Network Assessment and Increasing the Cybersecurity Posture for a Small Accounting Business

Team/Students: Randy Van and Sahana Nanaiah | Business Advisor: Tony Stark | Professor: Dr. Yair Levy, Professor of IS & Cybersecurity

Introduction

The unprecedented nature of the COVID-19 pandemic has significantly changed the way small businesses operate in order to survive. This includes transitioning their operations online to accommodate work from home policies and engaging with their customer bases in an online medium (Wong, 2020). These transitions have drawn the attention of cyber-criminals who have accelerated their attacks targeting small businesses through various means such as debilitating software attacks, impersonation, data exfiltration etc. (Tam et al., 2021). This mass digital adoption within a short time span has left small businesses increasingly reliant on Information Technology (IT) solutions that have some very glaring vulnerabilities that require professional support and maintenance. Consequentially these breaches, unavailability or tampering of data can also have serious legal and financial ramifications for a small business owner. According to a recent Small Business Administration (SBA) survey, 88% of small business owners felt their business was vulnerable to a cyber-attack. Yet many businesses that can't afford professional IT solutions either have limited time to devote to cybersecurity or they don't know where to begin (SBA, 2021). This project aims to improve the overall cybersecurity posture of Infinity Nails by conducting an assessment on the company's existing network architecture and web application security standards by using best practices that follow the National Institute of Standards and Technology (NIST) Cybersecurity Framework (2018).

Recognize and Define the Problem

According to the latest annual Internet Crime Complaint Centre (IC3) report published by the Federal Bureau of Investigation (FBI, 2020), the number of attacks in the United States rose over 400% during the COVID-19 pandemic. These attacks were primarily a result of cyber-criminals exploiting Remote Desktop Protocol (RDP) vulnerabilities, software vulnerabilities, and email phishing campaigns which resulted in losses of over $4.1 billion (FBI, 2020). The most common attacks targeting small businesses which included phishing, ransomware, and malware attacks (SBA, 2021). In these scenarios cyber-criminals often targeted the weakest link on the organizational cybersecurity chain - the people (IBM, 2020). This generally involved individuals falling victim to various social engineering attacks such as phishing, resulting in the unintentional download of malware causing disruptions in business.

Due to its effectiveness and impact on business, ransomware became a popular attack vector during the COVID-19 pandemic. Ransomware is a specific type of malicious software that infects and restricts access by crawling through a system and encrypting files. The only way to unencrypt the files is by obtaining the corresponding decryption keys which hackers may exchange for a paid ransom. Small businesses are often found to be much more likely to pay ransoms due to lack of data backups available (Witts, 2021). Information regarding their clientele, scheduling, and financial information are vital to the business's productivity and workflow (Zimba & Chishimba, 2019). Businesses may be inclined to pay a ransom to avoid any further business interruptions, financial penalties and/or even a loss of their customers' trust (Zimba & Chishimba, 2019).

Organizational Facts

Infinity Nails is a family-owned nail salon employing eight individuals including Mr. Tony Stark. Based on an initial assessment it can be determined that the employees of Infinity Nails are currently not familiar with any cybersecurity practices or policies. The network currently consists of one router and a variety of connecting devices that are currently being utilized both for both business/personal uses. The network setup of the business is flat with no segmentation between the device groups/for guest users.

Device	Anti-virus Installed	Software Updated (Yes/No)	Use (Business/Personal)
Xfinity Gateway 1 Router	Not applicable	Yes	Business
Dell XPS 13	No	No	Business
Ring Security Camera	Not applicable	No	Business
Samsung Smart TV	Not applicable	No	Business
*Employee connecting devices	No	Yes	Personal
*Customer connecting devices	Unknown	Unknown	Personal

***Connecting devices can consists of mobile phones, smart watches, laptops etc.**

The router currently has the following services set-up and enabled – Network Address Translation (NAT), Wi-Fi Protected Setup (WPS), Dynamic Host Configuration Protocol (DHCP), Firewall, WPA/WPA2 wireless security protocol, and Service Set IDentifier (SSID) broadcast on. The firmware on the router has been updated via automatic updates provided by Xfinity. The default router username and password has been changed, however the changed password for the router does not meet many of the password recommendations standards outlined by the Cybersecurity and Infrastructure Security Agency (CISA) such as password length and complexity. In addition, the company broadcasts the WiFi SSID publicly, does not practice password rotation and allows clients to access the network by requesting the password.

The company has a few technological devices that are semi-business related. The company uses a laptop (Dell XPS 13) to track employee/company earnings. The company's point of sales device is not connected to the internet, and it is used to keep track of all credit card sales locally. For physical security, the company uses a Ring security camera as a deterrent and currently records and stores a video-feed 24/7. The devices have weak password security, aren't updated regularly and don't have other preventive and detective controls like an anti-virus.

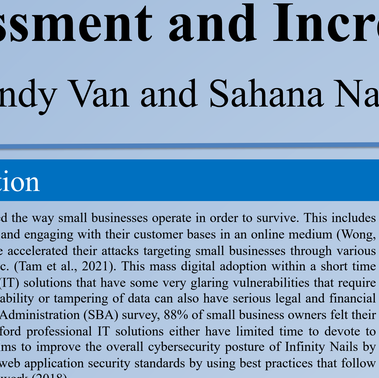

Figure 1: Current Network Diagram

The company has a business website that is used to advertise services and help employees and clients schedule/manage appointments. The website is hosted by a third-party company that specializes in online booking services. At the time of account creation, the form fields do support input sanitization and allow only the upload of specific file types providing some protection against injection attacks. The website also uses a valid Secure Socket Layer (SSL) certificate which is being cached by Cloudflare. The site supports Transport Layer Security (TLS) 1.0 and 1.1 which is susceptible to man-in-the-middle attacks and does not have various Hypertext Transfer Protocol (HTTP) response headers enabled which can provide protection against a variety of threats such as potential clickjacking or Cross-Site Request Forgery (CSRF) attacks.

Project Scope and Goals

The goal of this project is to improve the business's overall cybersecurity posture by implementing network configuration changes, web application configuration changes, and recommending security best practices, as detailed in Table 3. The impact on the Confidentiality, Integrity and Availability (CIA) triad is used to access the security controls and address any existing vulnerabilities in the systems against threats by determining technical and managerial goals. The proposed solutions are also aligned with the NIST Cybersecurity Framework (2018) technological and administrative objectives.

As a part of addressing some Technical Goals (TG) of the project listed in Table 1, the current network configuration diagram is shown under Figure 1 and the proposed changes to improve the network security and architecture are illustrated under Figure 2. These goals primarily align with the Identify, Protect, and Detect functions of the NIST Cybersecurity Framework (2018) such as: Asset Management, Identity Management and Access Control and Security Continuous Monitoring. The Managerial Goals (MG) align with the Identify, Respond, and Recover functions of the NIST Cybersecurity Framework (2018) such as Response Planning, and Recovery Planning. A detailed list of the Technical Goals, Managerial Goals, Risk Management Plan, Current Network Diagram, and Proposed Improved Network Diagram can be found by referencing Tables 1-5 and Figures 1-4 respectively.

TG	NIST Category	NIST Subcategory	Description
TG-1	Asset Management	ID.AM1 and ID.AM-2	Physical systems and software inventoried
TG-2	Risk Assessment	ID.RA-1 and ID.RA 2	Reviewing and documenting all asset vulnerabilities
TG-3	Identify Management, Authentication and Access Control	PR.AC-1	Implement a password policy for all device/network groups – business, security camera, router, network and personal services.
TG-4	Identify Management, Authentication and Access Control	PR.AC-5	Segment network traffic – guest users, physical security devices, business and employee devices.
TG-5	Identify Management, Authentication and Access Control	PR.AC-7	Enable use of multi-factor authentication across all supported devices and applications
TG-6	Data Security	PR.DS-1	Protect data at rest by enabling full disk encryption on relevant devices
TG-7	Data Security	PR.DS-2	Protect data in transit by supporting use of TLS1.2 or later.
TG-8	Data Security	PR.PT-4	Improve security settings on business email
TG-9	Security Continuous Monitoring	DE.CM-8	Install anti-virus on business laptop and mobile device and schedule regular scans for anomalies

Table 1: Technical Goals

MG	NIST Category	NIST Subcategory	Description
MG-1	Risk Assessment	ID.RA-4, ID.RA-5, ID.RA-6, ID.RA-7	Threats to business identified, potential impact, likelihood of impact used to determine and prioritize risk.
MG-2	Risk Management Strategy	ID.RM-1	Strategy to mitigate risks established and discussed with business advisor
MG-3	Awareness Training	PR.AT-1	Employee cybersecurity hygiene and awareness training
MG-4	Information Protection Processes and Procedures	RC.RP-1	Formulate a plan for response and recovery in the event of a cyber attack

Table 2: Managerial Goals

Risk Management Analysis

Table 3 outlines the cybersecurity threats that the business could potentially face and the risks that correspond to each of these threats are identified. As a part of the Risk Management Analysis process, the most impactful threats to the CIA Triad were documented. The impact and likelihood of occurrence are determined, and color coded to represent high, medium, and low risk. The last column represents the proposed solution that is recommend for the mitigation of the corresponding risk.

Risk Rank	Cyber Threat	Cyber Risk Description	Likelihood of Occurrence	Impact to Business	Mitigation Plan	Proposed ACT Item for Mitigation of Threat
1	Phishing	Various malware such as ransomware, adware, spyware etc., can result from phishing causing corruption or compromise of data.	High	High	Provide training to personnel on identifying social engineering, phishing attacks etc. Set up device encryption, MFA, configure email security settings and robust password policies.	ACT-1 ACT-2 ACT-3
2	Network Intrusion	Network intrusion can result in malicious actors being able to view sensitive data, making unauthorized changes to the network and disrupting business operations.	Medium	High	Set up network segmentation and robust password policies for access control. Training staff about basic cyber hygiene practices involving passwords, device security, enabling MFA, updating software, configuring firewall and ACLs on router.	ACT-1 ACT-2 ACT-3 ACT-4
3	Man-in-the-Middle (MITM)	Network traffic interception during MITM attacks can lead to sensitive information disclosure, result in large fines and a loss of customer trust.	Low	High	Update all device software, configure firewall and ACLs on router. Set up device encryption, MFA, configure email security settings and set up network segmentation.	ACT-2 ACT-3
4	Equipment Malfunction	Malfunctions can result in loss of data, business interruptions and unexpected cost for replacements.	Low	Medium	Setup data from local devices to backup to cloud storage to avoid interruptions to business continuity.	ACT-4

Table 3: Risk Management Analysis

Recommended Solution and Action Plan

As Infinity Nails has very minimal security controls in place, the business is identified at being at Tier 1 on the NIST Cybersecurity Framework (2018). The anticipated outcome of the project is to improve the security posture of the company to a Tier 2 with stronger cybersecurity controls and measures in place. Figure 3 shows a complete list of the NIST Cybersecurity Framework tiers (2018) starting with the lowest - Partial, Risk-Informed, Repeatable, and Adaptive. At Tier 1 the business is identified as having a limited awareness of cybersecurity risk (NIST, 2018). Businesses in this tier are generally more reactive than proactive (NIST, 2018). This project will provide a set of recommended solutions and action plan that will establish a risk management process that help enhance security controls to network security, web application security, physical security, access controls, and cybersecurity awareness through training.

Figure 3: NIST Cybersecurity Framework Tiers (2018)

Figure 4: NIST Cybersecurity Framework (2018)

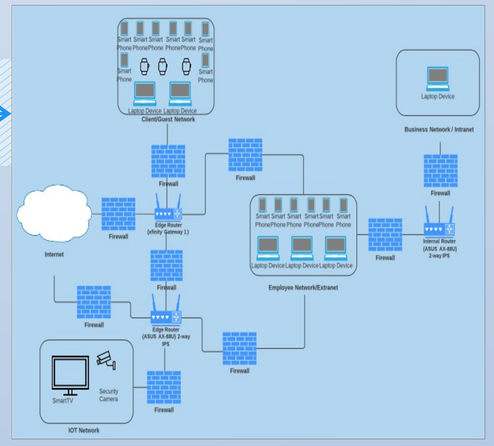

Figure 2: Proposed Improvements Network Diagram

Action Item	Action Description	Goals	NIST Category
ACT-1	Personnel – Training staff about basic cyber hygiene practices involving passwords, device security, enabling MFA, updating software and identifying social engineering, phishing attacks etc.	TG-3 TG-5 MG-3	Identify Management, Authentication and Access Control Information Protection Processes and Procedures
ACT-2	Devices and Systems – Upgrade hardware, update all device software, configure firewall and configure ACLs on router. Set up device encryption, MFA and configure email security settings.	TG-1 TG-2 TG-5 TG-6 TG-7 TG-8 TG-9 MG-1	Asset Management Risk Assessment Identify Management, Authentication and Access Control Information Protection Processes and Procedures Data Security Security Continuous Monitoring
ACT-3	Network – Set up network segmentation and robust password policies for access control.	TG-3 TG-4	Identify Management, Authentication and Access Control
ACT-4	Recovery Response – Setup data from local devices to backup to cloud storage to avoid interruptions to business continuity.	MG-1 MG-2 MG-4	Risk Assessment Risk Management Strategy Information Protection Processes and Procedures

Table 4: Recommended Solutions and Action Plan

Anticipated Results

After implementing this project, the anticipated result is that there is a significant improvement in the overall cybersecurity posture of this company. The solutions proposed in this project are derived by referencing the NIST Cybersecurity Framework (2018), the McCumber Cube, as well as the Cybersecurity and Infrastructure Security Agency (CISA) guidance which are the current industry standard for cybersecurity guidance for businesses to improve their cyber resiliency. Due to the improvements made to network security, web application security, the response and recovery plans, Infinity Nails can now move into the category of a Tier 2 cyber aware, prepared and resilient small business from its previous standing. Even though it is always pertinent to add that this does not make the business 100% secure – no system ever is, by following the recommendations and action plan charted out the cybersecurity aspect of the company can be significantly improved.

Projected Costs

The external consultation charges are at $100/hr, other additional charges for latest software purchases, anti-virus, an all-in-one small business router with advanced security features, security camera setup, cybersecurity awareness training and response planning etc., are detailed in Table 5. All the costs included in Table 5 are pre-tax and the final cost of the project will be slightly more than the projected amount.

Equipment/ Service Item	Service Details	Implementation	ACT#	Cost	Quantity	Total
Cybersecurity Training	* Training on cybersecurity best practices. * Employee would complete training via free online resources such as YouTube.	Training done by External consultants	ACT-1	$100/hr	4	$400
Asus RT-AX88U	* New WiFi router to provide faster speed, latest security features and reliability.	Installation and configurations done by External consultants	ACT-2	$270	2	$540
AiProtection Pro	* Includes Intrusion Prevention System (IPS) that protects various malware, DDOS attacks and botnet activity.	Free software included with Asus RT-AX88U. Setup done by External consultants.	ACT-2	$100/hr	2	$200
BitDefender Total Security	* Anti-virus threat detection to prevent malware * Compatible with desktop and mobile device.	Installation and setup done by External consultants	ACT-2	$50/year for 10 devices + 2hrs configuration ($200)	1	$250
Network Configuration	* Setting up firewall and ACLs * Setting up VLAN	Setup and testing done by External consultants	ACT-3	$100/hr	4	$400
Website Configuration	* Disable support for older deprecated versions of TLS. * Enable various HTTP response headers.	Implementation done by External consultants	ACT-3	$100/hr	3	$300
OneDrive 1Tb cloud storage plan	* For data backup via the cloud. * Provides availability in case drive on local machine fails.	Initial setup and testing done by External consultants. After initial installation, daily automatic backups enabled.	ACT-4	$60 annual cost of service + 2hrs configuration ($200)	1	$260
SanDisk 1 TB SSD	* Provides local access/storage * Training to manage data backups	Backups done manually by business owner after initial training and testing by External consultants	ACT-4	$145 device cost + 3hrs training ($300)	1	$442
Total Cost						$2,792

Table 5: Projected Costs

Conclusion

Infinity Nails discovered a variety of security weaknesses such as flaws in network topology, security misconfigurations and lack of security awareness during the initial evaluations. The goal was to enhance overall security as much as possible while keeping things simple and keeping costs down. The technical changes provided preventive measures to protect against various threats such as unauthorized access or malware. Although various technical changes were made and recommended to improve overall security posture, the top priority was to educate and train the business and its employees on proper security hygiene. End-users are the biggest threat to a company's overall cybersecurity infrastructure; the most expensive equipment and strictest preventive measures are meaningless if end-user's lack cybersecurity awareness. Initially the business and its employees had minimal to no knowledge of cybersecurity best practices to adopting a cybersecurity mindset. Employees were able to identify various cyber threats, understand why they are threats and have strategies to remediate and mitigates those threats. By NIST's Cybersecurity Framework (2018) the business went from Tier 1 (Partial) to Tier 2 (Risk Informed).

References

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* Version 1.1. US Department of Commerce. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Federal Bureau of Investigation (FBI) (2020). *Internet crime report: Cyber actors take advantage of COVID-19 pandemic to exploit increased use of virtual environments.* https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

IBM (2020). *The COVID-19 cyberwar: How to protect your business*. https://www.ibm.com/thought-leadership/institute-business-value/report/covid-19-cyberwar

U.S. Small Business Administration (SBA) (2021). *Stay safe from cybersecurity threats.* https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats

Tam, T., Rao, A., & Hall, J. (2021). The invisible COVID-19 small business risks: dealing with the cyber-security aftermath. *Digital Government: Research and Practice, 2*(2), Article 23. https://doi.org/10.1145/3436807

Witts, J. (2021). *The top 5 biggest cyber security threats that small businesses face and how to stop them.* https://expertinsights.com/insights/the-top-5-biggest-cyber-security-threats-that-small-businesses-face-and-how-to-stop-them/

Wong, M. (2020). *Stanford research provides a snapshot of a new working-from-home economy.* https://news.stanford.edu/2020/06/29/snapshot-new-working-home-economy/

Zimba, A., & Chishimba, M. (2019). On the economic impact of crypto-ransomware attacks: The state of the art on enterprise systems. *European Journal for Security Research, 4*(1), 3–31. https://doi.org/10.1007/s41125-019-00039-8

NOVA SOUTHEASTERN UNIVERSITY | NSU Florida
College of Computing and Engineering (CCE)

Center for Information Protection, Education, and Research (CIPhER)
https://InfoSec.nova.edu/