Mariam Adegbindin

CIDM 6340 Network Management & InfoSec

Audit Report

**What did I do?**

The audit was conducted to comprehensively assess the operations and security measures of the Office of Career and Professional Development (OPCD) at West Texas A&M University. Upon arrival at the OPCD, contact was made with Kat Kane, the director of the OPCD, to obtain authorization to proceed with the audit. Entry was granted, and an initial walkthrough of the office premises was conducted to gauge staff reactions and assess physical security awareness.

Subsequently, an audit meeting was convened with the participation of the auditor, Mariam Adegbindin, and relevant staff members. The audit plan documentation was completed in collaboration with Kat Kane and other staff members present. The audit plan served as a comprehensive guide, ensuring that all relevant areas were addressed and assessed according to predetermined criteria. Following the completion of the audit plan documentation, a post-audit meeting was held with Kat Kane to convey initial findings. This provided an opportunity to discuss observations, clarify any concerns, and lay the groundwork for further action planning.

The audit was conducted on April 23, 2024, from 9:00 am to 5:00 pm, with meticulous attention to detail and adherence to established audit procedures. The comprehensive nature of the audit plan facilitated a thorough assessment of the OPCD's operations and security measures, laying the foundation for subsequent analysis and recommendations.

**What were the results?**

The audit identified areas of compliance with regulatory standards, effective collaboration with IT entities, and the presence of multi-factor authentication (MFA) for critical systems. Other major findings include:

* ***Physical Security Vulnerabilities*:** The examination of physical security revealed several vulnerabilities, including unrestricted access to the office premises and lack of surveillance measures. This poses a significant risk of unauthorized entry and potential theft of sensitive information. The severity of this finding is high, as it directly impacts the organization's ability to protect confidential data and maintain the integrity of its operations.
* ***Inadequate Shredding Facilities:*** The absence of a designated shred box for proper disposal of sensitive documents raises concerns regarding secure waste handling practices. Without proper disposal methods, sensitive information could be compromised. While this finding may not seem critical on its own, the cumulative impact of improper data disposal practices can pose a substantial risk to the organization's data security over time.
* ***Password Weaknesses:*** While passwords were generally complex and did not contain dictionary words, some devices, such as iPads, lacked password protection altogether, exposing them to unauthorized access and potential data breaches. Password security is a fundamental aspect of cybersecurity, and any weaknesses in this area can significantly increase the organization's vulnerability to data breaches and unauthorized access.
* ***Surge Protection Absence:*** The absence of surge protection devices poses a risk of damage to organizational computers and data loss in the event of power surges or electrical faults. While power surges may seem like a rare occurrence, the potential impact of data loss or damage to critical infrastructure cannot be understated. This finding highlights a critical gap in the organization's infrastructure resilience and data protection measures.
* ***Room Access Controls:*** Although the server room is temperature-controlled, the lack of restricted access raises concerns about unauthorized personnel accessing critical infrastructure, increasing the risk of unauthorized data access or tampering. Unauthorized access to the server room can have severe consequences, including data breaches, service interruptions, and compromised system integrity. Therefore, addressing this finding is crucial to enhancing the organization's overall security posture.

**What are your recommendations?**

* ***Enhance Physical Security Measures:*** Implement access controls, such as ensuring the doors are closed when there is no one in the office. This can be achieved by being intentional and accountable for their actions.
* ***Implement Shred Box:*** Acquire and install a designated shred box for proper disposal of sensitive documents. This can be done economically by sourcing cost-effective shredding solutions. **Timeline: Implement within 1 month.**
* ***Strengthen Password Policies:*** Enforce password protection on all digital devices, including iPads, and conduct regular password audits to ensure compliance. Provide training on creating strong passwords. **Timeline: Implement within 1 month.**
* ***Install Surge Protection Devices:*** Procure and install surge protection devices for organizational computers to mitigate the risk of damage from power surges. This can be achieved economically by purchasing surge protectors in bulk. **Timeline: Implement within 1 months.**
* ***Enhance Room Access Controls:*** Implement access controls, such as getting authorised access from a staff member and ensuring the door is always locked and if access is needed getting the key from the authorised personnel. **Timeline: Implement within 2 months.**

**What is their risk posture?**

In conclusion, the Office of Career and Professional Development (OPCD) at West Texas A&M University exhibits a moderate to high level of vulnerability to cybersecurity threats and risks. The audit findings have highlighted several areas of concern that contribute to the organization's overall risk posture. The greatest risk facing the OPCD is the presence of physical security vulnerabilities, including unrestricted access to office premises. These vulnerabilities pose a significant threat of unauthorized entry and potential theft of sensitive information, thereby compromising the confidentiality, integrity, and availability of organizational data and resources. While all identified vulnerabilities are important to address, the greatest vulnerability lies in the inadequate protection of sensitive data due to physical security weaknesses. Unauthorized access to office premises and critical infrastructure increases the risk of data breaches, unauthorized data access, and tampering, posing a substantial threat to the organization's reputation, financial stability, and regulatory compliance.

Overall, the OPCD faces moderate to high risks associated with cybersecurity threats, including data breaches, unauthorized access, and potential service disruptions. While certain areas of compliance with regulatory standards and collaboration with IT entities were identified during the audit, they do not fully mitigate the risks posed by physical security vulnerabilities and other findings. To improve the organization's risk posture, it is imperative to address the identified vulnerabilities and implement the recommended measures outlined in the audit report. By prioritizing cybersecurity measures and enhancing security controls, the OPCD can strengthen its resilience to cybersecurity threats and minimize the risk of data breaches and unauthorized access.