# 3-3 Stepping Stone: Introduction to Threat Modeling

Joshua Merren

Southern New Hampshire University

CYB-250-11621-M01 Cyber Defense

Professor Tchinda Mbuna

15 July 2024

## I. Threat Modeling

| Incident | Target Breach | Sony Breach | OPM Breach |
|---|---|---|---|
| **Attackers** | the attackers were initially believed to be part of an organized crime group specializing in stealing credit card data. | Hacktivists with possible nation-state sponsorship, identified as 'Guardians of the Peace.' | Suspected state-sponsored Chinese hackers used sophisticated techniques to breach OPM's systems, possibly as part of a larger espionage strategy. |
| **Tools** | Malware including BlackPOS, which scraped memory from POS terminals to capture credit card data. | Custom malware tools, including data-wiping malware named Destover, were used to disrupt operations, delete critical data, and leak sensitive information. | The hackers utilized malware such as PlugX and Sakula, which provided them with remote access capabilities and the ability to move laterally within the network. |
| **Vulnerability** | Poor network segmentation and security practices at Target allowed the malware to access and transmit sensitive data. | Sony's network was insufficiently secured against sophisticated intrusion tactics, and there was a failure to respond adequately to previous security warnings. | Inadequate security measures including the lack of multi-factor authentication for system access and insufficient monitoring of sensitive systems. |

| | | | |
|---|---|---|---|
| **Action** | Attackers installed malware on POS systems to capture credit card information and transmitted it out of the network. | Deployment of destructive malware leading to the erasure of system data, dissemination of confidential communications, and public exposure of personal information of employees and celebrities. | Utilization of stolen credentials to install backdoors and malware on the network, enabling the exfiltration of sensitive data including SF-86 forms. |
| **Target** | Point of Sale (POS) systems handling credit card transactions. | Corporate networks, specifically systems containing sensitive employee data, intellectual property, and internal communications. | Databases containing detailed personnel records and background check information for government employees. |
| **Unauthorized Result** | Theft of 40 million credit and debit card numbers and 70 million records containing personal information. | Massive data destruction, public leakage of confidential emails, unreleased films, and severe reputational damage to Sony. | Theft of sensitive personal data for over 22 million current and former federal employees, including fingerprints and background check information. |
| **Objective** | To steal credit card information for fraudulent purposes. | Coerce Sony into altering or halting the release of a film ("The Interview") critical of | Gather extensive personal and biometric information for intelligence |

| | | | |
|---|---|---|---|
| | | North Korea, alongside punishing the company for perceived insults. | purposes, potentially for use in creating detailed profiles on U.S. government employees. |

## II. Incident Analysis: OPM Breach

Among the incidents studied, the "Confidentiality" component of the CIA triad is most applicable to the action category of the OPM breach. The unauthorized access and exfiltration of susceptible data breached confidentiality on a massive scale. This violation of privacy and security impacted individual employees and had broader national security implications.

Analyzing the attack using an adversarial mindset allows cybersecurity professionals to understand better and counteract the tactics employed. The attackers in the OPM breach likely had a detailed understanding of the systems they targeted, allowing them to maneuver through the network undetected for an extended period. They exploited less secure third-party connections, an often-overlooked vulnerability, to gain initial access. Recognizing such sophisticated strategies helps to craft layered defense mechanisms that are adaptive and robust against multi-vector attacks.

Proactively employing threat modeling at OPM could have led to significant changes in handling and protecting sensitive information. For instance, more rigorous identity and access management controls could have been established, including enforcing multi-factor authentication and stricter access protocols for third-party vendors. Regularly conducting security audits and penetration testing could have helped identify and mitigate vulnerabilities

before they could be exploited. Moreover, continuous monitoring of network traffic and anomaly detection systems alerted administrators to unauthorized access attempts sooner, potentially preventing extensive data exfiltration.

## III. Threat Modeling Extension

The necessity of threat modeling in cybersecurity is apparent, given its capacity to systematically identify and address potential vulnerabilities before they are exploited. To persuade a supervisor of the importance of threat modeling, one could argue that threat modeling enhances security and optimizes resource allocation by directing security efforts where they are most needed. Additionally, it supports compliance with various regulatory requirements by demonstrating due diligence in protecting sensitive information.

Threat modeling is critical for security practitioners because it provides a comprehensive method for assessing security from an attacker's perspective. Security teams can design systems and controls that effectively mitigate risks by understanding potential attack vectors. This proactive approach is far more cost-effective than the reactive handling of security breaches, often resulting in significant financial and reputational damage.

Beyond enhancing security controls, threat modeling can offer organizational benefits such as improved IT governance and risk management. It can foster a culture of security awareness throughout the organization, ensuring that all employees understand their role in maintaining security. This holistic approach not only improves security but also enhances the overall resilience of the organization against cyber threats.

Regarding role-specific applications, threat modeling differs significantly across various IT functions. For testers, the focus is on identifying and exploiting system vulnerabilities to

understand potential breach points. Designers use threat modeling to anticipate and design against potential security flaws, ensuring that systems are resilient from the ground up. Meanwhile, developers apply threat modeling to trace how data flows through systems and ensure that all data transactions are secure from interception or manipulation.