**Week6 Reflection on Cybersecurity**

Hang Yang

IS 5403: Cybersecurity

Prof. Jaime Martinez

April 20, 2024

**Week6 Reflection on Cybersecurity**

In the week6’s podcast videos, Dr. Mclver and Prof. Samuel Nop had a very sound and deep discussion around cyber threat intelligence and contested environment. Cyber threat intelligence contains lots of archive/up-to-date information on threats and threat actors. It benefits many aspects of the security defense team, like proactive security defense, risk management support, shifting from reactive defense to predictive defense, decision-making advantage, etc. The goal of threat intelligence is to help the security professionals to avoid or mitigate malicious events. There are also lots of open source or subscription required intelligence platforms externally. Both the speakers emphasized that good use of threat intelligence could make a huge difference to the success of the whole organization’s security defense goal. Usually the threat intelligence procedures are collect, process, analyze and share. Each procedure contains its specific activities to make the threat intelligence flow works seamlessly. Prof. Samuel Nop highlighted that threat intelligence driven threat detection automation in the above procedures. By gathering, aggregating, and analyzing cyber threat data information, threat intelligence offers insights to help you allocate financial and non-financial resources effectively. Ultimately, it empowers your organization to prioritize and address specific potential risks before they actually escalate into major concerns in your system.

Which one is better, open-source or paid threat intelligence? I don’t think there is a uniformed answer. Open-source intelligence is free, but it does not mean unsecure. In fact, those open-source intelligence contains almost lots of threat relative information or even popular cases in the world. For example, in Microsoft, or NIST official website, you can find some helpful information there to help you address security issues about security standards and regulations. While from Recorded Future, FireEyes, or IBM X-Force Exchange, you may get some categorized or domain specific information for your business. Prof. Samuel Nop suggested a mixture of open-source and paid threat intelligence to be first choice if budget allowed. That means the final decision is up to your budget.

Especially in a contested cyberspace, you could hardly isolate yourself from cyber-attacks. That does not mean that the network itself is hostile, but the people, malicious attackers. The cyber attackers could have unlimited time to sit there to try sneaking into your account or system for money or political benefits. What we should do is to plan and well prepared. Especially as a cybersecurity professional, it’s highly recommended by Dr. Mclver to have awareness and preparedness of the severity and emergency of the cyber threats. The first thing cyber security professionals could do is to identify the assets you need to secure. Secondly, prioritize those assets to focus on the highest priority ones. This can save money and energy as we could not secure everything in the network. Thirdly, we need to apply defensive strategies to those identified assets, including risk management, patching program, user training, and more. Additionally, understanding the business is a great plus in cyber security defense.

In conclusion, cyber professionals can feel confident in defending against internal and external threats by continuously sharpening their security skillsets, fully leveraging threat intelligence sources, and diligently planning ahead and preparing for potential attacks.

**References**

Life is a Special Operation.(2019, Nov 15). What is a P.A.C.E. Plan? PACE – Primary – Alternate – Contingency – Emergency[Video]. Youtube. Retrieved from

https://www.youtube.com/watch?v=52W-aoichfw