Digital Defense: The Role of Cybersecurity in the Computer Age

Allison Falcon, Olivia Fratangelo, Christopher Gonzalez, Ivan Urena

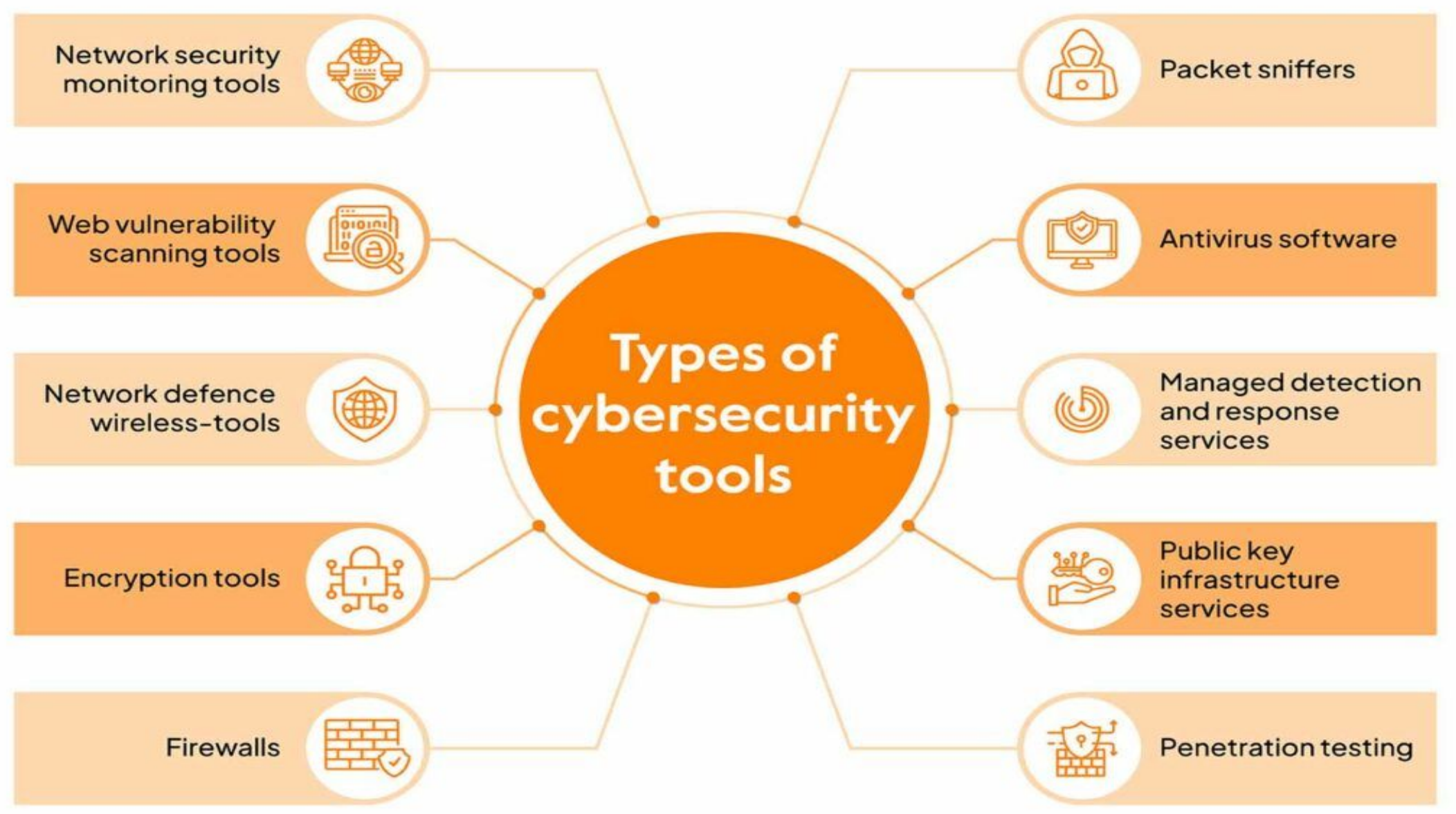
CSCI 400 Fall 2024

What is Cybersecurity?

Cisco Systems Inc. defines cybersecurity as the practice of safeguarding systems, networks, and programs from digital attacks, commonly referred to as cyberattacks. Whether applied in a large company like Amazon or in an individual's efforts to secure their personal online presence, cybersecurity can be understood through four key categories: technical skills/tools, the human factors at play, frameworks/legislation, and the protection of democratic institutions.

Technical Skills/Tools for Cyber Threats

Technical skills/tools are required to help industries and individuals protect themselves by detecting cyber threats, protecting systems, and applying cryptographic protocols to secure their communications. An example of one of these tools is Suricata, an open-source engine that can execute an intrusion detection system (IDS) and an intrusion prevention system (IPS), an alternative to Snort. This software was developed by the Open Information Security Foundation and aims to prevent, detect, and alert threats on Windows, Mac, Unix, and Linux. Moreover, as an IDS and IPS, Suricata greatly assists in taking action and blocking traffic. Suricata does good deep packet inspection, which inspects the content of network traffic beyond the header information. Furthermore, Suricata is multi-threaded, which allows us to process more data without revoking the rules implemented. Overall, his tool allows us to strengthen our detection rules and processes.


Types of cybersecurity tools
Network security monitoring tools
Web vulnerability scanning tools
Network defence wireless-tools
Encryption tools
Firewalls
Packet sniffers
Antivirus software
Managed detection and response services
Public key infrastructure services
Penetration testing

Human Factors in Cybersecurity

Due to the sheer complexity in the number of security measures, algorithms, precautionary actions embedded into cybersecurity, It's normal to think humans can do only so much. On November 24 2014, It was found that a malicious group of hackers named "Guardians of Peace" penetrated Sony Pictures Entertainment (SPE) architecture through tools of malware such as backdoors, listening implants and tools to erase information within a hard drive. In terms of human factors, this infiltration demonstrated the lack of cybersecurity awareness and improper control of devices that allowed the bad actors to run rampant within the company. Zero-day vulnerabilities can remain hidden for a long time and it is only with precise action that it is dealt with.

Sony's response to the attacks was to cancel video productions, used internal teams, contacted FBI and FireEye (cybersecurity firm) to ensure a speedy recovery. At the end, this costed millions of dollars (15-100, range can be higher) which meant a devastating financial loss as well as employee lawsuits for not protecting data securely enough. Had Sony invested earlier in better cybersecurity maintenance, better awareness of malware, planned incident response protocols, software patches, employee data protection and fewer human vulnerabilities then this outcome would have been different in a way that saves monetary value and resources so that Sony can focus more on it's products that it serves than things it doesn't.

Frameworks/Legislation for Cybersecurity

A cybersecurity framework is the collection of guidelines, standards, and best practices designed to help organizations manage/reduce cybersecurity risks. One example is the NIST Cybersecurity Framework 2.0, published on February 26, 2024. This updated version builds on the original 2014 framework, addressing modern cybersecurity challenges with enhanced guidance. NIST CSF 2.0 consists of three key components:

- CSF Core
- CSF Organizational Profiles
- CSF Tiers

The most critical component of the NIST CSF 2.0 is the CSF Core, which organizes its guidance into six functions:

Govern - Establishes and monitors an organization's cybersecurity risk management strategies.

Identify - Identifies opportunities to improve an organization's CS policies, procedures, and practices.

Protect - Implements safeguards to manage and mitigate identified risks. Outcomes covered may vary.

Detect - Enables organizations to identify CS incidents and anomalies in real time.

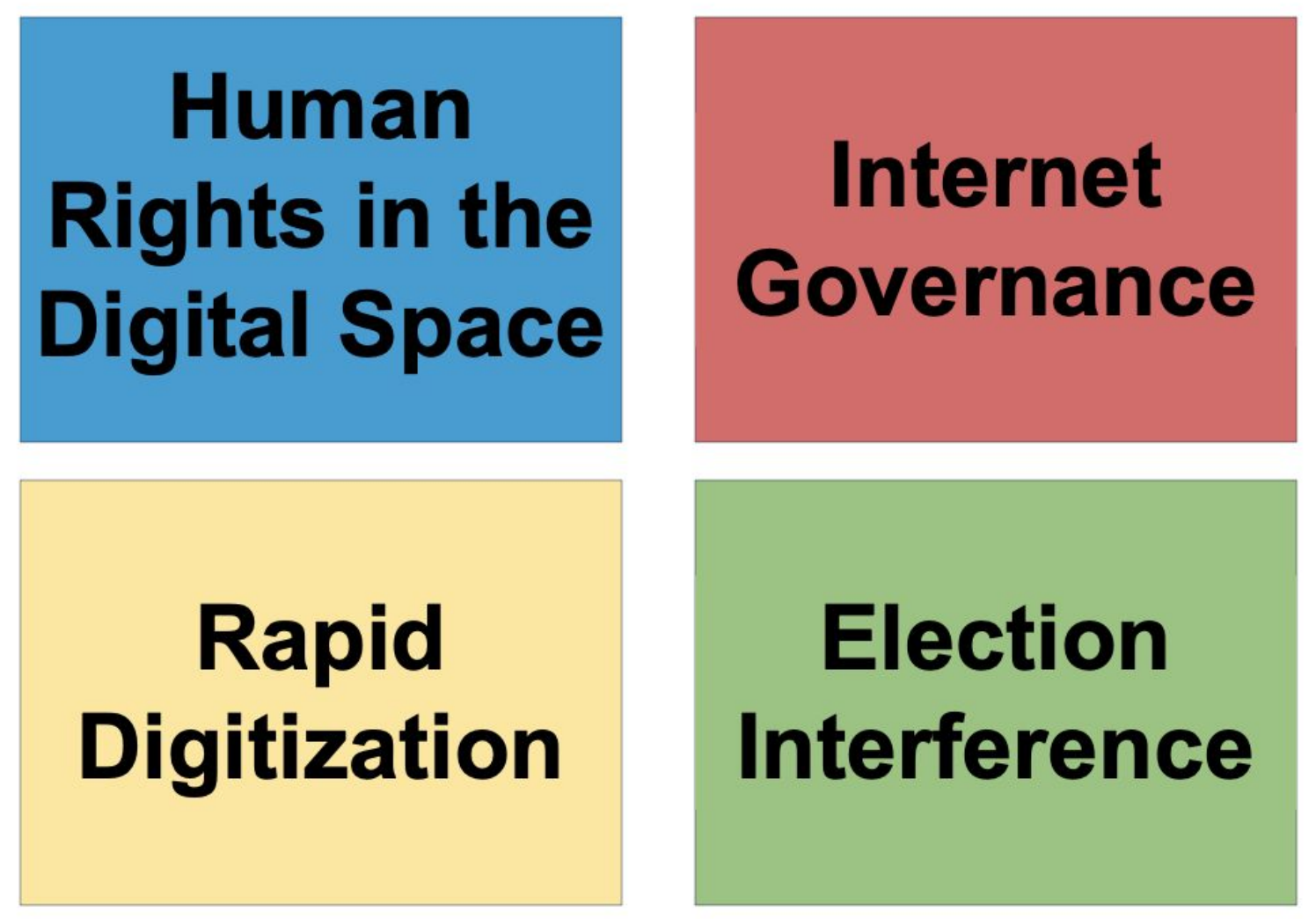
Respond - Containment on the effects of CS incidents.

Recover - The timey restoration of normal operations.

Protection of Democratic Institutions Through Cybersecurity

- Countries have not been able to compromise or agree upon internet governance. There is conflict regarding the multi-stakeholder approach in which private, social, and governmental sectors are included in the governance model versus a state-led model
- Rapid digitization of important democratic processes can lead to increased security risks (ex: 2020 U.S. Census was deemed a "high risk undertaking")
- Technology has improved human rights by helping bring violations to light and giving people a platform to voice opinions and concerns. However, digital threats to human rights can quickly become physical with surveillance and high availability of personal information online
- It is less common that the actual election infrastructure is affected by a cybersecurity threat, but rather campaigns and factors influencing elections are tainted by misinformation and malicious actors

Four Key Cybersecurity Concerns for Democracies



Why is Cybersecurity Imperative?

Since the public debut of the Internet in 1993, our reliance on technology has grown significantly, transforming daily life. While this has brought many benefits, it has also introduced new risks to computing. As a result, users must understand these risks and adopt safe practices. Studies have consistently shown that the weakest link in cybersecurity is the unsuspecting user, while cybercriminals remain the primary threat to online safety. Fortunately, a variety of technical tools are available to help both industries and individuals protect themselves from such threats. Furthermore, cybersecurity plays a vital role in preserving political stability and the integrity of democratic institutions. By strengthening the weakest link through frameworks and legislation, we can better protect ourselves from the dangers that exist online.

References

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Maurer, Tim, and Arthur Nelson. (2020). "How To Protect Democracy From Future Cyber Threats." *Carnegie Endowment*. carnegieendowment.org/europe/strategic-europe/2020/02/how-to-protect-democracy-from-future-cyber-threats?lang=en.

Piccone, Ted. (2017). "Democracy and Cybersecurity." *Brookings*. www.brookings.edu/articles/democracy-and-cybersecurity/

Young, Kelli. (2021, November 1). "Cyber case study: Sony Pictures Entertainment hack." *CoverLink Insurance*. https://coverlink.com/case-study/sony-pictures-entertainment-hack/

Viglione, M. (n.d.). *Suricata: What is it and how can we use it*. Suricata: What is it and how can we use it? https://www.infosecinstitute.com/resources/network-security-101/suricata-what-is-it-and-how-can-we-use-it/

Anwita, A. (2024, December 9). *Top 16 cyber security tools you must know in 2024*. Sprinto. https://sprinto.com/blog/best-cybersecurity-tools/

Acknowledgements

We would like to express our gratitude to Professor Jennifer Holst for the opportunity to research the importance of cybersecurity in modern computing. It has been a privilege to contribute our findings and raise awareness about the critical role of cybersecurity in the computer age. We hope this project inspires others to prioritize online safety and security.