Cyber Security

***“The ability to protect or defend the use of cyber space from cyber-attacks” – NIST***

McCumber Cube / Cyber Security Cube

Desired goals – C.I.A

Data States – Transmission, Storage, Processing

Safeguards – Human Factors, Policy and Practices, Technology

Terms:

Asset – What we are trying to protect

Vulnerability – Weakness or gap in out protection efforts

Exploit – How attackers leverage a vulnerability

Threat – What you are trying to protect against

Risk – intersection between assets, threats and vulnerabilities. Risk = Probability \* Impact

Causes of vulnerabilities:

Design and development errors

Poor system configuration

Human error

Connectivity

Complexity

Passwords

User input

Management

Lack of staff training

Communication

Attack types:

Untargeted vs Targeted (Phishing vs Spear Phishing)

Cyber Threat Actors and motivations:

Nation state – Geopolitical

Cyber Criminal – Profit

Hacktivist – Ideological

Terrorist groups – Ideological Violence

Thrill seekers – Satisfaction

Insider Threat – Discontent

Cyber Threats:

Malware – Software that does malicious task on a device/network

Spyware – Malware that hides on a device providing real-time information

Phishing Attacks – attempts to lure individuals into providing sensitive data

DDOS – Aims to disrupt a computer network by flooding with superfluous requests.

Ransomware – Type of malware that denies access to computer system or data until ransom is paid

Zero-day – Flaw in software, hardware or firmware that is unknown to victim systems which there is no patch for.

Trojan – Backdoor to your system

Wiper attack – Form of malware with the intention to wipe your HDD

Intellectual Property (IP) threat – Stealing or using someone else’s IP without permission.

Theft of money – access to card or account numbers to steal money

Data Manipulation – unauthorised change to data

Data Destruction – Attempts to delete data

Man in the Middle (MITM) Attack – Interception of communication

Drive-by Downloads – automatic download and execution of payload

Rogue Software – Software pretending to be something else

Unpatched Software

National Disasters

Water Holing – Impersonating sites to gather sensitive data

Spear Phishing – Targeted phishing attempts

Deploying a botnet

Subverting the supply chain – attack on equipment or software being delivered to the organisation.

Cyber Threat Surface:

All available endpoints that a threat actor may attempt to exploit in internet connected devices within the cyber threat environment. The many processes that produce, deliver and rely on information systems connected to the internet.

Cyber Kill Chain:

Reconnaissance – Harvesting Information

Weaponization – Coupling exploit with the backdoor into deliverable payload

Delivery – Delivering to victim via email, web, usb, etc.

Exploitation – Exploiting a vulnerability to execute code on victim system

Installation – Installing malware on the asset

Command and Control – Command channel for future manipulation

Actions on objectives – Hands on keyboard access; intruder completes their original goals

Retreat – destroy all evidence of you having been on the system