Liam Redman

7/11/2024

CYSE 368

Reflection #4

Internship Reflection 4

During the fourth 50 hours of my internship, I encountered two major events that significantly broadened my understanding of the Cybersecurity landscape and corporate dynamics. These events included our company's migration from Mimecast to Microsoft 365 (M365) and a cybersecurity incident involving a client’s payroll system. Both experiences provided practical insights into the complexities of implementing new technologies and security measures.

The migration from Mimecast to M365 was a significant project. Mimecast is a cloud-based email management service known for its robust security, archiving, and continuity features. The decision to migrate was driven by M365’s enhanced in-house functionalities, which rendered Mimecast's services redundant. This transition was not without its challenges. A notable aspect was the intense pricing negotiations with Mimecast, who proposed fees that we found unreasonable. Observing these discussions was a learning experience, showcasing the importance of assertive communication and strategic compromise in achieving favorable outcomes. It was fascinating to see how business negotiations unfold, balancing financial considerations with technological advancements.

The second significant event was a cybersecurity incident involving a client's payroll system. The system was compromised at the user level, resulting in an unauthorized change to an associate’s direct deposit information. Despite our long-standing recommendations to implement two-factor authentication (2FA), the client had resisted, citing concerns about complexity and potential employee dissatisfaction. This incident starkly illustrated the critical importance of 2FA in safeguarding sensitive information. Following the breach, the client finally agreed to implement 2FA, underscoring the adage that prevention is better than cure.

As a young cybersecurity professional, witnessing resistance to fundamental security practices like 2FA was eye-opening. It was particularly intriguing to see older professionals view these measures as burdensome, whereas to me, they seem indispensable. This experience highlighted the generational gap in attitudes towards cybersecurity and the ongoing challenge of advocating for robust security measures.