Daphnie Bruno
Professor: Bill Moran
CYB359-0 | C202503-01
March 25, 2025

4.5 - Assignment: New Security Policies with this Month's Content

1. System Development Life Cycle (SDLC)

Threat modeling forms a critical component of the SDLC as it helps organizations identify potential vulnerabilities at all stages, right from planning and design through to deployment and maintenance. Threat modeling at the stages of requirements and design facilitates security requirements establishment and anticipating potential attack vectors available for threat actors. During development and testing, threat modeling contributes towards security feature prioritization and adversary activity modeling so that the design is properly secure. When integrated early (also known as the "shift-left" strategy), threat modeling reduces expenses through the identification of issues before going into production. It also ensures controls are being mapped to business objectives and regulatory frameworks like NIST 800-53. In SnowBe Online, adding threat modeling in SDLC strengthens risk awareness throughout teams, boosts security defenses on applications handling customer data, and promotes cross-functional collaboration on security issues. This approach not only enhances system resilience but also lays the groundwork for an active security culture throughout the lifecycle.

---

2. Software Development Life Cycle (focused on Software, not Systems)

In the Software Development Life Cycle (SDLC), threat modeling helps developers, designers, and security teams collectively identify, classify, and counter potential threats to the application. Compared to system-focused SDLCs, software-focused threat modeling examines deeper into code logic, APIs, input validation, and data flow diagrams to view how attackers will take advantage of logic flaws or vulnerabilities. It's especially applicable in the current agile and DevSecOps settings, where the attack surface is increased by releasing more often. Threat modeling activities like STRIDE or DREAD help teams examine authentication flows, session state, and data exposure. To illustrate, if SnowBe Online's online store website is being built, threat modeling could identify vulnerabilities in the payment authorization or customer login code. Introducing this practice at each sprint allows teams to continually improve their application security posture. It creates security awareness among developers and eradicates vulnerabilities in the product, directly affecting user trust and regulatory compliance.

---

3. Security Maturity

Threat modeling most directly supports increasing an organization's security maturity, especially as it compared to a model like the CMMC or NIST Cybersecurity Framework. It indicates a move from reactive to proactive security practice, typical of a maturing organization. In a low maturity organization, threats are addressed ad hoc, typically after a breach has occurred. With greater maturity, organizations use formal processes like regular threat modeling to identify gaps prior to attacking them. SnowBe Online, for instance, can baseline where it currently is with regard to risks and then shift to a more mature posture by incorporating results into its risk management plan. Adding threat modeling to continuous improvement, risk assessment, and vulnerability scanning enables an organization to move from Level 1 (beginning) to Level 4 or 5 (optimized and controlled). Lastly, threat modeling enables a risk driven approach and continuous feedback loops, which are mandatory components of any high-maturity security program.

---

4. Security Plan and Policies

Threat modeling informs an organization's security plans and policies by giving insight into real attack patterns and mitigation suggestions. Policies can't be created in isolation but must be grounded in realistic risks, and threat modeling finds those for them. Take access control, data retention, encryption, or patch management policy; any one of these can be confirmed and refined by suggestions from threat modeling drills. SnowBe Online's security policy establishes roles and guidelines like NIST 800-53, but threat modeling gives it depth that is actionable by translating high-level controls into concrete threats. Additionally, since security policies evolve over time, threat modeling keeps technical implementations (e.g., utilization of MFA or VPN) aligned with the actual risk posture of the organization. It also aids in policy enforcement by creating traceable justification for the necessity of specific controls. This, in turn, leads to ever-more effective and specific security policies that reduce organizational risk while providing long-term compliance.