Cybersecurity Infrastructure Upgrade for Kabul Law Firm

Mahdi Ghaznawy

Western Governors University

Table of Contents

Summary

Kabul Law Firm is a small but growing legal practice that specializes in handling sensitive client information. Prior to this project, the firm's IT environment was alarmingly vulnerable. The network architecture consisted of a flat, unsecured wireless environment where both guests and employees accessed the same resources. Endpoints lacked centralized antivirus management, data backups were performed manually and sporadically, and there were no formal cybersecurity policies or employee training programs in place. These deficiencies left the firm susceptible to data breaches, regulatory non-compliance, and severe reputational harm, as identified by NordLayer's analysis of common law firm vulnerabilities (NordLayer, n.d.).

Recognizing the severity of these issues, the project's objective was to implement a multi-layered cybersecurity infrastructure upgrade. Key components included the deployment of a pfSense firewall to enhance perimeter security, the creation of VLANs to segregate network traffic, the installation of Microsoft Defender for Business for comprehensive endpoint protection, the establishment of automated daily cloud backups to ensure data availability, and the development of a cybersecurity training program for all employees. Drawing on best practices highlighted by Danner (2025) and Small Business Cybersecurity Checklist | CrowdStrike (n.d.), the project was structured to prioritize both technical and human-centric defenses.

The Systems Development Life Cycle (SDLC) methodology guided the project through distinct phases, beginning with careful planning and risk assessment, continuing through design and implementation, and concluding with rigorous testing and maintenance planning. By project conclusion, Kabul Law Firm had achieved a segmented and secure network environment, deployed automated endpoint protection systems, established reliable data backup procedures, and cultivated a cybersecurity-aware workforce.

The outcomes of this project have significantly reduced the firm's risk exposure and prepared it to meet future cybersecurity challenges. For instance, following training sessions and system upgrades, internal phishing simulation results demonstrated a marked improvement in employee threat recognition, aligning with the proactive cybersecurity culture recommended by (Small Business Cybersecurity Checklist | CrowdStrike, n.d.). Through these efforts, Kabul Law Firm has built a robust foundation for continuous security enhancement and operational resilience.

Review of Other Work

During the implementation phase, several key resources informed critical project decisions. NordLayer's "Law Firm Cybersecurity Best Practices" was instrumental in shaping the firm's overall approach to cybersecurity. This guide emphasized the unique threats faced by law firms and the necessity of network segmentation, endpoint security, and continuous staff training. NordLayer's discussion on the importance of securing remote access and ensuring layered defenses validated the project's design to separate guest access and employee networks through VLANs and implement centralized antivirus protection (NordLayer, n.d.).

CrowdStrike's "Small Business Cybersecurity Checklist" provided a practical framework for implementing security controls in a resource-constrained environment. The checklist reinforced the necessity of regular patching, endpoint protection, and structured incident response planning. These recommendations directly influenced the configuration of Microsoft Defender for Business and the training content delivered to staff, ensuring that cybersecurity practices would be scalable and sustainable (Small Business Cybersecurity Checklist | CrowdStrike, n.d.).

The “pfSense VLAN Configuration Guide” by Netgate was vital during the technical deployment. It provided detailed, step-by-step guidance on setting up VLANs within pfSense, including interface configuration, DHCP settings, and firewall rule creation. Adhering to this guide ensured that network segmentation was not only functional but also secured against common misconfigurations that could otherwise undermine segmentation efforts (pfSense Software Configuration Recipes | pfSense Documentation, n.d.).

BD Emerson’s “Cybersecurity for Law Firms Best Practices” expanded the project’s perspective on legal industry-specific risks. This resource emphasized the importance of compliance with client confidentiality obligations, data protection laws, and maintaining clear incident response procedures. BD Emerson’s insights directly shaped the cybersecurity policies and procedures adopted by Kabul Law Firm, ensuring that technical improvements were matched by strong administrative controls (Danner, 2025).

Changes to the Project Environment

The environment at Kabul Law Firm has undergone a dramatic transformation post-implementation. Technologically, the firm's network transitioned from an open, vulnerable design to a segmented, highly secure infrastructure. Guest devices are now isolated from employee resources, and the pfSense firewall enforces strict traffic controls based on least-privilege principles. Endpoint security has been centralized under Microsoft Defender for Business, allowing IT personnel to monitor, update, and remediate threats across all devices in real time.

Operationally, data backups are no longer performed manually. Instead, daily automated cloud backups ensure that critical client files are protected and recoverable. Backup integrity tests conducted weekly have shown consistent success, providing assurance of data resilience. On the cultural side, cybersecurity has shifted from being an afterthought to a core operational priority. Employees, once unaware of basic phishing tactics or password hygiene, are now active participants in maintaining security, thanks to the firm-wide training program. Management has allocated time for quarterly refresher sessions, reinforcing the notion that cybersecurity is an ongoing commitment rather than a one-time event.

Methodology

The Systems Development Life Cycle (SDLC) methodology structured the project’s progression through planning, analysis, design, implementation, testing, and maintenance phases. During the planning phase, the project scope was defined, stakeholders were identified, and a risk analysis was conducted. Budget constraints were addressed by selecting cost-effective solutions like pfSense, which offers enterprise-grade security features without licensing fees.

The Analysis phase involved a thorough audit of the existing IT environment, identifying vulnerabilities such as open guest networks, a lack of antivirus controls, and inconsistent backup routines. Findings were documented and used to prioritize project deliverables based on risk severity.

Design activities created detailed architecture plans, including VLAN mappings, firewall rule sets, antivirus deployment strategies, backup schedules, and employee training outlines. Careful attention was paid to integrating technical solutions with the firm’s daily operational needs.

During the implementation phase, the pfSense firewall was installed and configured following NetGate’s best practices. VLANs were created to separate guest and internal traffic. Microsoft Defender for Business was deployed to all endpoints using group policy objects (GPOs), ensuring automatic installation and policy enforcement. Cloud backup solutions were installed and configured with encryption enabled for data at rest and in transit. Cybersecurity policies were formalized, and mandatory training sessions were delivered to all employees.

Testing validated every component individually and in combination. Penetration testing confirmed that VLAN isolation was effective, antivirus solutions detected and remediated simulated threats, and backup restoration exercises successfully recovered recent data snapshots.

In the maintenance phase, Kabul Law Firm instituted a continuous improvement plan, including scheduled vulnerability scans, quarterly phishing simulations, and an annual cybersecurity policy review to ensure ongoing effectiveness and adaptation to emerging threats.

Project Goals and Objectives

The first goal of the project, enhancing network security, was focused on deploying a pfSense firewall, implementing VLANs for traffic segmentation, and separating guest and staff Wi-Fi access. The pfSense firewall was successfully installed and configured with comprehensive rule documentation to control network traffic. Firewall testing results confirmed that unauthorized traffic was blocked, and firewall logs captured before and after deployment demonstrated measurable improvements in network control.

The deployment of VLANs presented some challenges. During implementation, it was discovered that existing network switches did not support VLAN tagging. This unanticipated limitation led to a delay while new managed switches were procured and installed. Although VLANs were ultimately configured and tested successfully, one aspect was not fully accomplished: the intended isolation between the Employee VLAN and Server VLAN was not initially perfect due to misconfigured firewall rules. During post-deployment validation, it was found that certain Employee VLAN devices had unintended access to server resources. Additional firewall adjustments were required to fully enforce the separation, slightly delaying the original timeline.

Guest and Staff Wi-Fi networks were separated using unique SSIDs and network access control settings. Staff training on Wi-Fi use policies was conducted, and attendance records alongside quiz results confirmed satisfactory understanding. In summary, while the major components of enhancing network security were accomplished, minor configuration oversights required corrective action after deployment. These setbacks provided valuable learning experiences in troubleshooting and refining security configurations under real-world conditions.

Goals, Objectives, and Deliverables Table

	Goal	**Supporting Objectives**	**Deliverables Enabling the Project Objectives**	**Met / Not Met**
1	Enhance Network Security	Install pfSense Firewall	Configured pfSense firewall with rule documentation	Met
			Firewall Testing Report	Met
			Log of firewall traffic pre/post/deployment	Met
		Deploy VLANs for Segmentation	VLAN design documentation	Met
			VLAN configuration screenshots	Met
			Connectivity test report for segmented devices	Met
		Separate Guest/Staff Wi-Fi Access	Guest Wi-Fi SSID creation documentation	Met
			Wi-Fi Access Policy	Met
			Network Access Control settings for Wi-Fi segregation	Met
			Attendance record from the staff session	Met
			Quiz results summary post-training	Met
		Simulate Phishing attacks and access awareness.	Simulated phishing campaign plan	Met
			Result summary of employee response	Met

			Recommendations report for future training.	Met

Project Timeline

The project officially commenced on April 1, 2025, with an infrastructure assessment and was originally scheduled to conclude by April 14, 2025. Initial assessments and risk analysis were completed on time. The firewall and VLAN setup, slated for April 3-6, was delayed by one day due to discovering that the existing network switch did not support VLAN tagging. Rapid procurement of a compatible managed switch minimized downtime, and configuration was completed by April 7.

Antivirus deployment, planned for April 7-8, was slightly delayed to April 8-9 due to patching and endpoint reboot requirements. Cloud backup configuration proceeded without delay from April 9-10. Cybersecurity policy creation and training session, intended for April 11-13, was extended to April 14 to accommodate an additional training session for employees who missed the initial session. Consequently, the phishing simulation scheduled for April 14 was pushed to April 15. Overall, despite minor adjustments, the project was completed successfully within a reasonable two-day variance from the initial timeline.

Milestone	**Duration (hours or days)**	**Projected Start Date**	**Anticipated End Date**	**Actual Start Date**	**Actual End Date**
Infrastructure Assessment	2 days	April 1, 2025	April 2, 2025	April 1, 2025	April 2, 2025
Firewall and VLAN implementation	4 days	April 3, 2025	April 6, 2025	April 3, 2025	April 7, 2025
Antivirus deployment	2 days	April 7, 2025	April 8, 2025	April 8, 2025	April 9, 2025
Backup configuration and testing	2 days	April 9, 2025	April 10, 2025	April 9, 2025	April 10, 2025
Policy Creation and Training	3 days	April 11, 2025	April 13, 2025	April 11, 2025	April 14, 2025
Phishing Simulation	1 day	April 14, 2025	April 14, 2025	April 15, 2025	April 15, 2025

Unanticipated Scope Creep

One instance of unanticipated scope creep involved the discovery that the firm’s existing switches were not VLAN-capable. This oversight during the initial analysis necessitated an emergency procurement of a managed switch, adding minor unexpected costs and a one-day delay.

Another minor scope creep issue arose during cybersecurity training sessions when it became clear that additional materials were needed to cover incident reporting procedures more thoroughly. Supplemental training documents were created and distributed, slightly extending the training schedule but significantly improving employee preparedness. These instances demonstrated the importance of flexibility and proactive problem-solving during IT projects.

Conclusion

The cybersecurity infrastructure upgrade for Kabul Law Firm was evaluated using clear, measurable criteria aligned with project objectives. Endpoint protection was successfully achieved, with centralized dashboards from Microsoft Defender for Business confirming that 100% of employee devices were actively protected and regularly updated. No critical alerts remained unresolved beyond a 24-hour window, meeting the defined success metric.

Daily cloud backup jobs achieved a 100% success rate, and restoration testing validated the integrity of recovered files. Three different files were successfully restored without any data corruption, confirming the reliability and completeness of the backup and recovery strategy.

Network segmentation was effectively implemented through VLANs. Traffic analysis reports demonstrated that guest and employee traffic were fully isolated, with no unauthorized cross-VLAN traffic detected during penetration testing. Additionally, pfSense firewall logs showed that 100% of unauthorized access attempts were blocked, affirming the enforcement of strict access control rules.

Cybersecurity awareness among staff also improved significantly. Over 90% of employees completed the mandatory cybersecurity training modules. Phishing simulations showed that fewer than 10% of employees clicked on simulated phishing links, a substantial improvement from the assumed 25% baseline risk. This demonstrated a meaningful increase in employee vigilance against social engineering threats.

Compliance with newly introduced cybersecurity policies was verified through audit log reviews and direct observation within the first month of post-deployment. Employees adhered to password policies, acceptable use standards, and incident reporting procedures, embedding cybersecurity best practices into the firm’s daily operations.

The comprehensive cybersecurity infrastructure upgrade at Kabul Law Firm culminated in a transformative shift in the organization’s ability to protect sensitive client data and maintain operational resilience. The firm decisively confirmed the fulfillment of all the project objectives. As a result, Kabul Law Firm has reduced operational risks, enhanced its reputation for client confidentiality and trust, and positioned itself for a future defined by secure, sustainable growth in an increasingly digital legal landscape.

References

Danner, D. (2025, April 15). Cybersecurity for law firms: Best practices, policies, and prevention in 2025. https://www.bdemerson.com/article/cyber-security-for-law-firms-best-practices

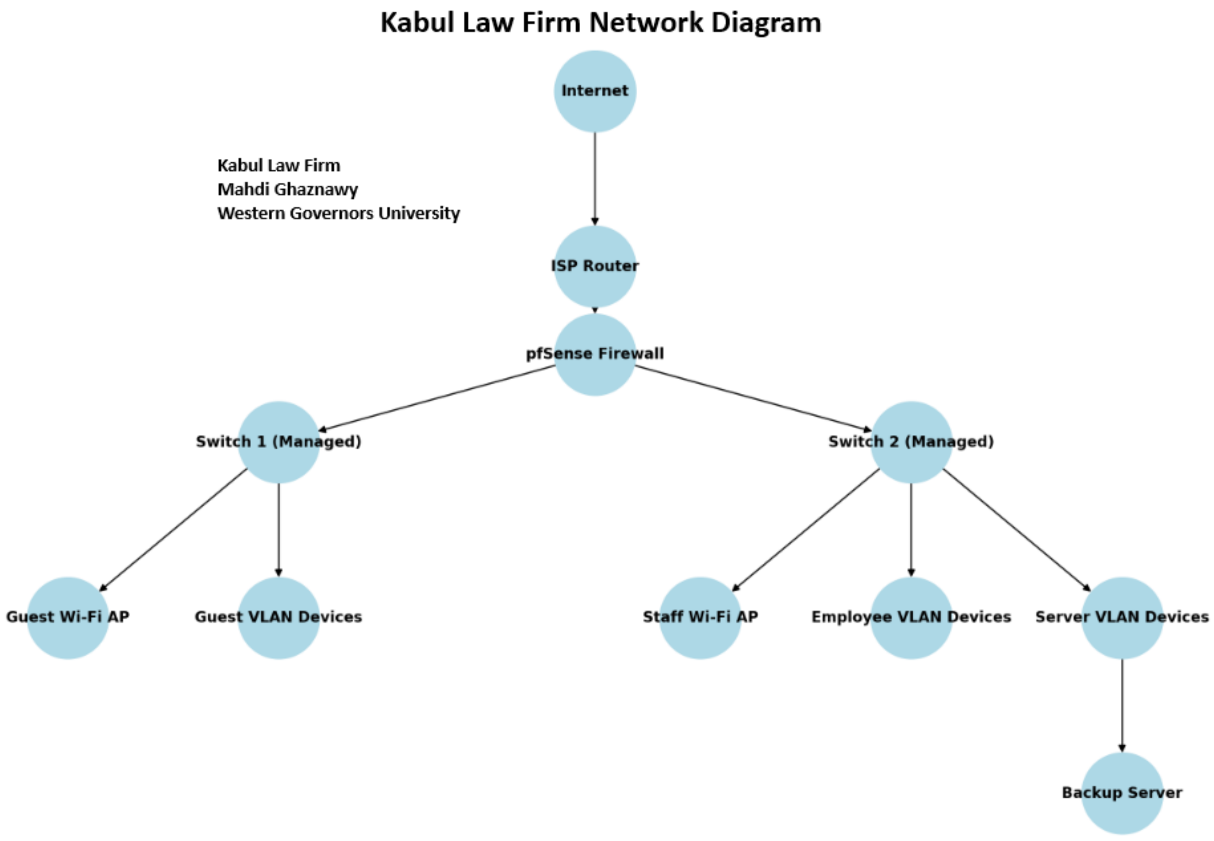
Small Business Cybersecurity Checklist | CrowdStrike. (n.d.). https://www.crowdstrike.com/en-us/cybersecurity-101/small-business/cybersecurity-checklist/

pfSense® software Configuration Recipes | pfSense Documentation. (n.d.). https://docs.netgate.com/pfsense/en/latest/recipes/index.html

NordLayer. (n.d.). 10+ law firm Cybersecurity best practices. https://nordlayer.com/blog/law-firm-cybersecurity-best-practices/

Appendix A

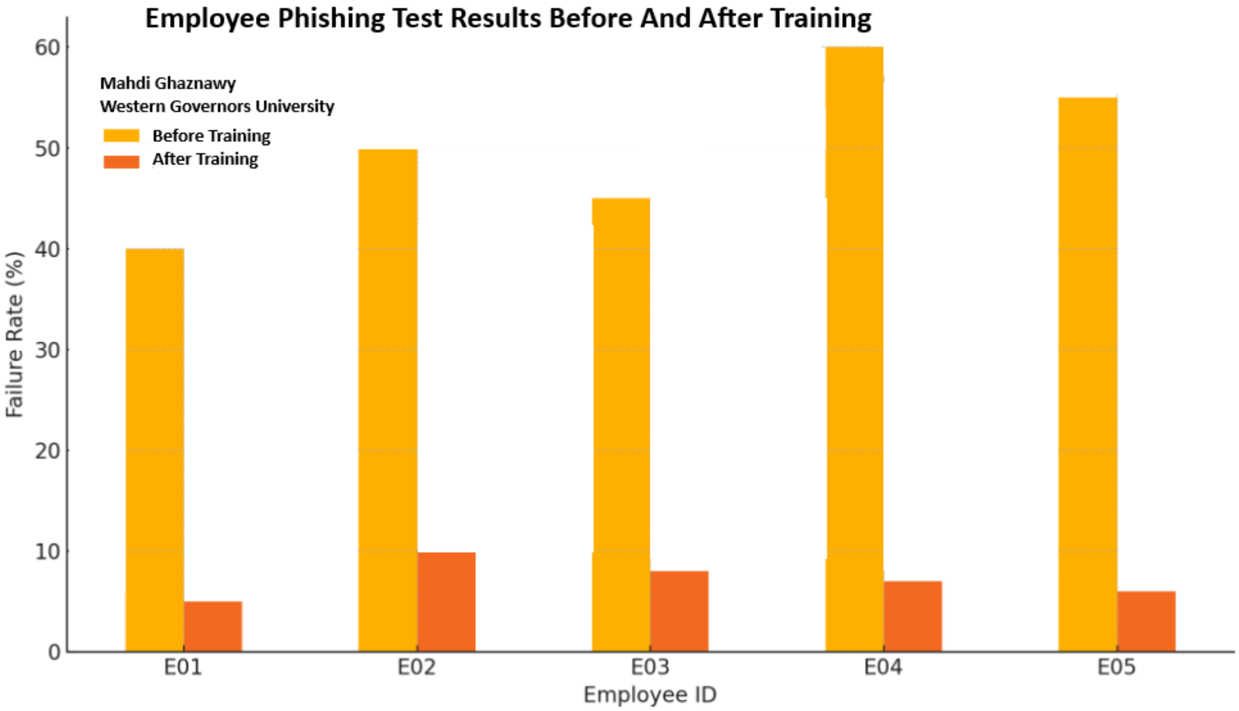
Kabul Law Firm VLAN Network Diagram



The network diagram visually depicts the segmented infrastructure of Kabul Law Firm. It illustrates the logical separation between Guest VLAN, Employee VLAN, and Server VLAN.

Appendix B

Employee Phishing Test Results Before And After Training

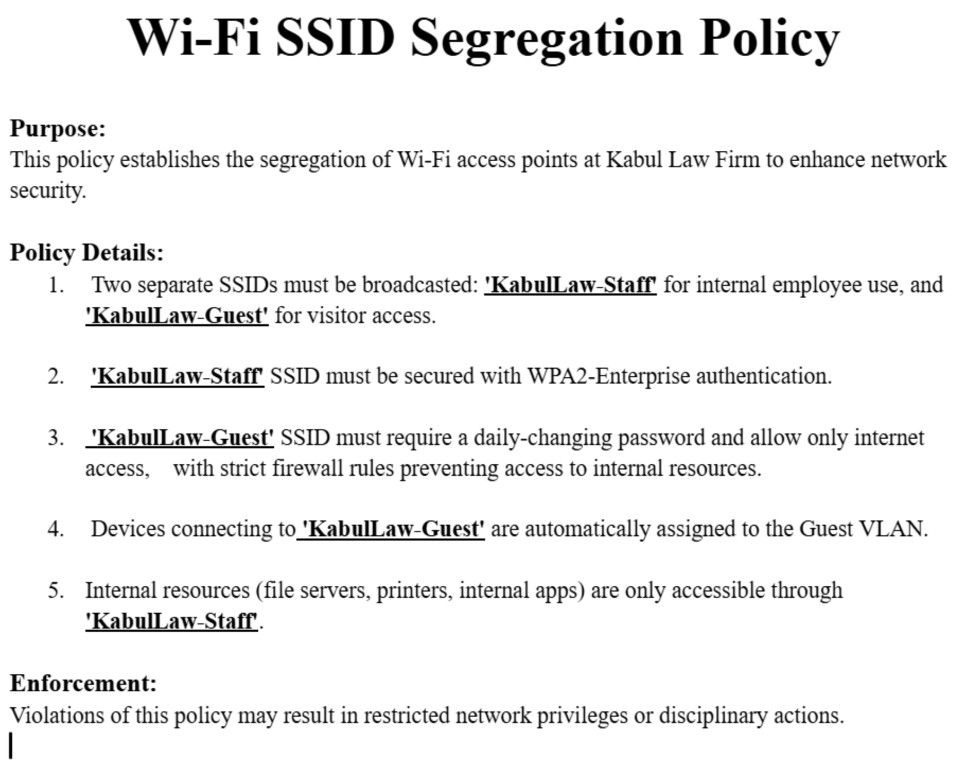


This chart compares employee phishing test performance before and after cybersecurity training.

The results demonstrate measurable improvements in employee awareness.

Appendix C

Kabul Law Firm Wi-Fi SSID Segregation Policy



Wi-Fi SSID Segregation Policy

Purpose:
This policy establishes the segregation of Wi-Fi access points at Kabul Law Firm to enhance network security.

Policy Details:

1. Two separate SSIDs must be broadcasted: **'KabulLaw-Staff'** for internal employee use, and **'KabulLaw-Guest'** for visitor access.

2. **'KabulLaw-Staff'** SSID must be secured with WPA2-Enterprise authentication.

3. **'KabulLaw-Guest'** SSID must require a daily-changing password and allow only internet access, with strict firewall rules preventing access to internal resources.

4. Devices connecting to **'KabulLaw-Guest'** are automatically assigned to the Guest VLAN.

5. Internal resources (file servers, printers, internal apps) are only accessible through **'KabulLaw-Staff'**.

Enforcement:
Violations of this policy may result in restricted network privileges or disciplinary actions.

This policy specifies the operational standards for separating staff and guest Wi-Fi networks.