UNIVERSITY OF
PLYMOUTH

Cyber Security Fundamentals

Dr Hai-Van Dang

Centre for Security, Communications and Network Research

- Resume at 12.05

ZP JB FP

Learning outcome checklist

LO1: Avoid confusion between cybersecurity and information security [1]

LO2: Apply CIA triad when justifying/ designing a product [2]

LO3: Apply Parkerian Hexad [3]

LO4: See how cybersecurity is relevant to the other disciplines

LO5: Apply Saltzer and Schroeder’s Design principles [4]

LO6: Identify risk scenarios

Further reading

1. Von Solms, Rossouw, and Johan Van Niekerk. "From information security to cyber security." *computers & security*38 (2013): 97-102.
2. https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html
3. http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf
4. Saltzer, Jerome H., and Michael D. Schroeder. "The protection of information in computer systems." *Proceedings of the IEEE*63.9 (1975): 1278-1308.
5. OWASP Secure Coding Practices Quick Reference Guide, https://owasp.org/www-pdf-archive/OWASP_SCP_Quick_Reference_Guide_v2.pdf
6. https://www.ncsc.gov.uk/collection/risk-management-collection

Session Content

Setting the scene

Defining Security

Security Perspectives

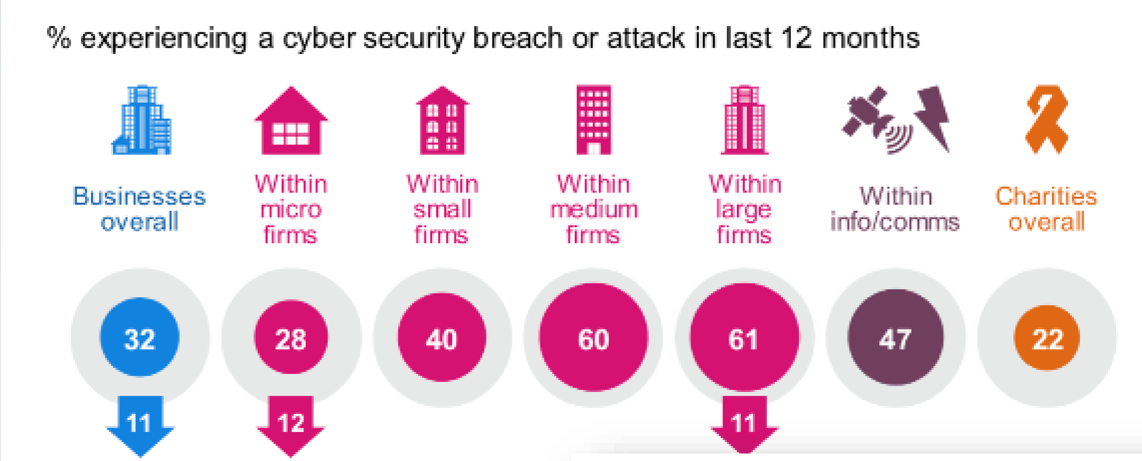
Threats, Vulnerabilities, Risks …

Conclusions

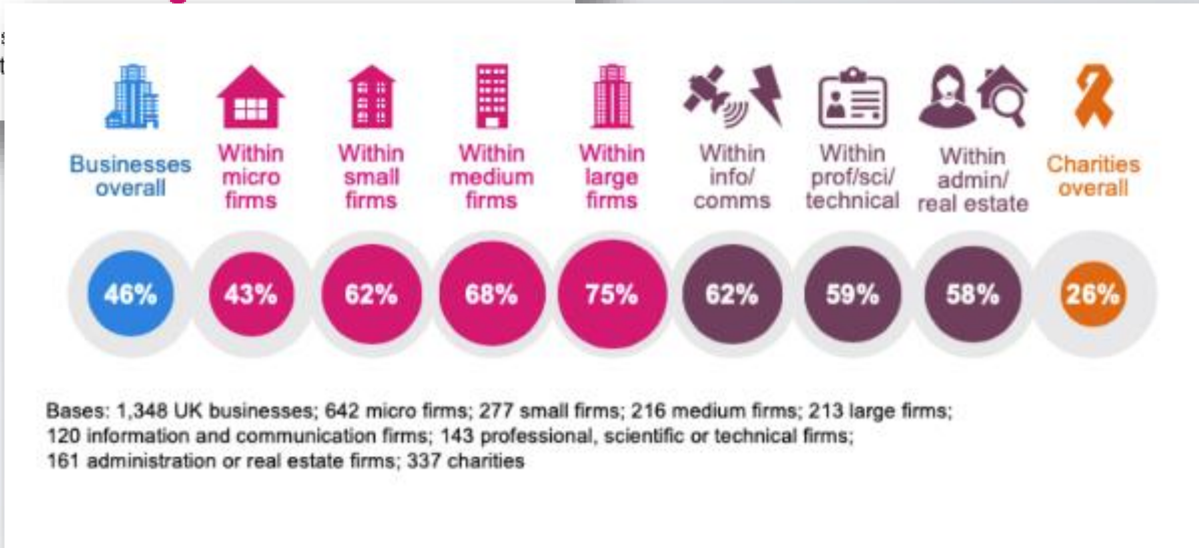
Setting the scene

Why we need security

% experiencing a cyber security breach or attack in last 12 months



Bases: 1,566 UK businesses; 757 micro firms; 321 s
102 information or communications firms; 514 charit



Bases: 1,348 UK businesses; 642 micro firms; 277 small firms; 216 medium firms; 213 large firms;
120 information and communication firms; 143 professional, scientific or technical firms;
161 administration or real estate firms; 337 charities

(Cyber Security Breaches Survey 2019, 2020)

Technology Dependence

"Today we are all linked together through powerful information systems and networks. We bank, conduct business, communicate with friends and family, pay bills, shop, do schoolwork, and listen to music through the marvels of information technology. Even more important, the critical infrastructures of our society rely upon the same information systems and networks"

Orson Swindle

US Federal Trade Commission (2002)

Defining Security

What is security?

Computer security is the protection of a company’ s assets by ensuring the safe, uninterrupted operation of the system and the safeguarding of its computer, programs and data files.

Prof. Harold J Highland
State University of New York

What is security?

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

ISO/IEC 17799
Code of practice for information security management, 2005

What is security?

The concepts, techniques, technical measures, and administrative measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use

IBM Dictionary of Computing, 1994

But what about ‘cybersecurity’?

“There are a number of terms currently being used by security practitioners that really annoy me, such as ‘threat vector’ and ‘threat landscape’. The worst among these is ‘cybersecurity’. What a wonderful word. Its real beauty is that it means whatever you want it to. It is now shortened to ‘cyber’ and is used and misused across the world by serious professionals, semi-literate journalists, snake-oil merchants and associated charlatans alike.”

Gregor Campbell, information security consultant
www.infosecurity-magazine.com/opinions/comment-cybersecurity-and-reality-whats-in-a-word/
May 2013

So what is cybersecurity?

The ISO ‘definition’

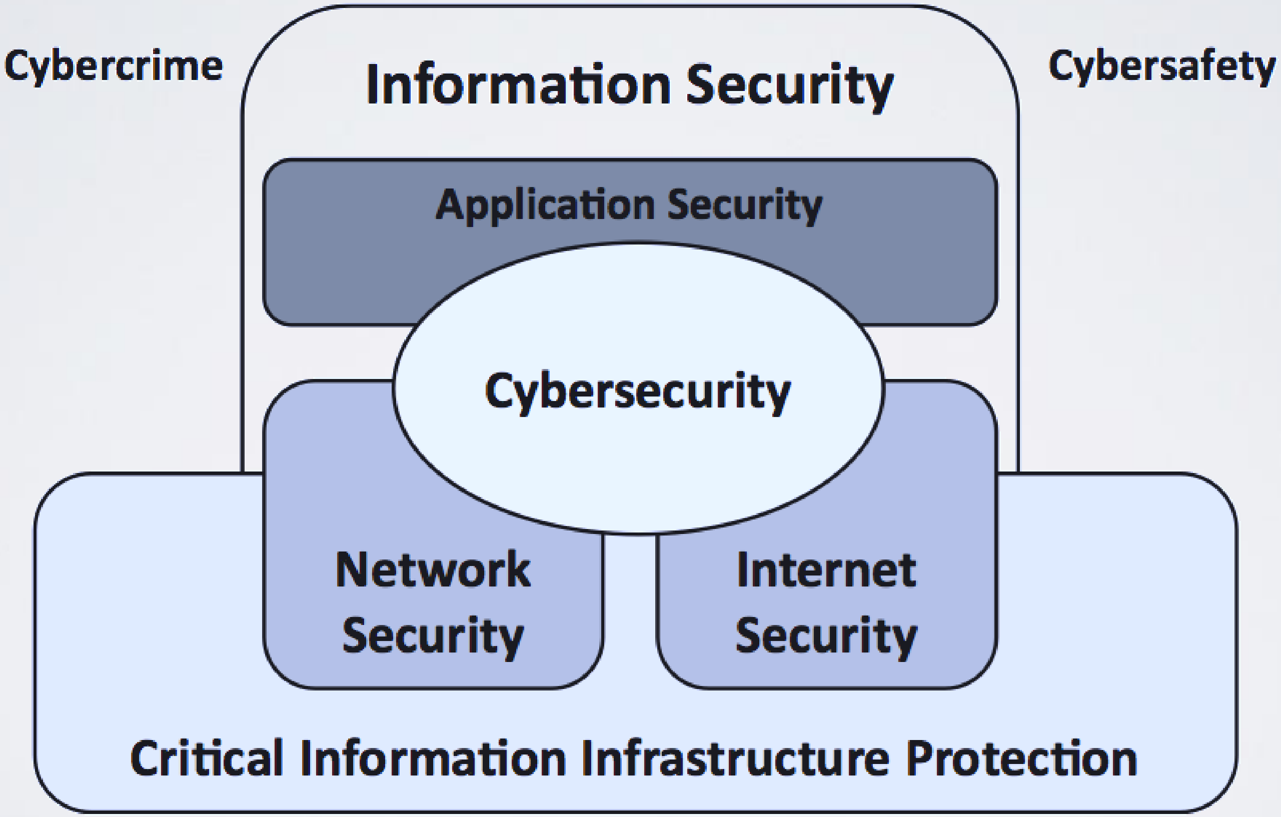
“Cybersecurity relates to actions that stakeholders should be taking to establish and maintain security in the Cyberspace.

Cybersecurity relies on information security, application security, network security, and Internet security as fundamental building blocks. Cybersecurity is one of the activities necessary for CIIP, and, at the same time, adequate protection of critical infrastructure services contributes to the basic security needs (i.e., security, reliability and availability of critical infrastructure) for achieving the goals of Cybersecurity.

Cybersecurity is, however, not synonymous with Internet security, network security, application security, information security, or CIIP. It has a unique scope requiring stakeholders to play an active role in order to maintain, if not improve the usefulness and trustworthiness of the Cyberspace*.”*

ISO27032 – Guidelines for Cyber Security
July 2012

Defining Security



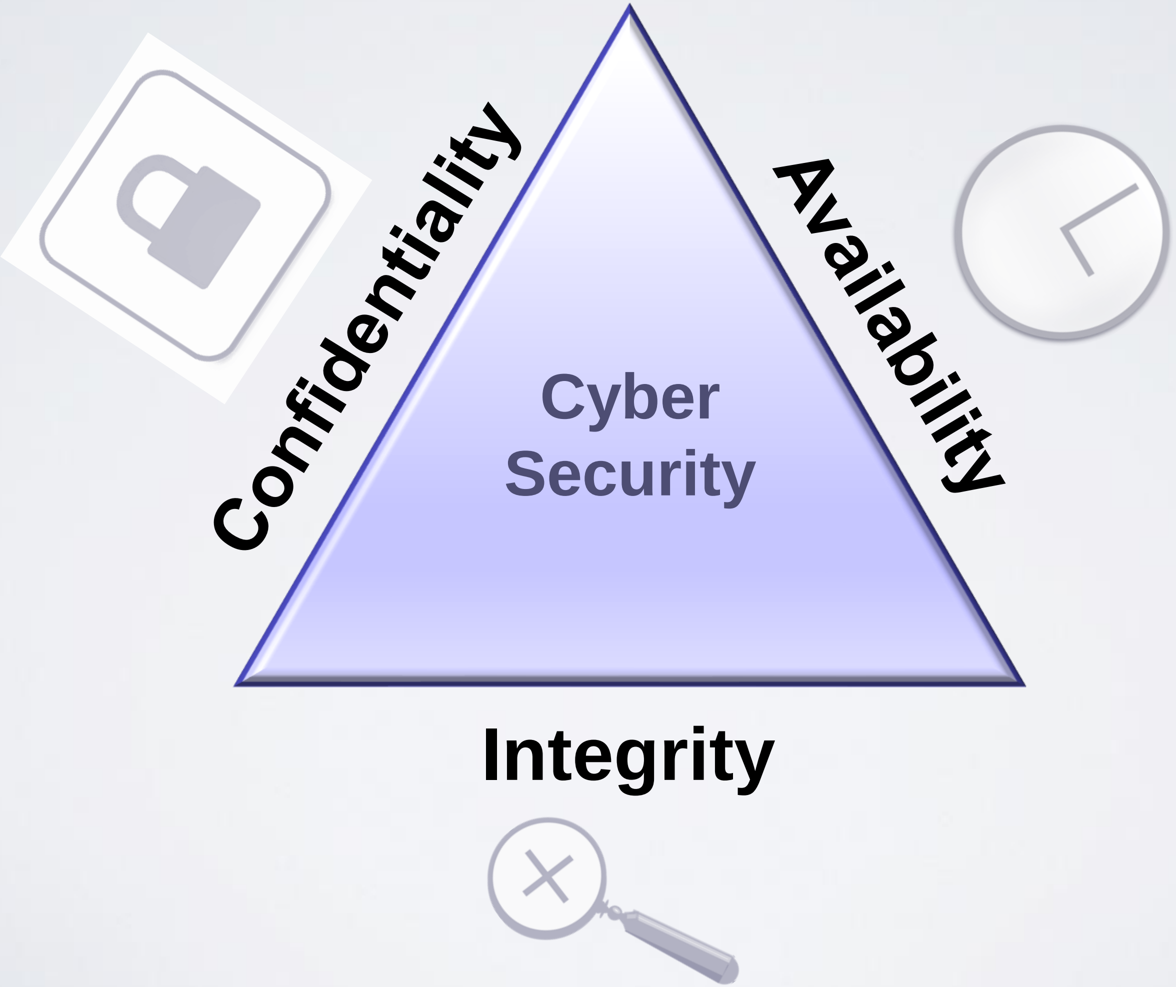
ISO27032 – Guidelines for Cyber Security
July 2012

Information security or cyber security?

“The advance of technology allows home owners to integrate home security systems, hot water geysers, fridges, stoves, televisions and other appliances with web-based management systems. Unfortunately, the increased convenience of managing one’s home via the web is accompanied by the increased risk that someone might gain unauthorised access to such systems and cause harm. This harm could range from “pranks” like turning off the hot water, to serious crimes like turning off the security system in order to burgle the home.”

Basic Cybersecurity requirements

The CIA triad



Example

An ATM has tools that cover all three principles of the triad:

- It provides **confidentiality** by requiring two-factor authentication (both a physical card and a PIN code) before allowing access to data
- The ATM and bank software enforce data **integrity** by ensuring that any transfers or withdrawals made via the machine are reflected in the accounting for the user's bank account
- The machine provides **availability** because it's in a public place and is accessible even when the bank branch is closed

CIA triad - Example 1

- Menti
- Identify which principle in CIA triad address the following loss:

“A rejected contract programmer, intent on sabotage, removed the name of a data file from the file directories in a credit union’s computer. Users of the computer and the data file no longer had the file available to them because the computer operating system recognizes the existence of information available for users only if it is named in the file directories. The credit union was shut down for two weeks while another programmer was brought in to find and correct the problem so that the file would be available. The perpetrator was eventually convicted of computer crime.” [Source: “Toward a new framework for information security”]

CIA triad - Example 2

- Menti
- Identify which principle in CIA triad address the following loss:

“We have discovered that between April 17 and April 19, 2011, certain PlayStation Network and Qriocity service user account information was compromised in connection with an illegal and unauthorized intrusion into our network.

Although we are still investigating the details of this incident, we believe that an unauthorized person has obtained the following information that you provided: name, address (city, state, zip), country, email address, birthdate, PlayStation Network/Qriocity password and login, and handle/PSN online ID....” [3]

CIA triad - Example 3

- Menti
- Identify which principle in CIA triad address the following loss:

In 2016, the hackers breached the systems of the World Anti-Doping Agency and released the medical data of many famous athletes. However, investigators discovered that much of this data was altered before release. [Source: https://www.zettaset.com/blog/data-integrity-attacks-data-manipulation-more-dangerous]

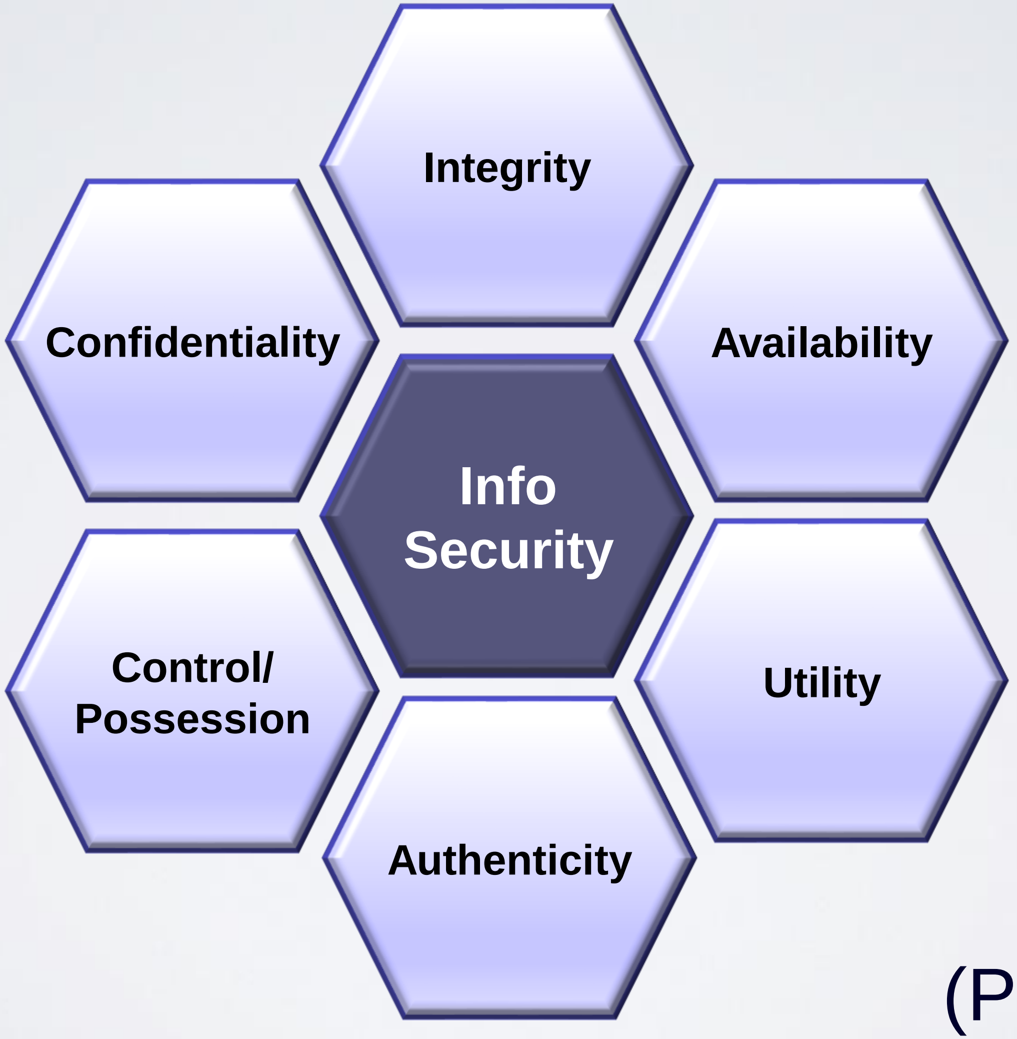
CIA triad - Security by design

Identify CIA requirements of your product in comp1004:

1. Choose 1 COMP1004 project
2. Describe the project in 1 sentence
3. Identify how it should cover C, I, A in CIA triad

Basic Cybersecurity

The Parkerian Hexad



(Parker, 1998)

Example

A company laptop is stolen. Fortunately, the laptop does not contain any critical information. The disk is encrypted. CIA cannot reflect this scenario, which is about loss of control/ possession.

The system is design to be very secure. They ask the users to remember and provide 20 characters password. It is not usable and can lead to the user to write down the password.

Alice sends Bob a message without signature, asking a friend to transfer some money. Later on, when Bob reminds, she denies me and Bob could not prove anything. It is the loss of authenticity or non-repudiation.

Parkerian Hexad – Example 1

- Menti
- Identify which principle(s) in Parkerian Hexad address the following loss:

“A gang of burglars aided a disgruntled, recently fired operations supervisor broke into a computer center and stole tapes and disks containing the company’s master files. They also raided the backup facility and stole all backup copies of the files. They then held the materials for ransom in an extortion attempt against the company. The company was unable to continue business operations” [Source: “Toward a new framework for information security”]

Parkerian Hexad – Example 2

- Menti
- Identify which principle(s) in Parkerian Hexad address the following loss:

“An employee routinely encrypted the only copy of valuable information stored in his organization’s computer and accidentally erased the encryption key. The usefulness of the information was lost and could be restored only through difficult cryptanalysis.” [Source: “Toward a new framework for information security”]

Parkerian Hexad – Example 3

- Menti
- Identify which principle(s) in Parkerian Hexad address the following loss:

Bob’s manager Alice is traveling abroad to give a sales presentation. Bob receives an e-mail with the following message: “Bob, I just arrived and the airline lost my luggage. Would you please send me the technical specifications for our new product asap? Thanks, Alice.” Bob sends the document without noticing that the email is sent from a personal email starting with “alice”.

Parkerian Hexad – Security by design

- *Consider how a company might deliver packages by drones. As a security engineer for the company, what Parkerian Hexad principle(s) violation risks can you identify?*

Ref: Sherman, Alan T., et al. "Cybersecurity: Exploring core concepts through six scenarios." *Cryptologia* 42.4 (2018): 337-377.

CIA AA…?

- Confidentiality
- Integrity
- Availability

- Authentication
- Authorisation
- Accountability

CIA AAA – Examples

- Menti
- Identify which A(s) in AAA addresses the following:

Example 1: Alice can log in her email with the correct username and password

Example 2: A computing student can use the university card to enter SMB101 lab, but a psychology student cannot enter the lab.

Example 3: Every entry to SMB101 is recorded by the card reader and the cameras inside the room.

Safeguarding the principles

Countermeasure	Confidentiality	Integrity	Availability
Passwords	✓	✓	
Data Encryption	✓		
Backup of data			✓
Anti-virus software	✓	✓	✓
Firewall	✓	✓	✓
Intrusion Detection	✓	✓	

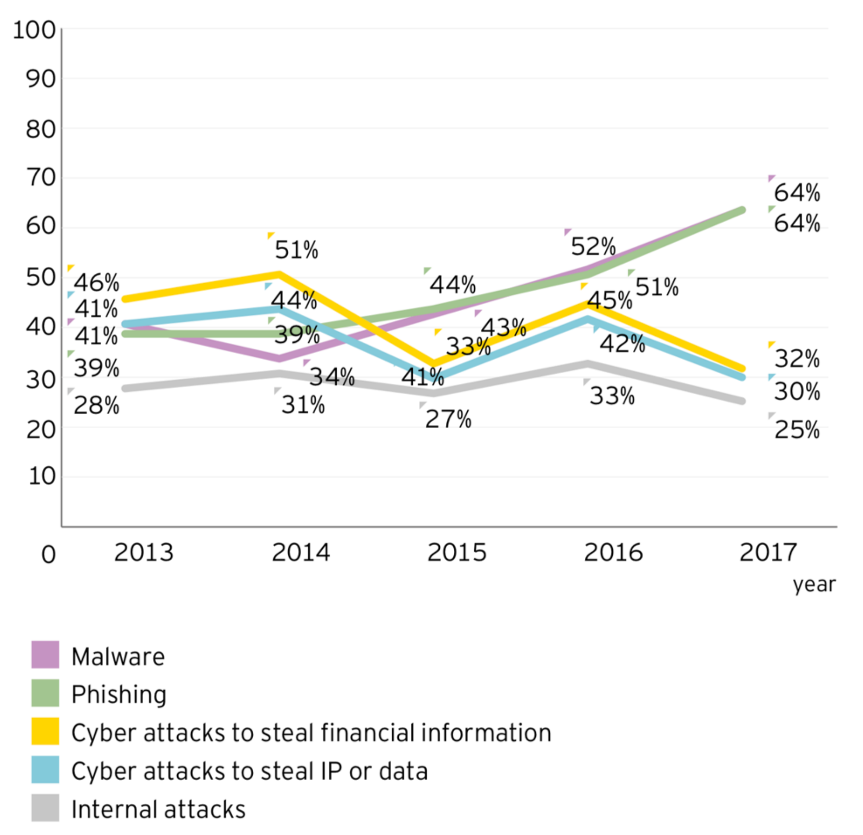
Defining Security

Information security: The preservation of confidentiality, integrity and availability of information. In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved

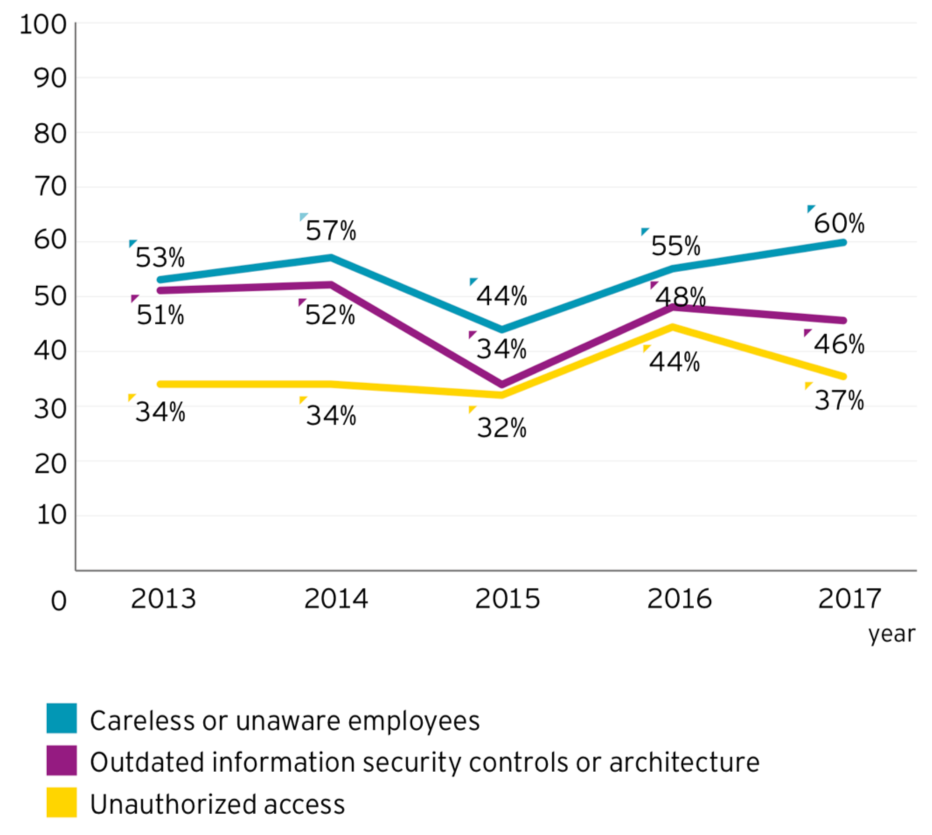
International Organization for Standardization
ISO/IEC 27000 - Overview and Vocabulary, 2016

Top-rated issues

Threats

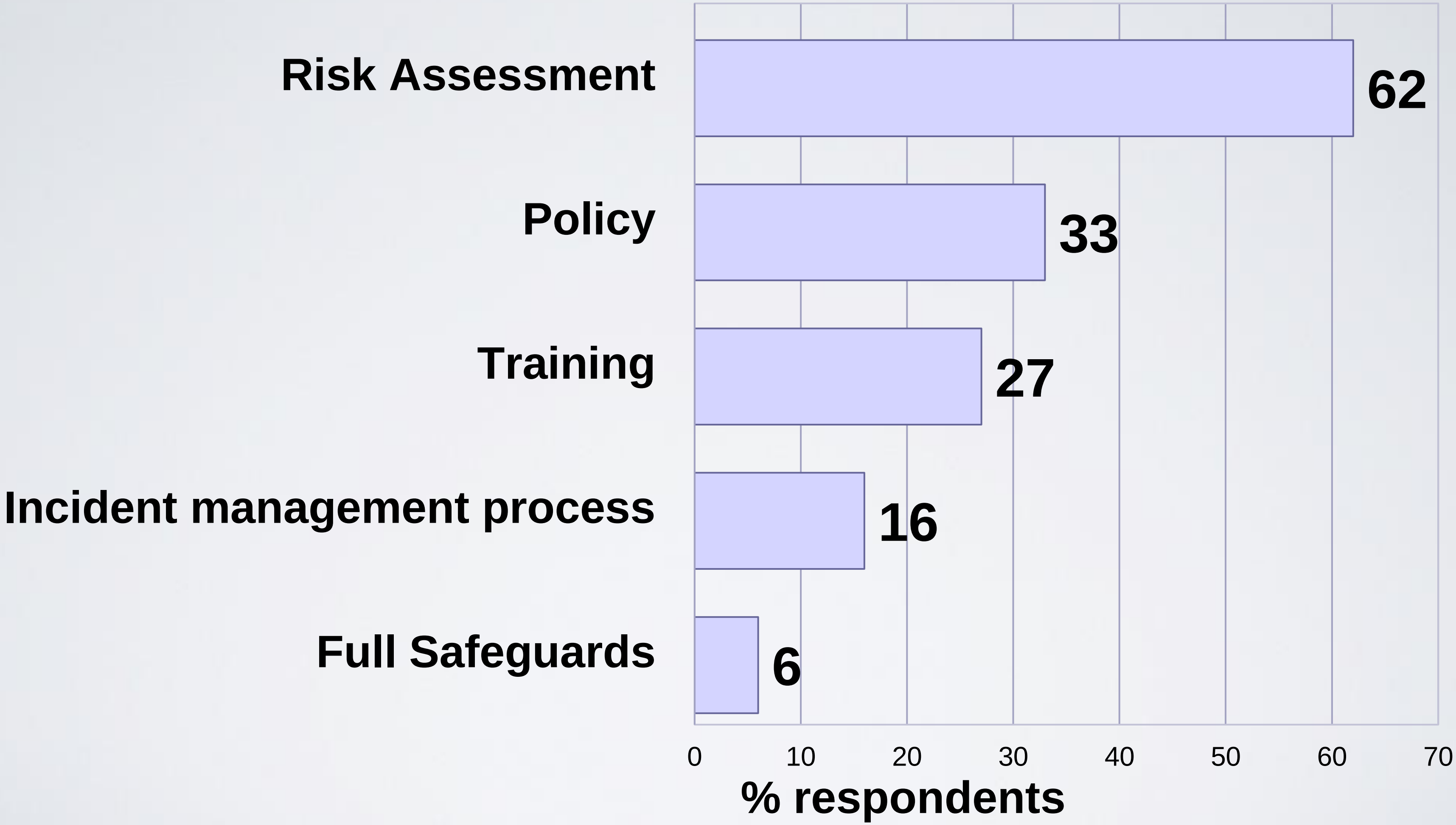


Vulnerabilities



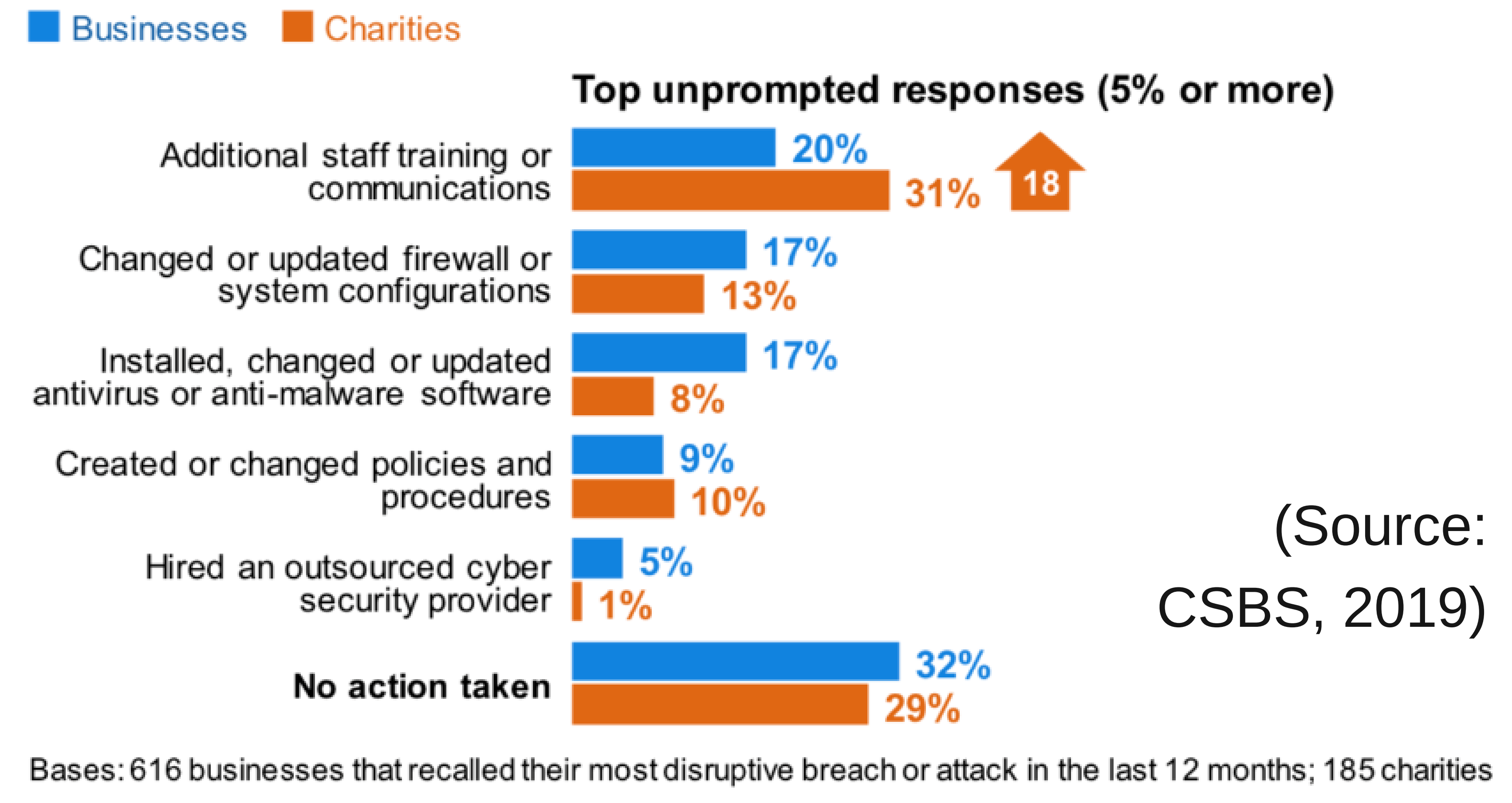
(EY GISS, 2013-17)

So, what do we do … proactively?



(CSBS, 2019)

And what do we do … reactively?



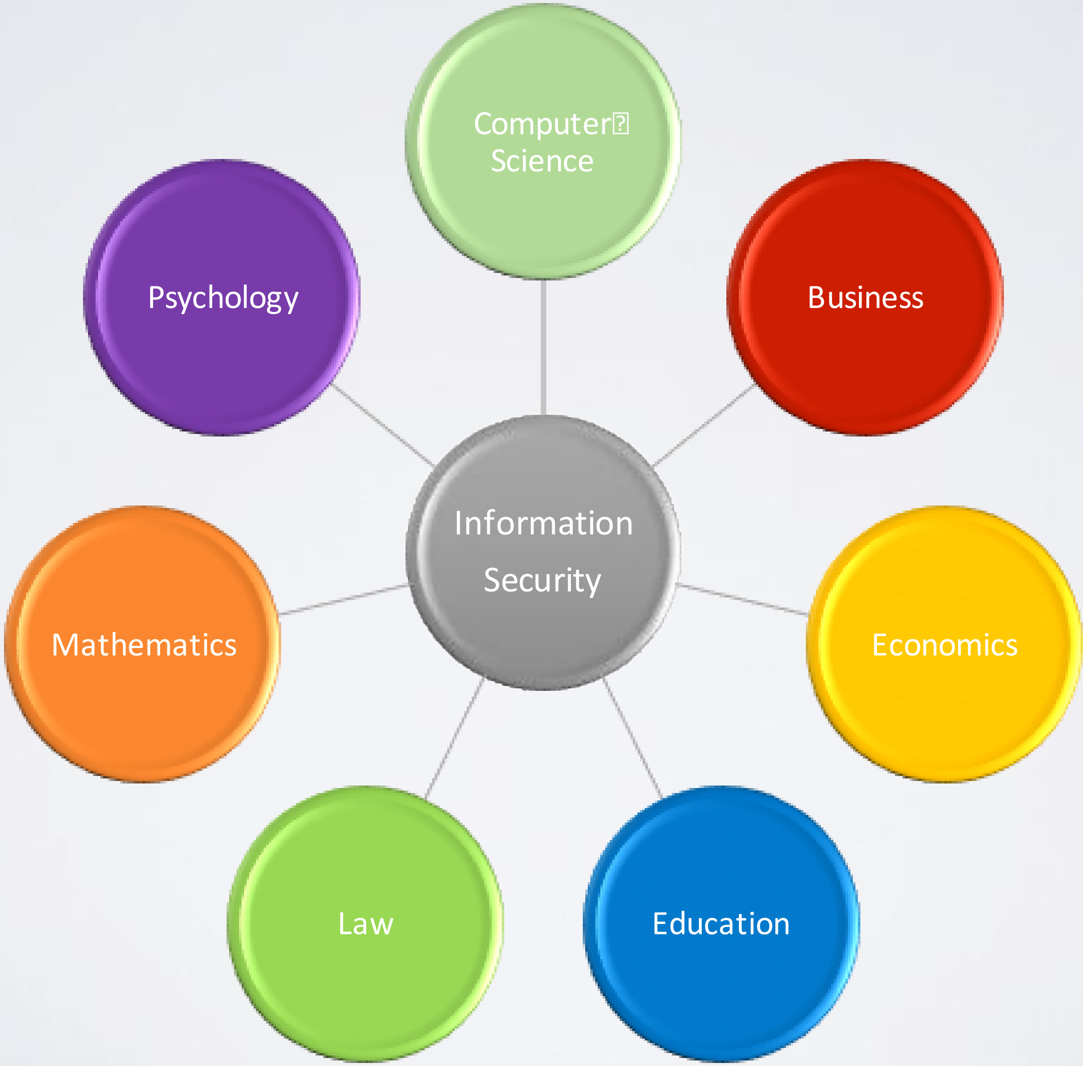
Bases: 616 businesses that recalled their most disruptive breach or attack in the last 12 months; 185 charities

(Source: CSBS, 2019)

- Responses to most disruptive breaches
- The top responses are potentially things that could/should have been done earlier

Security Perspectives

What disciplines contribute to information security?



Computer
Science

Psychology

Business

Information
Security

Mathematics

Economics

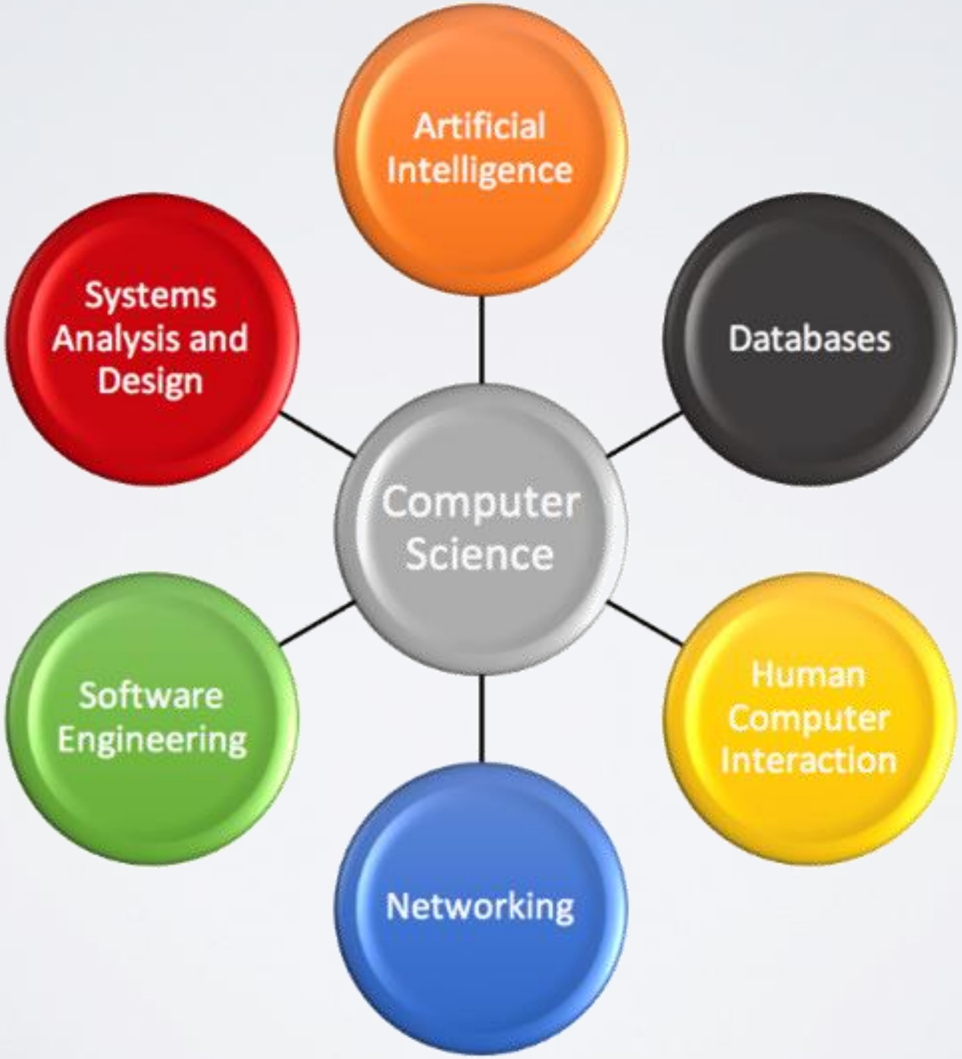
Law

Education

Relevant disciplines

- **Business** - appreciating the organisational context in which protection is required, and the importance of security in areas such as maintaining brand reputation, supporting business continuity, and minimising business risk
- **Economics** - understanding the value of security controls relative to costs of exposure, and linking to factors such as return on (security) investment
- **Education** - supporting areas such as user awareness and training, each being steps towards the boarder goal of achieving a security culture amongst the staff community
- **Law** - recognising the laws that require us to preserve security, and those relevant in response to incidents; linking to criminology in relation to understanding the nature and motivation of attackers
- **Mathematics** – providing the underpinnings for a variety of security techniques, including cryptography and access control
- **Psychology** – helping us to understand how users perceive issues such as security and trust; predicting how users may behave in risk scenarios and factors that may influence their responses

What parts of ‘computer science’ are security-relevant?



Security-relevant computing

- **Artificial Intelligence** – potential to aid security technologies and decision processes (e.g. identifying and responding to suspected intrusions by spotting patterns of anomalous behaviour)
- **Databases** – often used to store the most valuable asset (the data), the security considerations include preventing unauthorised disclosure and modification of the stored data
- **Human Computer Interaction** – This links to a requirement for systems to be understandable and useable (making them more tolerable, reducing mistakes)
- **Networking** – much of our data is sent over the network, and network connections establish paths between the systems we are seeking to protect
- **Software Engineering** – many vulnerabilities occur as a result of the way code was written, thus requiring security-aware coding practices
- **Systems Analysis and Design** – Security needs to be considered within the specification and design of new systems, so it is incorporated from the outset rather than needing to be retrofitted later

Secure-aware coding practice example

- OWASP Secure Coding Practices Quick Reference Guide
- Example:

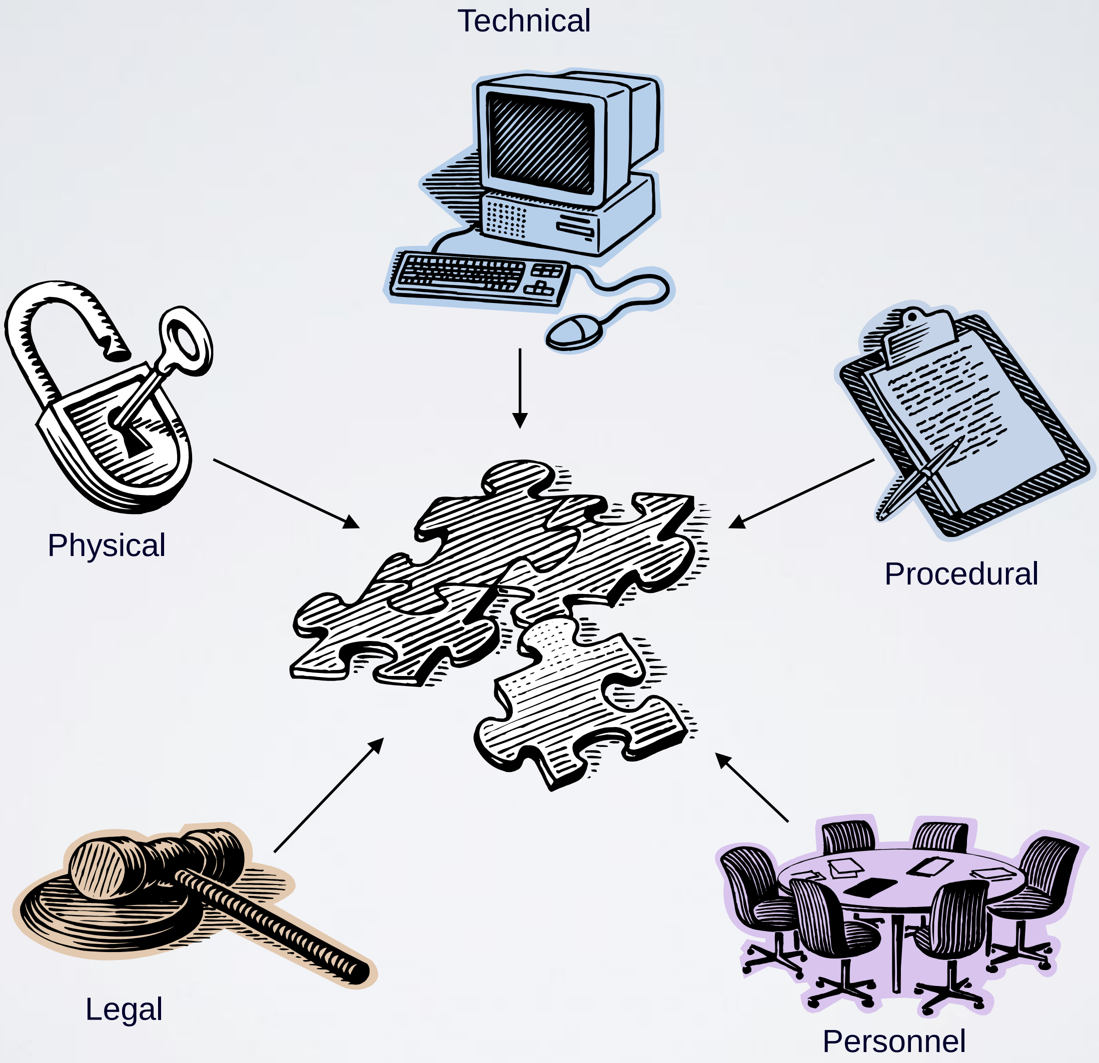
□ Require authentication for all pages and resources, except those specifically intended to be public

□ Use a centralized implementation for all authentication controls, including libraries that call external authentication services

□ Segregate authentication logic from the resource being requested and use redirection to and from the centralized authentication control

□ All authentication controls should fail securely

The Security Jigsaw



Technical

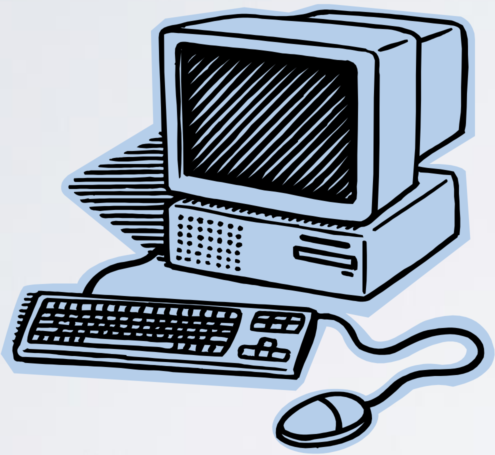
Physical

Procedural

Legal

Personnel

Technical Security



- System-based safeguards, such as:
  - authentication
  - access control
  - anti-virus protection
  - data encryption

Physical Security

- Issues such as:
  - physical access to systems
  - protection against theft
  - safeguards against fire, flood, and other environmental incidents

Procedural Security

- Issues such as:
  - the need for a security policy
  - conducting risk assessment
  - disaster planning and recovery
  - asset management

Personnel Security

- Controls relating to the people that use systems, such as:
  - recruitment procedures (e.g. checking references)
  - training and awareness programmes
  - termination procedures

Legal Security

- Issues such as:
  - the need to comply with relevant legislation (e.g. data protection law)
  - the need for awareness of laws that might become relevant as a result of a breach (e.g. computer crime and misuse)

Saltzer and Schroeder’s Design Principles (1975) [4]

- Economy of mechanism: Keep the design as simple and small as possible.
- Fail-safe defaults: Base access decisions on permission rather than exclusion.
- Complete mediation: Every access to every object must be checked for authority.
- Open Design: The design should not be secret.
- Separation of privilege: Where feasible, a protection mechanism that requires two keys to unlock it is more robust and flexible than one that allows access to the presenter of only a single key.
- Least privilege: Every program and every user of the system should operate using the least set of privileges necessary to complete the job.
- Least common mechanism: Minimize the amount of mechanism common to more than one user and depended on by all users.
- Psychological acceptability: It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.
- Work factor: Compare the cost of circumventing the mechanism with the resources of a potential attacker.
- Compromise recording: It is sometimes suggested that mechanisms that reliably record that a compromise of information has occurred can be used in place of more elaborate mechanisms that completely prevent loss.

Economy of mechanism

- Menti
- The *ident* protocol sends the user name associated with a process that has a TCP connection to a remote host. Suppose host A wants to know the name of the user who is connecting to its TCP port 23 (Telnet) from the client's (host B) port 6191. Host A would then open a connection to the ident service on host B, and issue the following query: 6191, 23. host B can unambiguously identify the program that has initiated the specified connection to host A's port 23, should it exist. Host B would then issue a response, identifying the user ("stjohns" in this example) who owns the program that initiated this connection and the name of its local operating system: 6193, 23 : USERID : UNIX : stjohns. A program X on host *A* allows access based on the results of an ident protocol result. Which design of X is more secure?

a. X makes the assumption that the originating host (B) is trustworthy

b. X does not make the assumption that the originating host is trustworthy

Fail-safe defaults

- Menti
- Look at the following (pseudo) code and select more secure code

(a)

```
DWORD dwRet = IsAccessAllowed(...);
if (dwRet == ERROR_ACCESS_DENIED) {      // Security check
 failed      // Inform user that access is denied
} else {      // Security check OK      // Perform task }
```

(b)

```
DWORD dwRet = IsAccessAllowed(...);
if (dwRet == NO_ERROR) {      // Security check OK      // Perform
 task
} else {      // Security check failed      // Inform user that access is
denied }
```

Complete mediation

- A developer needs to implement input validation for a web application. Which is good practice(s)?

a. The validation is performed in each area of the code that uses externally-controlled input.

b. Centralize all input validation, store these validated inputs in a separate data structure, and require that all access of those inputs must be through that data structure.

c. Use an external input validation framework such as Struts, which performs the validation before the inputs are ever processed by the code.

Open design

- Menti
- Look at the following products and choose which to buy
  a. A hard drive which support to encrypt files using AES (Advanced Encryption Standard) encryption algorithm
  b. A hard drive which support to encrypt files using an encryption algorithm which is created and kept secret by the selling company

Least privilege

- Menti
- Look at the following procedure and choose one with least privilege
  a. Anyone with staff card can enter any room in the company
  b. Staff can enter common rooms and personal room, but cannot enter the other rooms.

Separation of privilege

- Menti
- Look at the following procedure and choose one with separation of privilege
  a. Company checks for over $75,000 need to be signed by one senior officer of the company
  b. Company checks for over $75,000 must be signed by two officers of the company. If either does not sign, the check is not valid. The two conditions are the signatures of both officers.

Separation of privilege

- Menti
- Look at the following functionality design and choose one with separation of privilege
  a. Support two modes: file access, non-access
  b. Support: non-access, file read access, file write access, file execute access, file delete access

Least Common Mechanism

- Menti
- Choose one with least common mechanism
  a. Run web server in a virtual machine or a container
  b. Run web server in a computer which also hosts databases

Psychological acceptability

- Menti
- When a user supplies the wrong password during login, the system should

a. reject the attempt without any message

b. reject the attempt with a message stating that the password was incorrect

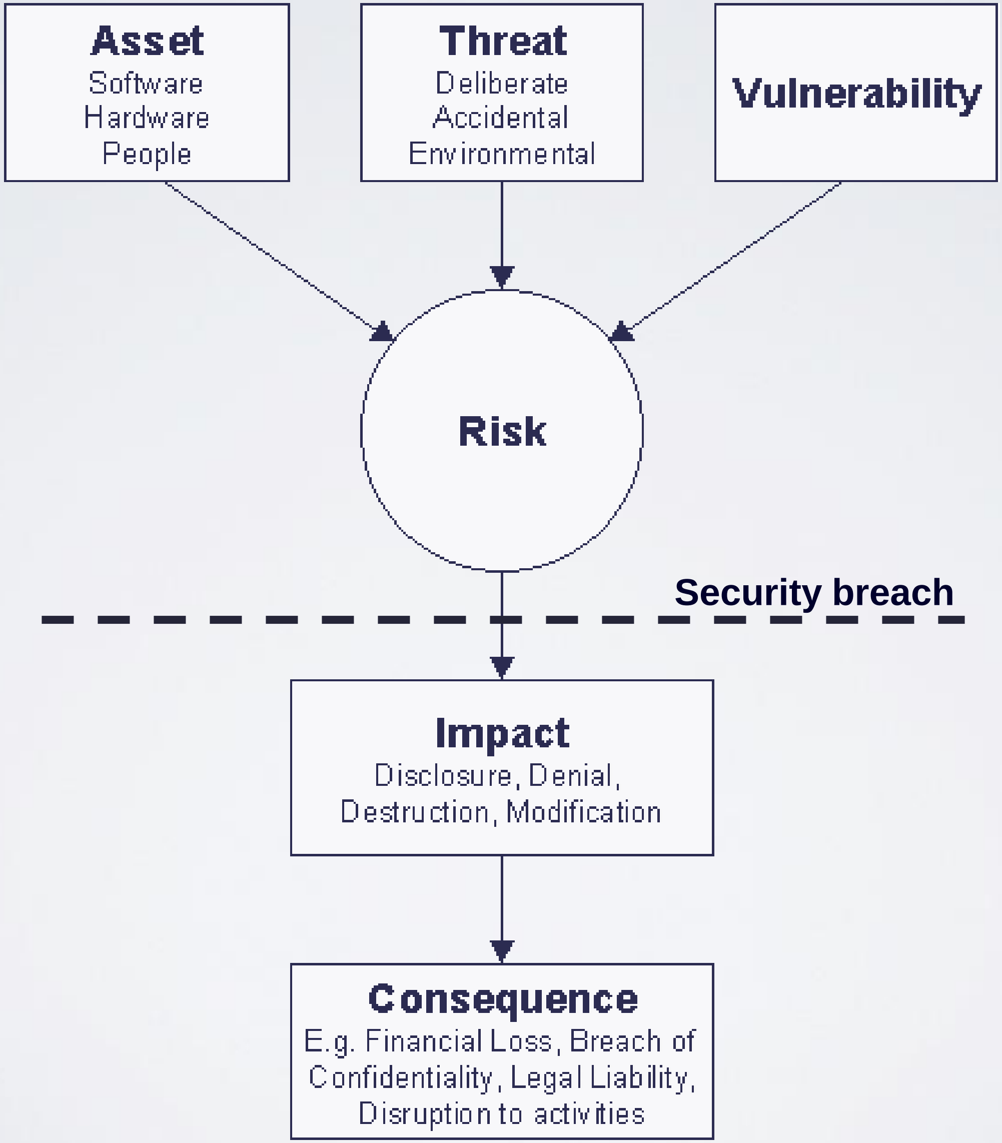
c. reject the attempt with a message stating that the login failed

Compromise recording example

- The servers in an office network may keep logs for all accesses to files, all emails sent and received, and all browsing sessions on the web.
- Internet-connected surveillance cameras are a typical example of a compromise recording system that can be placed to protect a building.

Risk Assessment

Visualising the problem



Asset
Software
Hardware
People

Threat
Deliberate
Accidental
Environmental

Vulnerability

Risk

Security breach

Impact
Disclosure, Denial,
Destruction, Modification

Consequence
E.g. Financial Loss, Breach of
Confidentiality, Legal Liability,
Disruption to activities

Terminology

- *Asset*
  - Everything and everybody forming part of an information system.
- *Threat*
  - A potential violation of security
- *Vulnerability*
  - The likelihood of a threat to become a reality

Threats

Accidental or Deliberate

CAUTION DO NOT ENTER

Physical
e.g. fire,
flood,
power failure

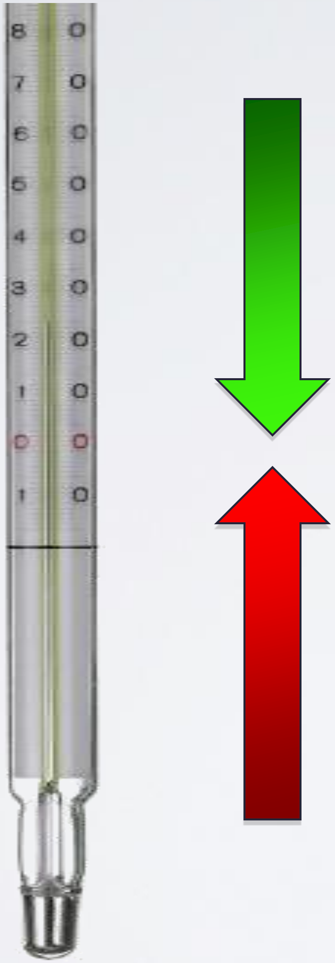
Human
e.g. operator errors,
misuse of resources,
hacking, malware.

Equipment
e.g. CPU,
network,
storage failure

More Terminology

- *Risk*
  - Threats and vulnerabilities of a particular asset
  - Traditionally viewed as Probability X Impact
- *Countermeasure*
  - A mechanism or procedure used to reduce one or more elements of risk
- *Impact*
  - The effect of a failure to preserve confidentiality, integrity and/or availability

The Risk ‘Temperature’



Countermeasures

Threats

Recognising your information assets

- Menti activity…

- Think about the information you have at home:
  - How much of it has value?
  - What makes it valuable?
  - Can you rank in order of importance?
  - What could go wrong?
  - How do you protect it?

Impact Types

The effects of a failure to preserve CIA :

- Disclosure
- Denial
- Destruction
- Modification

relate to *availability*

with particular consequences

Consequences

- Financial Loss
- Embarrassment
- Breach of Commercial Confidentiality
- Breach of Personal Privacy
- Legal Liability
- Disruption to activities
- Threat to personal safety

Examples

Identify asset, threat, vulnerability, consequences in the following risk scenarios

1. Attacker performs an SQL injection on an unpatched legacy web application to download sensitive patient medical records.
2. Internal staff makes a fraudulent payment instruction exceeding bank account balance on the payment system with no set limit, resulting in a bank overdraft.

Example

3. Unauthorised employee accesses the SCADA server using default login credentials and execute shutdown command to disrupt the water supply to the entire east side of Singapore.
4. Attacker delivers spear-phishing email to unsuspecting user, which when clicked, triggers the user account to perform SMB authentication with malicious server and discloses hashed credentials.

Risk identification - example

Using the project in COMP1004, identify and describe the risk scenarios. Each scenario should include the asset, vulnerability, threat and consequence.

Conclusion

- Security is a multi-faceted problem
  - Many definitions
  - Many perspectives
  - Many threats, vulnerabilities and potential impacts
- This leads to a complex issue in terms of the resulting security management

UNIVERSITY OF PLYMOUTH

Dr Hai-Van Dang

Centre for Security, Communications & Network Research

www.plymouth.ac.uk/cscan