CYSE Analytical Paper

Ava Love Dimaiwat

In this analysis paper, I took a deep dive into the topics of Cyber Threats, Enterprise Management Risk, and NIST Cybersecurity Frameworks. Throughout the paper, I talk about how they are all connected and view the topics through the “Short Arm of Predictive Knowledge” lens to reflect on the limitations we have in depending on predictions in cybersecurity.

Common Cyber Threats (Mod 02D)

Definition

Common Cyber Threats are common risks, threats, attacks, and weaknesses that target things like networks and information systems. What first came to mind when thinking about “Cyber Threats” was actions with malicious intent, like hacking and malware usage. After the end of this module, I learned that cyber threats can also be unintentional, like human error, which is actually a very common cyber vulnerability.

Example

According to the 200T Mod 02D class slides, the six most common types of threats are: Advanced Persistent Threats (APTs), Distributed Denial of Service (DDoS), Insider Attacks, Malware, Password Attacks, and Phishing Attacks.

Many devices are vulnerable to DDoS attacks. According to a report from Tripwire in 2016, it was discovered that 500,000+ IoT devices (devices that are connected to the internet) were at risk to the Mirai botnet. Examples of IoT devices include things you use every day, such as doorbell cameras, smart thermostats, sensors, control systems, smartwatches, and more. The Mirai botnet's designed to execute DDoS attacks by taking over these vulnerable and unprotected devices (Tripwire, 2016). If these are taken over, it can lead to many different consequences, like privacy and security risks, since they get control of appliances in your home, lead to widespread internet disruption, and more.

Mitigation Techniques

Some mitigation techniques that can defend against these cyber threats are using strong passwords and multi-factor authentication (MFA), doing regular software updates, using Antivirus tools, and, importantly, user awareness training.

The most important mitigation strategies for cyber threats are making people aware of attacks, using strong passwords and MFA, and keeping software updated. I think user awareness training is most important since many cyber threats come from human error. Training people to spot phishing attacks and suspicious links or emails can help prevent this. Also, strong passwords along with the use of MFA can make it much harder for attackers to get into accounts. Lastly, regular software updates are important so they can be updated to patch the latest vulnerabilities found and ways attackers could getting

access to sensitive data. All these and the other strategies I mentioned make many layers to defend against common attacks.

Connection to Other Topics

The topic of cyber threats and how to mitigate them directly connects to the next topic, *Managing Enterprise Risk (Mod 02E).* Because many different types of threats are always changing and developing with technology, it makes it hard for us to predict them and stop/ prevent them accordingly. This is why it's important to understand all risks and adapt to them over time so we can mitigate them.

Managing Enterprise Risk (Mod 02E)

Definition

According to slide 8 of *200T Mod 02E - Managing Enterprise Risk,* "Risk management is the process of identifying, assessing, and controlling threats to an organization's capital and earnings." This could be anything from financial uncertainties, Geopolitical Concerns, Technological change & threats, Natural Disasters, Management Mistakes, and more (2025, Mod 02E slide). There's a four-step process to risk management, which is first to identify & Prioritize Key Assets, then identify threats, weaknesses, and their likelihood, then mitigate, and then determine RACI (explained in examples).

Examples

In class, we learned about the RACI chart, which is a tool that's used to determine who's responsible in a situation (R), who's accountable (A), who's consulted (C), and

who's informed about it (I). This helped with organized mitigation and also helps to see who's held responsible in situations. Doing a RACI exercise in class helped me understand more about what each cybersecurity problem and situation leads to, and how every area almost has its own "checks and balances".

Along with RACI Charts, we also learned about the incident response lifecycle. This is the process of preparation, detection & analysis, containment & recovery, and then post-incident activity. I understood this as seeing risk management as a continuous cycle, instead of something that you do just when the risk comes along.

Connection to Other Topics

Managing risk enterprises helps give organizations an organized and structured way to go about identifying, dealing with, and prioritizing risks. But frameworks like the NIST Cybersecurity Framework (NIST CSF) are important to make sure there's a commonality across all areas. These frameworks give a common language and model that helps connect risk management strategies to their cybersecurity work. NIST CSF makes it easier for different teams to communicate and make decisions.

Even though managing enterprise risk helps to identify and prioritize risk, there's still a big reliance on predictions, like the chances of certain threats and how big their impact could be. Attackers and technology are still ever-changing, which limits how far enterprise risk management can help us.

NIST Cybersecurity Framework (Mod 02F)

Definition

According to slide 13 of 200T Mod 02F - The NIST Cybersecurity Framework, the NIST Cybersecurity Framework is a “set of standards, guidelines, and best practices for managing cybersecurity-related risk.” This helps organizations better understand and better their cybersecurity. The 6 main functions of the NIST Framework are govern, recover, identify, protect, detect, and respond. These all help with how to handle a cyber risk. Along with this, there are also 4 tiers to the maturity of the framework, ranging from reactive practices, limited awareness and understanding, to proactive practices, continuous monitoring and risk adjustments (Mod 02F Slides).

Example

In the framework, there’s identity, to get a better understanding of the risk and what could go wrong. Protect is the process of using safeguards like passwords or network defenses. Detect is focused on spotting unusual activity or alerts. Respond involved steps to contain or manage an incident, and Recover meant restoring systems and learning from the event. We also discussed Govern, which ties all these functions together by making sure policies and responsibilities are clear. These examples showed how the CSF works as a full cycle rather than just one-time tasks.

Mitigation Techniques

CSF makes cybersecurity strong because it gives a good structure for how it can continuously improve as time goes on, and it also forces continuous improvement since

organizations will have to regularly see where they stand and what weaknesses they have.

Connection to Other Topics

All of the topics I talked about, cyber threats, enterprise risk management, and the NIST cybersecurity framework, all fit together. Cyber threats show the many different threats we're vulnerable to in a time when we use technology for everything, and also show how technology is always changing and along with its vulnerabilities. Risk management shows how these risks and vulnerabilities are organized and prioritized. And the NIST CF shows the repeated cycle of how we respond to these uncertainties, with a standard of guidance that any organization can use.

The Short Arm of Predictive Knowledge

Limits of Prediction in Cybersecurity

Cybersecurity prediction has many limitations. The first notable one is that technology is rapidly changing and advancing, meaning that the threats will always be evolving along with the attackers. Systems also get more complex and advanced, making it even harder to predict and determine vulnerabilities and even to prevent them. Along with this, there's still human error that I mentioned in cyber threats. Humans aren't perfect and will always make mistakes, fall for scams, or phishing attacks. These two factors make it difficult to just rely on prediction alone in cybersecurity.

How this lens deepened my understanding of all 3 topics

With the three topics I had, they all had different ways they manage uncertainty. Cyber threats showed how still-developing technology and unpredictable attackers lead to many vulnerabilities. While enterprise risk management showed me that dealing with risks is never completely straightforward, it is calculated and based on many different factors. And then the NIST CSF shows how there's never a "perfect" outcome from the framework, but instead an ongoing cycle that enforces continuous monitoring, response, and improvement. All together, the lens helped show how cybersecurity is always going to be changing as we keep advancing, and it's important to work with this because we can never predict the future.

How my thinking changed over the semester

At the beginning of the semester, I knew close to nothing about cybersecurity. I knew that it was about protecting vital and personal technology. I thought that it was pretty straightforward: prevent attacks and attackers from doing damage. I did subconsciously think that threats and attacks would be predictable for the most part. Over the semester and while writing this paper in this lens, I learned about the true limits we have to effectively predict these attacks. After this paper, I think of cybersecurity as an always-changing system that will *always* have to be improved.

Disclosure

I used AI tools, Chat GPT and Gemini, to help pick the best topics for this paper, to rephrase concepts I didn't understand or technical jargon, to summarize the article from Tripwire, and to check if my ideas and claims were correctly following the paper's objectives. I mainly used AI to write the outline that I followed when writing this paper and to rewrite some sentences that seemed too wordy and difficult to follow. Along with this, I also used Grammarly to rewor.d throughout my paper. So AI helped me most with the structure of my essay, clarity, and simplifying the ideas I wrote. What I wrote on my own was almost the entire paper. I pulled things like definitions and examples from the class slides and websites within the slides.

Citations

Class Slides

Tripwire. (2016, October 10). Researchers discover 500,000+ IoT devices vulnerable to Mirai botnet. Tripwire. https://www.tripwire.com/state-of-security/researchers-discover-500000-iot-devices-vulnerable-to-mirai-botnet