Information Security

- Simon Chen

In “Human error: models and management” (Reason, 2000), details explained the need to apply a System Approach, based on the assumption of the inevitability of human error and the need to adapt to the conditions within which humans work rather than embarking on futile attempts to change the human condition (Castillo, 2013). It brings up the topic of the Information Security Management System (ISMS), which is not possible to measure security but conformance to a prescribed standard, so ISO-27001 is an internationally recognized standard that is widely applied around the world and is associated Code of Practice for information security management. It provides a taxonomy of 138 security controls plays an introductory clause introducing risk assessment and treatment (Castillo, 2013). Then referring to Teachers College’s Secure Computing and Information Management provides a more concrete and operable plan in school scope with purposes and policies. It defines the principles and terms of the college’s ISMP and the responsibilities of the members of the College community in carrying out the information security program (Teachers College Columbia University, 2014b). With 3 main focuses: Confidentiality, Integrity, and Availability, the TC keeps doing fine in cyber security through the efforts of the Teachers College Information Security Advisory Committee, IT Custodians, and CISO/CIO. However, the system still was attacked on July 30, 2020, because of a Teachers College vendor that may have compromised certain aspects of students’ demographic and philanthropic information. I think there is no unbreakable system around the

world, so we have to continuously enhance the security systems to keep our information relatively safe.

We saw crazy online blackmail events every day from thousands to billions of dollars. The most recent well-known one is from the NVDIA, focusing on graphics processing units production(largest GPU maker), mobile computing, and the automotive market. It should be a well-defenced company with a mature cyber security system. However, in Feb 2022, hackers (Lapsus$) have stolen data from NVIDIA. They hardened their network shortly after discovering the incident and notified law enforcement. While the crazy part is that Lapsus$ said if NVIDIA failed to agree to their demand(remove the mining hash rate limiters on RTX 3000-series GPU) by March 4, they would leak the latter's trade secrets. The hack happened in mid-February, and Lasus$ stole one terabyte of data, including a substantial amount of sensitive info on GPU designs, source code for an NVIDIA AI rendering system known as DLSS usernames, and passwords of more than 71,000 NVIDIA employees. Then the Lapsus$ also attacked Samsung and Ubisoft. No matter how mature you think your defense is, it still has vulnerabilities.

To maximize the capabilities of the security system, everyone who will use the system must contribute together to stop hackers. From my own experiences, every technology company will train employees about the importance of security and basic principles/ rules to regulate information privacy for the sake of the company's stakes. Like secured internet, encrypted communication channels, and formalized procedures to access databases or do some modifications.

From these readings, I know the international cybersecurity standards and ISMP which every company has their implementations. Also in the instance, I talked about above, there is never enough to rely on a security system. There are always some malicious people who want

valuable private information in illegal ways. As individual internet surfers, we need to protect our privacy by enhancing cybersecurity awareness.

References

Reason, J. (2000). Human error: Models and management. *BMJ*, *320*(7237), 768–770. https://doi.org/10.1136/bmj.320.7237.768

Castillo, F. D. (2013). *Information Security Explained*. UCL Data Management Planning for Secure Services (DMP-SS). https://web.archive.org/web/20140829142418/https://blogs.ucl.ac.uk/dmp-ss/2013/03/26/information-security-explained/

Teachers College Columbia University. (2014b). *Information Security Charter*. Teachers College - Columbia University. https://www.tc.columbia.edu/policylibrary/computing-and-information-services/information-security-charter/