Enhancing Cybersecurity Resilience at PPL: A Strategic Approach

Ngsnet Hawarya

Saint Mary's University of Minnesota

Cyber 630: Communication and Ethics for Cybersecurity Professionals

Dr. John Beleford

March 2, 2025

Abstract

As cyber threats evolve, nonprofit organizations must adapt to protect sensitive data. Project for Pride in Living (PPL), a nonprofit that manages housing and financial assistance programs, faces increasing risks from data breaches, unauthorized access, and phishing attacks. This paper explores these challenges, proposes strategic security measures, and evaluates their effectiveness. Key solutions include multi-factor authentication (MFA), employee training, and strict data protection policies. Ethical considerations, such as transparency in data handling and avoiding surveillance overreach, are also addressed. The paper concludes with a detailed plan for measuring improvement through incident reduction metrics, compliance audits, and industry benchmarking.

Keywords: Cybersecurity, Data Protection, Multi-Factor Authentication, Compliance, Phishing Prevention, Nonprofit Security

Introduction

In an era of escalating cyber threats, nonprofit organizations like Project for Pride in Living (PPL) must prioritize cybersecurity resilience to protect sensitive data and maintain public trust. PPL, a nonprofit dedicated to providing housing assistance, career readiness, and job training for low-income individuals and families, relies heavily on digital platforms to manage renter and financial data. However, the increasing risks of data breaches, unauthorized access, and phishing attacks pose significant challenges to its operations. This paper examines PPL's cybersecurity vulnerabilities, proposes strategic solutions, and evaluates their effectiveness

through measurable outcomes. By addressing these issues, PPL can safeguard its mission and the communities it serves.

Organizational Background and Structure

Project for Pride in Living (PPL) is a nonprofit organization serving the Twin Cities, providing housing assistance, career readiness programs, and job training to low-income individuals and families. PPL manages over 65 apartment buildings, two high schools, and multiple commercial properties, serving thousands of community members annually. The organization relies on Microsoft Azure cloud services for its IT infrastructure, Yardi for rent collection and property management, and NVR3 cameras for security monitoring across more than 40 commercial buildings and apartment complexes.

Given the sensitive nature of the data PPL handles, financial records, tenant applications, and personal identifiable information (PII) ensuring cybersecurity resilience is a top priority. A breach could result in legal liabilities, reputational damage, and regulatory fines under laws such as the Fair Credit Reporting Act (FCRA) and Minnesota tenant protection laws.

Critical Issues

PPL faces several critical cybersecurity challenges that threaten its operations and the privacy of its clients:

1. **Unauthorized Access to Sensitive Data**:

   The use of Yardi for property management and rent collection poses significant risks. If unauthorized individuals gain access to tenant financial data, PPL could face legal and financial consequences. For example, a breach could expose sensitive information such

as Social Security numbers, bank account details, and rental histories, leading to identity theft and financial fraud.

2. **Vulnerabilities in the NVR3 Surveillance System**:

   While the NVR3 surveillance system enhances physical security, it also introduces cybersecurity risks. Poorly configured systems could allow cybercriminals to exploit vulnerabilities, leading to unauthorized surveillance, footage leaks, or hacking attempts that compromise tenant privacy. For instance, attackers could gain access to live camera feeds or stored footage, violating tenant privacy and potentially using the footage for malicious purposes.

3. **Phishing Attacks and Human Error**:

   A recent phishing attack targeted a PPL employee, compromising login credentials and exposing weaknesses in access management. Since most breaches originate from human error, strengthening security awareness training, access controls, and incident response planning is critical.

Audience Analysis

The primary audience for this presentation includes PPL's executive leadership, IT staff, property managers, and administrative employees. Each group has different levels of technical expertise and varying concerns regarding cybersecurity:

- **Executive Leadership**: Needs to understand the financial, legal, and reputational risks of cybersecurity threats and support increased investment in security infrastructure and employee training.

- **IT Staff**: Requires actionable strategies to mitigate cyber risks, implement security policies, and monitor compliance with regulatory standards.
- **Property Managers and Administrative Staff**: Need practical guidelines for secure data management, password management, and phishing attack prevention, as they interact with tenant applications and financial transactions daily.

Communication Plan and Technology Needs

A robust and multi-faceted cybersecurity communication plan is essential to ensure that all employees at PPL are well-informed, trained, and prepared to handle potential cyber threats. This plan will be tailored to address the varying levels of technical expertise among different employee groups, ensuring that everyone—from executive leadership to administrative staff understands their role in maintaining cybersecurity. The key components of this plan include:

1. **Security Awareness Training**:
    - **Quarterly Phishing Simulations**: These simulations will test employees' ability to identify and respond to phishing attempts, which are one of the most common attack vectors. By conducting these exercises regularly, PPL can assess employee readiness and identify areas for improvement.
    - **Monthly Workshops**: Interactive workshops will be held to educate employees on the latest cybersecurity threats and best practices. These sessions will include real-world examples and case studies to make the training more relatable and impactful.
    - **Role-Specific E-Learning Modules**: Customized training modules will be developed for different roles within the organization. For example, property

managers will receive training in secure data handling, while IT staff will focus on advanced threat detection and response techniques.

2. **Incident Response Protocols**:
    - **Clear Reporting Guidelines**: Employees will be provided with straightforward instructions on how to report security incidents, including whom to contact and what information to provide. This will ensure that incidents are reported promptly and accurately.
    - **Steps for Breach Scenarios**: A detailed incident response plan will outline the steps IT staff should take in the event of a breach, including containment, investigation, recovery, and communication with stakeholders. This plan will be regularly updated to reflect emerging threats and lessons learned from past incidents.
3. **Multi-Factor Authentication (MFA) and Access Control**:
    - **Implementation of Azure Active Directory (AAD)**: MFA will be enforced across all systems to add an extra layer of security. AAD will also be used to provide the least privileged access, ensuring that employees only have access to the data and systems necessary for their roles.
4. **Data Protection Policies**:
    - **Encryption of Tenant Records**: All sensitive data, including tenant applications and financial records, will be encrypted both in transit and at rest to prevent unauthorized access.

- **Regular Data Backups**: Automated backups will be performed daily to ensure that data can be quickly restored in the event of a ransomware attack or other data loss incident.
- **Least-Privilege Access Enforcement**: Employees will only be granted access to the data and systems required for their specific job functions, reducing the risk of insider threats and accidental data exposure.

5. **Regular Cybersecurity Updates**:
    - **Monthly Newsletters**: These newsletters will provide updates on the latest cybersecurity threats, tips for staying safe online, and reminders about PPL's security policies.
    - **Executive Briefings**: Leadership will receive regular updates on the organization's cybersecurity posture, including metrics on incident rates and training completion.
    - **Security Policy Refreshers**: Employees will receive periodic reminders about key security policies, such as password management and data handling procedures.

Ethical Considerations

While implementing cybersecurity measures, PPL must balance the need for security with ethical obligations to protect client privacy and ensure fair access to services. Key ethical considerations include:

1. **Transparency in Data Handling**:
    - PPL will clearly communicate to residents how their data is collected, stored, used, and protected. This transparency will build trust and ensure that residents are aware of their rights regarding their personal information.
2. **Fair Access to Technology**:
    - Cybersecurity policies must not create barriers for clients seeking housing services or assistance. For example, overly complex authentication processes could prevent some clients from accessing online portals. PPL will strive to implement security measures that are both effective and user-friendly.
3. **Avoiding Surveillance Overreach**:
    - The NVR3 camera systems installed across PPL properties must be used strictly for security purposes. Clear policies will be established to prevent misuse of surveillance footage and ensure that tenant privacy is respected.
4. **Ethical AI Use**:
    - If AI tools are used in cybersecurity (e.g., for threat detection), PPL will ensure that these tools are free from bias and do not disproportionately impact certain groups. Regular audits will be conducted to assess the fairness and accuracy of AI algorithms.

How Will Improvement Be Measured? To assess the effectiveness of the cybersecurity initiatives, PPL will use a combination of quantitative and qualitative metrics. These metrics will provide a comprehensive view of the organization's cybersecurity posture and highlight areas for improvement. Key metrics include:

1. **Incident Reduction Metrics**:
    - The number of phishing incidents, unauthorized access attempts, and malware infections will be tracked before and after the implementation of security awareness training and other measures. A significant reduction in these incidents will indicate that the initiatives are effective.
2. **Employee Security Compliance**:
    - Completion rates for security awareness training, participation in phishing simulations, and adherence to IT security policies will be measured. High compliance rates will demonstrate that employees are engaged and taking cybersecurity seriously.
3. **Compliance Audits**:
    - Biannual audits will be conducted to assess PPL's adherence to relevant regulations, such as HIPAA, FCRA, and Minnesota Chapter 504B. These audits will identify any gaps in compliance and provide actionable recommendations for improvement.
4. **Industry Benchmarking**:
    - PPL's cybersecurity posture will be compared to that of similar nonprofit organizations. This benchmark will provide insights into best practices and help PPL identify areas where it can improve.
5. **Internal Security Assessments**:
    - Periodic internal assessments, including penetration testing, external audits, and employee surveys, will be conducted to evaluate the effectiveness of

cybersecurity policies and identify any gaps. These assessments will provide a holistic view of the organization's security readiness.

Conclusion

Cybersecurity resilience is essential for PPL to protect sensitive data and maintain compliance with regulatory requirements. By implementing security awareness training, multi-factor authentication, and strict data protection policies, PPL can significantly enhance its defense against cyber threats. Continuous assessment through audits and benchmarking will ensure ongoing improvement. By fostering a culture of cybersecurity awareness, PPL can effectively mitigate risks and safeguard its mission of providing housing and job assistance.

References

HIPAA Security Rule (2022) Best practices for protecting sensitive data.

Larkey, S. N. (2019). *Exploring the strategies cybersecurity specialists need to minimize security risks in non-profit organizations.* Retrieved from https://www.proquest.com/openview/8afffc36e46d41c80c98febbd1bcd00e/1?pq-origsite=gscholar&cbl=18750&diss=y

Microsoft Azure Security Best Practices (2024) – Implementing AAD and MFA for access control.

NIST Cybersecurity Framework (2023) – Guidelines on improving security resilience.

National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity.* Retrieved from https://www.nist.gov/cyberframework

Ray, J. R. (2014). *Training programs to increase cybersecurity awareness and compliance in non-profits (Master's capstone project).* University of Oregon. Retrieved from https://hdl.handle.net/1794/19638

SANS Institute. (n.d.). *Incident Response and Handling.* Retrieved from https://www.sans.org/cybersecurity-training