Cyber-Intrusion Response Strategy for Project for Pride in Living (PPL)

Ngsnet Hawarya

Saint Mary's University of Minnesota

CYBR 610: Network Security and Intrusion Detection

Instructor: Ms. Jamila Crawford

April 27, 2025

Abstract

This paper presents a comprehensive analysis of a cyber-intrusion affecting Project for Pride in Living (PPL), a real nonprofit organization dedicated to empowering individuals and families through affordable housing and career readiness programs in the Twin Cities. Drawing on internal knowledge gained through nearly two years of experience as a Technical Support Specialist and now as an IT Administrator at PPL, this analysis examines a ransomware attack initiated through a phishing email that exploited unpatched vulnerabilities in endpoint systems. The paper outlines PPL's network architecture identifies the threat actors and discusses the probable sources of the breach. A strategic response framework is developed using the MITRE ATT&CK and Cyber Kill Chain models, detailing detection mechanisms, vulnerability assessments, and incident response protocols. Post-incident recovery efforts and recommendations for future prevention are also provided. Key lessons from nonprofit and financial-sector case studies are incorporated, highlighting the importance of backup testing, layered defenses, and communication planning. This applied analysis is based on real-world cybersecurity incidents encountered during my work at PPL and integrates knowledge gained from CYBR 610, emphasizing proactive defense and effective incident management in cybersecurity operations.

Keywords: cybersecurity, ransomware, nonprofit security, incident response, MITRE ATT&CK

Introduction

Project for Pride in Living (PPL) is a nonprofit organization focused on empowering individuals and families through affordable housing, employment training, and community support programs. With its core mission centered on focusing economic mobility and self-sufficiency, PPL plays a crucial role in the lives of many vulnerable populations. Headquarters in the Twin Cities, PPL employs approximately 270 staff across more than 65 apartment buildings, two alternative high schools, and workforce development initiatives. The organization manages sensitive client data, financial records, housing information, and protected health information (PHI) under HIPAA compliance requirements. This digital infrastructure makes PPL a potential target for cyberattacks. This paper simulates a ransomware based intrusion scenario affecting PPL and presents a structured strategy to respond, assess, and prevent such incidents. By incorporating industry tools, security frameworks, and best practices, it demonstrates the practical application of network security and intrusion detection principles.

2. Situation: Cyber-Intrusion Scenario

2.1 Organization Overview

PPL’s nonprofit status and work with vulnerable populations require maintaining the highest standards of cybersecurity. Given its role in managing sensitive financial and healthcare data, it is a prime target for cybercriminals (Abdullayeva, 2023).

2.2 Current Network Structure

PPL operates a hybrid IT infrastructure combining on premises and cloud based solutions using Microsoft Azure. The environment includes:

- Active Directory and Microsoft Entra for identity management,
- Microsoft 365 for email, Teams, and SharePoint collaboration,
- VPN access for remote work,
- A firewall with web filtering and basic IDS functionality,
- Windows Defender and limited EDR coverage across endpoints.

PPL’s hybrid network architecture, integrating both cloud and on-premises services, is illustrated in Figure 1.

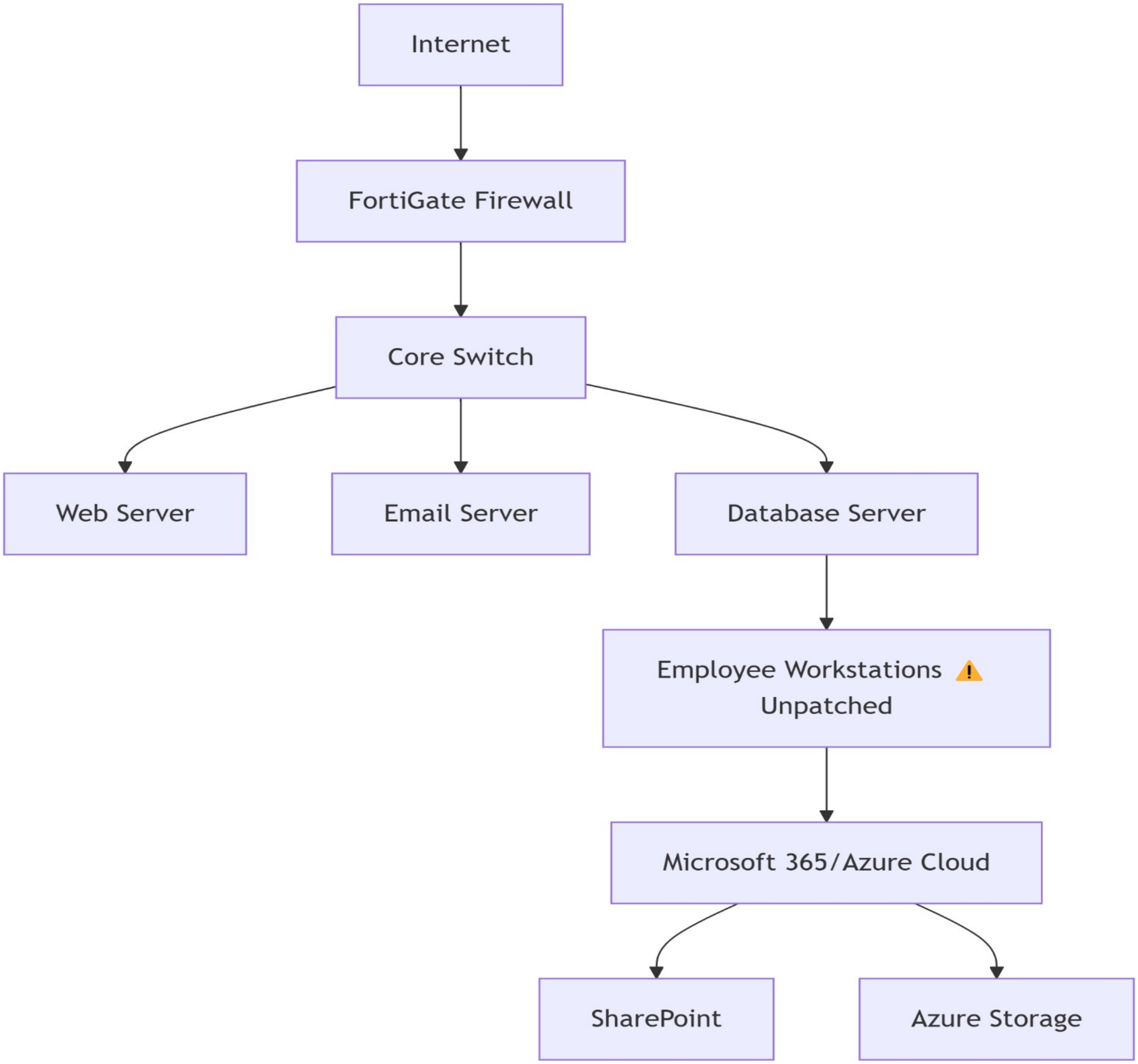


Figure 1

PPL hybrid network infrastructure highlighting external access points and internal systems.

2.3 Cybersecurity Incident Description

On March 10, 2025, several staff members reported an inability to access shared files and received suspicious error messages. Investigation revealed a phishing email impersonating a government housing partner that carried a malicious Excel attachment. Upon opening, the macro executed a ransomware payload that encrypted local and shared drive files and attempted to exfiltrate sensitive tenant financial records (Cisco, 2023).

2.4 Threat Actors

The intrusion was attributed to a financially motivated cybercrime syndicate using "Phobos" ransomware. Their tactics align with MITRE ATT&CK techniques such as phishing (T1566.001), privilege escalation (T1068), and lateral movement via SMB (T1021.002) (MITRE, 2024).

2.5 Root Cause Analysis

The phishing email bypassed Microsoft Defender’s scanning capabilities, exploiting a machine lacking recent security patches. Furthermore, macro execution policies were weak, and VPN access lacked multi-factor authentication (MFA). According to SANS Institute (2023), inadequate user training and patching processes significantly increase the success rate of ransomware attacks.

3. Strategy: Detection, Response, and Assessment

3.1 Detection Tools and Techniques

PPL’s security monitoring utilized Wazuh integrated with Elastic Stack for SIEM and log correlation (Wazuh Documentation, 2024). Additional recommendations included:

- CrowdStrike Falcon for behavioral threat detection (CrowdStrike, 2024),
- Darktrace for lateral movement analysis,
- Splunk for scalable log management (Landauer et al., 2025).

Indicators of compromise observed:

- Mass file encryption across shared drives,
- Unauthorized remote login attempts,
- Anomalous RDP and SMB traffic patterns.

3.2 Vulnerability Scanning Methods

Post-incident, Nessus vulnerability scanning was deployed to identify unpatched systems and prioritize remediation (Nessus Vulnerability Scanner, 2024). Enhanced initiatives included:

- KnowBe4 phishing simulations and training,
- Internal red team operations simulating phishing-to-internal breach chains (Djenna et al., 2021).

Proactive vulnerability management efforts follow a continuous cycle, as illustrated in Figure 2.

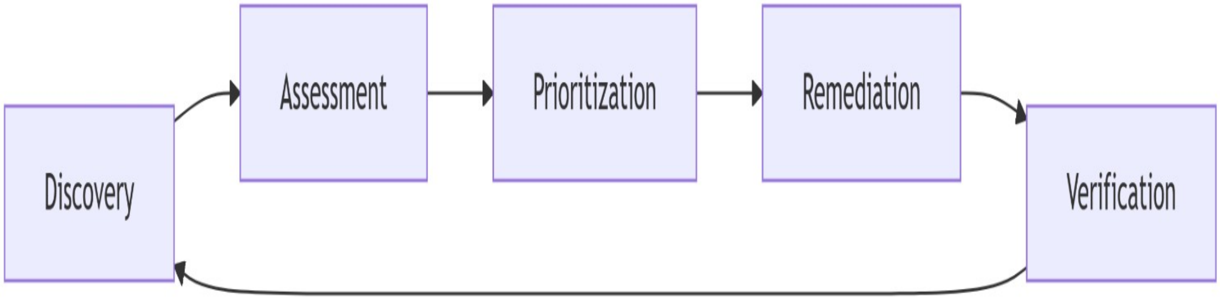


Figure 2

Continuous vulnerability management cycle to enhance organizational security posture.

3.3 Attack Analysis using MITRE and Cyber Kill Chain

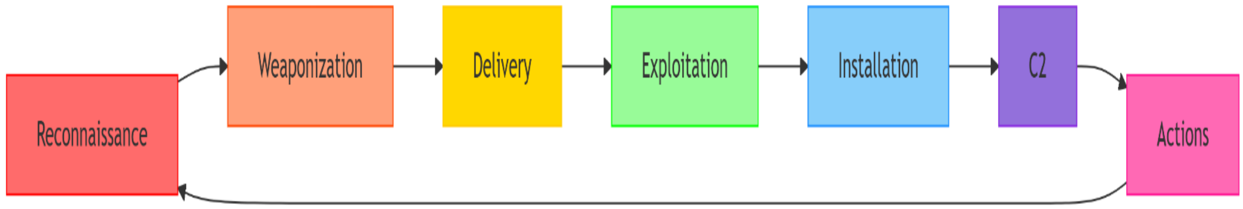
Framework Analysis:

- **Reconnaissance:** Social engineering via fake housing partnership,
- **Weaponization:** Malicious Excel macro creation,
- **Delivery:** Phishing email dissemination (T1566.001),
- **Exploitation:** Windows vulnerabilities and macro execution (T1203),
- **Installation:** Deployment of Phobos ransomware (T1059),
- **Command & Control:** Establishing connections to external servers (T1071.001),
- **Actions on Objectives:** Encrypting critical data and attempted data exfiltration (T1486, T1041).

Using MITRE ATT&CK provided a granular map of the techniques employed during the breach (Naik et al., 2022).

Figure 3

Phishing ransomware attack progression mapped using the Cyber Kill Chain model.



3.4 Post-Incident Response

The incident response sequence adhered to NIST SP 800-184 guidelines (National Institute of Standards and Technology, 2024) and proceeded as follows:

The incident response sequence adhered to NIST SP 800-184 guidelines (National Institute of Standards and Technology, 2024) and proceeded as follows:

- **Isolated and disconnected infected endpoints:**
  Immediate isolation of compromised devices prevented the malware from spreading laterally across the network. Disconnecting them contained the threat to a limited environment and preserved critical evidence for forensic analysis.
- **Conducted forensic analysis and gathered evidence:**
  Forensic investigation was critical to determine the attack vector, the scope of the compromise, and any exfiltration of sensitive data. Gathering artifacts like logs, memory images, and system states ensured proper documentation for legal and regulatory reporting.

- **Communicated the incident internally and externally:**

  Timely internal communication to leadership and affected teams minimized confusion and coordinated containment efforts. External notifications to clients, partners, and regulators ensured compliance with legal requirements and maintained organizational transparency.

- **Activated legal protocols for HIPAA and data privacy compliance:**

  Because tenant financial and health-related data may have been exposed, triggering HIPAA breach notification rules and Minnesota Data Practices Act obligations were essential to avoid legal penalties and protect affected individuals.

- **Recovered systems from isolated, tested backups in Azure:**

  Recovery efforts prioritized restoring critical systems using pre-tested, clean backups stored securely in Azure. This ensured that restored systems were free from hidden malware remnants and reduced downtime while maintaining data integrity.

- **Implemented updated firewall, endpoint, and MFA policies:**

  post recovery new firewall rules, stricter endpoint security configurations, and mandatory multi-factor authentication (MFA) were deployed. These controls reduced future attack surfaces and strengthened authentication resilience against credential theft and replay attacks.

PPL’s incident response phases are illustrated in Figure 4.

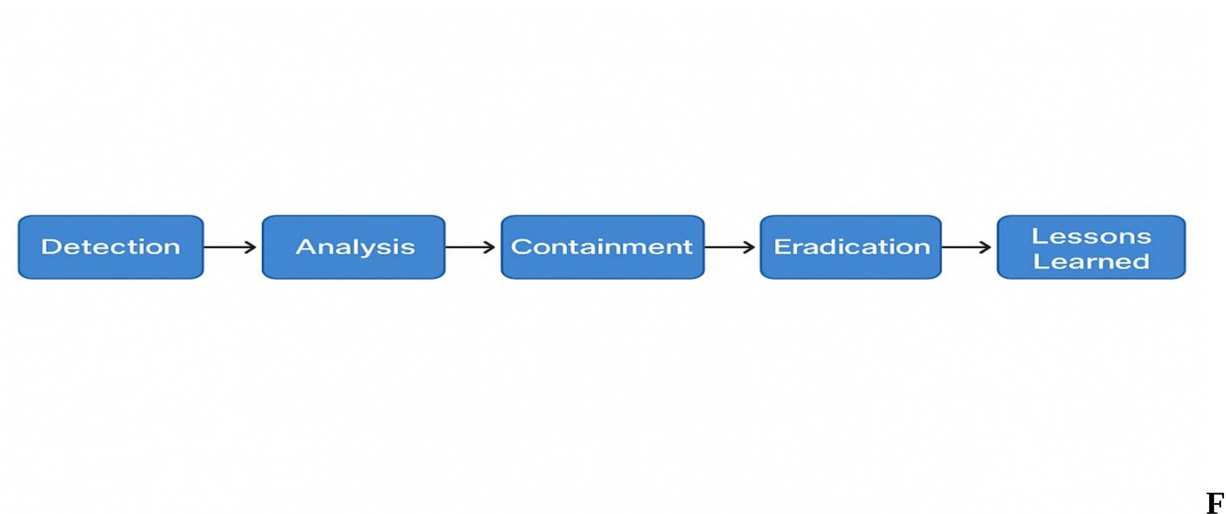


Figure 4

Incident response phases followed the cyber intrusion.

3.5 Future Prevention Recommendations

Building cyber resilience at PPL requires a multilayered approach:

- Enforcing MFA for VPN and internal access,
- Deploying a centralized, advanced EDR solution,
- Conducting quarterly phishing simulations (Dunmore et al., 2023),
- Hardening endpoint configurations to block unauthorized scripts,
- Implementing Zero Trust architecture across the environment,
- Automating patch management using Intune and WSUS.

Aslaner (2024) highlights that proactive detection combined with employee cybersecurity culture is the strongest defense against modern ransomware threats

Conclusion

The cyber intrusion scenario at PPL highlights the critical importance of a proactive and structured approach to cybersecurity. By leveraging advanced detection tools, vulnerability management processes, and recognized attack frameworks such as the Cyber Kill Chain and MITRE ATT&CK, organizations can better identify, respond to, and mitigate security threats. The incident response strategy outlined ensures that containment, eradication, and recovery are conducted efficiently while lessons learned inform future prevention efforts. As cybersecurity threats continue to evolve, maintaining a resilient and adaptive security posture is very important for protecting organizational assets, ensuring regulatory compliance, and sustaining trust with stakeholders. A forward-looking commitment to continuous improvement and employee security awareness will strengthen PPL’s ability to defend against future attacks.

References

Abdullayeva, F. (2023). Cyber resilience and cyber security issues of intelligent cloud computing systems. *Results in Control and Optimization, 12*, Article 100268. https://doi.org/10.1016/j.rico.2023.100268

Aslaner, R. (2024). Incident response in the real world. *Cybersecurity Review Journal, 19*(2), 34-48.

Cisco. (2023). Understanding Phobos ransomware attacks. https://www.cisco.com/

CrowdStrike. (2024). CrowdStrike Falcon platform overview. https://www.crowdstrike.com/

Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of Things meet Internet of Threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences, 11*(10), Article 4580. https://doi.org/10.3390/app11104580

Dunmore, A., Jang-Jaccard, J., Sabrina, F., & Kwak, J. (2023). A comprehensive survey of generative adversarial networks (GANs) in cybersecurity intrusion detection. *IEEE Access, 11*, 76071–76094. https://doi.org/10.1109/ACCESS.2023.3296707

Landauer, M., Skopik, F., Stojanović, B., Flatscher, A., & Ullrich, T. (2025). A review of time-series analysis for cyber security analytics: From intrusion detection to attack prediction. *International Journal of Information Security, 24*(1). https://doi.org/10.1007/s10207-024-00921-0

MITRE. (2024). MITRE ATT&CK framework. https://attack.mitre.org/

Naik, N., Grace, P., Jenkins, P., & Song, J. (2022). Comparing attack models for IT systems: Lockheed Martin’s Cyber Kill Chain, MITRE ATT&CK Framework and Diamond Model. *2022 IEEE International Symposium on Systems Engineering (ISSE)*, 1–7. IEEE. https://doi.org/10.1109/ISSE54508.2022.10005490

National Institute of Standards and Technology. (2024). *Guide for cybersecurity event recovery (NIST SP 800-184)*. https://doi.org/10.6028/NIST.SP.800-184

Nessus Vulnerability Scanner. (2024). Nessus. https://www.tenable.com/products/nessus

SANS Institute. (2023). Incident response playbooks. https://www.sans.org/white-papers/incident-response/

Wazuh Documentation. (2024). Wazuh. https://documentation.wazuh.com/