5-2 Project Two Milestone: Presentation Planning

Joshua Merren

Southern New Hampshire University

CYB-400-13637-M01 Security Assessment & Auditing

Professor Jillian Seabrook

29 November 2024

When presenting the findings from Project One to Grey Matter's board of directors, it is essential to simplify complex technical details into clear and concise insights that align with the company's goals. I would begin by summarizing the critical vulnerabilities identified during the security assessment, focusing on their potential impact on business operations, finances, and reputation. For example, I could explain how unpatched SMB server vulnerabilities might lead to unauthorized data access, resulting in significant financial losses or reputational harm. To effectively communicate urgency, I outline prioritized remediation steps, such as immediate actions like applying critical patches and longer-term strategies like updating security policies and training staff. By focusing on the business implications rather than technical specifics, I can ensure the board understands the risks and the proposed solutions (Freund, 2020). Additionally, connecting these findings to real-world examples, like the WannaCry ransomware attack exploiting SMB vulnerabilities, will highlight the importance of swift action (Gelnaw, 2023).

I would use strategies prioritizing clarity and engagement to communicate technical findings to a less technical audience. One effective approach is avoiding technical jargon and using plain language to describe vulnerabilities. For instance, rather than discussing "SMB brute-force login vulnerabilities," I would explain it as "a system weakness that could allow hackers to break into our network." Visual aids, such as charts and infographics, can also simplify complex data and make key points more accessible (Freund, 2020). Real-world analogies are another helpful tool—for example, comparing outdated encryption methods to using a weak lock on a door makes the issue relatable. Storytelling is another effective method, such as recounting an incident where companies faced fines for failing to address similar vulnerabilities. Engaging the audience with examples and providing opportunities for questions ensures they understand how these risks align with the company's goals and priorities (Gelnaw, 2023).

In developing a visual aid for the presentation, I would create a table categorizing the vulnerabilities based on severity and the remediation timeline. This table would include columns for vulnerability names, potential impacts, recommended actions, and the timeframe for resolution (e.g., one week, one month, or two months). For example, I might include "Unpatched SMB Server Vulnerability" with a listed impact of "Risk of unauthorized data access," a recommended action of "Apply security patch," and a resolution timeframe of "Immediate (within one week)." This format helps board members quickly grasp the scope of issues and understand prioritization (Freund, 2020). Organizing the information this way emphasizes the most pressing concerns and supports informed decision-making.

The visual aid itself would take the form of a clean, well-organized table with clear headings. Each row would represent a specific vulnerability, and color-coding could highlight severity levels—for example, red for high-risk vulnerabilities needing immediate action, yellow for medium-risk issues, and green for lower risks. This visual scale draws attention to critical areas while keeping the overall design simple and focused. A single-slide presentation of the table ensures clarity and prevents the audience from being overwhelmed (Gelnaw, 2023). By keeping the design clean and simple, I can ensure that the visual aid effectively supports the critical points of my presentation.

Incorporating this visual aid into the presentation would enhance the board's understanding of the security assessment findings. It provides a clear snapshot of the current security posture, showing which vulnerabilities pose the most significant risks and the steps required to mitigate them. Presenting this information as a visual ensures that even non-technical stakeholders can follow along and make informed decisions. Furthermore, the visual aid takes center stage during the discussion, actively guiding the conversation and ensuring systematic coverage of all critical points. Translating technical data into an accessible format allows me to effectively communicate the urgency and importance of these vulnerabilities, aligning the discussion with the organization's strategic goals (Freund, 2020; Gelnaw, 2023).

References

Freund, J. (2020, April 30). *Communicating Technology Risk to Nontechnical People: Helping Enterprises Understand Bad Outcomes*. ISACA. https://www.isaca.org/resources/isaca-journal/issues/2020/volume-3/communicating-technology-risk-to-nontechnical-people

Gelnaw, A. (2023, August 30). Cybersecurity visualization Techniques to gain Executive Buy-In. *Bitsight*. Retrieved November 29, 2024, from https://www.bitsight.com/blog/cybersecurity-visualization-techniques-to-gain-executive-buy-in