Cybersecurity Infrastructure Upgrade for Kabul Law Firm

Mahdi Ghaznawy

Table of Contents

Proposal Overview

Problem Summary

Kabul Law Firm is a small, fictional law firm that serves private clients in sensitive legal matters. The firm has a total of 10 employees and relies heavily on digital tools to manage case files, contracts, and client communications. However, the firm lacks basic cybersecurity protections. Currently, all devices run on a flat network with shared access; there is no centralized antivirus protection, backups are not automated, and guest and employee devices use the same Wi-Fi. These security gaps create serious risks, particularly related to data loss, unauthorized access, and potential violations of ethical and legal obligations regarding client confidentiality.

IT Solution

To address these issues, a comprehensive cybersecurity infrastructure upgrade is proposed. The proposed pfSense firewall will act as a robust perimeter defense, actively filtering unauthorized traffic and providing detailed logs for ongoing monitoring. This directly mitigates the risk of unauthorized access, one of the most pressing vulnerabilities in the current setup.

Segmenting the network using VLANs will isolate guest and staff devices, limiting lateral movement across the network. This segmentation ensures that a compromised guest device can not access sensitive staff resources, reducing the impact of potential breaches.

Centralized antivirus protection using Microsoft Defender for Business will ensure that all devices are consistently protected and monitored, addressing the current inconsistency in security software deployment. Real-time alerts and automatic remediation features will enhance the firm's response to malware threats.

An automated cloud-based backup system will protect against data loss by ensuring that critical legal documents and client information are securely stored and easily recoverable. This reduces reliance on manual backups, which are often neglected and prone to human error.

Finally, the creation of tailored cybersecurity policies and staff training will address human factors in security, improving employee awareness and reducing risks from phishing and social engineering attacks. These combined measures form a comprehensive and proactive approach to the firm's cybersecurity challenges. These interventions aim to enhance data confidentiality, integrity, and availability while also aligning the firm with industry best practices.

Implementation Plan

The project will begin with a review of the current environment to assess the firm's infrastructure and define a deployment plan. The firewall will be configured and installed to secure the perimeter and filter network traffic. Using managed switches to isolate sensitive resources from guest access, VLANs will be created. Antivirus software will be installed on all endpoints, with centralized monitoring enabled. Cloud-based backup tools such as Veeam or Acronis will be configured to perform daily backups. Cybersecurity policies covering acceptable use policy, password management, and remote access will be written and distributed to staff. Training materials will also be created and delivered to educate employees on cyber hygiene and social engineering risks.

While the IT consultant (Mahdi Ghaznawy) will lead the technical planning, configuration, and implementation steps, key roles will also be assigned to firm personnel. A designated administrative representative will assist with internal communication, staff coordination for training, and review of security policy drafts to ensure they align with internal workflows. Additionally, a senior legal assistant will participate in the policy feedback loop and help coordinate scheduling for endpoint installations. This collaborative approach ensures shared ownership of changes and promotes internal engagement for long-term adoption. This project is expected to be completed within a defined three-week timeline.

Review of Other Work

Summary of Four Works

1. **Cisco: Small Business Cybersecurity Best Practices**

   Cisco provides comprehensive cybersecurity guidelines specifically tailored for small businesses that often lack dedicated IT departments. Their guide emphasizes the importance of deploying layered security, such as business-grade firewalls, antivirus software, and network segmentation using VLANs. It stresses that small firms are particularly vulnerable to ransomware and phishing attacks due to minimal security investments. Cisco recommends using intrusion prevention systems (IPS), maintaining encrypted Wi-Fi networks, and segmenting networks to isolate sensitive resources (Gross, 2022).

2. **Microsoft: Microsoft Defender for Business Overview**

   Microsoft Defender for Business documentation outlines how small and medium-sized businesses can deploy enterprise-grade endpoint security without complex infrastructure. It describes how Defender provides real-time threat detection, antivirus protection, and automated investigation and response across all connected devices. The guide also details centralized management dashboards for monitoring device health, detecting vulnerabilities, and enforcing compliance policies (Chrisda, n.d.). This document was critical in shaping the endpoint protection strategy for the firm, helping to define policies around antivirus updates, alerting, and endpoint monitoring.

3. **Cybersecurity and Infrastructure Security Agency (CISA): Cyber Essentials for Small Businesses**

CISA's Cyber Essentials framework offers actionable guidance for small businesses to build a strong cybersecurity foundation. This guide introduces six key steps, including developing a cybersecurity strategy, protecting critical assets, managing vulnerabilities, and preparing for incident response. CISA strongly recommends practices like segmenting networks, securing backups, training employees, and assigning a cybersecurity lead within the business (CISA, n.d.). This framework heavily influenced the project's inclusion of backup strategies, staff training, policy development, and the recommendation to appoint a firm-level cybersecurity coordinator.

4. Auvik: What is Network Segmentation and Why Does It Matter?

Auvik's article provides an in-depth explanation of network segmentation strategies for businesses. It discusses how logical segmentation through VLANs can contain security breaches and prevent lateral movement inside networks. The article also emphasizes that segmentation not only enhances security but also improves network performance and simplifies management of sensitive resources (Petryschuk & Petryschuk, 2025). This resource validated the technical decision to separate guest and employee traffic using VLANs, a critical part of the project's network redesign.

Relation of Works to Proposal Design

The Cisco guide by Andrea Gross laid the groundwork for the layered security architecture proposed for Kabul Law Firm. It reinforced the need to deploy a business-class firewall, enforce encrypted Wi-Fi access, and separate guest traffic from internal resources through VLANs. These ideas directly influenced both the network design and firewall deployment phases of the project.

The Microsoft Defender for Business documentation was essential in defining the endpoint protection framework. By following Microsoft's recommended practices, the proposal includes real-time antivirus, threat monitoring, and centralized management of all employee laptops and workstations, ensuring continuous protection without overwhelming IT administration (Chrisda, n.d.).

The CISA Cyber Essentials framework shaped the non-technical elements of the project, particularly the creation of cybersecurity policies, the design of regular employee training programs, and the emphasis on backup and recovery planning. The recommendation to assign an internal cybersecurity point person was incorporated into the governance structure of the project.

Auvik's explanation of network segmentation guided the VLAN architecture proposed in the redesign of the firm's network. The article's emphasis on limiting lateral movement and securing sensitive resources led to the creation of separate logical networks for guest devices, administrative staff, and legal data systems, drastically improving overall network resilience (Petryschuk & Petryschuk, 2025).

Project Rationale

This project is necessary due to the growing volume and complexity of cyber threats targeting small firms in the legal industry. Kabul Law Firm holds confidential legal data that, if compromised, could severely harm clients and damage the firm's reputation. Furthermore, regulatory compliance and ethical obligations require the safeguarding of sensitive information. The implementation of this cybersecurity solution ensures that the firm operates securely while positioning it for future growth.

Current Project Environment

Kabul Law Firm operates a very basic IT infrastructure. All employees' and guests' devices connect to the same wireless network through a consumer-grade router that lacks enterprise-level features such as advanced firewalling or traffic monitoring. There is no network segmentation in place, which means a breach from a single infected guest device could allow lateral movement across the network, potentially reaching confidential client files or sensitive business data.

Workstations are individually managed without centralized antivirus or update controls, leading to inconsistent patching and software protection. Antivirus software varies across systems, and some machines have outdated or expired security solutions. Backup procedures are either manual or non-existent, which places the firm at significant risk of permanent data loss in the event of ransomware or hardware failure. There are also no systems in place to alert administrators of critical changes or threats within the network.

The firm lacks documented security policies, and cybersecurity training has never been formally conducted. This means employees may not recognize phishing attempts, practice poor password hygiene, or unknowingly violate basic security practices. This environment lacks

foundational security measures, leaving the firm exposed to potential threats. The proposed upgrades will close these gaps by adding structure, automation, and proactive defenses.

Methodology

This project will use the Systems Development Life Cycle (SDLC) methodology to ensure a structured and methodical approach to implementation. SDLC provides a step-by-step process to plan, develop, implement, and maintain a robust IT solution. The SDLC approach consists of six stages: planning, analysis, design, implementation, testing, and maintenance.

In the Planning phase, key project requirements will be defined, stakeholders identified, resources allocated, and project timelines established. A preliminary assessment will be performed to identify the scope of vulnerabilities and determine realistic goals.

The analysis phase will involve gathering specific technical and business requirements by closely collaborating with internal stakeholders at the law firm, such as administrative personnel and legal assistants. A gap analysis will be conducted to compare the current environment to desired security standards.

In the design phase, detailed plans will be created, including firewall rule sets, VLAN layouts, antivirus rollout procedures, and automated backup architecture. Each design component will include diagrams, configuration scripts, and implementation steps.

The implementation phase will involve configuring and deploying the firewall, creating VLANs using managed switches, installing endpoint protection software on all firm devices, and setting up automated backup solutions using secure cloud platforms. Team collaboration will be vital, with both IT consultants and designated firm representatives assisting in device access, policy distribution, and testing.

During the testing phase, each component will undergo validation. For example, firewall logs will be monitored to verify blocked traffic, VLANs will be tested for proper isolation, and antivirus systems will be executed to ensure data integrity.

Finally, the maintenance phase will include drafting operational documentation, policy enforcement, and training users. Staff will be provided with how-to guides, and follow-up assessments will ensure all systems are maintained securely and efficiently. Using SDLC allows for thorough tracking and adjustments at each phase, ensuring both the project's technical soundness and long-term success.

Project Goals, Objectives, and Deliverables

Goals, Objectives, and Deliverables Descriptions

This project is structured around three primary goals: enhancing network security, improving data and endpoint protection, and building cybersecurity awareness and policy adherence across the organization.

To begin with, the first goal, enhancing network security, focuses on protecting the perimeter and internal structure of the firm's IT environment. This includes deploying a pfSense firewall to manage traffic and block unauthorized access. VLANs will be established to isolate sensitive segments of the network, effectively limiting lateral movement by attackers. Additionally, separate SSIDs for staff and guests will be configured to prevent unauthorized devices from accessing internal resources. Each of these actions results in deliverables such as configuration logs, documentation of network policies, and connectivity tests that confirm the intended segmentation.

The second goal involves improving data and endpoint protection. Kabul Law Firms must ensure all devices are safeguarded against malware and that sensitive client data is securely backed up. To meet this goal, Microsoft Defender for Business will be deployed organization-wide, enabling real-time detection and response to threats. Automated cloud-based backup processes will be implemented, followed by restore tests to confirm data integrity and availability. These objectives will produce deliverables such as antivirus deployment logs, backup schedules, system alerts, and successful recovery documentation.

The final goal centers on developing staff awareness and improving adherence to cybersecurity policies. This will be achieved by drafting essential internal documents, such as an Acceptable Use Policy and Password Policy. Cybersecurity awareness training sessions will be delivered to all staff, culminating in a brief assessment. To reinforce the importance of these sessions, a simulated phishing campaign will be run to evaluate real-world awareness. Deliverables will include finalized policy documents, attendance records from training sessions, and a report on phishing test results with recommendations for improvement.

Goals, Objectives, and Deliverables Table

	Goal	**Supporting Objectives**	**Deliverables Enabling the Project Objectives**
1	Enhance Network Security	Install pfSense Firewall	Configured pfSense firewall with rule documentation
			Firewall Testing Report

			Log of firewall traffic pre/post/deployment
		Deploy VLANs for Segmentation	VLAN design documentation
			VLAN configuration screenshots
			Connectivity test report for segmented devices
		Separate Guest/Staff Wi-Fi Access	Guest Wi-Fi SSID creation documentation
			Wi-Fi Access Policy
			Network Access Control settings for Wi-Fi segregation
2	Improve Data and Endpoint Protection	Deploy Microsoft Defender for Business	Antivirus install logs and screenshots
			Microsoft Defender Dashboard Report
			Antivirus alert test result logs
		Implement Automated Cloud Backups	Backup configuration files
			Schedule of automated backups
			Screenshots and logs of the successful backup job
		Test and verify recovery processes	Data recovery test documentation
			Validation report on data integrity
			Staff walkthrough guide on restoring files
3	Build Cybersecurity Awareness and Policy Adherence	Draft and implement security policies	Acceptable Use Policy Document
			Password Policy Document
			Remote Access Policy PDF
		Deliver Staff Cybersecurity Training	Training Presentation Slides
			Attendance record from the staff session
			Quiz results summary post-training
		Simulate Phishing attacks and access awareness.	Simulated phishing campaign plan
			Result summary of employee response
			Recommendations report for future training.

Project Timeline with Milestones

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

Outcome

The success of this project will be evaluated using clearly defined, measurable criteria to ensure that each objective has been effectively met. Specifically, centralized dashboards will confirm antivirus protections, showing that 100% of endpoints are actively protected and regularly updated, with no critical alerts unresolved after 24 hours. Backup success will be determined by daily job completion rates of 100%, and restore functionality will be validated through a successful test restore of at least three different files, with data integrity verified in each case.

For the network segmentation, VLANs must successfully isolate guest and staff traffic, as confirmed through traffic analysis reports. The firewall will be assessed based on its ability to enforce access control rules, with logs demonstrating that 100% of attempted unauthorized connections were blocked during testing.

In the area of staff cybersecurity awareness, the outcome will be measured through participation and performance in training and phishing simulations. At least 90% of staff must complete the training module, and phishing tests will be considered successful if fewer than 10% of employees click on a simulated phishing email, representing a marked improvement over an assumed baseline of 25%. Compliance with the newly implemented cybersecurity policies will be evaluated through audit logs and direct observation within the first month post-deployment.

Data will be collected from firewall logs, antivirus dashboards, backup validation reports, network monitoring tools, phishing campaign software, and training completion records. These quantifiable results will provide the necessary evidence to determine the effectiveness and impact of the project.

References

Cyber Essentials | CISA. (n.d.). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/resources-tools/resources/cyber-essentials

Chrisda. (n.d.). *Microsoft Defender for Business documentation - Microsoft Defender for Business*. Microsoft Learn. https://learn.microsoft.com/en-us/defender-business/

Petryschuk, S., & Petryschuk, S. (2025, April 15). Network segmentation: what it is & how it works. Auvik. https://www.auvik.com/franklyit/blog/network-segmentation/

Gross, A. (2022, March 16). *The essential guide to Cybersecurity for the small business*. Cisco Umbrella. https://umbrella.cisco.com/blog/cybersecurity-for-small-business