended Security Strategy and Proposed Security Solutions

The key to developing a sound disaster recovery and business continuity plan is to establish a strategy that first includes identifying the business assets (people, processes, and technology including infrastructure, applications, and systems). Once assets are identified, as part of the business impact analysis (BIA) process, the business should prioritize these assets in some manner to establish their criticality to the organization. For example, processes, systems, and applications can be categorized based on tiers and grouped together based on the criticality or required recoverability (e.g., considering recovery time objectives [RTO]). Next, the organization should consider various physical and logical threat events that may impact these assets. For example, at the process level, the impact can be evaluated for various natural disasters (hurricanes, earthquakes, tornados, floods, etc.) and information security threats (network intrusions causing a loss of confidentiality, integrity, and/or availability of a system or the information stored, transmitted, or processed by it). Next, the organization must implement solutions to protect the critical assets and document the recovery procedures. Last, all employees must be trained to perform their roles in a disaster. The Department of Homeland Security (DHS, n.d.) has online information to assist organizations in developing information technology disaster recovery and business continuity plans. Visit https://www.ready.gov/business/emergency-plans/recovery-plan for details.

Network and application security and continuity must be constantly maintained, regardless of the development or implementation status of the disaster recovery and business continuity plans. In the case of Bank Solutions, this means that segregation of duties must be implemented to protect system activity and event logs; system administrators must not be able to write over event logs. Current backup failures must be investigated to ensure errors and issues are corrected. The network architecture should be re-evaluated to ensure backup circuits exist between the two data centers. Last, the institution should consider performing full backups versus daily incremental backups. Failure to take these steps immediately could seriously impact the institution in the case of a disaster, potentially causing reputational harm and/or financial loss.

Timeline, Resources, and Estimate; Recommended Next Steps

It is recommended that Bank Solutions consider the following timeline to correct the material deficiencies discovered:

Task	Description	Duration	Start Date	End Date	Resources Required	Estimated Cost
BIA	Perform Business Impact Analysis	4 weeks	1/23/17	2/13/17	DR manager, LOB managers, IT personnel	N/A
BIA: Identify and Prioritize Assets	Identifies and prioritizes assets as they relate to the business	2 weeks	1/23/17	2/6/17	DR manager, LOB managers, IT personnel	N/A
Refresh DRBCP Documentation	Refresh DRBCP Documentation	1 week	2/20/17	2/27/17	40 hours to collect information from BIA and document	N/A
Print and Distribute DRBCP Plan	Print and Distribute DRBCP Plan	1 day	2/27/17	2/28/17	1 hour for project manager	N/A
Training	Train employees on disaster recovery and business continuity plans	1 week (2 hours per employee)	2/28/17	3/7/17	Every employee	N/A
DRBCP Testing	Perform monthly table-top and quarterly live testing of plan	8 hours monthly for table-top, 16 hours quarterly for live testing	3/13/17	Ongoing	IT resources, LOB resources as required	N/A

Task	Description	Duration	Start Date	End Date	Resources Required	Estimated Cost
Correct Access Control Issues with Logging	Ensure power users are unable to overwrite logs and test	1 day	ASAP	+1 day	IT resources, LOB resources as required	N/A
Develop Backup Circuit Connectivity	Design and implement backup circuits between data centers	1 month	ASAP	+1 month	IT resources	$50,000 for implementation
Redesign backup strategy	Redesign and reengineer backup strategy	1 week	ASAP	+1 week	IT resources	N/A
Assess backup failures	Troubleshoot and resolve backup failures at item processing facilities	1 week	ASAP	+1 week	IT resources	N/A

Closing

In 2011, our company was hired to assess the business continuity and disaster recovery plan for Bank Solutions to prepare the company for a potential buyout. As a conclusion of this assessment, it was determined that issues and challenges exist as outlined in this report. Issues exist in the backup strategy, system and security access controls, network architecture, and backup applications. Issues also exist with the business impact analysis process, DRBCP plan documentation, training, and testing. WeSecure, Inc. has concluded that the issues can be corrected by considering regulatory requirements (FFIEC) and industry best practices within a small amount of time and for a minimal amount of money, as outlined within this report. Bank Solutions should take these steps immediately to ensure compliance and resiliency to threats and resulting business risk. This will help to limit the impact of insider threats and business continuity failures, helping to continue to provide imaging services to Bank Solutions' clients and indirectly to bank customers nationally.