Introduction to Cybersecurity

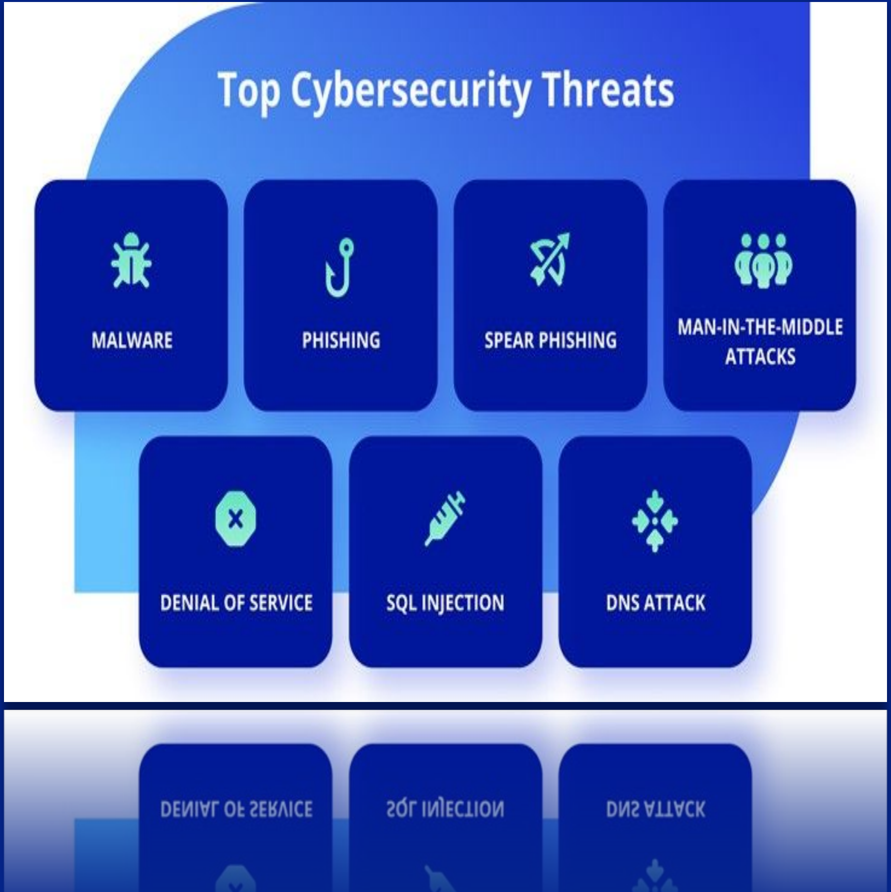
Myles Damoah, Jayce Clancey, Christopher Watkins, Isaiah Browne

BLUF

Understanding the importance of five cybersecurity topics, and the philosophical considerations of rapid datafication of our environment.

Common Threats

- In 2023 there were 6 billion cyberattacks (roughly **1 attack** every **39 seconds**)
- In 2024, 72% of businesses were targeted by ransomware attacks (**1 Billion dollars** paid to attackers)
- Since 2023 Phishing has become the most common cyber threat. Increasing by **58.2%**



Scada Systems

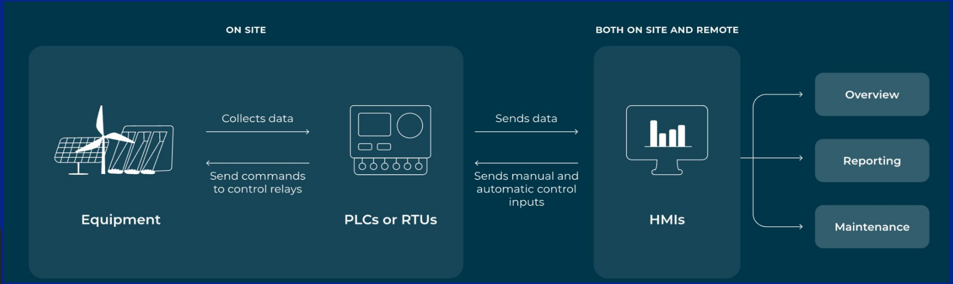
Supervisory Control and Data Acquisition (SCADA) refers to Industrial Control Systems used to control infrastructure processes, facility based, processes, or industrial processes.

1. **How does a SCADA System Work?**

- SCADA Systems consists of three different components. Combined these components ensure data is transmitted from the equipment that needs to be monitored and controlled

2. **Why is a SCADA system important**

- SCADA Systems help ensure production and control the production according to regulations within the industry. They are also used for troubleshooting purposes 5555s

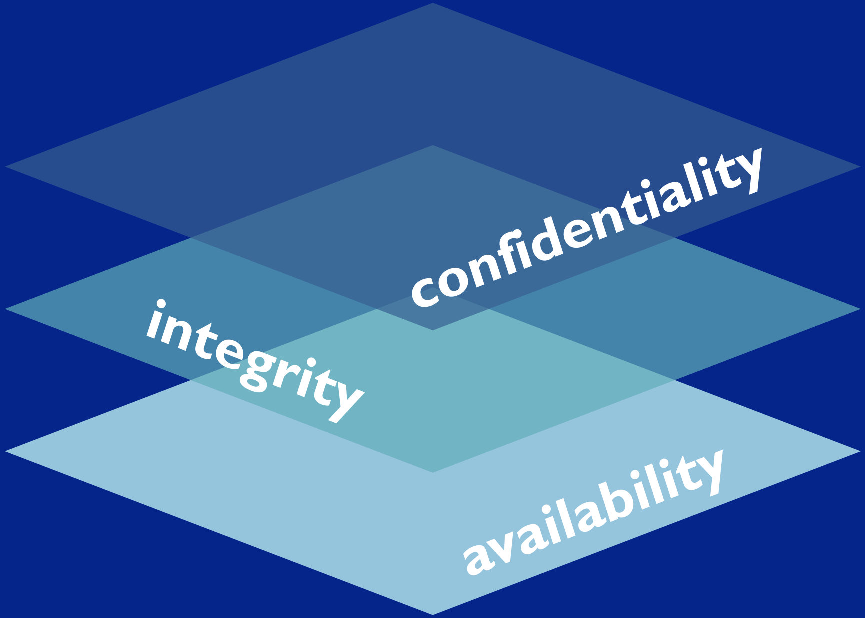


The CIA triad

The CIA triad stands as the foundation of information security and serves as a guideline for maintaining the security and integrity of data.

What each of the componentes represent:

- Confidentiality: Ensures that information is protected from unauthorized entities
- Integrity: Protects information from unauthorized modification
- Availability: Ensures that information and resources are accessible and usable when needed



Biological Systems & Cybersecurity

The integration of biosecurity and cybersecurity into cyber biosecurity is an effort to safeguard biological information and systems from cyberattacks. Safeguarding the authenticity of pharmaceuticals, bioengineering systems, and biological data is part of this.

Biological systems within the world:

- DNA, fingerprints, and retinal scans are examples of biometric security systems that use distinct biological characteristics to verify identity..(iPhones

Biosecurity Risks:

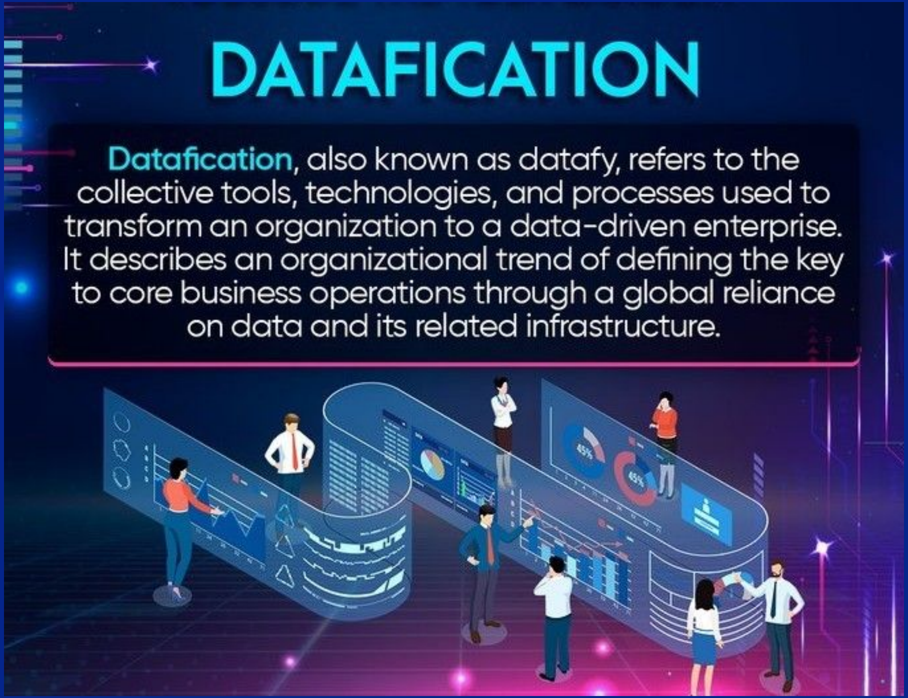
- Unlike passwords, stolen biometric information cannot be altered once it has been accessed. Attackers can tweak security measures or use databases holding biometric data for identity theft if they manage to get access to them.

Philosophical Question

Do we need to consider regulatory changes in the face of rapidly evolving datafication and ' intellification 'of our environment, or not?

Our Response: Yes!!!

- Ethical transparency
  - Companies must inform their users of what data is being collected
  - Data must not be used to target certain people/survey certain demographics as this is a serious breach of privacy
- Environmental impacts
  - E Waste: many servers become obsolete with demand of datafication
- Carbon FootPrint
  - Most data centers rely on fossil fuel energy (coal, oil, and natural gas)



DATAFICATION

Datafication, also known as datafy, refers to the collective tools, technologies, and processes used to transform an organization to a data-driven enterprise. It describes an organizational trend of defining the key to core business operations through a global reliance on data and its related infrastructure.

Thank
You

Works Cited

Mapsted. (2017, April 17). *What is Datafication*. Mapsted. https://mapsted.com/blog/what-is-datafication

Learn all about SCADA systems: What is SCADA? | SCADApedia.