# Case Study: Comprehensive Security Assessment for a Leading Medical Institution by Grab The Axe

Introduction: A leading medical institution recognized the need for a holistic security assessment to safeguard its digital and physical assets. They engaged Grab The Axe, a premier security consultancy, to conduct a comprehensive cybersecurity and physical security assessment.

Published by :

Grab The Axe

Phoenix, Arizona
September 8th, 2023
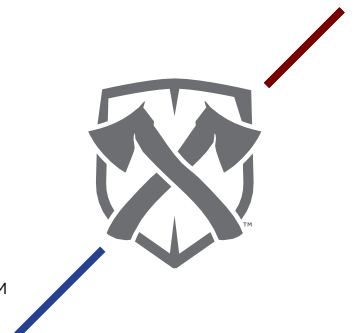
1. Objectives:

To evaluate and enhance the security posture of the medical institution by identifying vulnerabilities in both digital infrastructure and physical premises, and to provide actionable recommendations for improvement.

"Conducting both physical and cybersecurity assessments is crucial as it provides a holistic view of an organization's vulnerabilities. This comprehensive approach enhances overall operational resilience and trustworthiness."

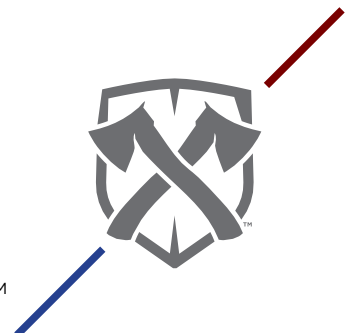**Methodology:**

1. Cybersecurity Assessment:

    -   External and internal penetration testing.
    -   Open Source Intelligence Gathering (OSINT).
    -   Evaluation based on NIST SP 800-115, OWASP Testing Guide (v4), and custom testing frameworks.

2. Physical Security Assessment:

    -   On-site inspection of premises.
    -   Evaluation of access controls, surveillance systems, and potential vulnerabilities.

2. Key Findings:

Cybersecurity

1. **Critical Vulnerabilities**: Unsecured internal network access, potential for social engineering exploitation, compromised email accounts, a printer with direct outside access used for scanning and printing sensitive documents like driver's licenses and social security cards, and a medical scanning machine running on outdated Windows 98 software.

2. **Website Vulnerabilities**: Directory listing enabled, outdated security certificates, and misconfigured DMARC records.

As a result, they successfully negotiated a 50% monthly cost reduction in their security service fees, saving more than $1,500/month.

Recommendations: Update and patch systems, enforce password policies, secure network printers, rectify website vulnerabilities, and update outdated software on medical devices.

Physical Security

1. **Access Control**: Unsecured server room door, providing easy access to critical infrastructure.

2. **Surveillance**: Lack of monitoring in key areas, including the network room.

Recommendations: Install locking mechanisms, enhance surveillance, and conduct regular security training for staff.

Note: Printers and outdated medical devices have been identified as significant vulnerabilities in healthcare settings, posing risks to patient privacy (Morse, S., 2023).

Evaluation & Analysis

Financial Impact: Upon presenting the findings, the medical institution confronted their existing security provider with the vulnerabilities identified. As a result, they successfully negotiated a 50% monthly cost reduction in their security service fees, saving more than $1,500/month. This significant cost savings not only validated the value of the assessment but also provided the institution with substantial financial benefits.

Outcome: Grab The Axe's comprehensive assessment provided the medical institution with a clear understanding of their security posture. The actionable insights and recommendations ensured that the institution could address vulnerabilities promptly, enhancing their overall security and achieving significant cost savings.

Client Testimonial: "Engaging with Grab The Axe was one of our best decisions. Their holistic approach to security ensured that we not only fortified our digital assets but also our physical premises. Their recommendations were invaluable, and we've since implemented them to great effect. The added benefit of a 50% cost savings was the cherry on top. We now feel more secure and confident in our operations, all while saving money."

- **Clinic Operations Manager & Case Manager**, Leading Medical Institution

Conclusion: In today's interconnected world, a comprehensive approach to security is paramount. Grab The Axe's dual assessment for the medical institution underscores the importance of evaluating both digital and physical vulnerabilities. Their expertise, actionable recommendations, and the resulting financial benefits have fortified the institution against potential threats, ensuring the safety, trust, and financial well-being of their operations.

References:

Morse, S. (2023). Medical devices are the next security nightmare. Healthcare IT News. Retrieved from https://www.healthcareitnews.com/news/medical-devices-are-next-security-nightmare