Cybersecurity For Beginners

Part 3 Cybersecurity Basics

WOMEN CYBERSECURITY SOCIETY

Contributing Partner

IMMERSIVELABS

Thank you!

Agenda

- Presenter Introductions
- WCS2 Overview
- Attendee Introductions
- **Cybersecurity Basics**
- What you'll learn in the lab
- Practical Exercise
- IWCD
- Free Chapter Sign-Up & Benefits
- Survey
- Closing Remarks

Lisa Kearney
Founder, President & CEO

Introduce Yourself!

Please introduce yourself in the chat with the following information:

- Your name;
- location;
- Why you are here today; and
- Anything else you would like to share.

Cybersecurity Basics Part 3

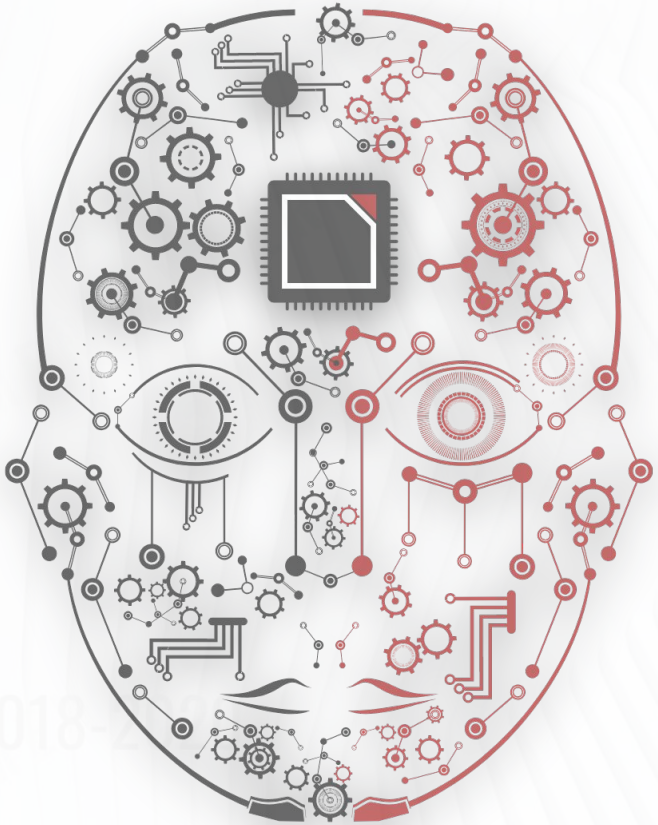
In This Lab

This lab introduces you to some **fundamentals of cybersecurity**, including the **CIA triad, digital assets, malware, and some common cyber-attacks**.

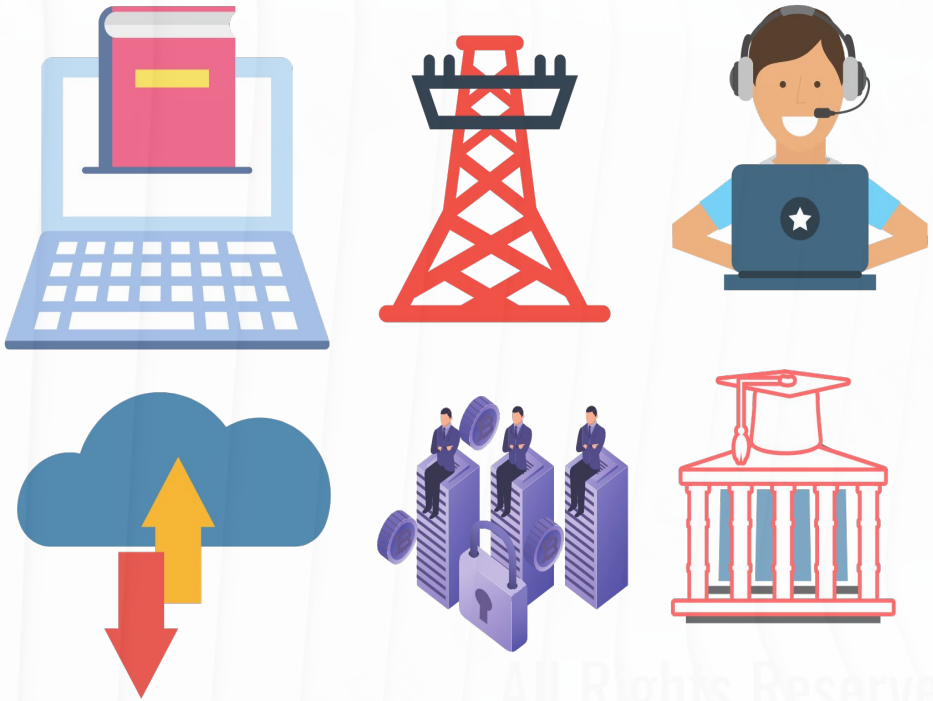
During the exercise portion, you'll ***use your knowledge of cybersecurity basics* to *match statements to corresponding words***.

Cybersecurity is Evolving

Cybersecurity is the act of protecting assets which include networks, systems, data and people from **destruction, unauthorised access and other forms of damage**. As **attacks evolve**, the *industry pivots to stay current with the latest vulnerabilities.*



Industry Players

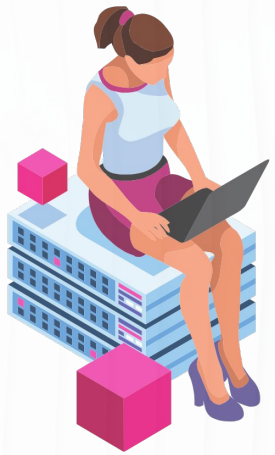


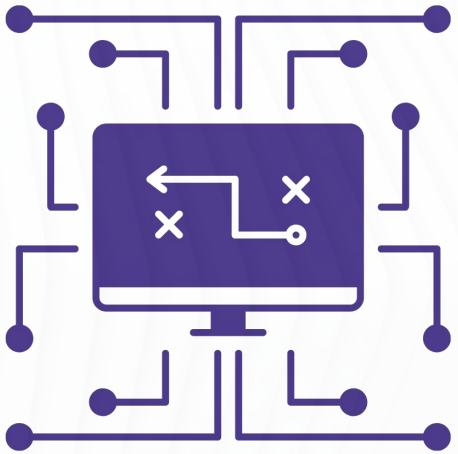
The cybersecurity industry is made of of four distinct groups.

- **Technology Providers**
- **Service Providers**
- **Education & Training Providers**
- **Workforce**

Dynamic Roles

There are **literally hundreds of different types of roles in cybersecurity**. Just like there are many specialities of medical, there are several **domains** of cybersecurity. There are many **misconceptions** which I explain in my '**Getting Started in Cybersecurity Workshop**'.





Workforce Jobs

Security Analyst

White Hat Hacker

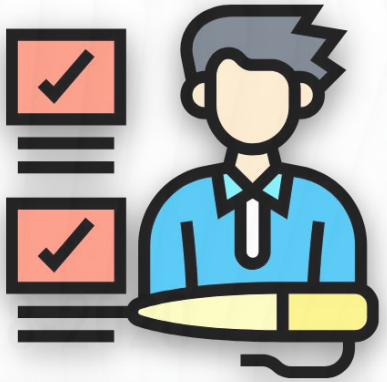
IT Security Auditor

SECOPS

Digital Forensics

CISO/Director

Secure Programmer



Compliance & Governance

CIA Triad

Standing for **confidentiality, integrity, and availability**, the **CIA** triad is used by the cybersecurity industry to ensure there is **limited impact to networks, systems, data and people**.

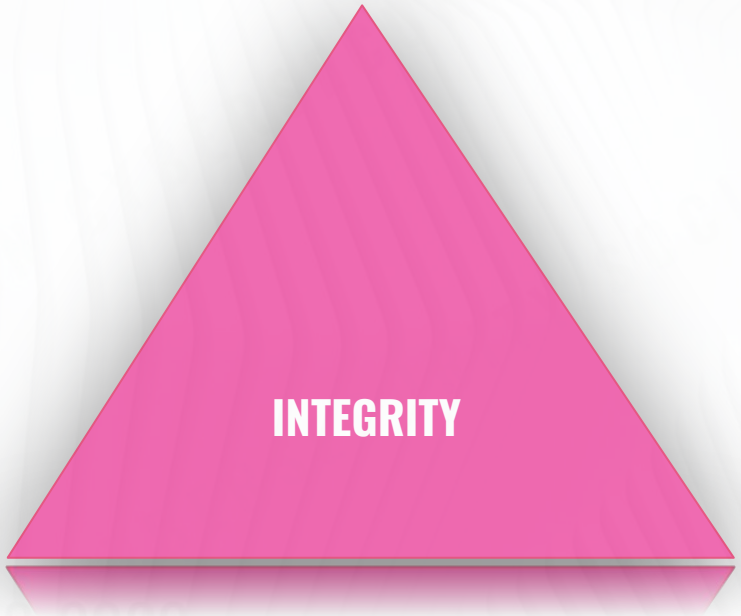
CONFIDENTIALITY

Confidentiality is like **privacy**.

Measures are taken to prevent sensitive information being accessed by those not intended to view it.

INTEGRITY

Integrity is about **maintaining the accuracy and trustworthiness of data**.



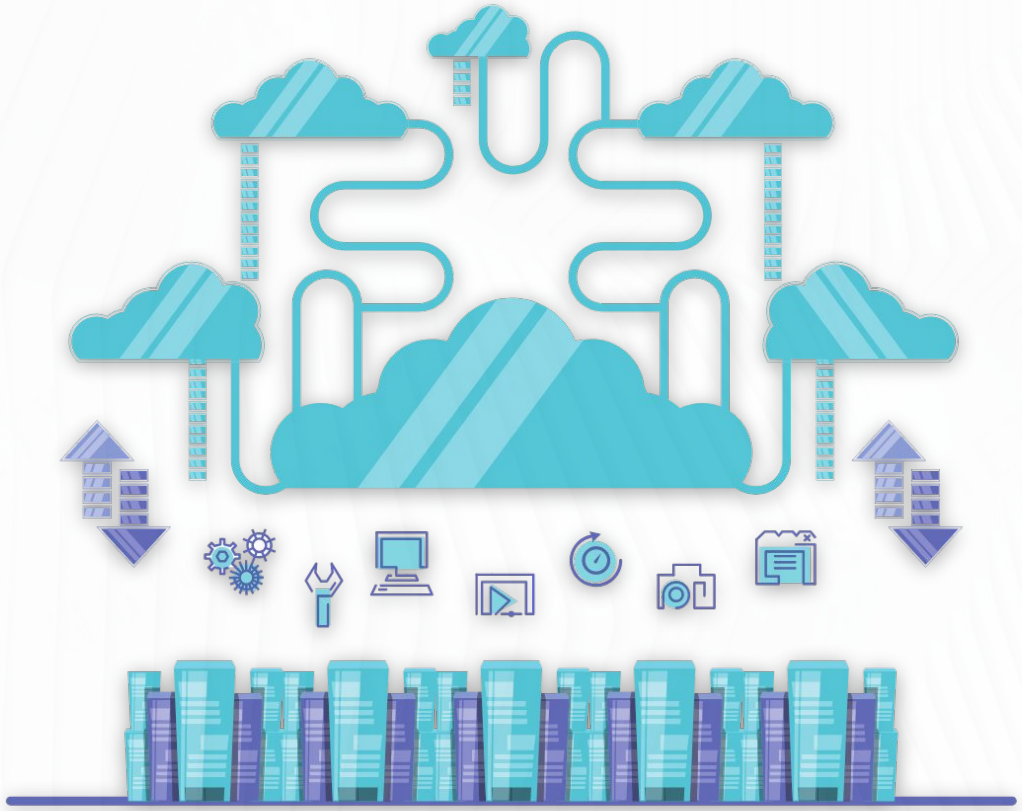
AVAILABILITY

Availability refers to your **ability to access your data whenever** and **however you want to access it**.

Cybersecurity Defined

Cybersecurity is the **act of protecting assets** which include **networks, systems, data and people** from cyber attacks and insider threats.

ASSETS

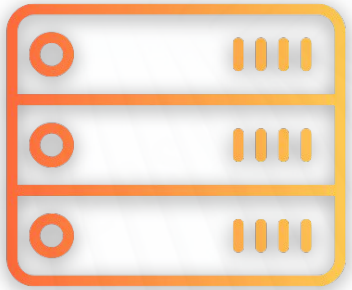


Networks

Networks are a series of **private** and **public connected devices** which provide **access to systems.**

Data centers contain **routers, switches, servers, firewalls, anti-malware, logging, monitoring and alerting systems.**

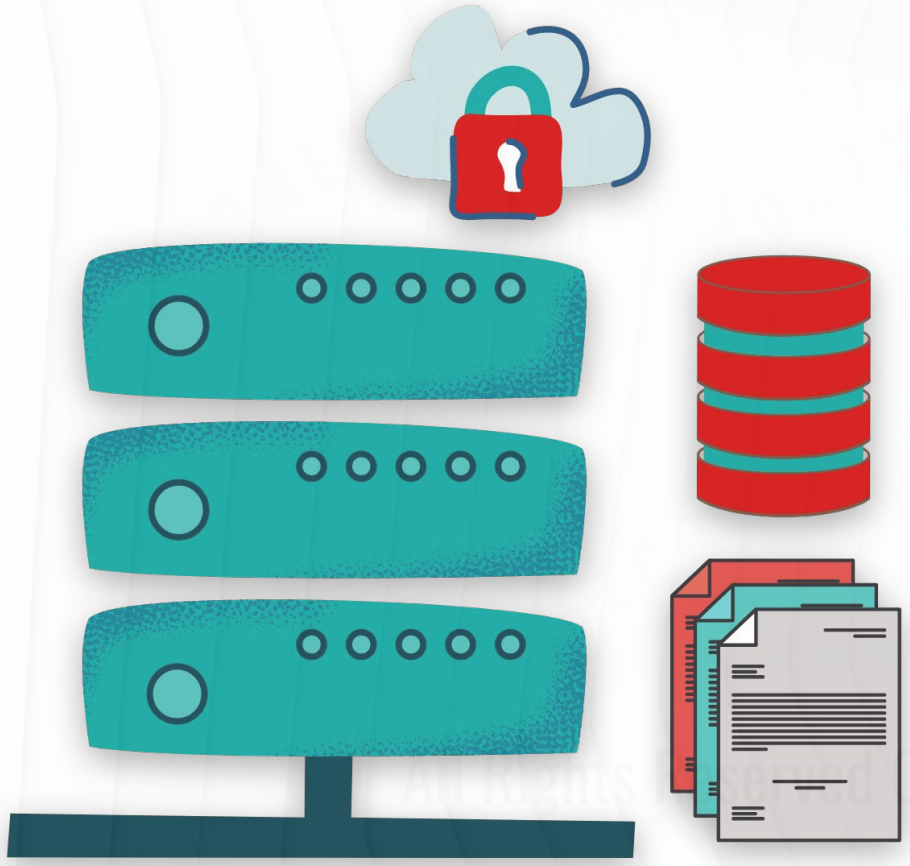
Systems



People

People work in high risk jobs across many industries which include **construction**, **mining**, **oil & gas** to name a few. These industries have globally connected devices and systems which depend on them working as expected. The same is true within **healthcare** where medical equipment **test, report and monitoring** people where **confidentiality**, **integrity and availability** is of utmost importance.

Data

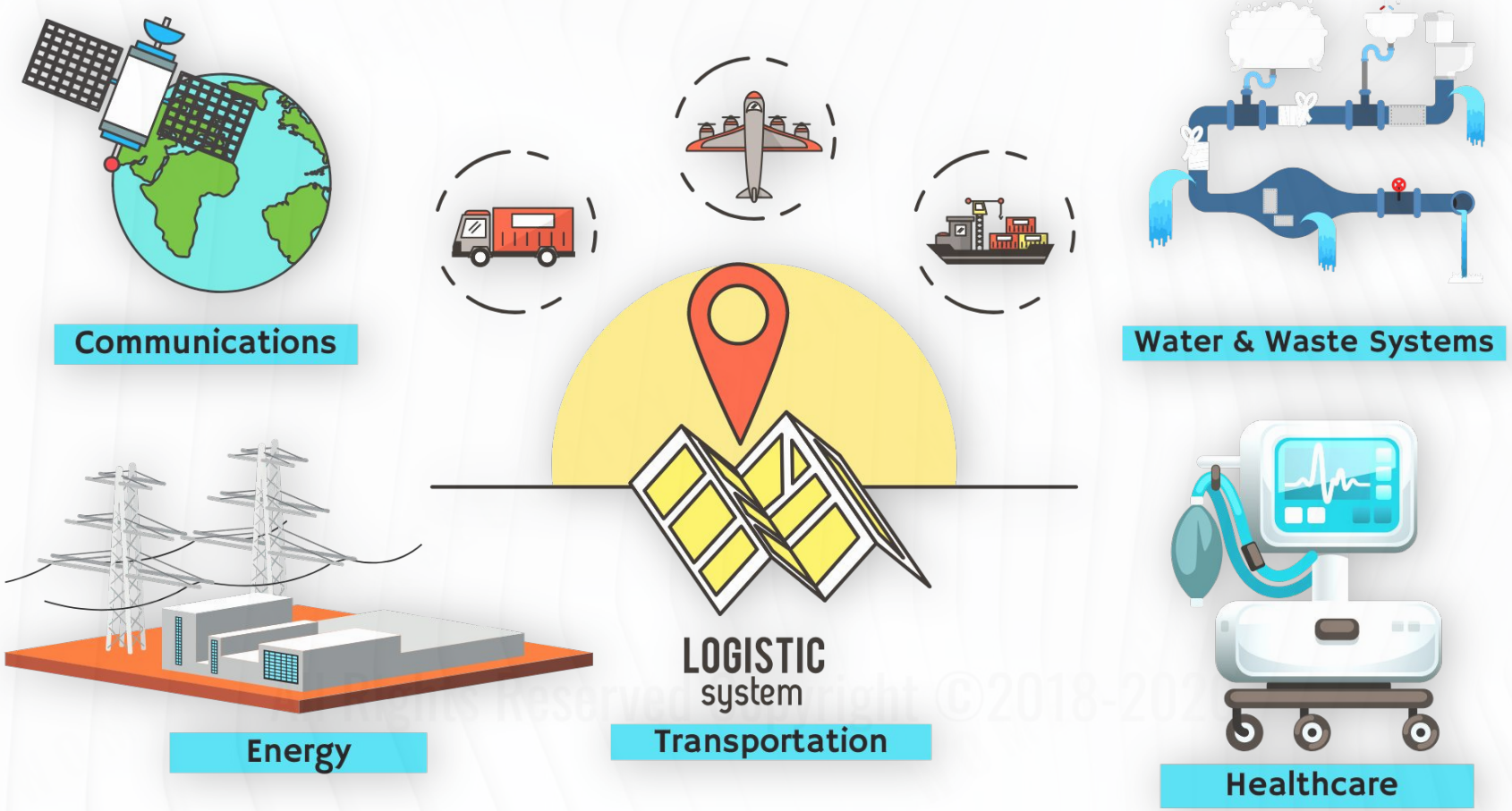


Data is a asset which is considered more valuable than gold on the stock market. It is shared and sold across white, grey and black markets globally and the motivation behind cyber attacks globally. For example a single **PCI** record can sell up for $10-20 USD on the dark web. **IP, PII, PHI** data records are equally valuable.

Personal & Social Impact

How does cybersecurity impact our society and us personally?

CRITICAL INFRASTRUCTURE



MALWARE

Malware, short for malicious software, is any software designed to cause damage to assets.

Malware in the media refers to viruses, ransomware, spyware, adware, and Trojans; however, there is more to malware than this.

Attackers will use malware to maintain access to a system in order to automatically transfer information or to leave a backdoor in which they can easily regain entry.

CYBER ATTACKS

Cybersecurity revolves around preventing cyberattacks and halting malware. While the media implies that most unethical hackers sit in basements, cyberattacks can actually begin anywhere, including state sponsorship, teen curiosity, and the creativity of unethical developers.

There is often some form of financial gain motivating the perpetrator.

#TipTheScale

#Ambassador

#Recruit

#Retrain

#Retain

Community

Join A Chapter & Slack

Join or lead a local chapter to receive discounts and special offers

- https://womencybersecuritysociety.org/join-or-lead-a-chapter

Connect with other women in our Slack Community

- https://join.slack.com/t/womencssociety/shared_invite/zt-e3uf3ksn-xIMky5~I3wQjacYIbvs8zm

Q&A

Closing Remarks

Thank you!