32548-48730 Cybersecurity

Week 1- Introduction to Cybersecurity

Dr. Priyadarsi Nanda
School of Electrical and Data Engineering
Priyadarsi.Nanda@uts.edu.au

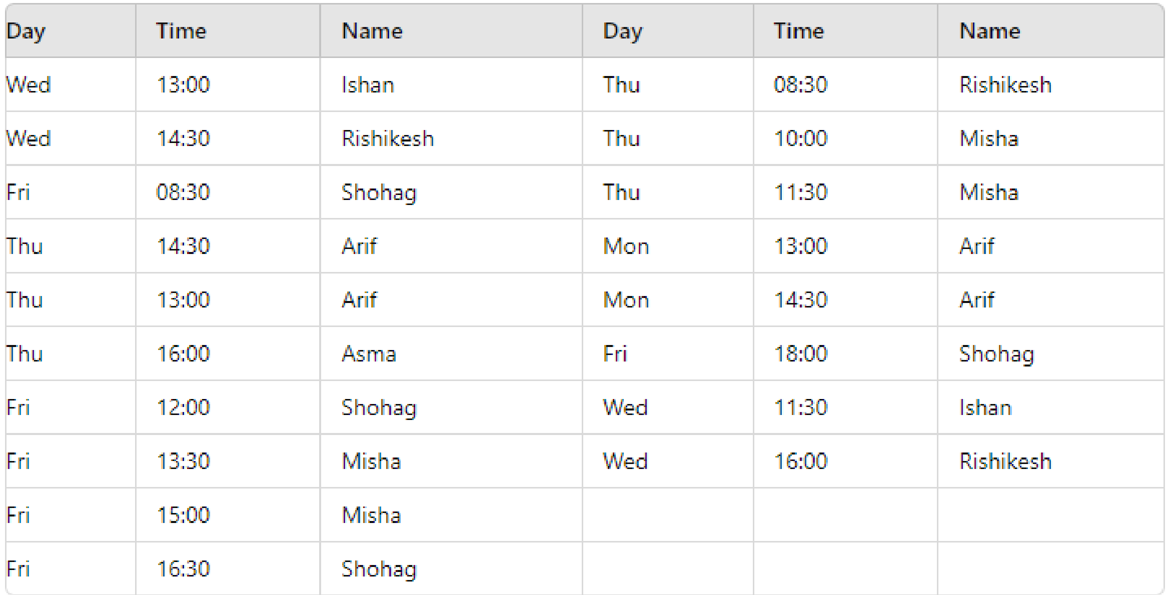
Objectives

- Subject organisation and class logistics
- A preview on recent and ongoing Cybersecurity incidences
- Cybersecurity Threat, Attacks and Vulnerabilities
- Goals of Cybersecurity
- Security approaches (mitigation)

Subject overview: Teaching staffs

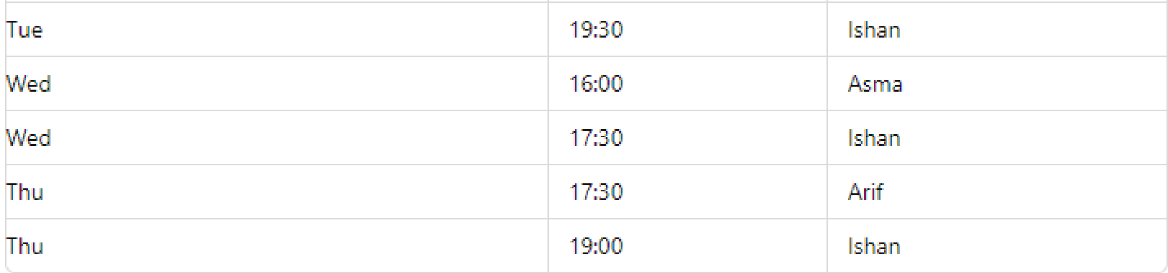
- **Subject Co-Ordinator and Lecturer, Workshop/Lecture Venue: To be filled up before 2 weeks of start**
  - Dr. Priyadarsi Nanda, Email: Priyadarsi.Nanda@uts.edu.au
- **Lab/Tutorial instructors, lab locations CB11.06.101 and CB11.B1.102 (please check your lab location before attending)**

48730, Tutorials



Day	Time	Name	Day	Time	Name
Wed	13:00	Ishan	Thu	08:30	Rishikesh
Wed	14:30	Rishikesh	Thu	10:00	Misha
Fri	08:30	Shohag	Thu	11:30	Misha
Thu	14:30	Arif	Mon	13:00	Arif
Thu	13:00	Arif	Mon	14:30	Arif
Thu	16:00	Asma	Fri	18:00	Shohag
Fri	12:00	Shohag	Wed	11:30	Ishan
Fri	13:30	Misha	Wed	16:00	Rishikesh
Fri	15:00	Misha			
Fri	16:30	Shohag			

32548, Tutorials



Tue	19:30	Ishan
Wed	16:00	Asma
Wed	17:30	Ishan
Thu	17:30	Arif
Thu	19:00	Ishan

Remember, all lab/tutorial activities will be conducted face-to-face in the lab, NO online lab activities

Weekly Activities

- 1.5-hour Workshop/Lecture + Live zoom Session, Tuesday, 18.00 – 19.30
  - Join URL: https://utsmeet.zoom.us/j/85662811961
  - 1.5-hour Lab session
  - Check your lab enrolment (Activity) and attend accordingly
- Dr. Nanda’s consultation: Tuesday, 16.00-17.00, FEIT Learning Precinct, Building 11, Level 5
  - If you want to meet personally, please send email at:
    - Priyadarsi.nanda@uts.edu.au
  - Arif Hassan – mdarif.Hassan@uts.edu.au
- For All Lab related matters, Contact your Lab instructor

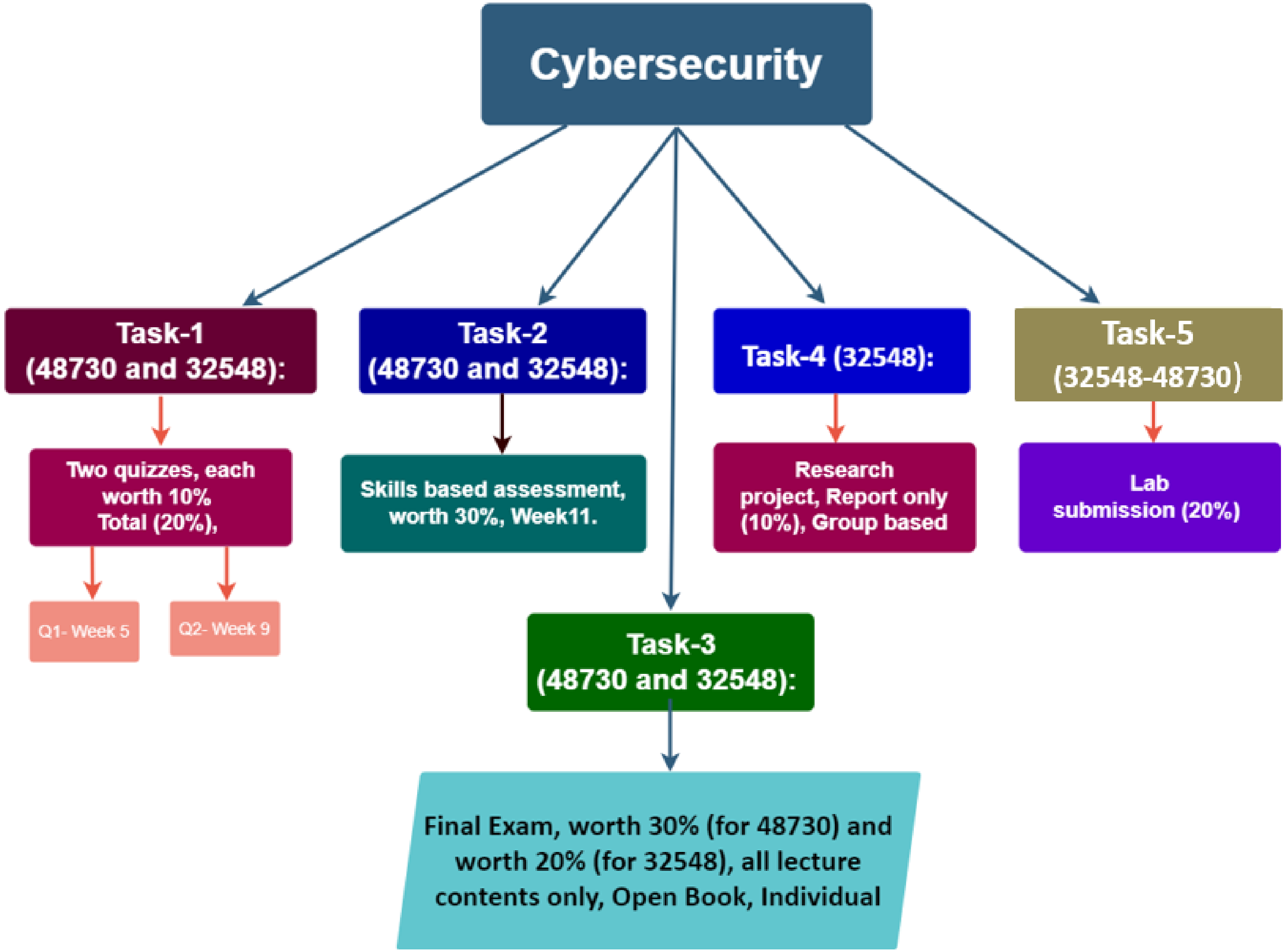
Workshop/Lecture and Lab materials

- All materials will be posted at CANVAS
  - Lecture and Lab materials will be available before the weekly session
  - Lecture recordings will be posted after the workshop/lecture every week
- Please read the materials before the workshop/lecture and lab session
- All additional reading materials (when required) will be posted at CANVAS
- Week-10, Week-11 are meant to be guest lectures
  - Guest Lecture contents will be examined

Assessments and Examination

- Task-1 (48730 and 32548): Two quizzes, each worth 10% (Total 20%), Only multiple-choice, multiple-answer, True/False type questions, Closed Book, Individual
  - Quiz-1: Week-5; will cover lecture materials from Week-1 to Week-4
  - Quiz-2: Week-9; will cover lecture materials from Week-5 to Week-8
- Task-2 (48730 and 32548): Skills based assessment, worth 30%, questions will be based on lab scenario and similar questions performed during the lab, Closed Book, Individual
  - Week-11
- Task-3 (48730 and 32548): Final Exam, worth 30% (for 48730) and worth 20% (for 32548), all lecture contents only, Open Book, Individual
  - Short answer type questions
  - During UTS exam period
- Task-4 (32548): Research project, Report only (10%), Group based
- Task-4 (48730): Lab submission after the lab, through CANVAS and due date will be provided in CANVAS, 20%, Individual
- Task-5 (32548): Lab submission after the lab, through CANVAS and due date will be provided in CANVAS, 20%
- Make sure you check CANVAS regularly on any updates!
- To pass the subject, a student must achieve an overall mark of 50% or more.

Assessments and Examination



Cybersecurity

Task-1 (48730 and 32548):

Two quizzes, each worth 10% Total (20%),

Q1- Week 5

Q2- Week 9

Task-2 (48730 and 32548):

Skills based assessment, worth 30%, Week11.

Task-3 (48730 and 32548):

Final Exam, worth 30% (for 48730) and worth 20% (for 32548), all lecture contents only, Open Book, Individual

Task-4 (32548):

Research project, Report only (10%), Group based

Task-5 (32548-48730)

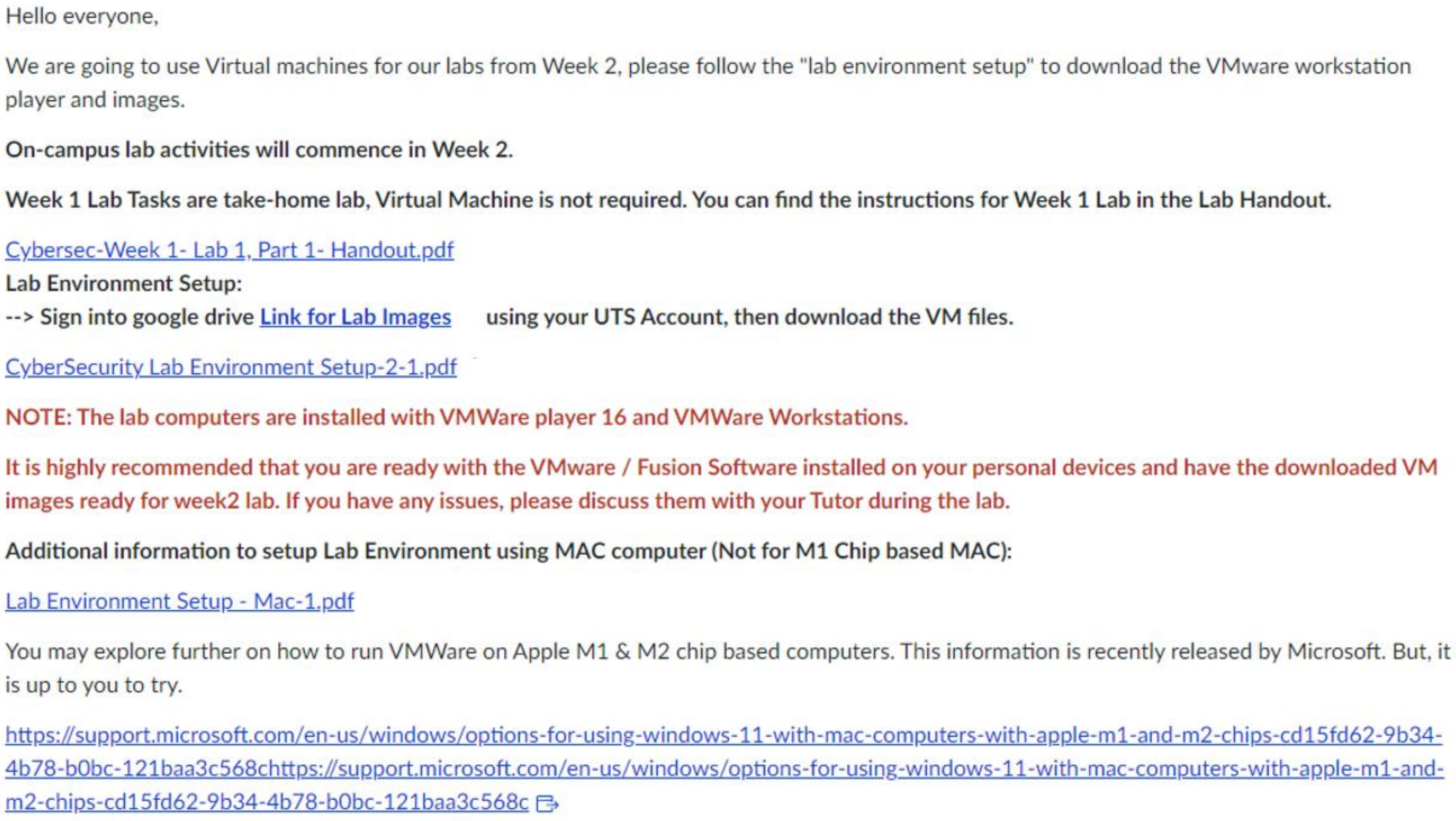
Lab submission (20%)

Tips to do Well in this subject

- Read your Lecture notes and attend workshop/lecture and listen to recordings
- Perform the lab exercises and submit your lab works timely
- Complete all assessment tasks
- Consult your subject coordinator
- Consult your Lab/Tut instructor

Best of luck !!!

Pre-lab Activities



Hello everyone,

We are going to use Virtual machines for our labs from Week 2, please follow the "lab environment setup" to download the VMware workstation player and images.

On-campus lab activities will commence in Week 2.

Week 1 Lab Tasks are take-home lab, Virtual Machine is not required. You can find the instructions for Week 1 Lab in the Lab Handout.

Cybersec-Week 1- Lab 1, Part 1- Handout.pdf
Lab Environment Setup:
--> Sign into google drive Link for Lab Images using your UTS Account, then download the VM files.

CyberSecurity Lab Environment Setup-2-1.pdf

NOTE: The lab computers are installed with VMWare player 16 and VMWare Workstations.

It is highly recommended that you are ready with the VMware / Fusion Software installed on your personal devices and have the downloaded VM images ready for week2 lab. If you have any issues, please discuss them with your Tutor during the lab.

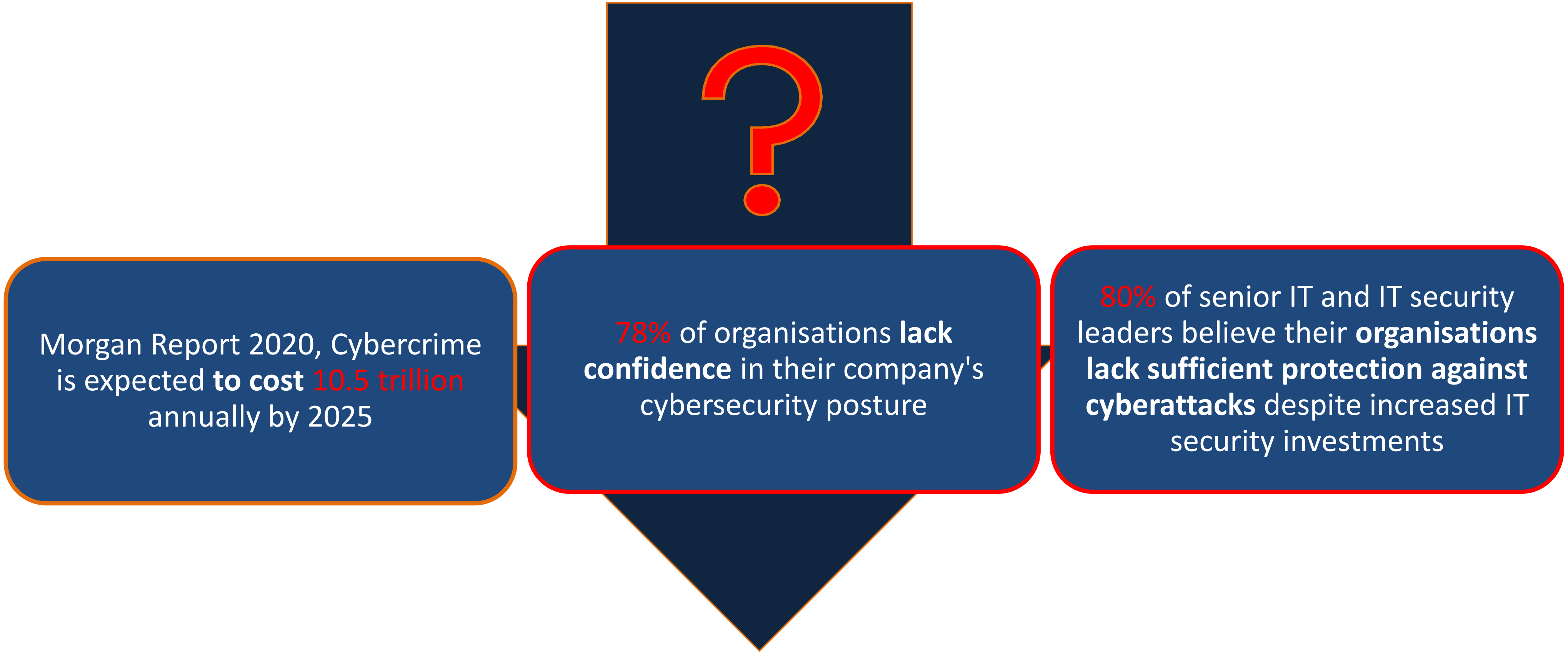
Additional information to setup Lab Environment using MAC computer (Not for M1 Chip based MAC):

Lab Environment Setup - Mac-1.pdf

You may explore further on how to run VMWare on Apple M1 & M2 chip based computers. This information is recently released by Microsoft. But, it is up to you to try.

https://support.microsoft.com/en-us/windows/options-for-using-windows-11-with-mac-computers-with-apple-m1-and-m2-chips-cd15fd62-9b34-4b78-b0bc-121baa3c568chttps://support.microsoft.com/en-us/windows/options-for-using-windows-11-with-mac-computers-with-apple-m1-and-m2-chips-cd15fd62-9b34-4b78-b0bc-121baa3c568c

Why Cybersecurity is important in today’s context?



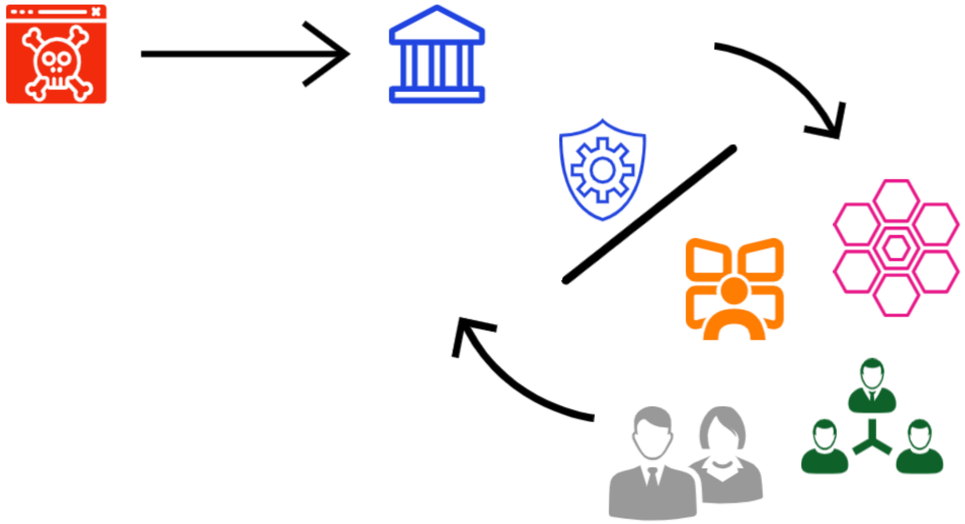
Morgan Report 2020, Cybercrime is expected **to cost** 10.5 trillion annually by 2025

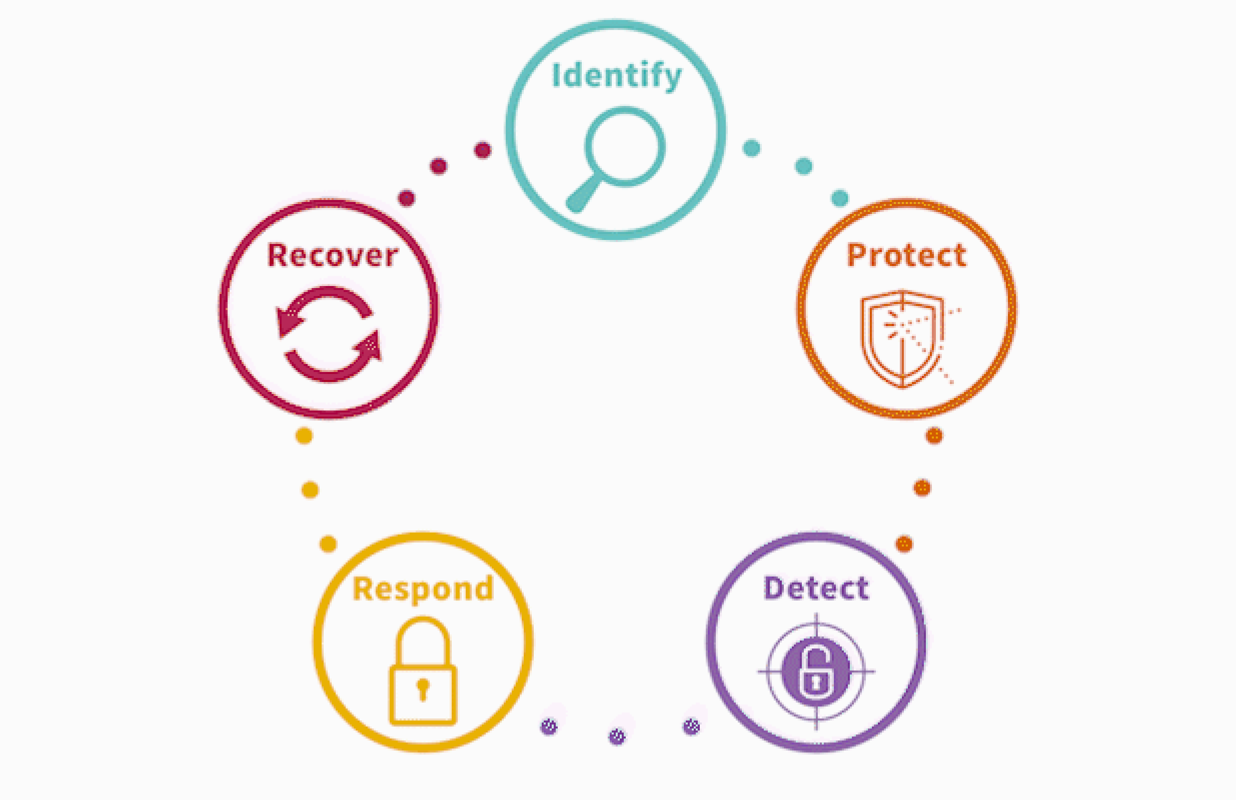
78% of organisations **lack confidence** in their company's cybersecurity posture

80% of senior IT and IT security leaders believe their **organisations lack sufficient protection against cyberattacks** despite increased IT security investments

https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-------what-you-need-to-know-for-2021/?sh=87964c158d3d

Cyber Attack Incident Diagram





Defence will be based on the following:

- Vendor tools and products
- Frontline technical staff
- The SOC monitoring team
- The management decision making

https://livethreatmap.radware.com/

What is Cybersecurity?

- Hard to quantify?
  - Protecting information/data stored on computers, data warehouse, mobile device…. (some say anything part of the Internet!)
  - Bad guys (adversaries) always ***aim to steal, corrupt or exploit data***
- Cybersecurity measures
  - Deploying people, policies, processes and technologies and managing overall aspects
  - Can help combat attacks and protect
    - Reputations, livelihoods as well as competitiveness of people and organizations using various technologies

Some definition

- Information Security
  - All forms of information
    - Physical (paper form), digital, software management, networks etc…
- Data security
  - Valuable data and information assets
- Cybersecurity
  - Almost everything
    - Computers, servers, mobile devices, Networks, Critical Infrastructure assets…

Introduction: Understanding Cybersecurity

- Cybersecurity is young, but fast evolving due to ongoing risks faced by organizations, countries and individuals
- Cyber incidences are growing almost exponentially!
- A list of resources for you to understand Cyber incidences
  - https://en.wikipedia.org/wiki/2024_CrowdStrike_incident
  - https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
  - https://purplesec.us/security-insights/data-breaches/
  - https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
  - https://portswigger.net/daily-swig/cyber-attacks
  - https://www.cyber.gov.au/
  - https://www.dst.defence.gov.au/sites/default/files/publications/documents/Future-Cyber-Security-Landscape.pdf
  - https://www.itgovernance.co.uk/blog/global-data-breaches-and-cyber-attacks-in-2024
- How success we are in Detecting and Preventing Cyber-attacks?

Some well-known attack types

- Botnet Attacks
  - Coordinated attack using compromised program, computers launching DDoS attack
- Spoofing
  - Impersonating legitimate source; phishing email, fraudulent websites, SMS….
- Spyware
  - Collecting user information from different sources without user consent
- Malware
  - Corrupted and fabricated programs
- Phishing
  - Key player, social engineering carrying out scams

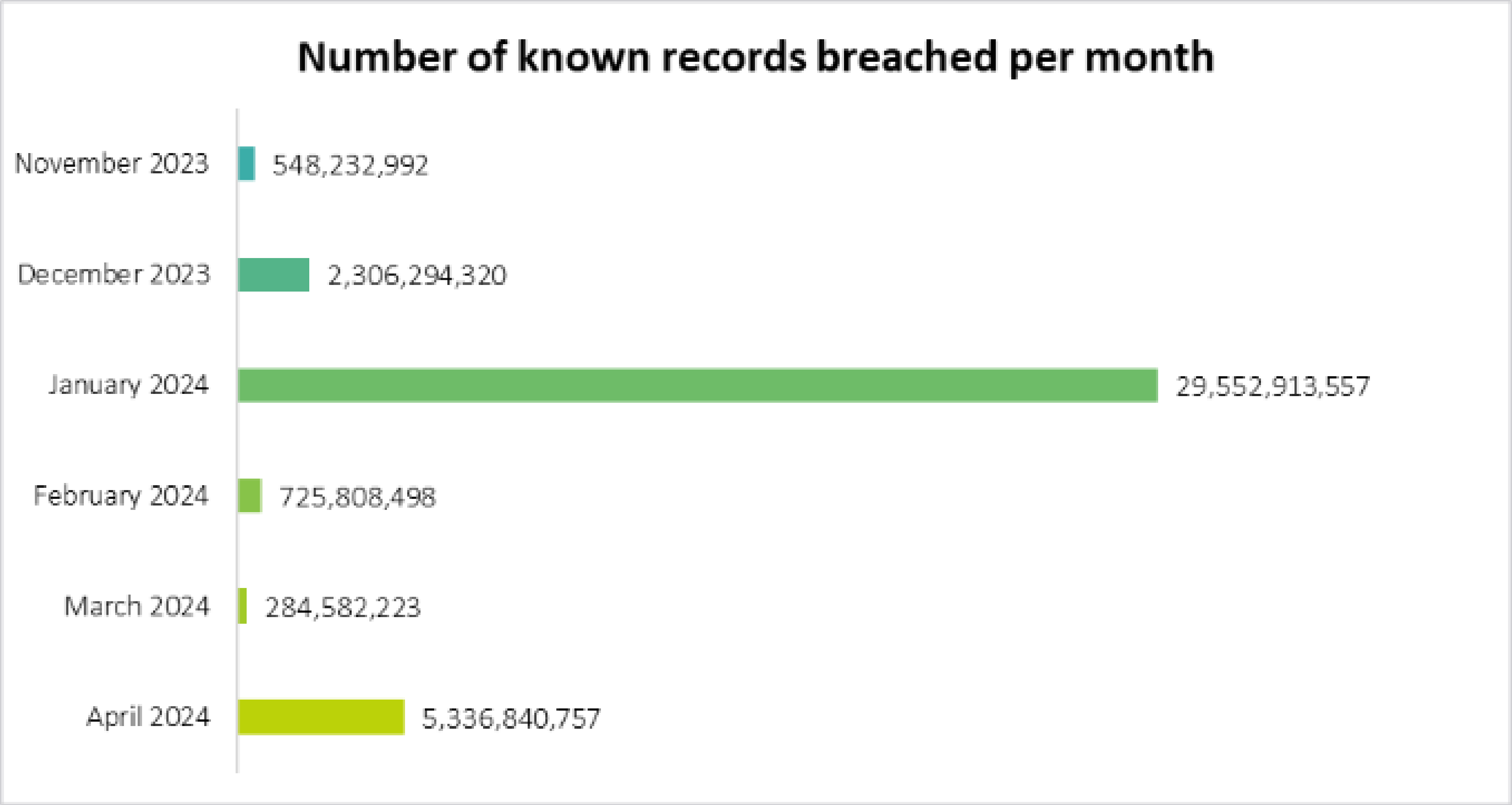
Motives behind Cyber attack

- Damaging Trust, Security and Privacy aspects
  - Achieve monetary gains
  - Damage brand value of other party
  - Inflicting damages through cyberterrorism
  - Obtaining government and business secrets
  - Launching Cyber warfare
- Implications after the cyber attack are huge
  - Discuss in group

Some Common origin of Cybersecurity threats

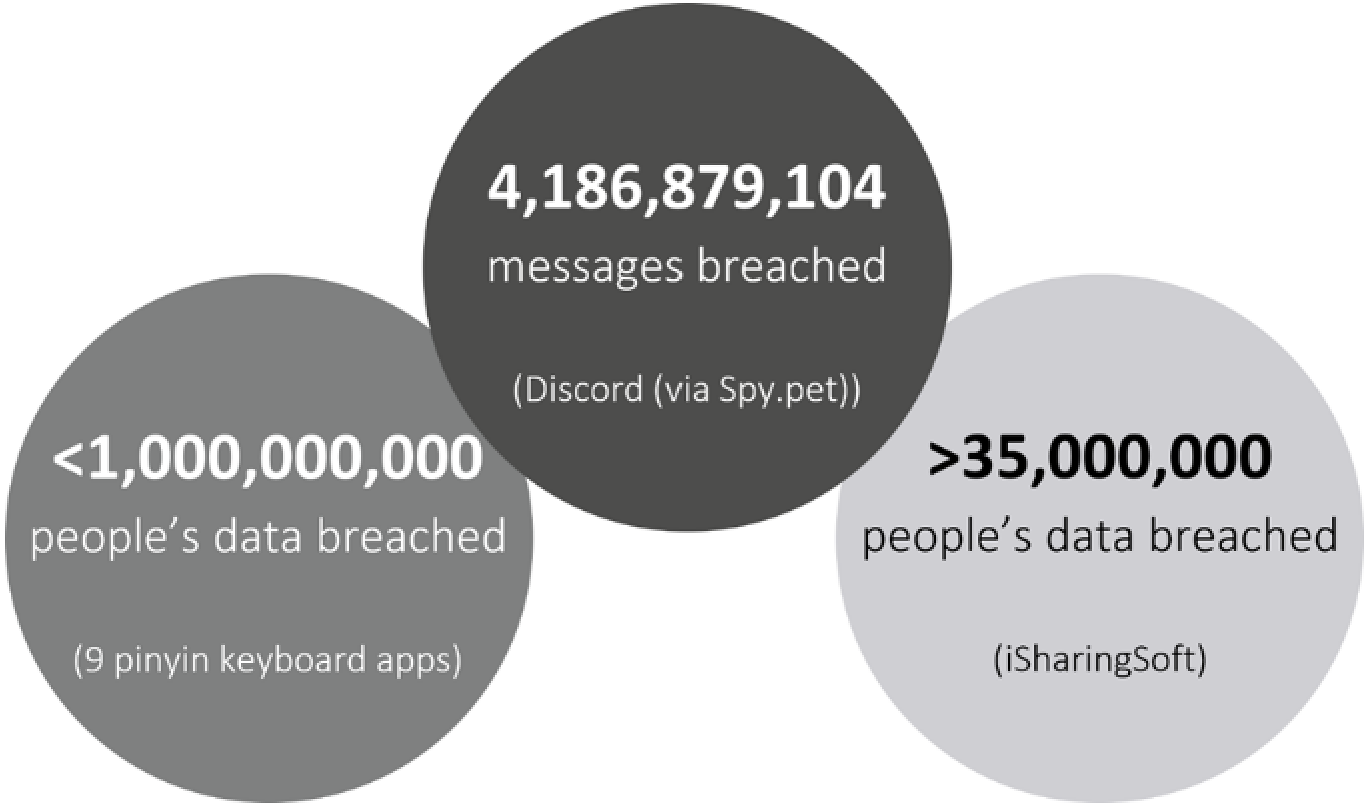
- Opening email from unknown senders
  - How to do common check?
- Weak login credentials
  - Fix it using strong pass words and change them regularly
- Old antivirus S/W with no updates
  - Patch, update regularly
- Un-protected mobile devices
  - What can you do?
- Failing to update system software (OS) regularly
  - Patch, update regularly
- Third-party Apps
  - Do not trust always, verify completely the source

Global Data Breaches and Cyber Attacks in 2024



https://www.itgovernance.co.uk/blog/global-data-breaches-and-cyber-attacks-in-2024

The top 3 biggest breaches in April 2024



4,186,879,104

messages breached

(Discord (via Spy.pet))

<1,000,000,000

people's data breached

(9 pinyin keyboard apps)

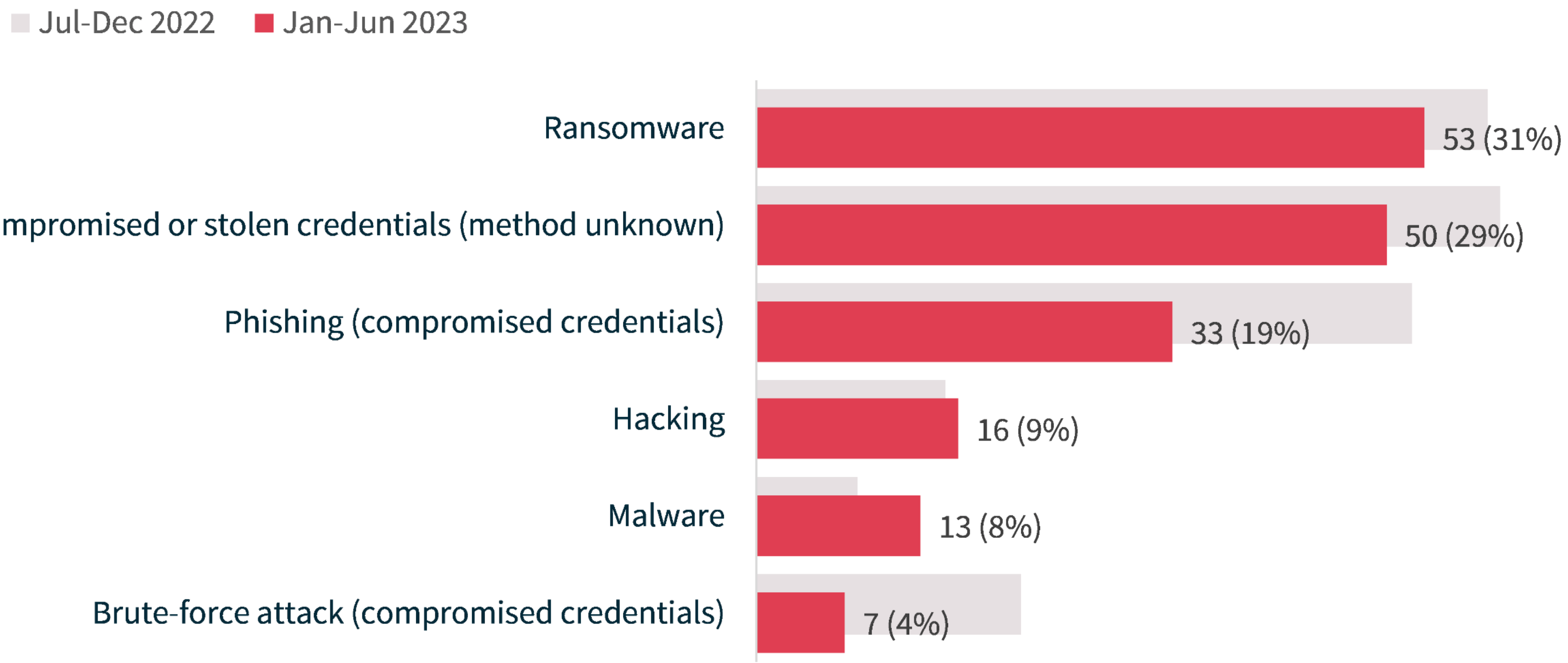
>35,000,000

people's data breached

(iSharingSoft)

https://www.itgovernance.co.uk/blog/global-data-breaches-and-cyber-attacks-in-2024

Data Breaches Report: January to June 2023- Australia



Jul-Dec 2022
Jan-Jun 2023
Ransomware
53 (31%)
Compromised or stolen credentials (method unknown)
50 (29%)
Phishing (compromised credentials)
33 (19%)
Hacking
16 (9%)
Malware
13 (8%)
Brute-force attack (compromised credentials)
7 (4%)

https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-january-to-june-2023

Who are the Attackers?

Security strategy

- Detection
  - Detect attackers' violation of security policy
- Prevention
  - Prevent attackers from violating security policy
- Recovery
  - Stop attack, assess and repair damage
  - Continue to function correctly even if attack succeeds
- Constant awareness on the latest cyber threats must be a priority and best defense is intelligence

- Also, Cyberspace has now become the backbone of digital society as well as economic growth

Security Goal (1)

- Confidentiality:
  - Goal: prevent unauthorized disclosure of information
  - Confidentiality breach scenarios
    - Theft of employee laptops
    - Leaving computers with confidential information unattended
    - Providing unauthorized access to the unconcerned person
    - Unauthorized access by hacker through malware
    - Consulting company employees violating confidentiality agreements
    - Unlawful use of information for personal or business gains
  - What constitutes confidential data?
    - Intellectual Property (IP), Personal identity information, Credit card information, Bank account information, Personal health information, Business and trade secrets etc….

Security Goal (2)

- Integrity:
    - Data integrity
        - Information and programs are changed only in a specified and authorized manner (origin integrity)
    - System integrity
        - Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system
- Integrity breach scenarios:
    - Injecting Malware on servers
    - Undoable malicious encryption of data
    - Manipulation of original data
    - Virus injection
    - Insider threat

Security Goal (3)

- Availability:
  - Allow prompt access to data and resources for authorized users
  - Availability breach scenarios:
    - Launching DoS attack
    - Making redundant arrangements failed
    - Making software to malfunction
    - Choking data bandwidth
    - Making the hardware to fail

Other desirable security goals

- Authenticity:
  - Confirm identity
    - Verifying that users are who they say they are and that each input arriving at the system came from a trusted source
- Accountability and non-repudiation:
  - Another notch of an authentication’s feature
    - The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity
- Access control:
  - Only permit the access to resources for designated user/process

Security vulnerability, penetration testing and security threats

- Vulnerability is a failure of security policies, procedures, and controls that allow an attacker to commit an action violating the security policy
  - Whether a system satisfies certain constraints can be verified mathematically or using formal verification
  - One must be aware of the vulnerabilities, else, little chance to prevent cyber attacks
- Penetration testing is a testing technique which is used to prove presence of vulnerabilities, not absence of vulnerabilities
- Security Threats happen when Vulnerabilities are exploited and represent potential security harm to an asset

Security Attack

- Threats are carried out to launch security attack
  - May involve sequence of actions creating violation of security policies
    - Attackers aim to gain access to corporate computer system by discovering contacts of the employees (learning about the organization) and impersonating employees
  - Attack categories:
    - Passive – attempt to learn or make use of information from the system that does not affect system resources
    - Active – attempt to alter system resources or affect their operation
    - Internal/Insider – initiated by an entity inside the security parameter
    - External/Outsider – initiated from outside the perimeter

Cyber attacks: Network-based exploits

- Attacks to OS, applications, hardware, and network equipment vulnerabilities
  - Malware
  - Configuration weaknesses
  - Syntax and semantics weaknesses
  - Validation weaknesses
- Attacks to confidentiality
  - Memory scraping
  - Eavesdropping
  - Packet sniffing
- Attacks on integrity
  - Modifications of information content
- Attack on Authenticity
  - Identity theft
  - Password crack
  - Phishing attack
  - DNS attack
  - Cache poisoning
- Evasion on security equipment/measures
  - Mutated attacks
- Attacks on Availability
  - Distributed Denial of Service (DDoS)
- Social engineering

List of Security Vulnerabilities

1. SQL Injection
2. Cross-site scripting
3. Buffer Overflows
4. Format String Issues
5. Integer Overflows
6. Command Injections
7. Failing to handle errors properly
8. Failing to protect network traffic
9. Using magic URL’s and hidden form fields
10. Improper use of SSL/TLS
11. Weak password systems

12.Failing to store and protect data securely

13. Ransomware

14.Improper file access

15.Trusting network name resolution

16.Race conditions

17.Unauthenticated key exchange.

18.Not cryptographically strong random nos.

19. Phishing attack

20.Cross-site request forgery

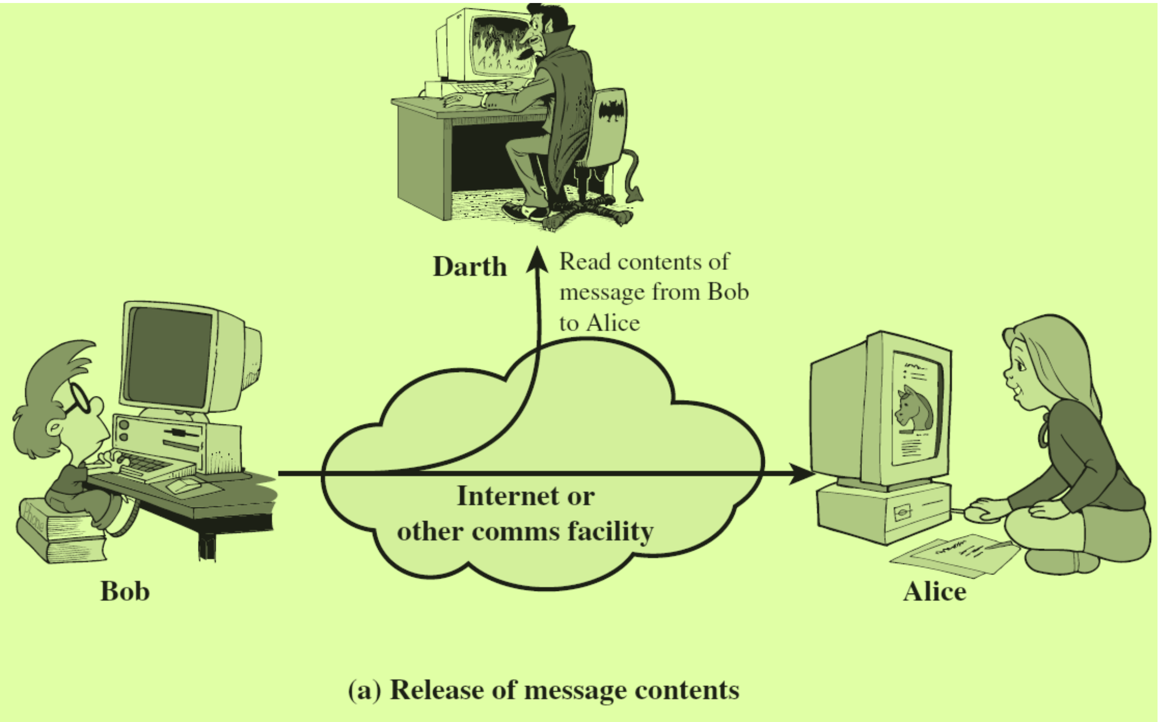
Human Error and security attacks

1. Failure to sanitize special characters
2. Failure to control system state
3. Failing to handle errors properly
4. Failing to protect network traffic
5. Depending on obscurity for security
6. Weak cryptography
7. Weak authentication model
8. Weak authorization model
9. Failing to store and protect data securely
10. Improper trust in unreliable data/component
11. Failure to handle race conditions securely

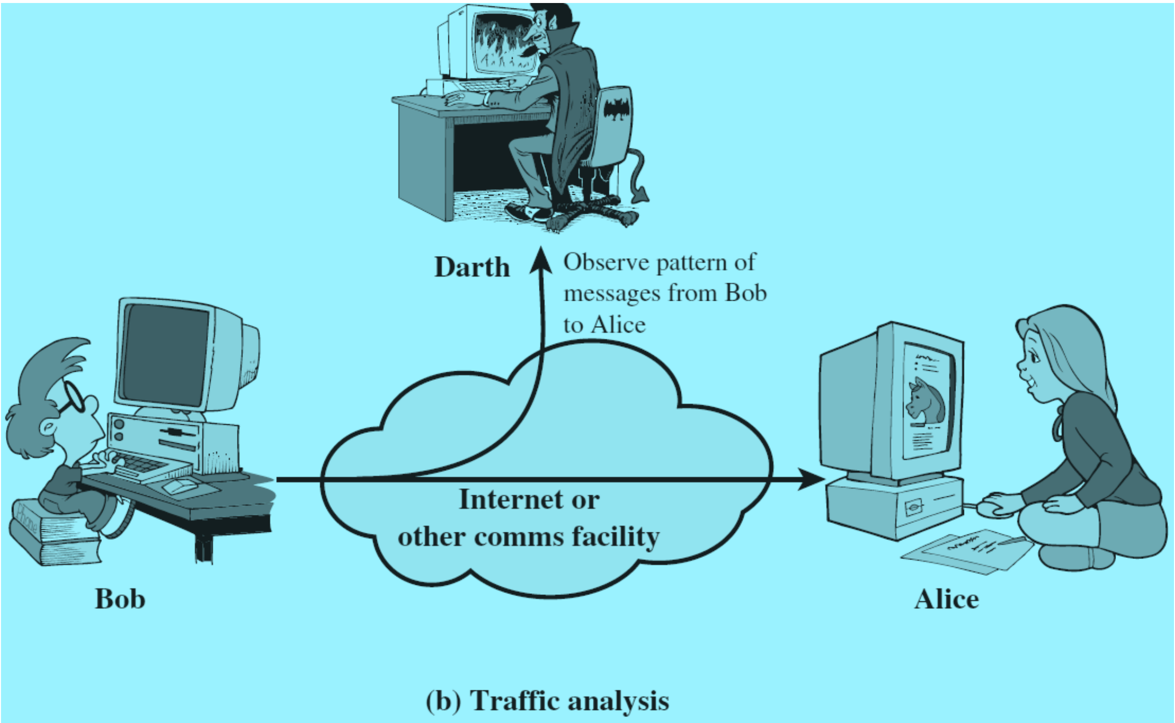
As a Cybersecurity professional we should answer followings:

1. How does an attack happen?
2. How nasty an attack can become?
3. How to detect an attack?
4. How to prevent an attack?

A simple Attack Scenario


Darth
Read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

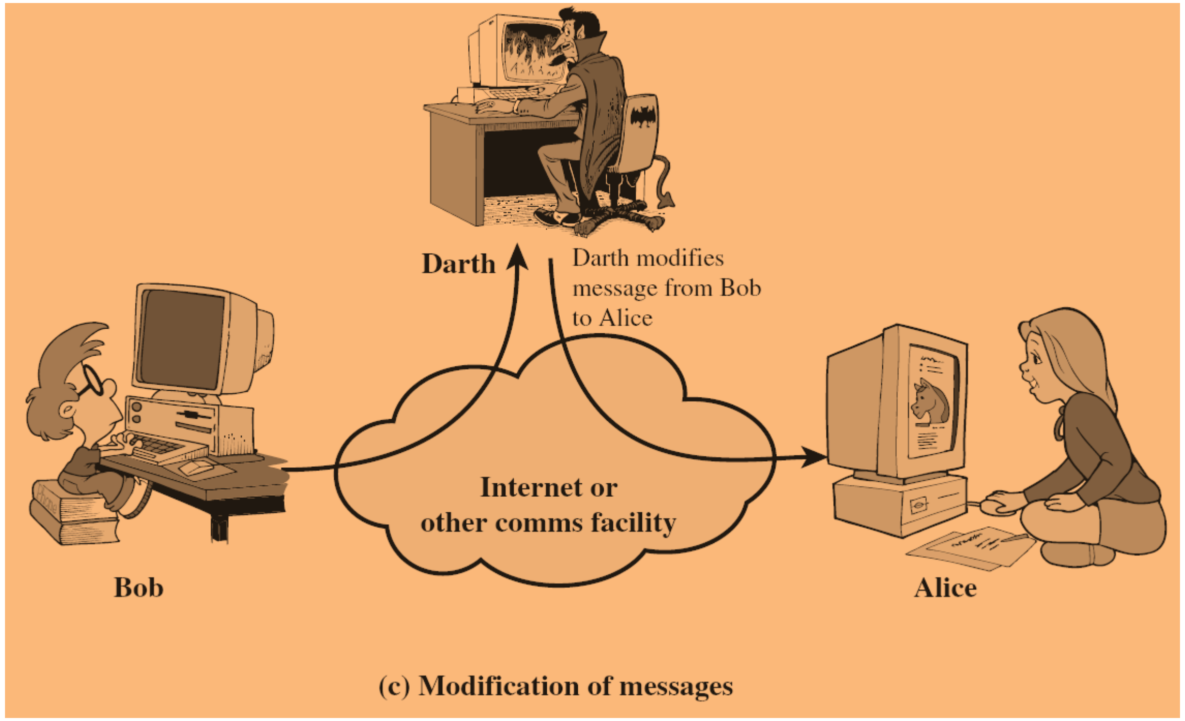
(a) Release of message contents


Darth
Observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

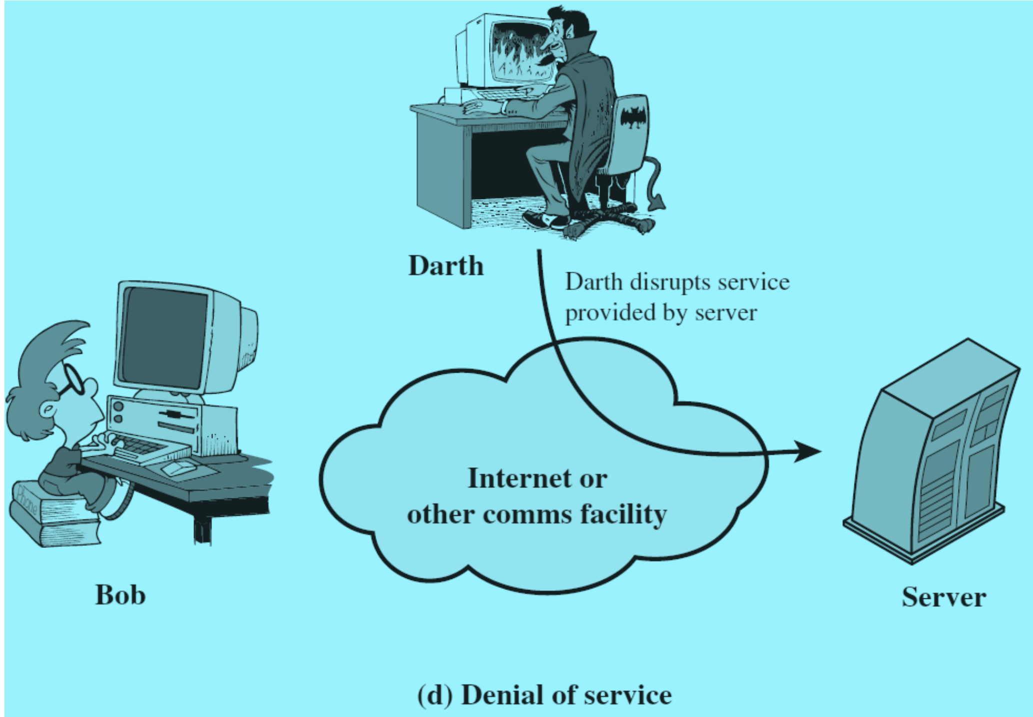
(b) Traffic analysis

Source: “Network Security Essentials: Applications and Standards”, 4th Edition by William Stallings

Attack Scenario Cont.


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

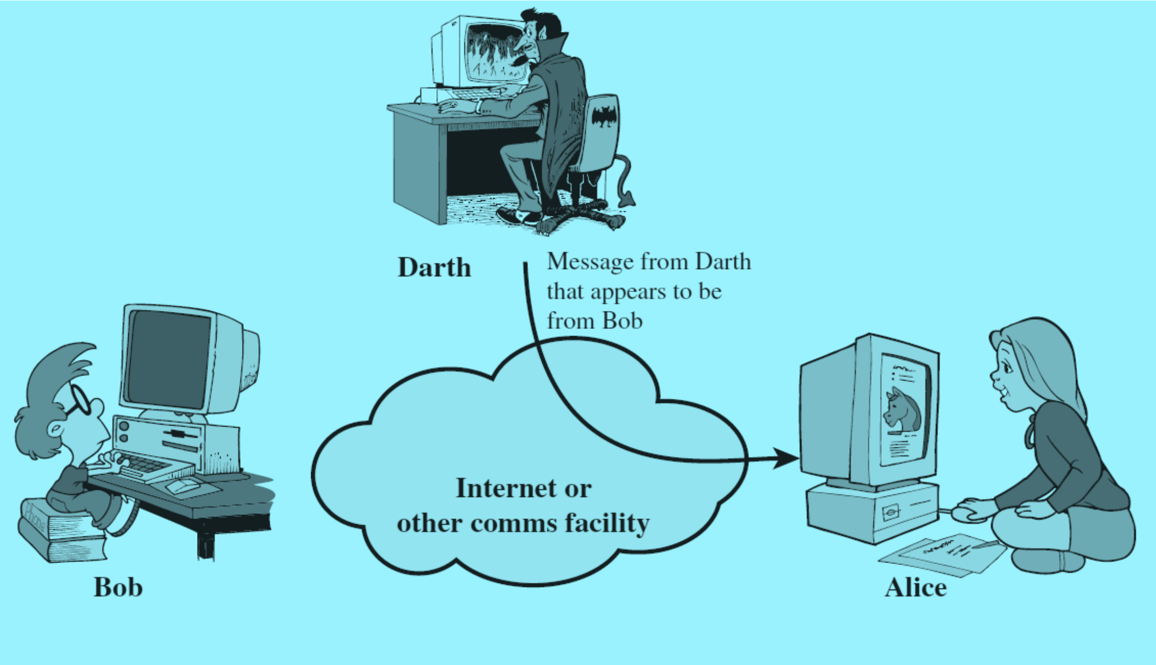
(c) Modification of messages


Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

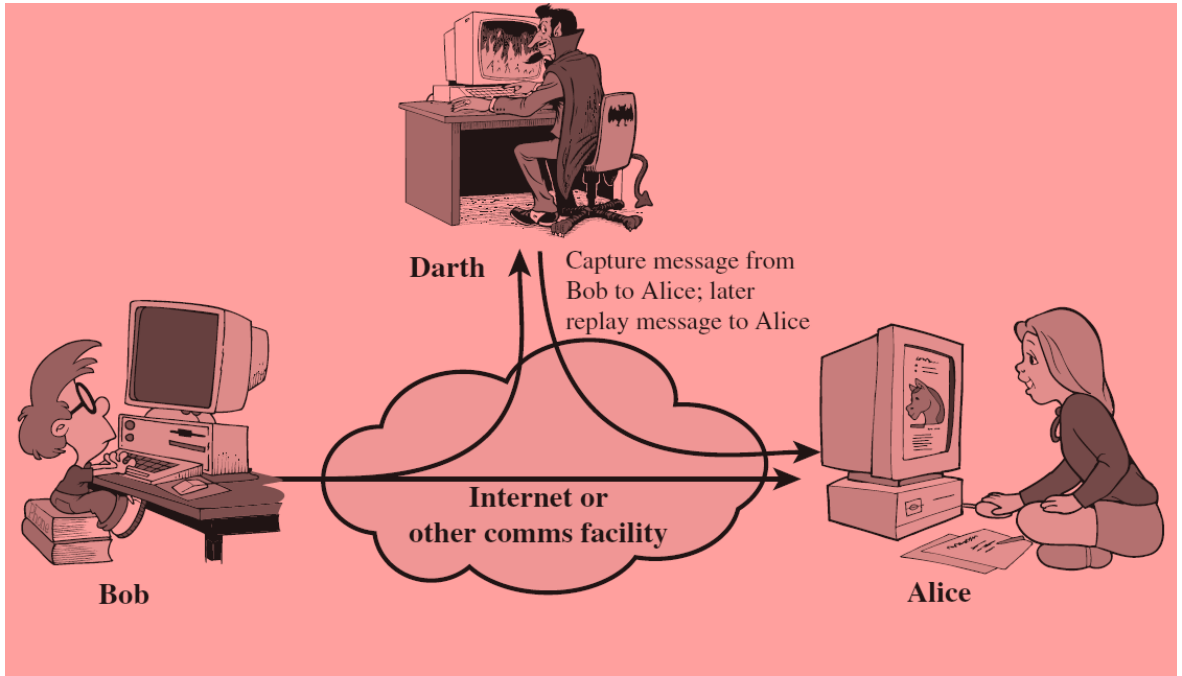
(d) Denial of service

Source: “Network Security Essentials: Applications and Standards”, 4th Edition by William Stallings

Attack Scenario Cont.


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

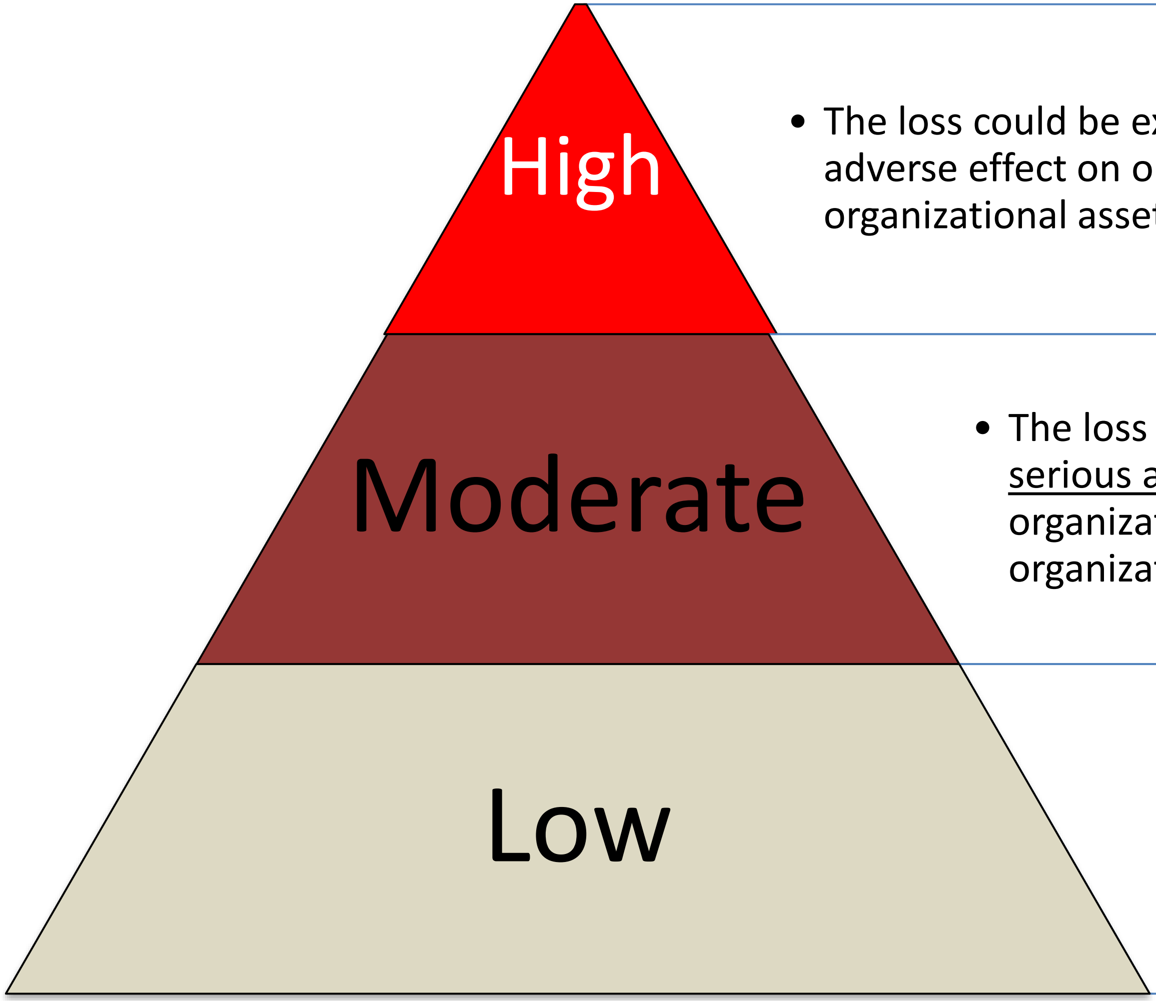
(a) Masquerade


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

(b) Replay

Source: “Network Security Essentials: Applications and Standards”, 4th Edition by William Stallings

Security breach classification



- The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals

- The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals

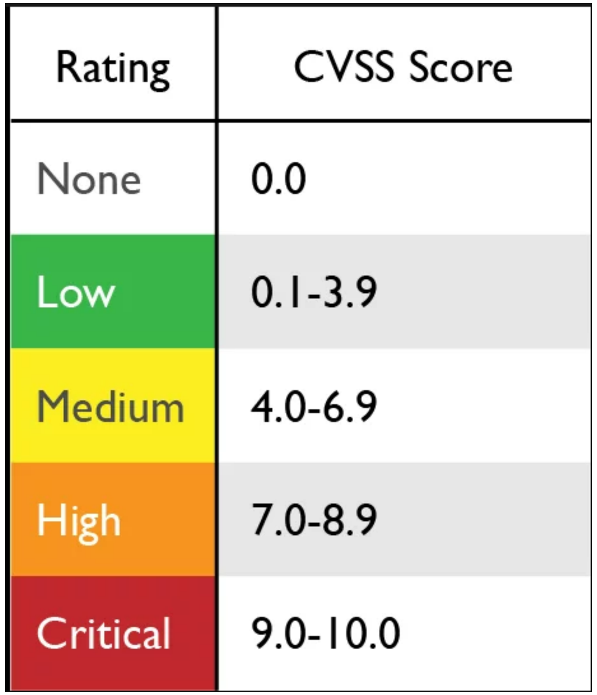
- The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals

What are the challenges in Cybersecurity?

- Combination of right Technology and right Public policy
  - Right Technology
    - What, When and Where to apply?
    - Simple Vs. Complex
  - Right Public Policy
    - Policy is crucial
    - User awareness is equally important
- Cybersecurity hurdles
  - There are no metrics measuring in-security
  - Internet has no boundary
  - No limit on how many device can be connected to Internet?

Risk Assessment

Common Vulnerability Scoring System (CVSS) Calculator



Rating	CVSS Score
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

- NIST outlined
  - Method of calculating vulnerability score
    - http://nvd.nist.gov/cvss.cfm?calculator&version=2
- Mitre corporation mentioned a number of products for vulnerability assessment (CVE: Common Vulnerabilities and Exposures)
  - https://cve.mitre.org/compatible/vulnerability_management.html
- Security Requirements, Federal Information Processing Standards (FIPS 200)
  - https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

Attacks on industrial control systems (ICS)

(Cybersecurity for critical infrastructure)

- Stuxnet: World's most sophisticated malware on ICS in 2010
  - Aimed at industrial Supervisory Control and Data Acquisition (SCADA) systems
- WannaCry:

- attack’s effect on the UK’s National Health Service,

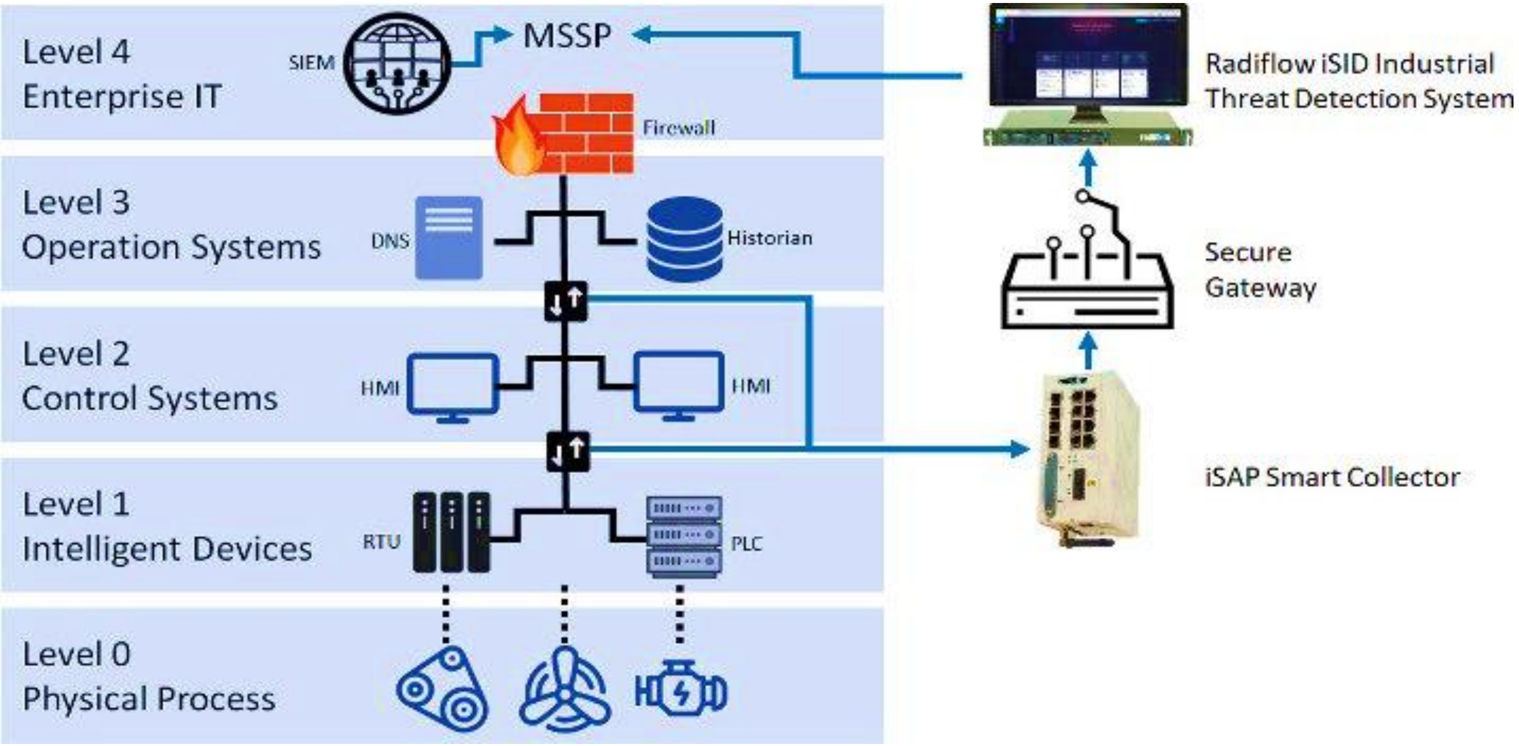
- cyber attacks against the Ukrainian power grid,

- Mirai botnet attack on DNS provider Dyn,

- the attack on Saudi Aramco etc…

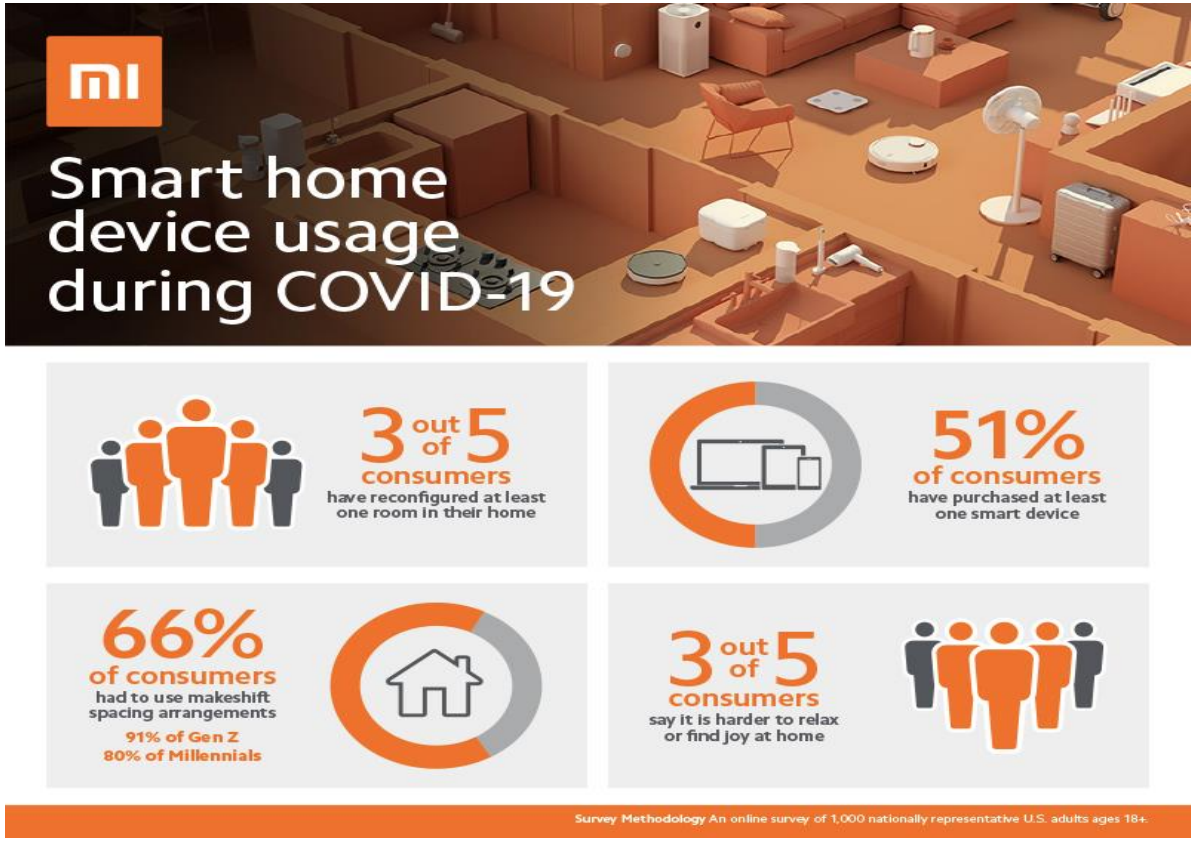
- ICS is redefined as Industrial IoT (IIoT) in Industry 4.0
  - Driven by Artificial Intelligence (AI), advanced automation and data analytics
  - Real-time interactions between connected devices

IIoT Security Threats



ICS network topology example, Radiflow,
https://radiflow.com/ot-mssp-partner-program/

Smart home device threats



MI

Smart home device usage during COVID-19

3 out of 5 consumers have reconfigured at least one room in their home

51% of consumers have purchased at least one smart device

66% of consumers had to use makeshift spacing arrangements

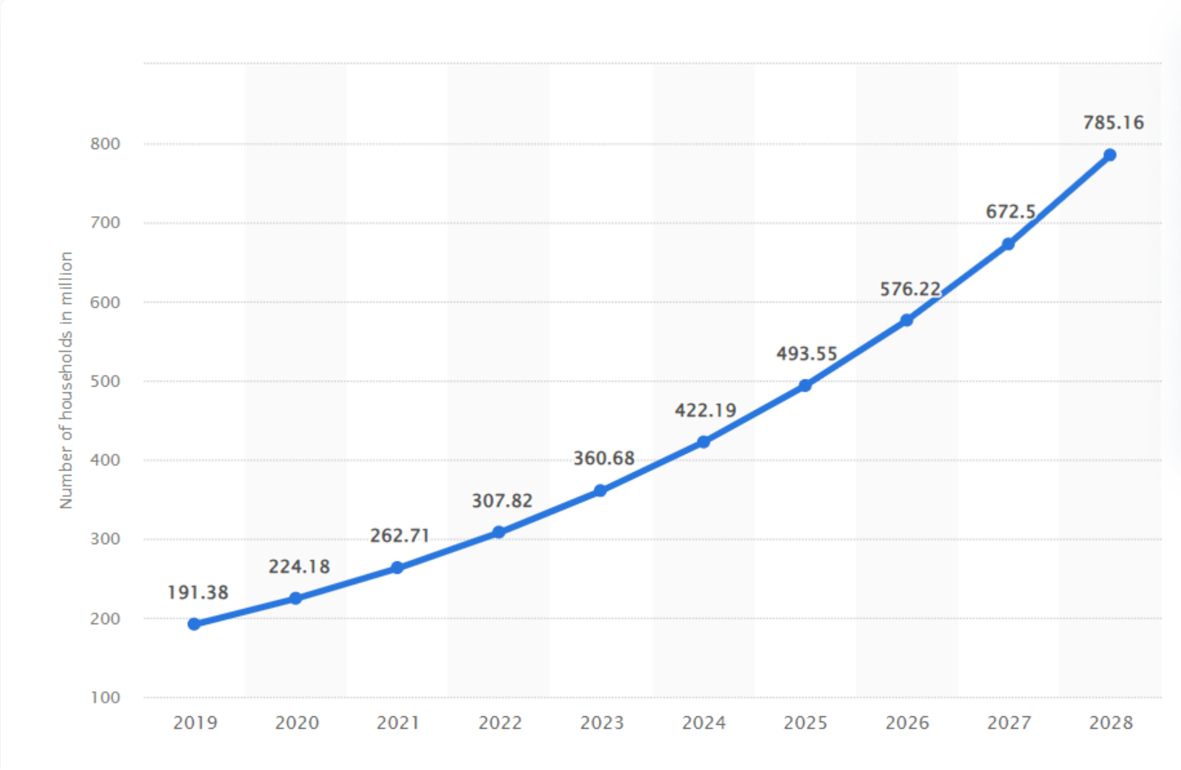
91% of Gen Z

80% of Millennials

3 out of 5 consumers say it is harder to relax or find joy at home

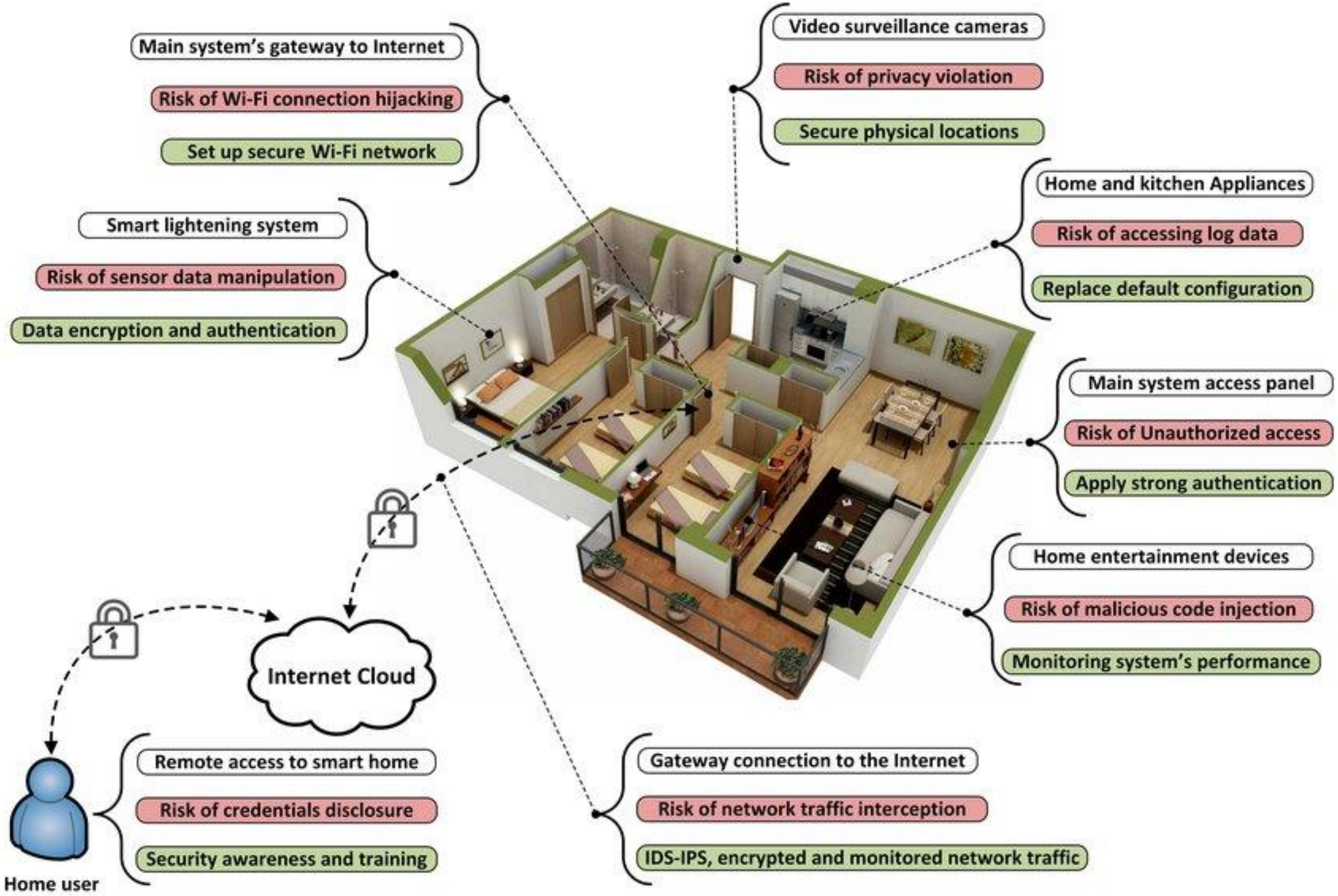
Survey Methodology An online survey of 1,000 nationally representative U.S. adults ages 18+.

Number of users of smart homes worldwide from 2019 to 2028



https://www.statista.com/forecasts/887613/number-of-smart-homes-in-the-smart-home-market-in-the-world#:~:text=The%20global%20indicator%20'Smart%20Homes,a%20new%20peak%20in%202028

Smart home device threats


Main system's gateway to Internet
Risk of Wi-Fi connection hijacking
Set up secure Wi-Fi network
Video surveillance cameras
Risk of privacy violation
Secure physical locations
Smart lightening system
Risk of sensor data manipulation
Data encryption and authentication
Home and kitchen Appliances
Risk of accessing log data
Replace default configuration
Main system access panel
Risk of Unauthorized access
Apply strong authentication
Home entertainment devices
Risk of malicious code injection
Monitoring system's performance
Internet Cloud
Remote access to smart home
Risk of credentials disclosure
Security awareness and training
Home user
Gateway connection to the Internet
Risk of network traffic interception
IDS-IPS, encrypted and monitored network traffic

https://www.researchgate.net/publication/323649445_Cyber_and_Physical_Security_Vulnerability_Assessment_for_IoT-Based_Smart_Homes

The Security Landscape

- Recent trends on Cyber incidents:
  - About 39.3% of reported vulnerabilities received Common Vulnerability Scoring System (CVSS) scores above 7.0.
  - This means that not only has the number of vulnerabilities been increasing but also that the CVSS scores have been trending higher over the last five years.

- ENISA https://www.enisa.europa.eu/
- Microsoft www.microsoft.com/sir
- IT Governance -https://www.itgovernance.co.uk/blog/global-data-breaches-and-cyber-attacks-in-2024
- Kaspersky Lab Security report: https://securelist.com/
- 2024 Identity Security Threat Landscape Report: https://www.cyberark.com/threat-landscape/
- Annual Cyber Threat Report: https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf

- Also, many more organizations have been publishing their own reports, Look through those reports.

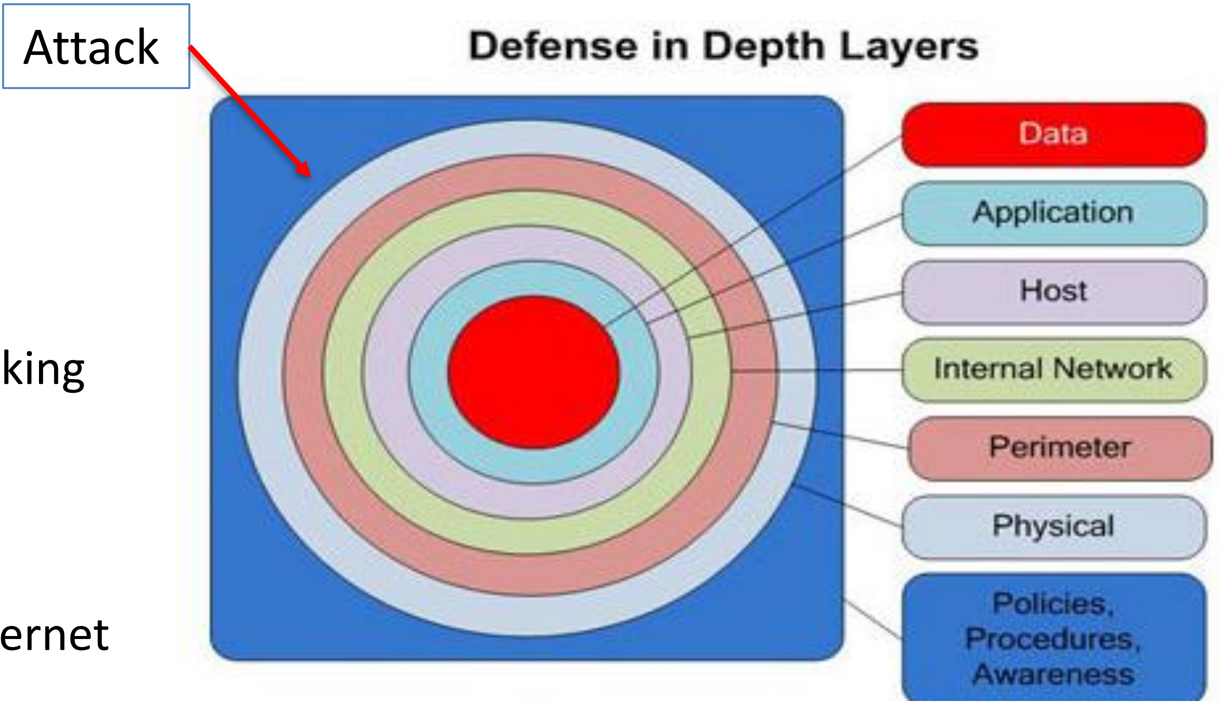
The Top 4 Mitigation Strategies # 1

1) Application whitelisting
   - only allow your clients to run tested software

2) Patching systems
   - set your systems to auto update
   - there is a risk that some applications will stop working after a patch is applied

3) Restricting administrative privileges
   - administrators should have two accounts
   - the one with root access should not access the internet

4) Creating a defence-in-depth system



How to Stay Cyber safe?

- Cyber hygiene
- Assess and manage potential risks
- Determine security metrics and use them efficiently
- Strategy to recover from cyber incident
- Be aware and constantly educate using various resources

How many of you have noticed the signage “#Think Securely signs of phishing ” across the University?

User awareness and Education contributes significantly maintaining a secured environment

Readings, Textbook and references

- Stallings: Chapter 1
- Chwan-Hwa Wu and David Irwin: Chapter-17
- Internet Resources as mentioned throughout the slides
- William Stallings,"Network Security Essentials Applications and Standards" (5th Edition/ 6th Edition) ISBN-10:0133370437, ISBN-13: 978-0133370430.
- Chwan-Hwa (john) Wu & J.David Irwin, "Introduction to Computer Networks and Cyber Security", CRC Press,ISBN: 978-1-4665-7213-3.
- Wenliang Du, Wenliang Du, “Computer and Internet Security, A Hands-on approach", Second Edition, ISBN: 978-1-7330039-3-3
- There are other recommended texts mentioned in your Subject Outline
- Note: I will also use materials from other resources and will be advised to you during the semester