# CYB 250 Stepping Stone One Template

|  |  |  |  |
| --- | --- | --- | --- |
| Howard Threat Model | | | |
| Incident | Target Breach | Sony Breach | OPM Breach |
| Attackers | A Professional Hackers | A Professional Hackers | Maybe a hacker in China |
| Tools | Trojan | Data leaks, malware, and data destruction | User credential taken tool |
| Vulnerability | Network was fragile, and lacked effective security | Zero-day assaults | Failed to restrict access |
| Action | Probe, read, scan, steal, and Bypass information | Scan, probe, steal, and bypass information | Authentication to get into the network, scan, steal, bypass, read, and probe information |
| Target | The information in the business, the network for the business, and the user accounts | The IP address, sensitive documents, employee information, and email addresses | Mainly information on the current employees |
| Unauthorized Result | Increased access for the users, information disclosure, and resources stolen | Increased access for users, information disclosure, and resources stolen | Increased access for users and resources stolen |
| Objective | Money | Money and harm to the business | Not yet determined |

For the incident analysis for Target that I have decided on for the CIA triad is confidentiality. This is where only authorized users can view the information. The hackers that attacked Target went for the information on the business, their network, and the user accounts. Since the hackers went for the information part of Target and attacked the POS system as well as other systems like that it was easy to see which of the triad matched this breach. This means that they got all kinds of information on customers including their credit card numbers. They accessed more then a billion in credit card numbers.

By using an adversarial mindset to observe the incident through the attackers’ eyes, it allows the response team to see the goal of the attackers. You can adopt a perspective that allows you to adopt the attacker’s mindset. Even though at times the attacker is more determined than the analyst, this could allow them to anticipate where they could hit. This type of mindset has been used in several ways over the years and can be used in several more ways.

If I were an analyst at this organization, I would look into some of the threat models and see if it is a threat or not. One of the big problems that Target had with this was that the analysts ignored the warning signs for this. If they hadn’t ignored the signs, they could have stopped it from happening. The best way for me to help with this is treat all signs as a potential breach.

To convince my supervisor that the threat modeling is worth the time and resources to complete it I would give examples of how the modeling has helped organizations. I would show different models of different threats that have worked against hackers. I would also show different types of threats that have been successful and the model that could have prevented it. One of these models that I would show my supervisor would be a stride model (securitymadesimple.com). This stands for spoofing, tampering, repudiation, information disclosure, denial of service (DoS), and elevation of privilege. The aim for the model is to help applications meet the security directives of the CIA Triad as well as authentication, authorization, and non-repudiation. I would give more examples of these models to prove my point that using them would be best for the company.

When doing threat modeling some of the roles in IT change somewhat. Like the role of testers, they need to test the model to see if it would work. If not, they would have to test other models to see what one would work. As you see the roles would change but not by much.

**References**

Brathwaite, S./Dec. 11/[Top 7 Popular Cyber Threat Models for identifying threat actors, vectors and cyber threat surface. — SecurityMadeSimple](https://www.securitymadesimple.org/cybersecurity-blog/top-7-popular-cyber-threat-models)

Shu, X./Jan. 18, 2017/[1701.04940.pdf (arxiv.org)](https://arxiv.org/pdf/1701.04940.pdf)