Cybersecurity Assessment & Compliance Strategy for a Non-Profit Organization

Team/Students: Frank Castro & Reda Haj Nassar | ***Business Advisor:*** Jane Smith | ***Professor:*** Dr. Yair Levy, Professor of IS & Cybersecurity

Introduction

Non-profit organizations provide a variety of services to the public. In doing so, these non-profit organizations often obtain and share sensitive and Personal Identifiable Information (PII) (Bruce, 2020, p. 4). Often operating with limited budgets and relying on grants and federal funding, these organizations often encounter difficulty implementing adequate safeguards to prevent data breaches, and further lack the resources and knowledge to react appropriately in the event of such a breach(Founders Technology Group, LLC, 2020). The impact of such a breach, if identified, could have significant consequences of the organization's ability to provide its services, by both hindering operations, and having State law consequences which can force a shut-downs of operations due to the size of monetary penalties (de Groot, 2021). As such, the goal of this project is to assess the business processes and tools of a small South Florida non-profit organization, identify gaps and risks in how they work with client information, and to provide the non-profit with an Information Security and compliance strategies. This information security policies will outline the steps needed to protect user data in storage and in transit, and the compliance strategy will outline ways in which the non-profit organization can maintain and test for adherence to state and federal regulations related to the handling of PII.

Problem

The problem which this project will focus on is privileged account compromise. Privilege account compromise occurs when one or more accounts holding elevated access to critical systems and data is compromised (Gegick, Barnum, 2013). There are several ways the account can be compromised; it can occur through the unintended installation of malware, fraudulent emails, fraudulent login sites, key-logging, phishing, and brute force (Linden, 2019). Once the user with elevated access has their account compromised, the account can be used to perform cyberattacks directly, or to create and elevate access to additional accounts and processes for even broader access to internal systems. Cyberattacks related to privileged accounts and elevated access are quite common. In fact, it has been reported that nearly all damaging cyberattacks involved privileged account compromise (Linden, 2019, p. 1). As reported at the start of the COVID 19 pandemic, the number of severe ransomware attacks increased, with several government and hospital entities falling victim to these attacks (Waldman, 2021). The key detail, however, identified as the root cause for most of these attacks is that a highly privileged individual had their account compromised and provided the attackers with the initial point of entry. Once the attackers gain access via the privileged account, they proceed to elevate access to additional users and resources, resulting in what is described as an irreversible network takeover attack (Linden, 2019). In fact, of the top 10 ransomware attacks of 2021, the 3rd largest attack was to CNA Financial, which is one of the largest insurance carriers in the U.S. It cost the company two months of downtime and $40 million dollars to recover, as CNA paid the ransom requested as a last resort (Waldman, 2021).

Facts

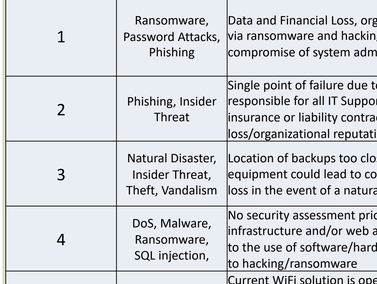
This project proposal will focus on a small non-profit organization named Auxilio. This organization obtains federal funds and grants to provide services to migrant workers and their families. The services include childcare, rent assistance, education and language services, immigration services, social work, food and clothing. The organization runs with limited internal resources; between three locations there are a total of 15 employees providing services, with occasional assistance from student volunteers. Of the 15 employees, there are no dedicated Information Technology (IT) or Infosec resources. Instead, the organization relies on a single, private company with one IT resource. This technical resource administers server maintenance, server access, storage allocation and access, hardware and software maintenance, security escalations requests. As there is very little IT knowledge within the organization, this external resource has been provided with the proverbial 'keys to the kingdom' and has admin/system level access to all technology resources in the organization. Support services are often provided remotely via remote desktop sessions, without the usage of a secure VPN connection. The liaison to this external resource is the executive assistant/program manager/business advisor. Along with the external IT resource, she also has access to most of the passwords (not all). Individual user security access is managed ad-hoc, as the organization has no policies or recommendations to employees related to passwords. There are no minimum passwords enforced, and no cycle in place requiring routine updates to system passwords. System access is limited to the individual systems that the employees use and allocated network resources. Some employees (specifically accounting and program manager) have remote access via Windows remote desktop (and RDT services for Windows server). Types of sensitive information that employees work with on a daily basis include social security numbers, work permit numbers, names, addresses, and income information. It has been explained that Social Security information is not retained electronically; the individual information is uploaded into a web-accessible application which then provides a unique ID for the individuals, with additional documents stored on network drives and email. In regard to current strategies for managing risk and compliance, the organization does have a disaster recovery plan, however this plan is limited to employee contact information and procedures in the event of an office closure. The initiation of the emergency/incident response plan fall on the Director, as well as the business advisor/program manager and contacts throughout the satellite locations. In total, four individuals are authorized to initiate the incident response plan. The details within the disaster recover plan are audited routinely every September.

Project Scope & Goals

The goal of this project is to develop an IT Security Policy and Compliance plan for a non-profit. The scope of the policy will focus heavily on system and resource access following the principle of least privilege, implementation of controls related to passwords and network resource usage, and the centralization of important secrets/details within the organization. The implementation of the compliance strategy for securing these assets will follow the NIST guidelines below:

ID.GV-1	ID.RA-3	ID.DV-4
PR.AT-2	PR.DS-1	PR.MA-2
PR.PT-3	DE.CM-1	DE.DP-1

Once the IT Security and Compliance strategy Has been implemented, the organization should Graduate up the NIST tier to 'Risk Informed'.



Function	Category	Subcategory
Identify	Governance	ID.GV-1: Organizational cybersecurity policy is established and communicated
		ID.GV-4: Governance and risk management processes address cybersecurity risks
	Risk Assessment	ID.RA-3: Threats, both internal and external, are identified and documented
Protect	Awareness & Training	PR.AT-2: Privileged users understand their roles and responsibilities
	Data Security	PR.DS-1: Data-at-rest is protected
	Maintenance	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
	Protective Technology	PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
Detect	Security Continuous Monitoring	DE.CM-1: The network is monitored to detect potential cybersecurity events
	Detection Processes	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability

Action Plan

No.	Action Item	Action Description	Type	Goal
ACT-1	Impelmentation of Firewall device with secure VPN technology to provide secure connections for remote admnitrative users	Implementation of Password Protection Policy	Managerial	MG-1
		Inform and educate managerial and technical staff on the new requirement for remote connections	Managerial	MG-2
ACT-2	Implementation of appropriate policies and access groups to address risks with 3rd party vendor access and employee remote access	Implementation of Remote Access Policy for internal users and 3rd party vendors for system maintenance.	Managerial	MG-3
		Training on Remote Access and Password Policies	Managerial	MG-4
		Implement AD Access groups with restrictions, ensuring Policy of Least Privelage (PoLP)	Managerial	MG-5
ACT -3	Implementation of off-site backup process using cloud services to ensure that data at rest is protected and can be restored in the event of a cyber event	Implementation and training of Disaster Recovery plan	Managerial	MG-6
		Coordination of data categorization activities to identify critical data that needs to be restored	Managerial	MG-7
ACT -4	Implementation of policies to prevent unauthorized application installations and modifications, and security assessments of all new software acquisitions	Implementation and training on Software Installation Policy	Managerial	MG-8
		Implementation and training on Internet Usage Policy	Managerial	MG-9
		Implementation and training on Wireless Communication Policy	Managerial	MG-10
ACT -5	Purchase and installation of updated WiFi solution	Setup of WiFi solution and implementation of network segmentation to ensure data separation along the following network device types: - Internet of Things (IoT) - Employees - Guests - Admin	Technical	TG-1
ACT-6	Implementation of Physical Controls (Cameras, logbook, doorlocks)	Implementation of physical controls to restrict direct access to sensitive systems and facility.	Managerial	MG-11

Risk Management Analysis

Risk Rank	Cyber Threat	Cyber Risk Statement	Likelihood of Occurance	Impact to the Organization	Proposed Mitigation Plan	Action Item
1	Ransomware, Password Attacks, Phishing	Data and Financial Loss, organizational reputation via ransomware and hacking due to account compromise of system admin/user	High	High	Implement password policies regarding shared accounts, password length, complexity, and password expiration to prevent unauthorized access. Implementation of NIST Password Protection Policy and annual Cyber Awareness training	ACT-1
2	Phishing, Insider Threat	Single point of failure due to external party responsible for all IT Support with no known insurance or liability contract can lead to data loss/organizational reputation	High	High	Immediate implementation of liability clause as well as requirement for insurance in the event of a breach. Implementation and Training on Remote Access Policy	ACT-2
3	Natural Disaster, Insider Threat, Theft, Vandalism	Location of backups too close to network equipment could lead to complete data/financial loss in the event of a natural disaster/insider threat	Medium	High	Moving of all backs to a separate room/location to ensure viability in the event of a disaster/catastrphic failure. Implementation of Disaster recovery policy and action plan	ACT-3
4	DoS, Malware, Ransomware, SQL injection,	No security assessment prior to acquisition of IT infrastructure and/or web applications could lead to the use of software/hardware that is vulnerable to hacking/ransomware	Medium	High	Implementation of Software Installation Policy	ACT-4
5	Data Theft, Man-in-the-middle	Current WiFi solution is open, allowing personal devices which may be infected to join the network. Additionally, malicious actors can join the network freely and target the organizations systems	Medium	High	Implement Wireless Communication Standard policy with regards to adding personal devices to network, establish updated WiFi encryption (WPA-PSK or WPA-2) protocols, and segment networks	ACT-5
6	Theft, Vandalism,	Lack of physical security controls could lead to the theft of sensitive information and hardware assets; damaging confidentiality, integrity, and availability.	Low	High	Contract a security company to provide onsite security services. Implement CCTV surveillance to deter threat actors. Implement key card access control to secure locations where sensitive information is stored.	ACT-6

Anticipated Results

It is expected that the results of the recommended changes will provide a significant drop in high-risk activities, while in-itself providing management with a lot of insight in regard to how the organizational resources are being used. As a non-profit reliant on government funding and grants, this visibility should significantly reduce risks while providing significant information and abilities to recover critical data in the event of catastrophic loss.

Proposed Costs

Equipment/ IS Policy Item	Internal/ External labor	Action ID	Cost Per Item/HR	Quantity/ Hrs	Total
Implementation of Password Protection policy	External	ACT-1	$125	3	$375
Cyber Awareness Training on All Implemented Policies and Compliance	External	ACT-1	$125	20	$2,500
Implementation of Remote Access Policy	External	ACT-2	$125	3	$375
Implementation of AD groups ensuring Policy of Least Privilege (PoLP)	External	ACT-2	$175	15	$2,625
Implementation of Disaster Recovery Policy and Incident Response Plan	External	ACT-3	$125	5	$625
Implementation of Software Installation Policy	External	ACT-4	$125	3	$375
Implementation of Internet Usage Policy	External	ACT-4	$125	3	$375
Updated WiFi solution	External	ACT-5	$800	1	$800
Updated WiFi solution Administration	External	ACT-5	$125	8	$1,000
Logbook for Server Room Access	External	ACT-6	$20	1	$20
Security Cameras	External	ACT-6	$100	4	$400
Security Company (Annual cost)	External	ACT-6	$1,200	1	$1,200
Biometric lock for server room (Nest lock, provides management of multiple users and logging online)	Internal	ACT-6	$279	1	$279
				Grand Total :	**$10,949**

Conclusion

In conclusion, this project proposal thorough identifies Auxilio's immediate high priority risks related to user access and data transmission. Through the action plan defined via thorough analysis using the NIST framework and risk identification/mitigation strategies, it is possible to elevate the security posture of Auxilio from Tier 1, which is Partial, to Tier 2, which is Risk informed. In doing so, the organization would be better equipped to respond to identify and respond to potential threats. Finally, the final policy and compliance strategy will enable the organizations leaders to be more proactive in identifying key risks and securing their data to the benefit of the community which they serve.

References

Bruce, A. (2020). *Cybersecurity for nonprofits a guide*. NTEN. https://www.nten.org/wp-content/uploads/2020/02/Cybersecurity-for-Nonprofits_-February-2020.pdf

de Groot, J. (2021, August 12). *What you need to know about Florida's information protection act of 2014 (FIPA)*. Digital Guardian. https://digitalguardian.com/blog/what-you-need-know-about-floridas-information-protection-act-2014-fipa

Founders Technology Group, LLC. (2020, October 1). *Why do cybercriminals target nonprofits?* Founders Technology Group, LLC. https://www.founderstech.com/2020/10/why-do-cybercriminals-target-nonprofits/

Gegick, M., & Barnum, S. (2013). *Least privilege* [Knowledge Topic]. https://us-cert.cisa.gov/bsi/articles/knowledge/principles/least-privilege

Harkins, M. W. (2016). Introduction. In *Managing risk and information security* (pp. 1–16). Apress. https://doi.org/10.1007

Linden, I. (2019, January 12). Nearly all damaging cyber attacks involve privileged account compromise. *CyberCrime Magazine*. https://cybersecurityventures.com/reduce-risks-with-a-privileged-access-security-hygiene-check/

Miller, M. (2021, February 19). What is least privilege & why do you need it? *BeyondTrust*. https://www.beyondtrust.com/blog/entry/what-is-least-privilege

National Institute of Standards and Technology. (n.d.). *Cybersecurity Framework - NIST Framework version 1.1* (2018). https://www.nist.gov/cyberframework

Red Canary. (2021). *2021 Threat detection report* (2021) [Report]. https://resource.redcanary.com/rs/003-YRU-314/images/2021-Threat-Detection-Report.pdf?mkt_tok=MDAzLVlSVS0zMTQAAAGAc2PD_MsVjxko5spvCj14LkyRbCBy0DhJ43nrjuZowC95EvIOERQe9PhHiPlhBk7IFrtUFiqh7oQiOCRpFeuafKH4NNIUtHtJ6rCCrnJekA

Rosencrance, L. (n.d.). *Principle of least privillege (POLP)*. TechTarget. https://searchsecurity.techtarget.com/definition/principle-of-least-privilege-POLP

SANS Institute. (2014). *Information security policy templates* (SANS). https://www.sans.org/information-security-policy/?page=7

Waldman, A. (2021). *10 of the biggest ransomware attacks of 2021 -- so far*. TechTarget. https://searchsecurity.techtarget.com/feature/The-biggest-ransomware-attacks-this-year

Williams, B. L. (2016). *Information security policy development for compliance* (1st ed.). Taylor & Francis.

NOVA SOUTHEASTERN UNIVERSITY | NSU Florida

College of Computing and Engineering (CCE)

Center for Information Protection, Education, and Research (CIPhER)

https://InfoSec.nova.edu/