Summer, 2020

Mitigating Client Data Breaches Through an Increased Network Security Posture at Small Law Firms

Team/Students: Kristi Bothe & Lazaro Herrera | Business Advisor: Dominic Sussman | Professor: Dr. Yair Levy, Professor of IS & Cybersecurity

Introduction

Attorneys have a requirement to maintain the confidentiality of the client's information and any conversations, evidence or testimony they have collected on the client's behalf. This is known as the attorney-client privilege (Krebs, 2020). The American Bar Association (ABA) deems network security as a crucial element to any law practice and any data breaches must be communicated to the client or they could face regulatory or state disciplinary action (Standing Committee on Ethics and Professional Responsibility, 2018). The ABA Standing Committee on Ethics and Professional Responsibility issued formal opinions 477R and 483 stating lawyers have the responsibility to keep client data safe whether files are stored electronically, business is conducted via the Internet, emails or video-teleconferencing, with just the same steadfastness used for paper files or client property (Standing Committee on Ethics and Professional Responsibility, 2018). The purpose of this project proposal is to help mitigate data breaches at Jacobs and Stone Law Firm by applying network security engineering to redesign the existing network infrastructure, which lacks appropriate controls to mitigate cyber attacks, to one that can reduce the risks of such attacks.

Recognize and Define the Problem

Law offices around the United States (U.S.) are targeted by bad actors through ransomware (Mulvaney, 2017) or through data exfiltration (Winder, 2020). The attackers remain anonymous since the ransom is paid in untraceable bitcoins. A recent attack on a Providence firm of 10 lawyers cost them $25,000 in ransom and $700,000 in lost billing hours (Mulvaney, 2017). The newest ransomware attacks are called Maze attacks. The data is stolen first and the law firm's computers are encrypted, leaving the lawyers locked out; then the attacker demands two ransoms. One ransom is to unencrypt their files and the second ransom is to not release their files publicly but destroy the ones that were stolen instead (Sullivan, 2020). This type of attack usually costs law firms about $2 million, plus the hundreds of thousands in lost clients and billing.

Lawyers are bound by the ABA to safeguard their client's information to every extent possible (Krebs, 2020) since loss of confidentiality can make clients lose faith in the legal profession and its practitioners. However, unlike the health professionals that have had legal requirements laxened (Office for Civil Rights, 2020) during the current times, legal practitioners are expected to be essential businesses (Moran, 2020) as well as maintain the highest levels of security with minimal technical knowledge and a reduced budget. Many law firms are not aware of which assets they need to protect and what cybersecurity threats they might encounter. A security audit, a continual cybersecurity strategy, and a plan to manage and recover from a cyber breach are critical for every law firm (Teichholz, 2019). In the last four years, at least 40 law firms have been directly attacked with data breach and ransomware. About 52% of those firms had one to 19 lawyers, meaning small firms are still prime targets. Hundreds of law firms were indirectly attacked or affected by their service provider being the target of attack (Schreider, 2020).

Facts

As a small law office, Jacobs & Stone Law Firm, has not had the benefit of an Information Technology (IT) consultancy. Operating on a small budget, their network consists of a few computers, a laptop and mobile devices connected to a Wi-Fi router. The company's website is unsecure and since their email is set up with the same web host provider, it is also at a high risk for data breach. Once an attacker gains access to the email, they can search for sensitive data in the inbox or sent folders. They can change the passwords and lock the lawyer out of the email system. They can also possibly gain access to other devices and accounts linked to the email. The attorney uses a MacBook for client data storage and with a recent operating system upgrade, the backup files on a single external hard drive became temporarily irretrievable. The firm does not employ a firewall or switch for internal network protection and mobile devices used on the field are not currently set up to use a Virtual Private Network (VPN) to allow secure data access. This small law firm is handling all files internally on Wi-Fi connected devices and all email is routed through their web hosting service mail server in the cloud. Since the mobile devices like laptops and phones can move in and out of the office with confidential files onboard, it is industry best practice to enable full disk encryption either natively or through a third-party library to ensure client privacy.

Project Scope and Goals

One of the main goals of this project is to educate Jacobs & Stone Law Firm about vulnerabilities they face as a law firm, as shown in Table 3. The project will detail network upgrades that can help mitigate the impact of cybersecurity attacks, as detailed in Table 1. The focus is on the missing Secure Sockets Layer (SSL) on the website, email and web conferencing. During the coronavirus emergency, social distancing is important. Every law firm should be able to offer secure web conferencing with their clients. The office Wi-Fi will be configured with encryption and a strong passphrase. A firewall will be added and a Virtual Local Area Network (VLAN) to isolate office computers from external / internal threats. The VPN will be configured for mobile connections back to the office. A secure backup method will be established for the client data. Role-Based Access Control will be implemented with audits and logging. Policies will be developed for office-wide response and recovery plans to cyber-attacks. Employees will be trained on password policies and how to detect a suspicious email or social engineering request. Figure 2 shows the current network configuration. Through the technical goals outlined in Table 1, the network configuration will be upgraded to the design shown in Figure 3. The managerial goals in Table 2 will better prepare the firm for response and recovery efforts should there be an issue with loss of confidentiality, integrity or availability.

Table 1 *Technical Goals*

Technical Goal	NIST Category (National Institute of Standards and Technology, 2018)	Description
TG-1	Protective Technology – communication and control networks	Install encrypted Wi-Fi router with strong passphrase
TG-2	Protective Technology - communication and control networks	Install firewall with appropriate rules
TG-3	Data Security – Data at Rest	Install drive encryption
TG-4	Data Security – Data in Transit	Install VPN
TG-5	Data Security – Data in Transit	Upgrade to SSL web hosting
TG-6	Access Control – Credentials and Permissions	Implement Role-Based Access Control
TG-7	Access Control – Network Segregation	Install and configure VLAN Switch wired to office computers
TG-8	Information Protection - Backups	Implement fault tolerant backup
TG-9	Data Security – Data in Transit	Implement web video conferencing for clients with layers of security

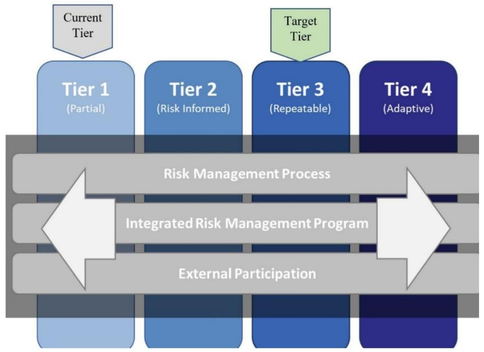
Table 2 *Managerial Goals*

Managerial Goal	NIST Category (National Institute of Standards and Technology, 2018)	Description
MG-1	Information Protection – Response Plans	Develop office-wide password policy and cyber-attack response and recovery plans
MG-2	Awareness & Training	Ensure law practice is aware of vulnerabilities, threats and ways to mitigate loss. Train on password policies and suspicious emails. Practice response and recovery plans

Recommended Solution and Action Plan

By following the National Institute of Standards and Technology (NIST) Cybersecurity Framework (2018) guidance on how to mitigate cyber threats, the law firm will have a comprehensive cybersecurity strategy. As referenced in Figure 1, it is a continual cycle where the first step is to **identify** all assets, and a risk assessment is performed. ***Table 3*** shows the risk analysis performed during this project. Step two of the cycle is to **protect** those assets with layers of security. ***Table 4*** shows these protection measures in all five of the action items. Following the added layers of security, the firm needs a way to **detect** any issues. This is covered by the firewall alerts to suspicious activity and the access control auditing logs of ACT-1 and ACT-3. How the firm will **respond** to an incident is a matter of policy development and training. This is covered in ACT-4. **Recovery** from an incident involves following a standard protocol, practice and training. ACT-4 provides this policy development and training.

Figure 4 *NIST Tiers*



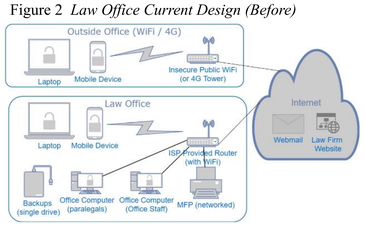
NIST Cybersecurity Framework Version 1.1 (2018)

Figure 1 NIST Cybersecurity Framework

NIST, (2018)

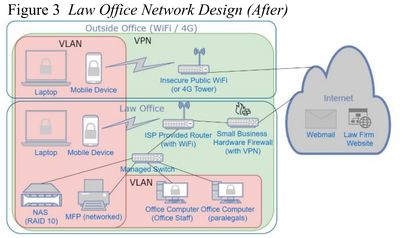
Before

Figure 2 *Law Office Current Design (Before)*



After

Figure 3 *Law Office Network Design (After)*



Risk Management Analysis (RMA)

The risk management analysis provided in Table 3 covers immediate risks and vulnerabilities that the law office faces. They have been prioritized by the impact each could have on the law firm. Every risk has a mitigation proposal in the action plan in Table 4.

Table 3 *Risk Management Analysis (RMA) Outline*

Risk Rank	Threat Type	Risk Description	Likelihood of Occurrence	Impact on Organization	Proposed Action Item	ACT #
1	Data Breach	Sensitive and confidential client data can be disclosed to unauthorized third parties	HIGH	HIGH	Install encrypted Wi-Fi router with strong passphrase. Install proper firewalls and drive encryption, add VPN tunneling for cloud storage	ACT-1
2	SSL Vulnerability	Sensitive and confidential communications can be disclosed to unauthorized third parties	HIGH	HIGH	Upgrade web hosting service to secure SSL for client contact forms, email and video-conferencing	ACT-2
3	Easy device penetration due to lack of access controls	Loss of company and client data due to limited access control to devices on the network	MEDIUM	HIGH	Analyze and implement Role-based access controls. Use VPN and VLAN for additional layer of security for remote access. Protect office computers with VLAN switch	ACT-3
4	Malware and/or Ransomware	Ransomware can encrypt data on devices in the network, which can then be used to demand ransoms for decryption and preventing release to the public.	MEDIUM	HIGH	Provide training to staff and lawyer on password policies, phishing attempts, and malware. Develop response and recovery plans	ACT-4
5	Loss of backup data files	Data loss due to current backups without redundancy and unavailable because of operating system issues that may cause delays in helping clients and reduce effectiveness of legal defense	HIGH	MEDIUM	Design secure backup storage locally using Redundant Array of Inexpensive Disks (RAID) Level 10 also known as RAID-10 for fault tolerance	ACT-5

Table 4 *Recommended Solution and Action Plan*

Action Item	Description	Goals	NIST Categories (National Institute of Standards and Technology, 2018)
ACT-1	Install encrypted Wi-Fi router with strong passphrase. Install proper firewalls and drive encryption, add VPN tunneling for cloud storage	TG 1 – TG 4	• Protective Technology • Data Security
ACT-2	Upgrade web hosting service to secure SSL for client contact forms, email and video-conferencing	TG 5 & TG 9	• Data Security
ACT-3	Analyze and implement Role-based access controls. Protect office computers with VLAN switch, mapping remote users to printers and backup Network Attached Storage (NAS) only	TG 6 & TG 7	• Access Control
ACT-4	Provide training to staff and lawyer on password policies, phishing attempts, and malware. Develop cybersecurity attack response and recovery plans.	MG 1 & MG 2	• Information Protection • Awareness & Training • Response Planning • Recovery Planning
ACT-5	Implement NAS backup system using a Redundant Array of Independent Disks - RAID 10 for fault tolerance and increased security	TG 8	• Information Protection

Anticipated Results

At the conclusion of this cybersecurity project, the network security posture at the law firm is expected to improve significantly. The law firm will have an increased sense of awareness to risks and risk management. Implementing a Backup Device with RAID-10 will support for easier backup management and increased fault tolerance. The VPN allows accessing resources with increased security while outside of the physical premises, allowing for easier remote access to backup and physical resources, like the printer. The VLAN and firewall will help mitigate attacks on the office computers and backup files. Implementing Wi-Fi with increased security will reduce the chances of unauthorized entities gaining access to their mobile network. The current NIST cybersecurity tier of the law firm is Tier 1. They have limited cybersecurity and risk awareness. They are reactive using ad-hoc risk management. The goal of this proposed project is to get the law firm to NIST Tier 3, where Jacobs & Stone Law Firm will be proactive and have a formal risk management plan in place.

Proposed Costs

Table 5 *Costs Linked to Action Items*

Equipment or Service Item	Who Performs it	ACT #	Cost per Item	Qty	Total
Cybersecurity Project and Audit	External	ACT 1- 5	$3,000	1	$3,000
Full Disk Encryption	External	ACT 1	$100/hr. for configuration	4	$400
Small Business Firewall w/VPN	External	ACT 1	$179 + 1 hr. configuration ($100)	1	$279
Managed Switch	External	ACT 3	~$215 + 2hr. configuration for VLANs ($200)	1	$415
CAT-6 for Wired Connections	External	ACT 3	$66 + 2hr. for wiring ($200)	6	$596
SSL Certificate	Internal	ACT 2	Upgrade web hosting site contract to $24.95 a month	1	~$300 annually
WebRTC Secure Video Conferencing	Internal	ACT 2	Choices: BlueJeans by Verizon (7-day free trial, $9.99 a month), LifeSize (6 months free, or 14-day trial and $12.50 a month)	1	~$150 annually
Backup Device	External	ACT 5	$910 + $200 setup	1	$1110
Policy Development	External	ACT 4	$100/hr.	4	$400
Training	External	ACT 4	$100/hr.	6	$600
		Grand Total			**$7,250**

Conclusion

Law offices are locations that contain critical private information that could be damaging to clients if it were to become lost or public. Changes to the cybersecurity posture can allow for enhanced confidentiality and availability of these critical resources to authorized employees of the law firm. Providing system backups on separate dedicated hardware using RAID-10 will reduce the amount of time that backups are unavailable improving availability. Providing VPN service will allow more access with more security to office files and backups from offsite unsecure locations. Providing firewall and VLANs will ensure devices and users are only available to communicate with devices for which they are authorized. Providing SSL capabilities will ensure any communication or web forms hosted on the law firm's website uses layered security measures to mitigate threats to client privacy on video, email and contact forms. Ensuring these networks are hardened reduces the likelihood of data breaches or data loss. It also will reduce the chance of reputation loss for the legal office that comes from a data breach.

References

Krebs, C. (2020, April 27). Privacy considerations for remote client conversations. American Bar Association: https://www.americanbar.org/groups/litigation/committees/childrens-rights/articles/2020/privacy-considerations-for-remote-client-conversations/

Moran, L. (2020, March 26). Law firms are considered essential businesses in some states amid the coronavirus. ABA Journal. https://www.abajournal.com/web/article/lawyers-considered-essential-workers-in-some-states-amid-coronavirus

Mulvaney, K. (2017, May 1). Ransomware locks down prominent Providence law firm. *Providence Journal.* https://www.providencejournal.com/news/20170501/ransomware-locks-down-prominent-providence-law-firm

National Institute of Standards and Technology. (2018, September). Cybersecurity framework version 1.1 [graphic]. *US Department of Commerce.* https://www.nist.gov/sites/default/files/images/2018/09/19/cybersecurity_framework_version_1.1_nice.png

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

Office for Civil Rights. (2020, March 30). Notification of enforcement discretion for telehealth remote communications during the COVID-19 nationwide public health emergency. *HHS Health Information Privacy.* https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html

Schreider, T. (2020, May 26). Ransomware attacks in the legal profession. *Law.com.* https://www.law.com/corpcounsel/2020/05/26/ransomware-attacks-in-the-legal-profession/?slreturn=20200529124919

Standing Committee on Ethics and Professional Responsibility. (2018). Formal Opinion 483. *American Bar Association.* https://www.americanbar.org/content/dam/aba/images/news/formal_op_483.pdf

Sullivan, C. (2020, March 5). Ransomware hits law firms hard—and it's worse than ever before. *Logikcull Blog.* https://www.logikcull.com/blog/maze-ransomware-law-firms

Teichholz, A., &.-H. (2019, December 16). Insight: Four steps law firms should take to reduce cybersecurity risks. *Bloomberg Law News.* https://news.bloomberglaw.com/privacy-and-data-security/insight- four-steps-law-firms-should-take-to-reduce-cybersecurity-risks

Winder, D. (2020, May 15). Hackers claim to have Trump's dirty laundry and demand $42 million to keep quiet. *Forbes.* https://www.forbes.com/sites/davewinder/2020/05/15/hackers-claim-to-have-trumps-dirty-laundry-and-demand-42-million-to-keep-quiet/#3c63554c37d1