**Q. Watch the following video: https://vimeo.com/560370018**

**Describe a scenario where a cybersecurity control may be recommended for an environment but is deemed not practicable for an organization. What advice can you give to an organization to establish a compensating control to address the fact that you chose not to implement the recommended cybersecurity control? What are the pros and cons of this approach? What concepts can you apply to a system in order to improve the resilience against adversarial cyber activity? What considerations should you take into place when considering which concepts to apply to your organization?**

**The Challenge of Implementing Cybersecurity Controls at ThalesGroup**

ThalesGroup (ThalesGroup. (n.d.)), as a global leader in aerospace, defense, and security, operates in a highly complex and regulated environment. A scenario where a recommended cybersecurity control may be deemed impracticable involves the implementation of multifactor authentication (MFA) across legacy systems integral to the organization's operations. While MFA is a critical defense mechanism against unauthorized access, certain divisions of Thales Group may face challenges such as the high cost of implementing MFA across a sprawling IT environment or the incompatibility of MFA solutions with legacy systems essential for operations (Hildreth & Gonzalez, 2021). For instance, production environments in aerospace manufacturing may depend on legacy equipment that cannot integrate with modern MFA solutions without costly upgrades, leading to delays in critical projects (National Institute of Standards and Technology (NIST). (n.d.)).

**Establishing Compensating Controls**

When a decision is made not to implement MFA due to operational constraints, ThalesGroup (ThalesGroup. (n.d.)) must establish compensating controls to address the residual risk. For example, robust password policies combined with strict access controls and advanced endpoint monitoring can mitigate the risk of unauthorized access. These policies might include enforcing strong password complexity, mandating regular password updates, and conducting audits of privileged account activities (Smith, 2020). Additionally, deploying network segmentation and real-time intrusion detection systems (IDS) can provide an additional layer of security to sensitive systems. Thales (ThalesGroup. (n.d.)) should also enhance employee training programs to educate staff about phishing and social engineering attacks, which often exploit weak authentication mechanisms. Documenting the decision-making process, including an evaluation of the compensating control's effectiveness, ensures compliance with industry standards and serves as a basis for revisiting this decision as technology evolves (Hildreth & Gonzalez, 2021).

**Pros and Cons of Compensating Controls**

The implementation of compensating controls at Thales offers significant advantages. These measures allow the organization to address security risks while maintaining operational continuity and avoiding extensive modifications to critical systems. For example, implementing network monitoring solutions and conducting

regular threat hunting can provide immediate protection at a fraction of the cost of an MFA overhaul (National Institute of Standards and Technology (NIST). (n.d.)). However, compensating controls also have inherent limitations. They may not be as robust as the originally recommended controls, leaving the organization exposed to a higher level of residual risk. Additionally, maintaining compensating controls requires significant resources for ongoing monitoring, updates, and training, which can strain IT teams (Smith, 2020).

**Improving System Resilience Against Cyber Threats**

To enhance resilience against adversarial cyber activity, Thales should prioritize strategies such as defense-in-depth and zero trust. Defense-in-depth ensures that multiple layers of security, such as network segmentation, encryption, and intrusion prevention systems, protect critical assets (National Institute of Standards and Technology (NIST). (n.d.)). Zero trust principles, which require continuous authentication and access verification for all users and systems, align with Thales' need to secure sensitive data and operations against evolving threats (Smith, 2020). Implementing continuous monitoring and leveraging artificial intelligence to detect and respond to anomalies in real-time can further improve resilience. Thales (ThalesGroup. (n.d.)) should also integrate advanced threat intelligence platforms into its cybersecurity strategy. These platforms enable the organization to proactively identify and neutralize threats targeting its industry. Establishing and regularly updating incident response plans ensures that Thales is prepared to mitigate the impact of security breaches quickly.

**Key Considerations for ThalesGroup**

When applying cybersecurity concepts, ThalesGroup must consider its unique operational and regulatory landscape. As a key player in defense and aerospace, the organization faces stringent compliance requirements, such as those from the European Union’s General Data Protection Regulation (GDPR) and defense-specific cybersecurity mandates (National Institute of Standards and Technology (NIST). (n.d.)). Balancing these regulatory requirements with the practical realities of managing a global IT infrastructure is critical. Moreover, Thales (ThalesGroup. (n.d.)) should evaluate the potential impact of security measures on operational efficiency. For instance, while zero trust principles are highly effective, they may introduce latency in workflows, which could disrupt mission-critical activities. Conducting a cost-benefit analysis and piloting new measures in isolated environments before full implementation can help mitigate potential disruptions (Hildreth & Gonzalez, 2021).

**Conclusion**

At ThalesGroup (ThalesGroup. (n.d.)), balancing security with operational feasibility is essential for sustaining business and maintaining leadership in aerospace, defense, and security. While recommended controls like MFA may sometimes be impractical, compensating controls such as advanced monitoring and robust access policies can effectively mitigate risks. By adopting strategies like defense-in-depth and zero trust, Thales can enhance its

resilience against cyber threats while adhering to its unique operational and regulatory requirements. Tailoring cybersecurity measures to the organization's needs and constraints ensures a robust and adaptive security posture that protects its critical assets and operations.

**References**


Hildreth, S., & Gonzalez, M. (2021). Cybersecurity strategies: Balancing cost and risk. *Journal of Information Security Management*, 14(2), 45-60.

National Institute of Standards and Technology (NIST). (n.d.). Cybersecurity framework. Retrieved January 12, 2025, from https://www.nist.gov/cyberframework

Smith, J. (2020). Zero trust: A comprehensive approach to cybersecurity. *Cyber Defense Quarterly*, 9(3), 22-29.

ThalesGroup. (n.d.). *Thales Group: Building a future we can all trust*. Retrieved January 12, 2025, from https://www.thalesgroup.com/en