Lesson 1.7

Introduction to Cyber Threats

Lesson Content

- Introduction / Definitions
- Cyber Threats
- Cyber Attack Techniques
- UN Principles
- Cyber threat impacts

Lesson Outcomes

- Explain what cyber threats are
- Define the key cyber-attack terminology
- Describe cyberattacks and why do they happen
- Describe in general the policies and principles that guide cyber security in the UN
- Describe the relationship between Cyber Attacks and UN units i.e., force protection
- List the predominant cybersecurity threats to UN Units

We think of operations as land, sea and air; and we recognised a fourth – space. Now there's a fifth – **<u>cyber</u>**

Cyber is the new frontier

Definitions

Cyber- Definition

- No universally accepted definition for Cyber
- Relating to information technology, Internet and virtual reality
- Cyberspace- interconnected communication, information technology, electronic systems, networks, data, stored or transmit

Definitions

- Cyber attacks- refers to a deliberate and malicious attempt to exploit computer systems, networks, communications, or digital devices with the intention of disrupting, stealing, or damaging data, information
- Misinformation and disinformation offensives- distortion and manipulation of the information by groups / actors that impact UN operations

Cyber Threat- Examples

- Stealing sensitive Information
- Identity theft
- Reconnaissance
- Shut down / Interruption / distributed denial of service
- Damage of digital systems- malware, ransomware
- Undermine social cohesion
- Posting harmful untrue info on social media

Actors behind the Attacks

Groups

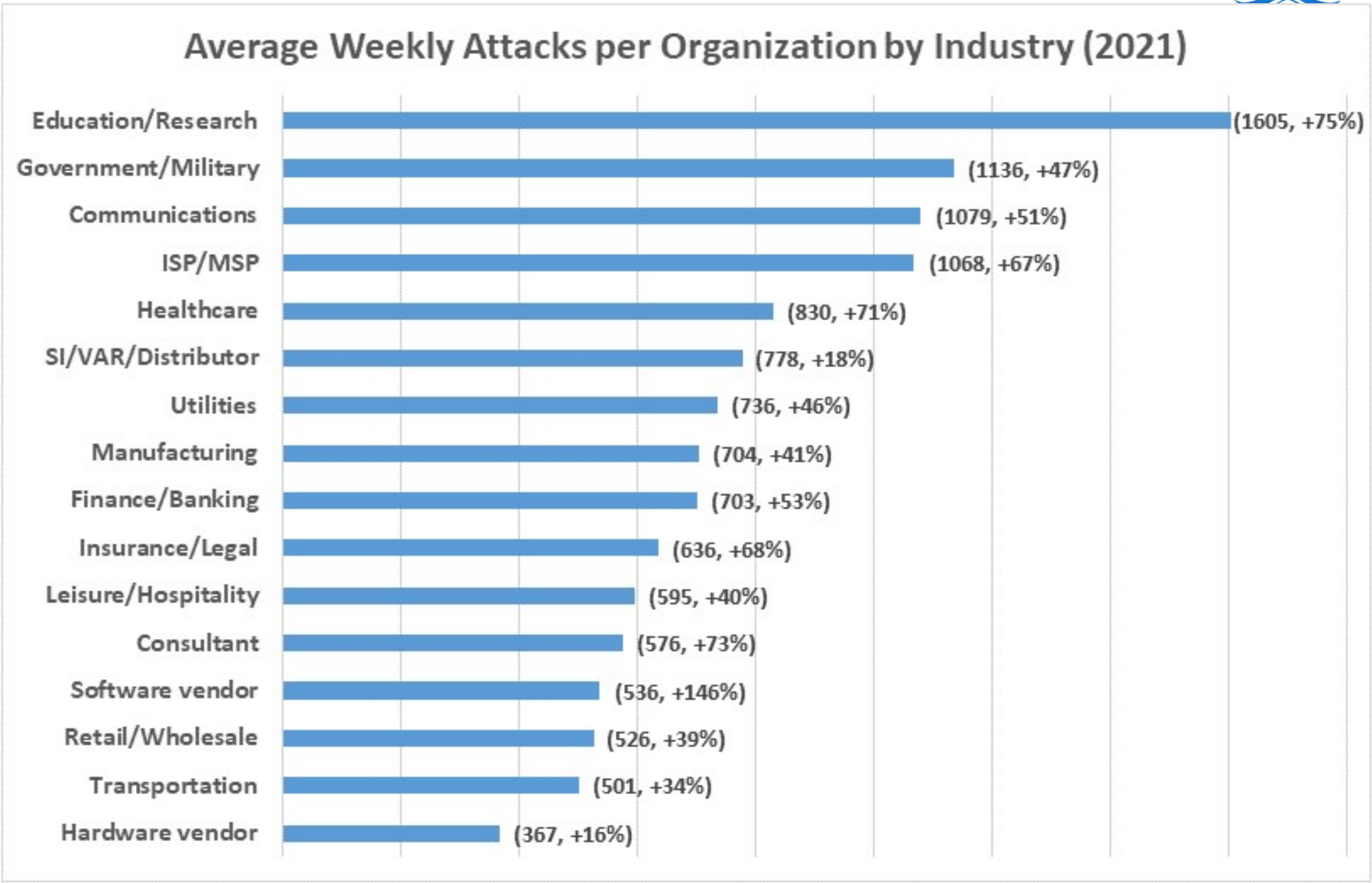
- Armed and unarmed
- Organised and unorganised

(criminal groups, terror groups, state actors, political parties)

Can also include

- Professional hackers, amateur hackers, hacktivists
- Insider actors: careless or disgruntled employees, partners, clients, contractors

Cyber Attacks



Cyber Attack- Toolbox

- Malware
- Ransomware
- Social engineering
- Supply chain corruption
- Local physical access

Cyber Attack Techniques

Cyber Attack Techniques

Malware:

Malicious software that is an overarching term for software designed to infiltrate or damage a computer / computer system

Cyber Attack Techniques

Malware Types	
Virus	• Malicious computer code • Replicates and spreads between computers • Corrupting or deleting files • Normally spread by human interactions • By inserting USB sticks or opening emails
Worm	• Related to a virus • Replicate itself without having to infect files • Spreads over networks without human intervention • It can inflict similar damage to a virus
Spyware	• Software • Collects information without permission or knowledge • Can be for malicious commercial purposes • Some online advertising resembles spyware

Cyber Attack Techniques Cont.

Malware Types	
Trojan Horse	• Malicious code • Masquerading as a legitimate application • Entices a user to launch it • Deceiving users into downloading and running
Ransomware	• Secures and encrypts a victim's data • Releasing, once a suitable passcode is entered • Passcode is available once ransom is paid • Typically using untraceable crypto-currency

USB Disruptors

- USB keylogger, small 20 mm in length, accessible as a USB flash drive
- Transparent to operators
- No software or drivers requiredall
- Keystroke data will be recorded
- Stealthy, does not pop-up as a system device

Social Engineering

Cyber Attack Techniques

Social engineering:

- Manipulation of individuals to carry out actions, or to divulge information

- Commonly used to deliver malicious software

Social Engineering Techniques

Social Engineering Techniques	
Phishing	• Attempts to acquire info • usernames, passwords and credit card details • Masquerades as trustworthy • spoofed emails; directing one to enter details at a fake website • Occurs via social media posts, short message service (SMS)
Spear Phishing	• Builds on phishing • Targeting against a specific individual, organisation or business • Emails appear to originate from individuals, organisations the target recognises • Often conducted for financial gain or espionage

Social Engineering Techniques Cont.

Social Engineering Techniques	
Whaling	• Malicious hacking in the category of phishing • Hunting for data to be used by the hacker • Targets senior executives and other high-profile targets
Baiting	• Attacker places removable in a target premises • USB memory sticks or DVDs • May be labelled in such a way as to provoke interest • Relies on employees to load it out of curiosity • Once running on a computer, malware is loaded • Usually run automatically

Social Engineering Techniques Cont.

Social Engineering Techniques	
Telephone	• Victim telephoned by individual • Posing as a figure of authority • Persuade victim to perform a task on computer • Masquerades as employee of the Internet service • Victim is persuaded to carry out alterations • Weakens computer defences • Attacker gets victim to navigate to a website • Malware is loaded • All on pretext of fixing a supposed problem

Social Engineering Techniques Cont.

Social Engineering Techniques	
Social Network	• Opportunities for social engineering • Messages pretending to be a friend stranded abroad needing funds • Uses spoof accounts which tell a tale of hardship • Victim goes to criminal website pages requesting personal information • Criminals exploit information • Uses embedded links to malware • Intelligence can be gathered and analysed from links • Perpetrators use software for analysis of targets • With intelligence they craft damaging misinformation

Cyber Attacks-Operational Impact

- Disruption to Communication networks impacting C2
- Disrupt the decision-making cycle- resulting in uninformed decisions
- Manifest mis/dis information; increasing anti-UN sentiment
- Intelligence gathered to be used against unit
- Equipment sabotage, malfunction; Exp. UAS/Drones
- Psychological- erode morale

Take Aways

- Cyber threats are prevalent and will continue to plague UN Missions and UN military and police units
- It is important to recognise cyber threats
- Cyber attacks can impact tactical operations

Learning Activity Lesson 1.7

- Turn to the person on the left or right; find a **WILLING** partner; ask to use their name. Using the internet to "Phish" for information on that person:
  - *Google*
  - *LinkedIn*
  - *Facebook*
  - *Twitter*

- What did you find out about your neighbour that is open source? Links to family members, hobbies, location, habits like food or travel?

- Question: Now, how exposed do you believe you are and what information are you giving away that might be harmful?