



THE UNIVERSITY
OF QUEENSLAND
AUSTRALIA

CREATE CHANGE

Business Information Security

Week 01: Introduction to Information Security

Dr Alex Pudmenzky

Semester 2, 2024

Overview

- Course staff
- Textbook
- Discussion board
- Consultation
- Assignment 1
- History
- Computer networks
- Network devices
- Defining security
- Security model
- Balance security vs access
- Security professionals
- Data responsibilities

Some things about myself...



Cologne Cathedral

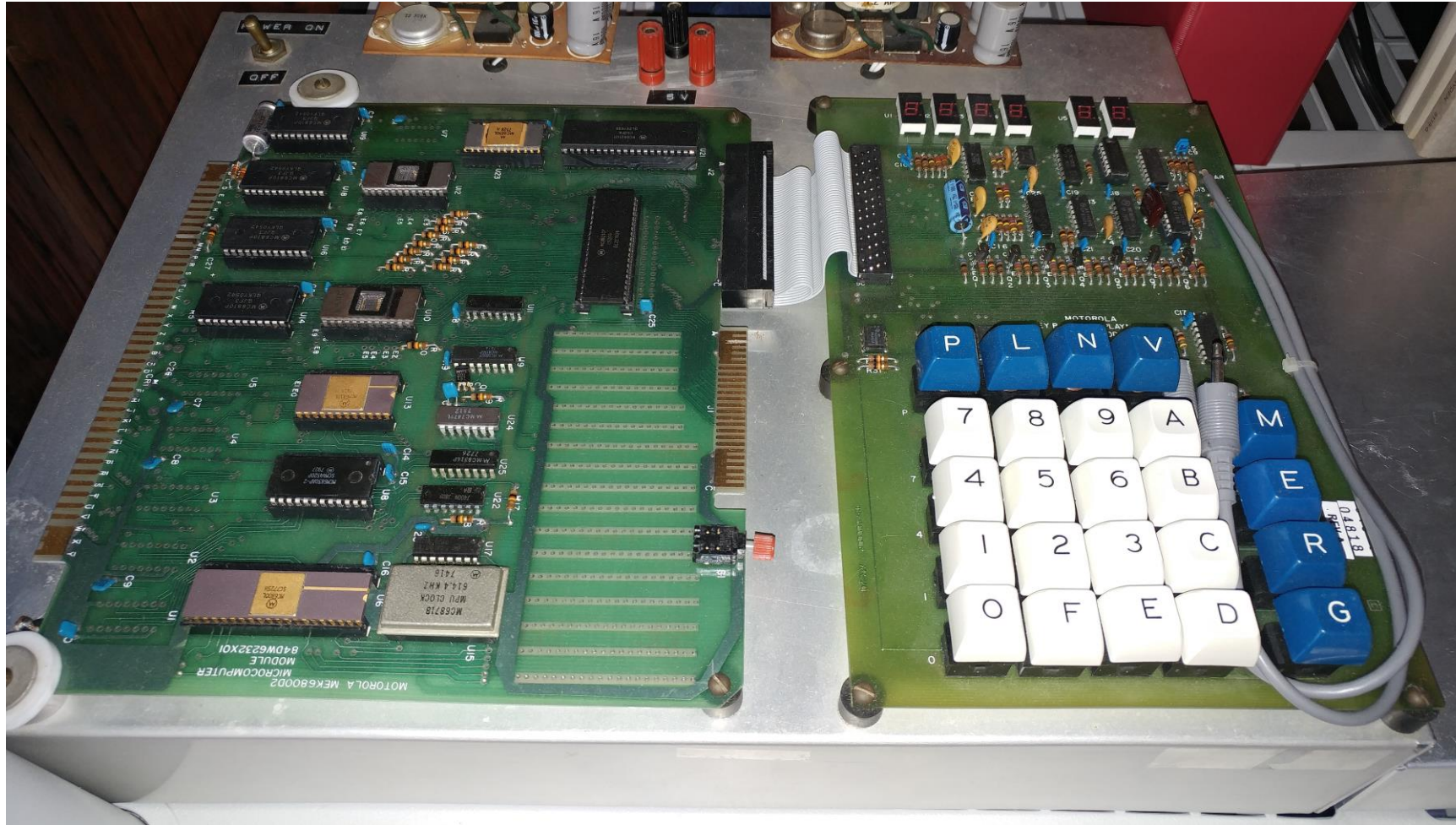


Some things about myself...



Apprenticeship at Bayer HQ (11 square kilometers, 48,000 people)

Some things about myself...



UG degree in Process Engineering
Final thesis: Motorola 6800 Development Kit to control temperature in a heat chamber

Some things about myself...

- Private Industry
- Qld Government
- Universities

...all in IT



Runge
Mining Associates



Some things about myself...



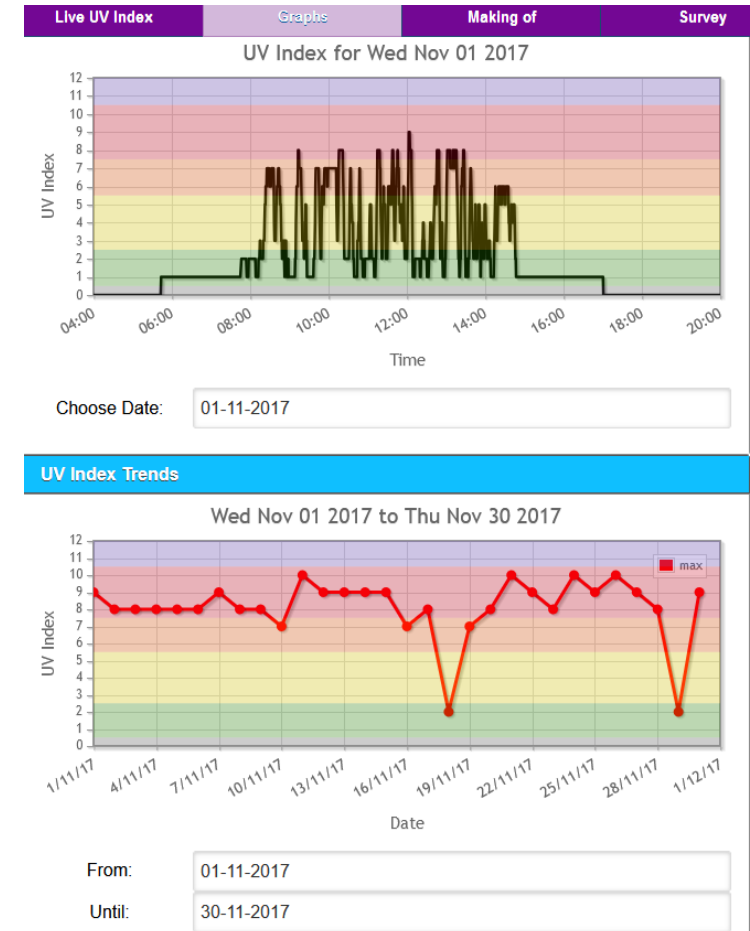
Some things about myself...



Design Exhibition at UQ Hall, industry clients are pitching the designs of their 1st semester teams to the 2nd semester build students (<https://alexpudmenzky.com/studio3>).

Some things about myself...

UQ Smart Campus Final Year
Thesis projects using IoT
devices connected to
LoRaWAN access points
(<https://smartcity.uqcloud.net>).



UV index display panel thesis project: Installation of the sign on 10 October 2017.

About the course

Course staff

- **Dr Alex Pudmenzky** (course coordinator and lecturer)
- **Mr. Daniel Lewis** (tutor)

Textbook (optional)

- Michael E. Whitman and Herbert J. Mattord (2017). *Principles of Information Security* (7th Edition). Course Technology CENGAGE Learning.
(available as e-book and paper-based book at UQ Library).

Ed Discussion Board (via Blackboard)

- We're using Ed Discussion for questions and discussion about:
 - **General topics** (for example: curricular or administrative questions)
 - **Seminar** (for example: about the content in our weekly seminars)
 - **Assignments** (for example: about the requirements or questions themselves)
 - **Social** (for example: for social interactions with staff or students)
- You will get **faster answers** here from staff and peers than through email (please only email us in exceptional circumstances, e.g. personal matters)
- **Search before you post** (if your question has already been raised and answered)
- **Anonymous** posting and comments available (that means you can hide your real name)
- **Private posting for personal matters** available (that means your question is visible to course staff only)

Office Hours / Consultation via Zoom

- Consultation hours are **available on Blackboard** (under *Course Staff*)
- We may suggest to contact us via Zoom and email you a Zoom link then
- Please be aware that other students may be in the queue before you, and you may need to wait
- We won't give you the answers to the assignment questions

Assignment 1 (40%)

Four questions with several sub-parts. One question **published every week on Friday afternoon** starting this week. Due **Mon 2 September 2024 3pm** via Turnitin on Bb. Requires own research.

Pay attention to the following:

- The **completeness** of the answer - does the answer show that you have grasped the full meaning of the question, and that you have included **all relevant points** in the answer?
- Have you performed **your own research** in addition to the information presented to you in the course?
- Is the answer presented in plain English **business language**. You must present answers (often discussing technical issues) in terminology/language that is clearly and easily understood by a business analyst/business manager.

Do not learn slides 'by heart' – do not copy slides/information – understand what you are analysing/discussing and express this in your own words.

*Do not answer a question with an 'information dump' – that is, by just writing all you know. Make sure you write "**as much as necessary as short as possible**".*

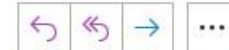
Warning: Educational Material is for Educational Purposes Only




- The material presented in this course is intended solely for educational purposes.
- The course content is not to be used for any malicious or illegal activities, including hacking or unauthorized access to computer systems.
- We strongly condemn any misuse of the knowledge gained from this course.
- Any violation of this policy will result in disciplinary action and may lead to legal consequences.
- As responsible members of the academic community, we expect all students to use the knowledge gained from this course ethically and responsibly.
- Remember that with knowledge comes great responsibility. Use it wisely and for the betterment of society and your present/future workplace.



Office of the Vice-Chancellor and President <noreply@uq.edu.au>
To Alex Pudmenzky



11:06 AM

 If there are problems with how this message is displayed, click here to view it in a web browser.

[View online](#)



A message from the Vice-Chancellor



Dear Alex,

As this year's momentum starts to build and there's increasing activity across our campuses and sites, I wanted to give you an update on recent news from across the UQ community.

Staying cyber aware

Over recent months there has been a growing number of cyber-attacks across Australia, with cyber-criminals using increasingly sophisticated tactics.

While UQ makes a significant investment in our cyber-security controls, many of these attacks involve targeting individuals with phishing attacks. For instance, some of our colleagues have just this week received a fraudulent email from someone pretending to be me.

Given the threat posed by cyber-criminals, I would encourage you to be vigilant, report anything suspicious to our ITS team, and learn what you can do to [protect yourself and UQ online](#).



Professor Deborah Terry AO
Vice-Chancellor and President
The University of Queensland

Recent major events

SolarWinds

Date: December 2020.

SolarWinds issued a normal software update for its Orion network monitoring platform that contained malware. The malware allowed attackers to gain access to the networks of thousands of organizations, including several U.S. government agencies and numerous private companies. Attackers had inserted a backdoor into SolarWinds' product called Orion. When customers downloaded SolarWinds updates, they unwittingly installed a Trojan Horse containing the backdoor. This allowed attackers to access systems running SolarWinds products. The attack persisted undetected for months.

Optus

Date: September 2022.

About 10 million Optus customers (approximately 40% of the population) had personal data stolen in a cyber attack. The breach affected Windows PCs and involved a defect in a recent update. A coding error in Optus' system allowed attackers to exploit vulnerabilities for years before the breach occurred.

Medibank

Date: October 2022.

The personal and highly sensitive information of 9.7 million current and former Medibank customers was stolen and eventually posted on the dark web. The breach was attributed to a lack of basic cybersecurity measures, including multi-factor authentication. An employee of a Medibank contractor saved their username and password to a personal internet browser profile on a work computer. Threat actors stole these credentials and gained access to Medibank's systems.

CrowdStrike

Date: Friday, July 19, 2024.

A global IT outage unfolded due to a single software update by CrowdStrike, a US-based cybersecurity company. The update targeted the Falcon sensor program, which provides cybersecurity features like malware protection, antivirus support, and incident response. Unfortunately, this seemingly innocuous update triggered a logic error that led to an operating system crash on Windows systems worldwide (Mac and Linux users were unaffected). Millions of computers worldwide suddenly displayed the dreaded "Blue Screen of Death," rendering them unusable and unbootable. Importantly, this outage was not caused by a cyber attack. Instead, it was an unintended consequence of a routine software update.

What is Information Security?

"A **well-informed sense of assurance** that the **information risks** and **controls** are **in balance**."

Jim Anderson, Inovant* (2002)

What does this mean?

well-informed sense of assurance = we have an opinion that's based on evidence;

information risks = risk is normally associated with the prospect or the possibility of loss;

controls = anything that reduces risk: business policy, training/education or technology;

in balance = are both the same (\$ gain/loss).

Security professionals must review the origins of this field to understand its impact on our understanding of information security today - let's do this now!

*Inovant is a subsidiary of Visa (<https://www.utc.edu/sites/default/files/2021-06/3600-lecture1-introduction.pdf>)

History of information security - 1940s and 50s

- Computer security began immediately after the first mainframe computers were developed in the 40s and 50s
 - Groups developing code-breaking computations during World War II created the first modern computers
 - Multiple levels of security were implemented
- **Physical controls to limit access to sensitive military locations to authorized personnel**
- Rudimentary in defending against **physical theft, espionage, and sabotage**



The Enigma,
invented: 1918,
used: 1944

The Enigma machine

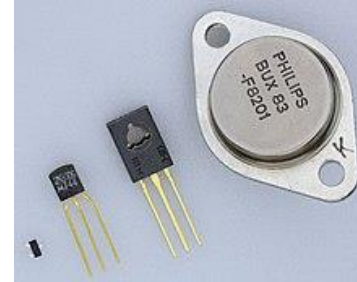
<https://enigma.virtualcolossus.co.uk/VirtualEnigma/index.htm>

<https://piotte13.github.io/enigma-cipher/>

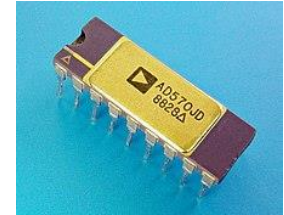
Size of computers driven by size of components



Valve (1904)

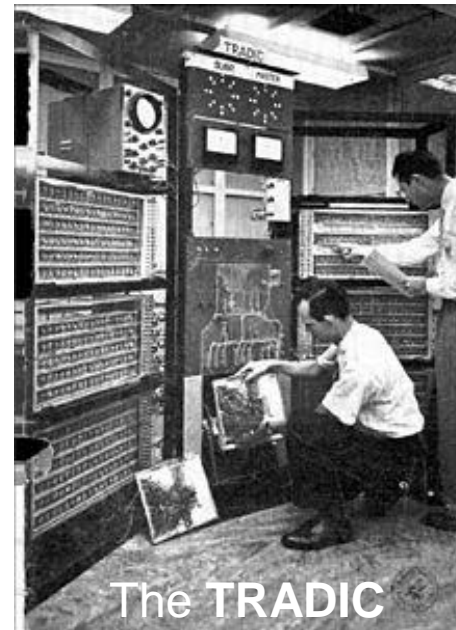


Transistor (1947)



Integrated Circuit (1958)

The 1946
ENIAC
computer used
more than
17,000 vacuum
tubes -
analogue
computer



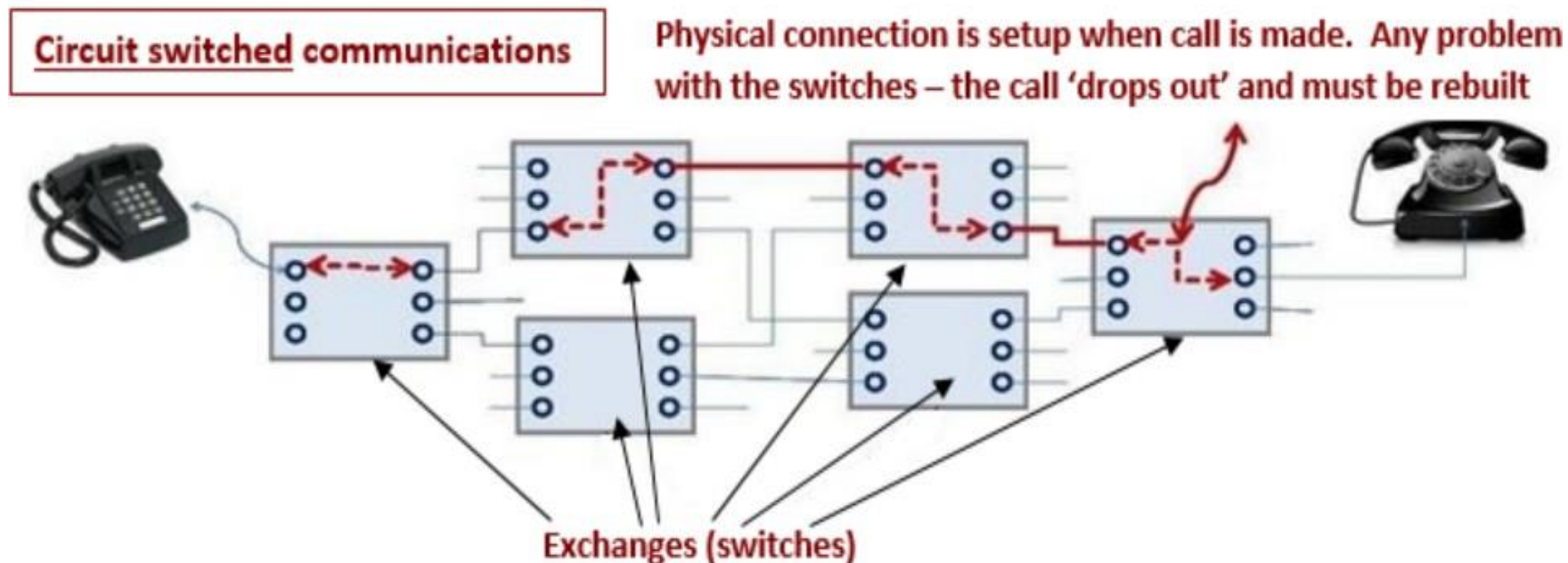
The TRADIC



50 years of
computing at UQ

The 1960s, 70s and 80s – what was the communication model?

- Communications – based on '**circuit switched**' telephony:
 - Very old technology – lots of problems – not at all versatile or 'fault tolerant'
 - Many countries wanted improvement – the US commissioned a research project (effectively ARPANET).

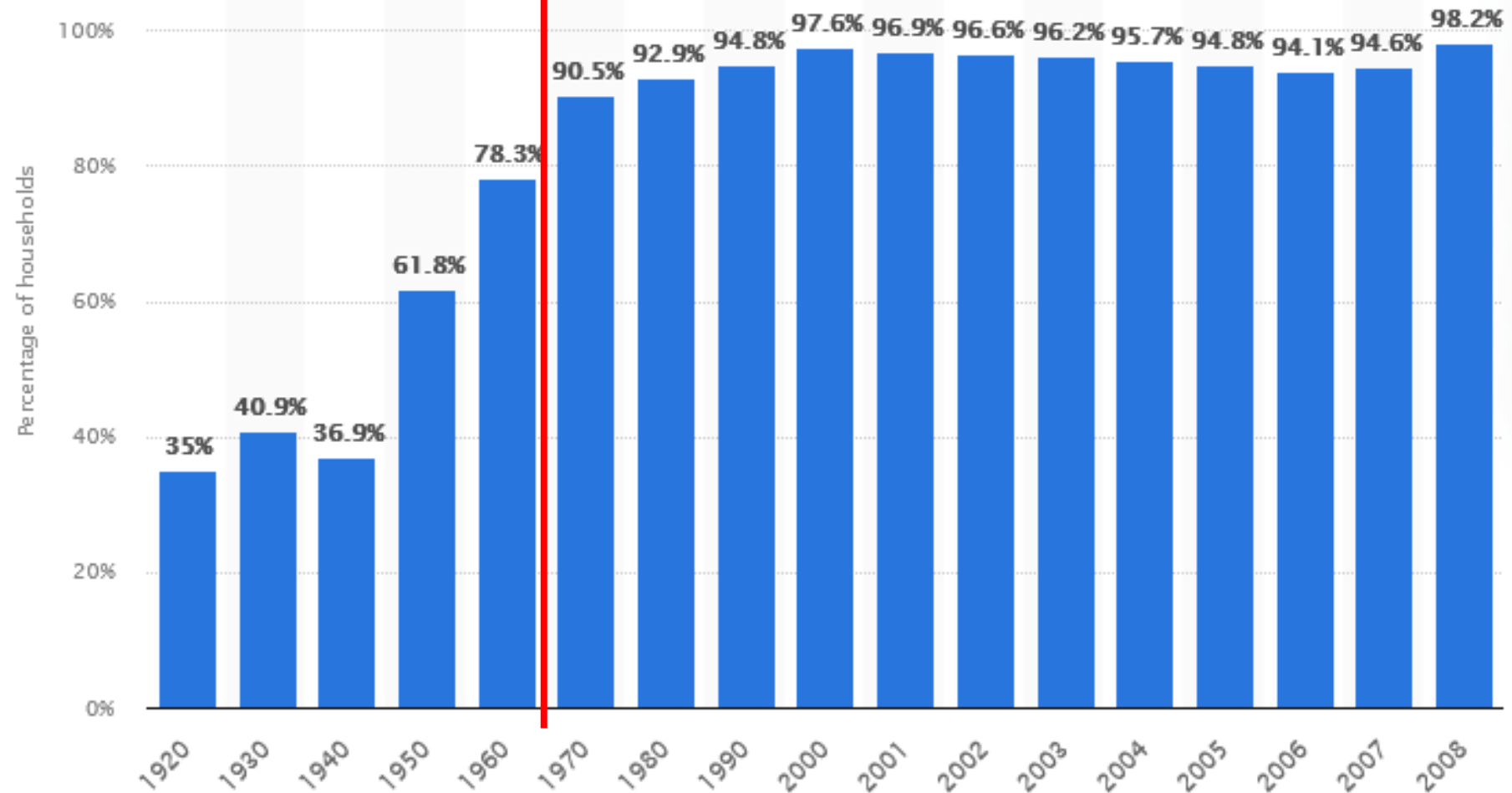






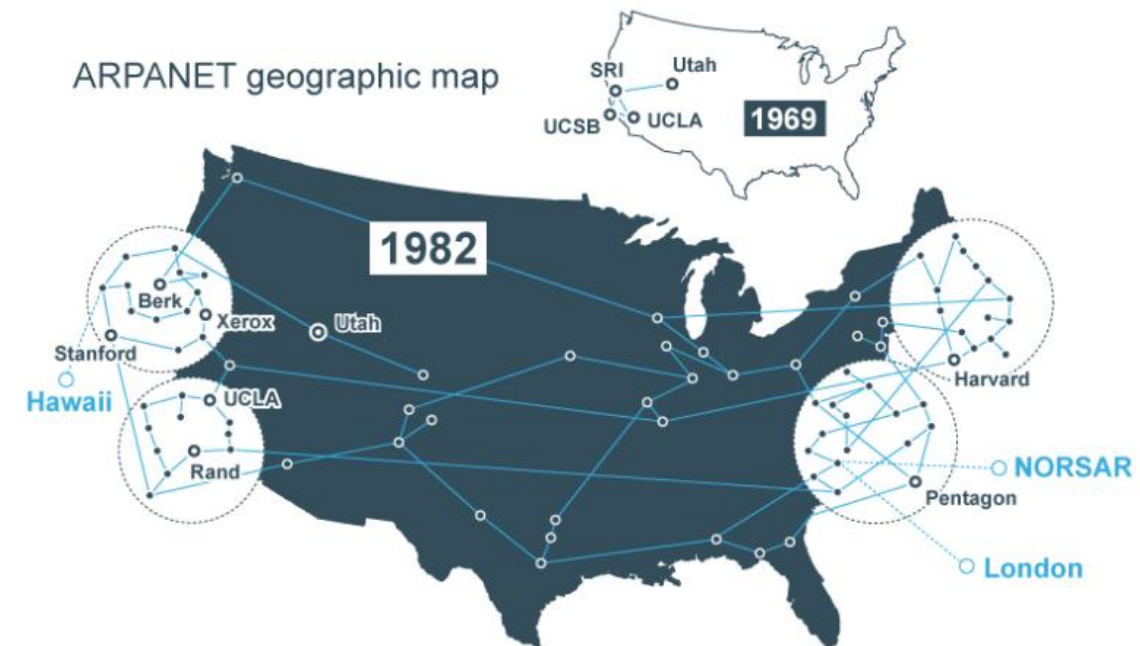
Percentage of housing units with telephones in the USA from 1920 to 2008

Switchboards obsolete in 1967



History of information security - 1960s, 70s and 80s

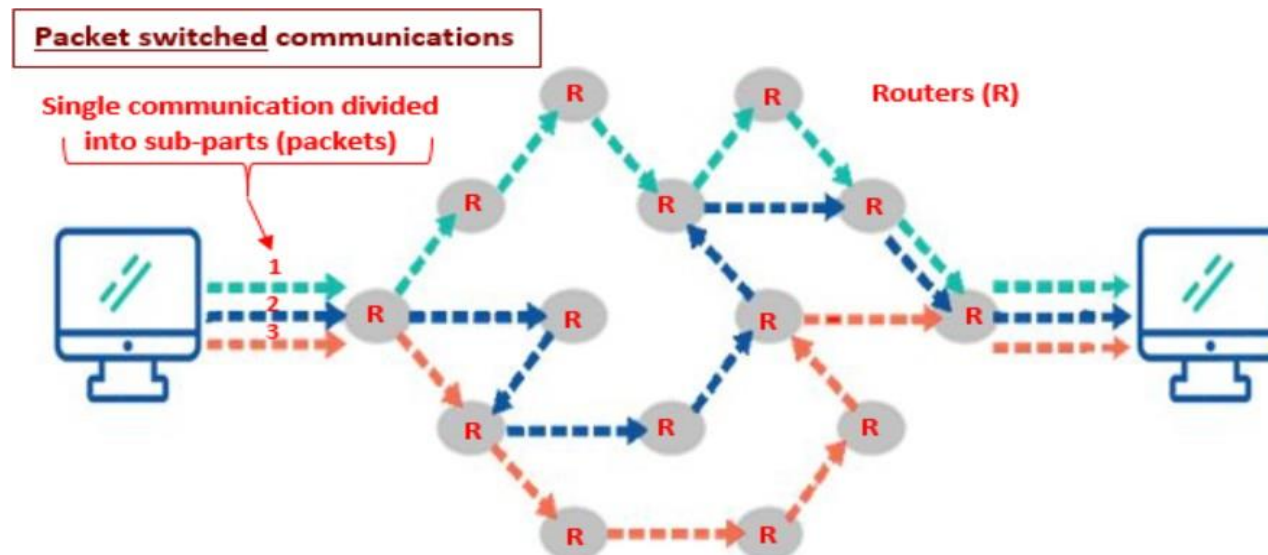
- **Advanced Research Project Agency (ARPA)** began to examine feasibility of redundant networked communications (to improve the existing 'circuit switched' model).
- ARPANET initially **connected four independent network nodes** situated at UCLA, SRI, UCSB, UofU*
- ARPANET – **international** in 1973 with connections to London and Norway.
- Further expansion across the US in 1982 – the foundations of the Internet had been set up!



*University of California, Los Angeles (UCLA), Stanford Research Institute (SRI), the University of California-Santa Barbara (UCSB) and the University of Utah (UofU).

The 1960s, 70s and 80s – networks

- ARPANET moved '**circuit switched**' telephony into '**packet switched**' data communications.
- Some of the main benefits:
 - No single defined physical path between sender – receiver
 - Packets travel independently – no interdependence
 - Supports '*store and forward transmission*' – much greater versatility



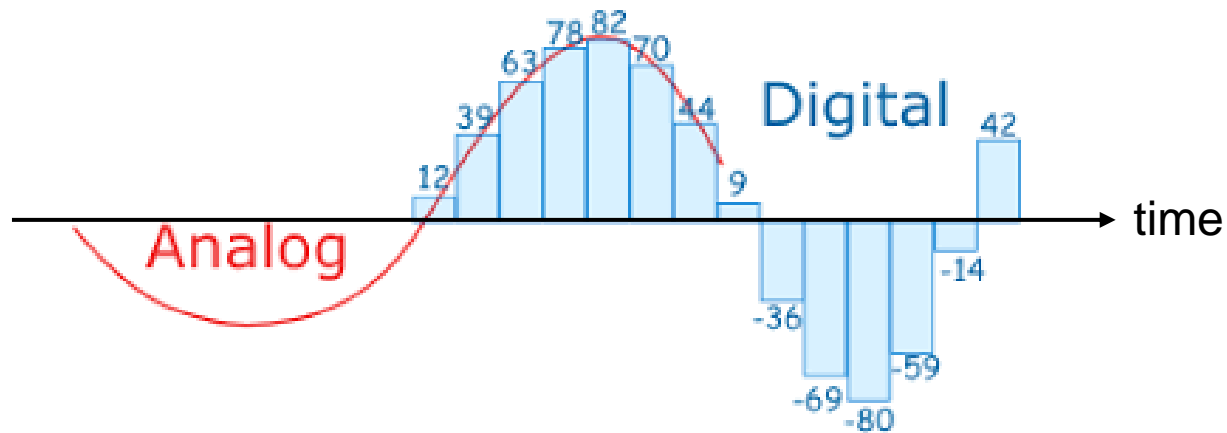
Try DOS commands:
ping uq.edu.au
tracert google.com

Analogue to Digital

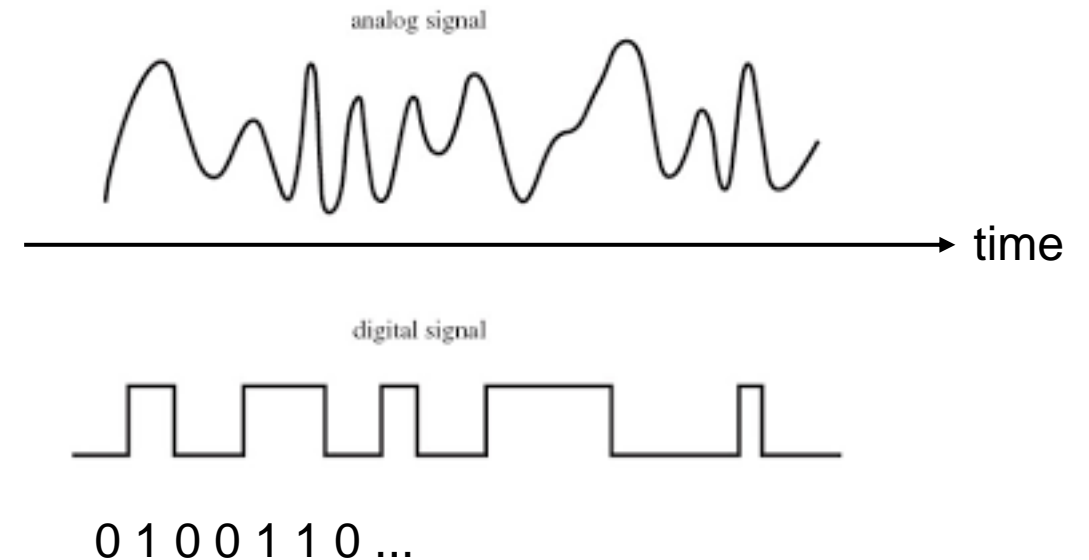


How long is the voltage kept high to signal a “1” in digital communication?

Depends on the data rate, at 1Mbps 1 μ s.



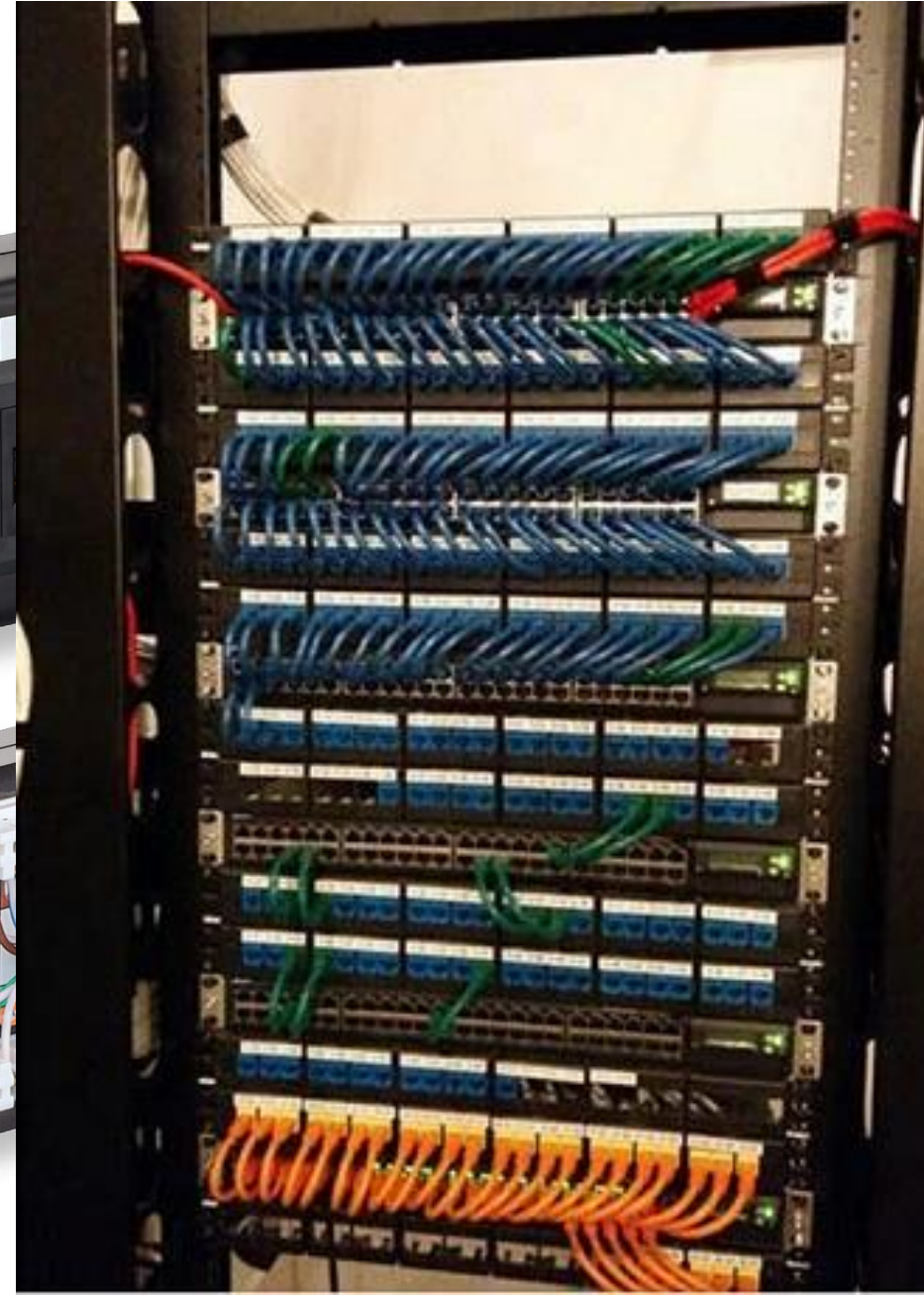
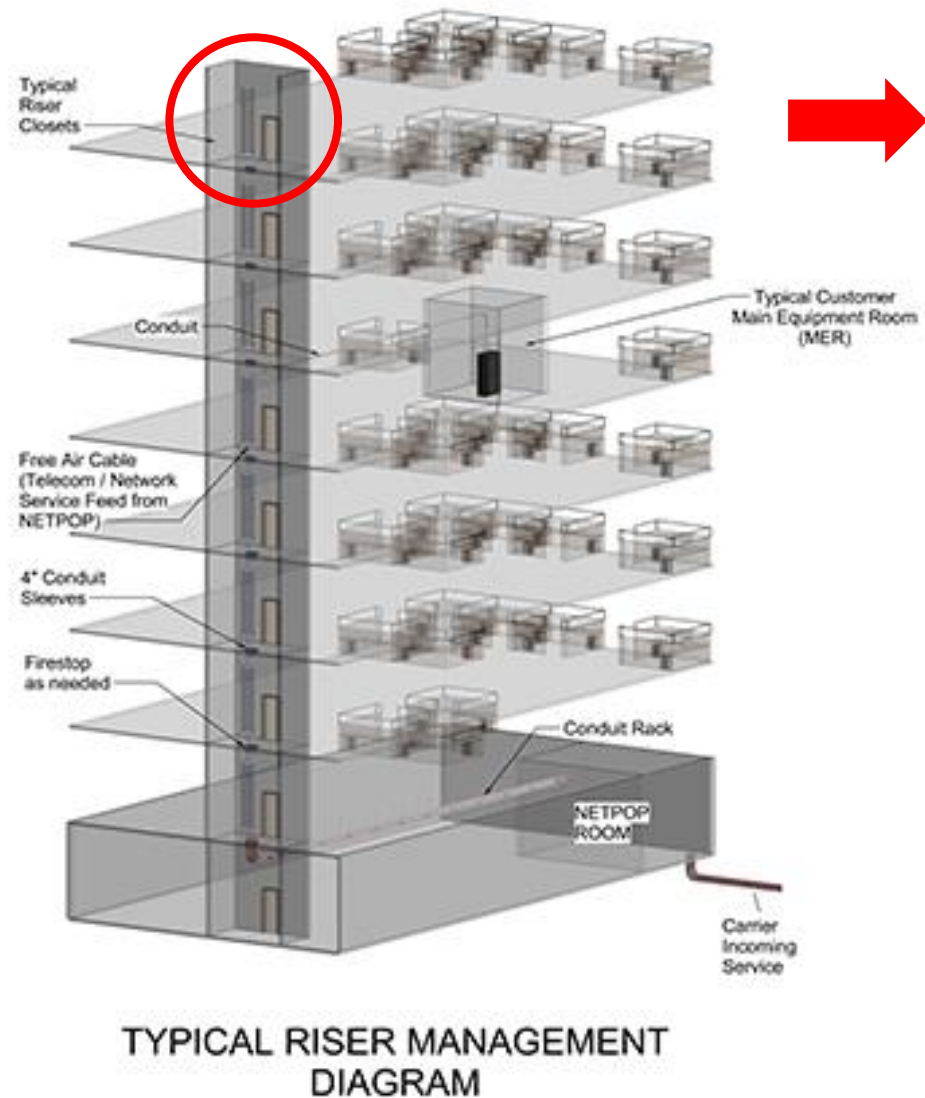
12 (decimal) = 1100 (binary)



Packet switching Router



Network gear in riser

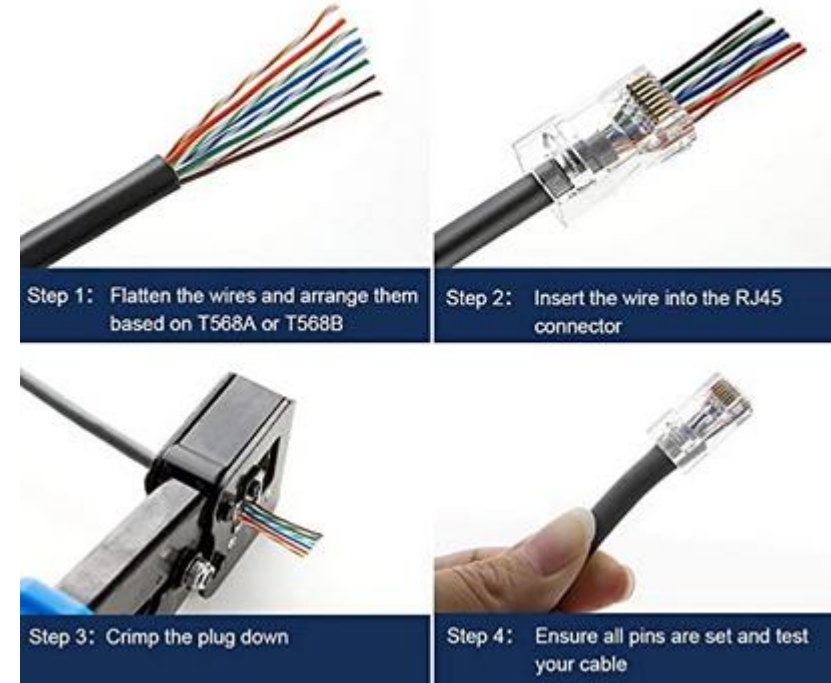


Network UTP (copper) cable

Unshielded Twisted Pair (UTP)

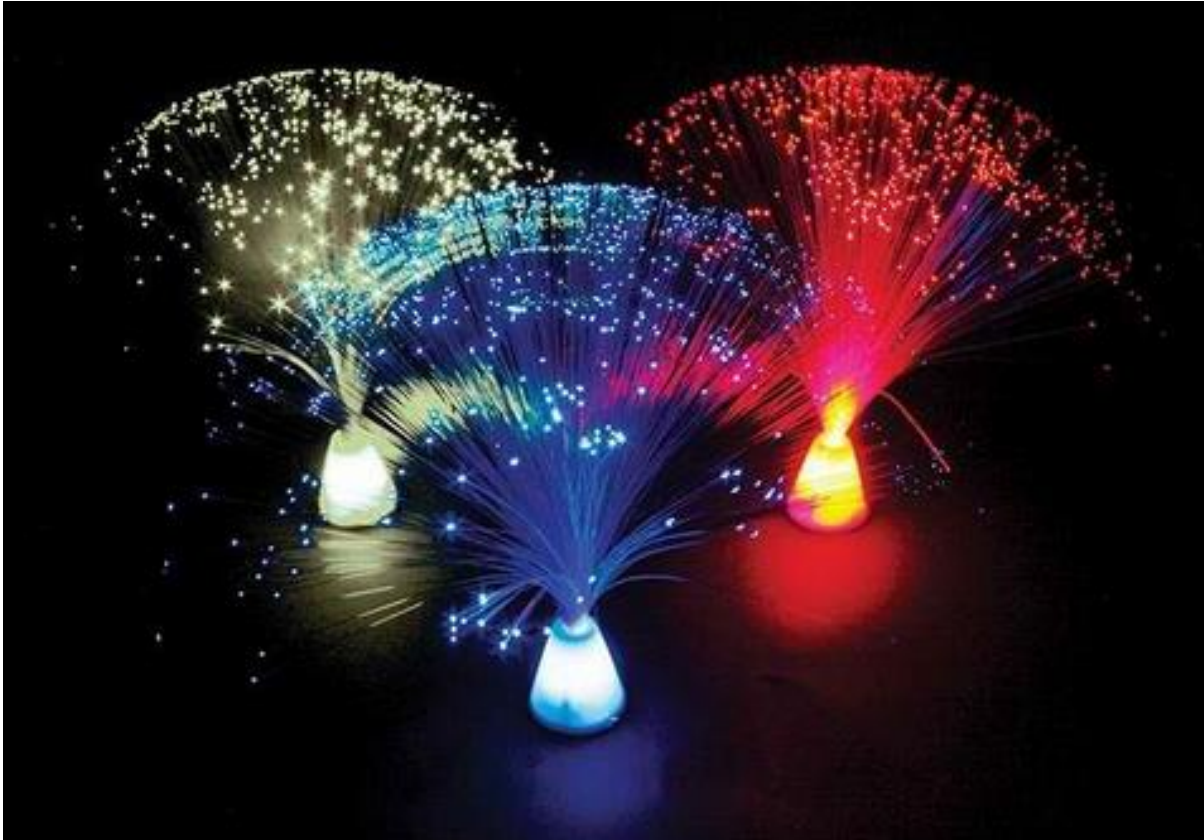


How to Make an Ethernet Cable?



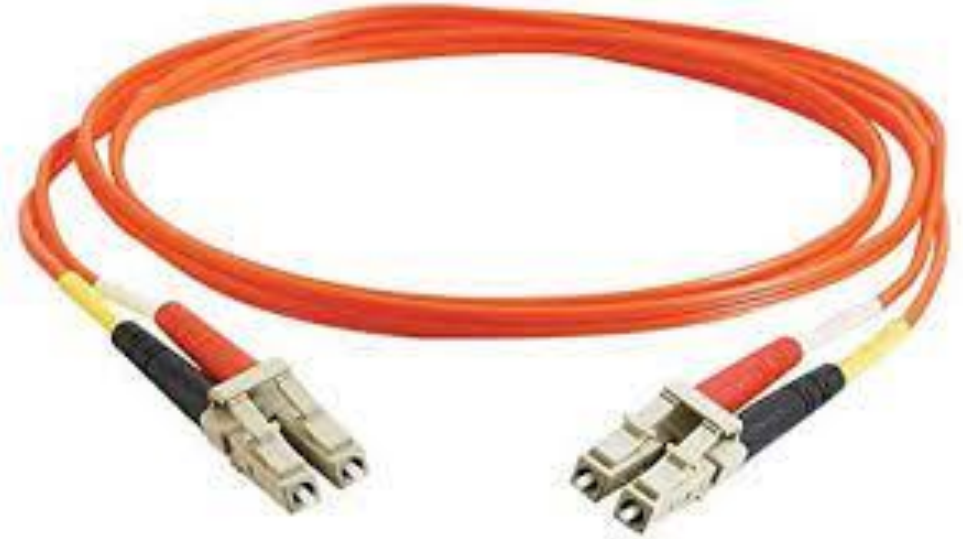
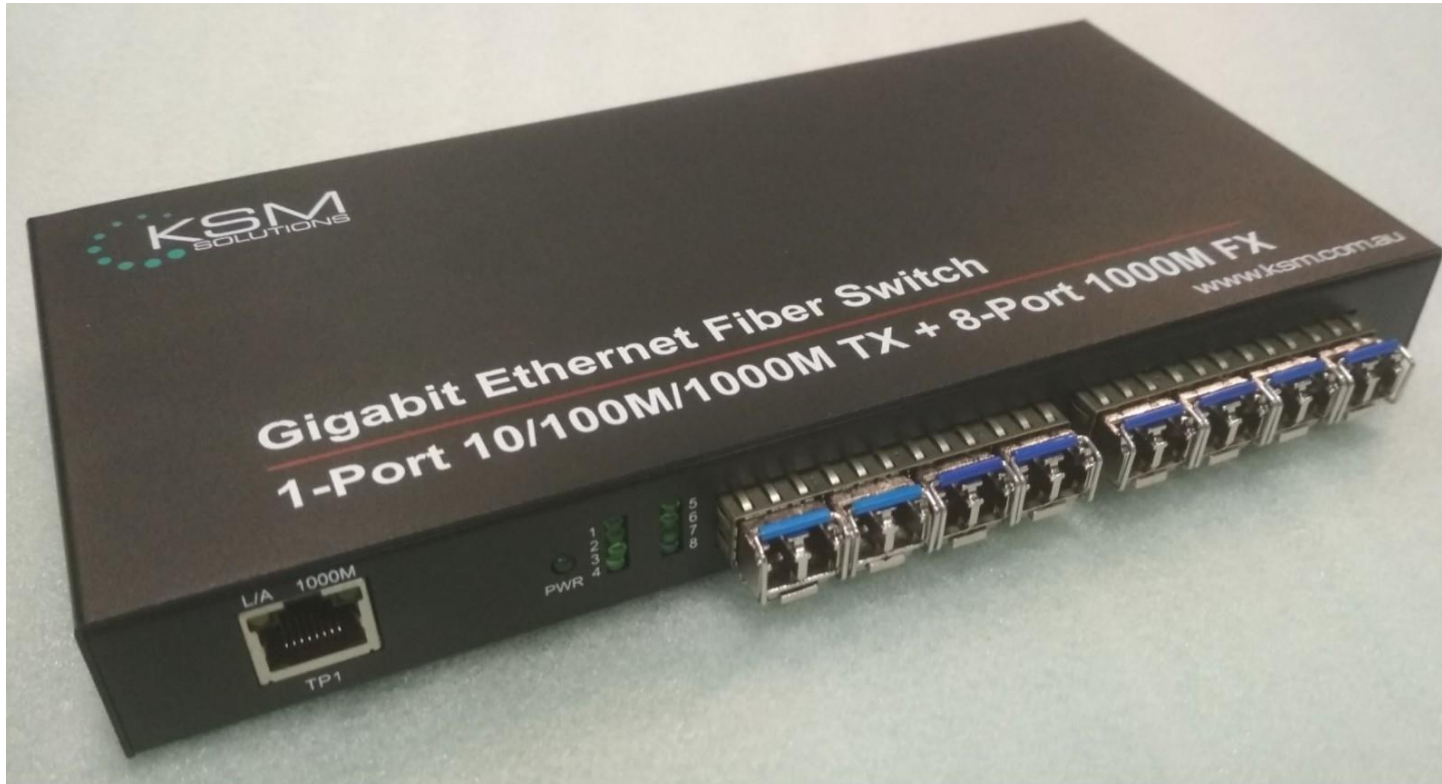
CAT5e, CAT6, CAT8:
(difference in data transfer rates
also depending on length of cable)

Network fibre optics cable



Information sent via fiber optic cables is much more difficult to intercept because light can't be read in the same way signals sent via copper cabling can be.

Network fibre switch



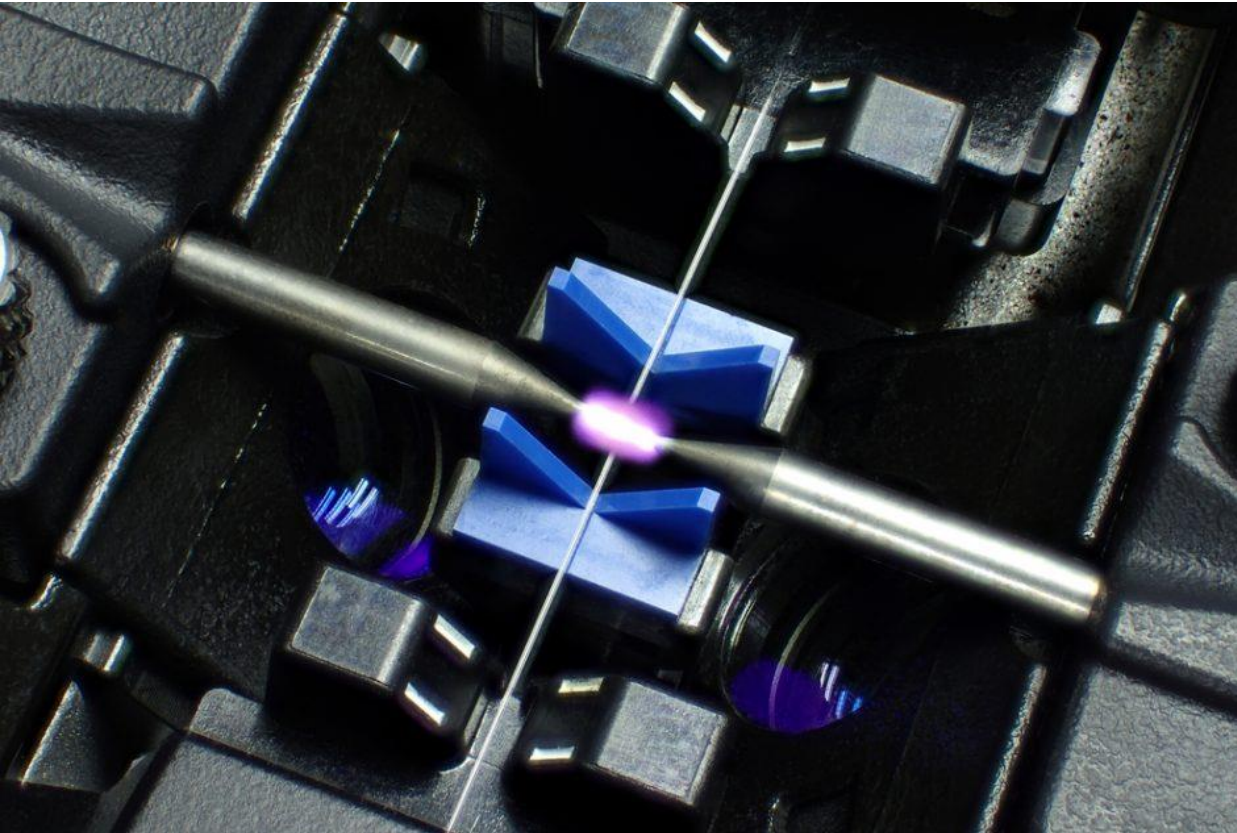
Information sent via fiber optic cables is much more difficult to intercept because light can't be read in the same way signals sent via copper cabling can be.

Fibre splicing machine



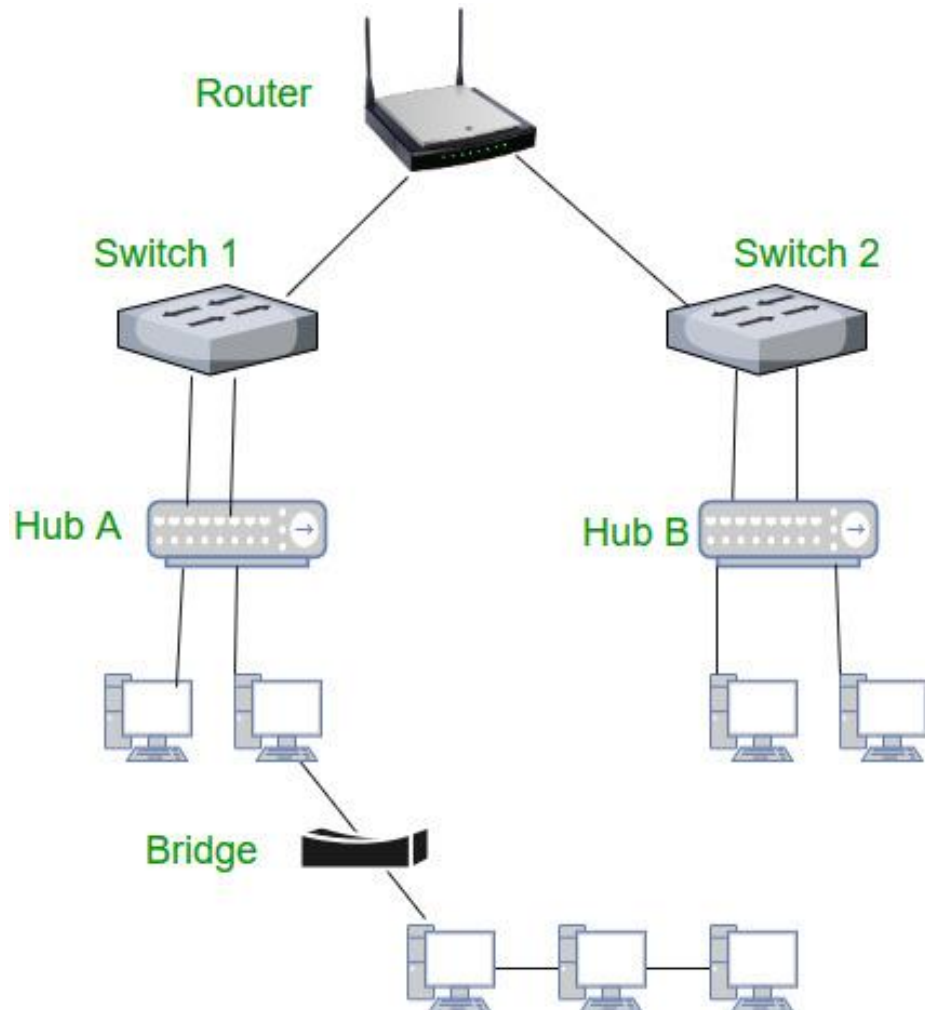
Information sent via fiber optic cables is much more difficult to intercept because light can't be read in the same way signals sent via copper cabling can be.

Fusion splicing in action



Information sent via fiber optic cables is much more difficult to intercept because light can't be read in the same way signals sent via copper cabling can be.

Network devices



Router – A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs.

Switch – A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only.

Hub – A hub is a basically multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

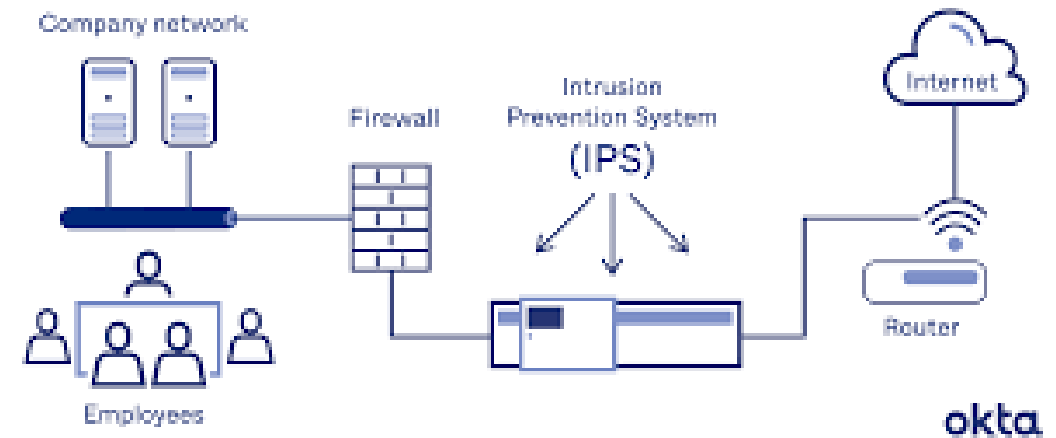
Bridge – A bridge operates at the data link layer. A bridge is a repeater, with the add-on functionality of filtering content by reading the MAC addresses of the source and destination. It has a single input and single output port, thus making it a 2-port device.

1990s to present time

- Networks of computers became more common; so too did the need to interconnect networks (Internet). Initially based on **de facto standards**.
- In early Internet deployments, **security was treated as a low priority**.
- The Internet brings millions of unsecured computer networks into continuous communication with each other.
- Ability to secure a computer's data influenced by the security of every computer to which it is connected.
- **Growing threat of cyber attacks** has increased the need for improved security
Example: the advent of the “Web” and “executable content”
- From late 1990s, we started to **'add on' security to our existing software architecture**.

Why did we look at computer network cables & devices?

- Network security encompasses all the steps taken to protect the integrity of a computer network and the data within it. Network security is important because it keeps sensitive data safe from cyber attacks and ensures the network is usable and trustworthy.
- Many of the devices in a computer network are susceptible to potential attacks.
- Network security involves the use of a variety of software and hardware tools such as **Firewalls**, **Intrusion detection systems (IDS)** and **Intrusion prevention systems (IPS)** to protect the integrity of a computer network and the data within it.



Defining security

“The quality or state of being secure - to be free from danger”

A successful organization should have multiple layers of security in place:

- 1) **Physical:** This involves securing the physical infrastructure and assets of an organization, such as buildings, servers, and other equipment, from theft, damage, and unauthorized access.
- 2) **Personnel:** This includes implementing policies and procedures to ensure that employees and contractors are aware of their security responsibilities and are trained to respond to security incidents.
- 3) **Operations:** This involves the day-to-day procedures and controls that are put in place to protect the organization’s data and IT infrastructure, such as regular system backups, patch management, and incident response.
- 4) **Communications:** This layer focuses on securing all forms of communication (emails, phone calls, video conferences, etc.) to prevent eavesdropping, interception, or disruption.
- 5) **Network:** This involves protecting the organization’s network infrastructure from threats such as malware, hacking, and denial-of-service attacks, often through the use of firewalls, intrusion detection systems, and secure network architectures.
- 6) **Information:** This layer focuses on protecting the confidentiality, integrity, and availability of the organization’s data, both in transit and at rest, through measures such as encryption, access controls, and data loss prevention strategies.

Each of these areas contribute to the security program as a whole.

Defining security (continued)



“The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information” (CNSS*)



How do we achieve information security?
Policy, awareness, training, education, technology



C.I.A. triangle (Basis for CNSS model of Information Security)

Was a standard based on **Confidentiality**, **Integrity**, and **Availability**

Now expanded into a more comprehensive list of critical characteristics of information

**** CNSS = U.S. Committee on National Security Systems***

Key information security concepts

- Access
- Asset
- Attack
- Control, Safeguard, or Countermeasure
- Exploit
- Exposure
- Loss

- Protection Profile or Security Posture
- Risk
- Subjects and Objects
- Threat
- Threat Agent
- Vulnerability
- Attack vector

- A typical security analyst's comment:

Good security is a mix of ***risk management*** AND ***continuity management*** (in that order)

Information security characteristics (quality of service)



Non-repudiation:
This refers to the ability to ensure that a party to a communication cannot deny the authenticity of their signature on a document or the sending of a message



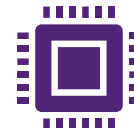
Authenticity:
This involves verifying that users are who they say they are and that each input arriving at the system came from a trusted source. It often involves credentials, such as usernames and passwords.



Confidentiality:
This is the protection of information from disclosure to unauthorized individuals or systems. In terms of data security.



Integrity: This refers to maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle.



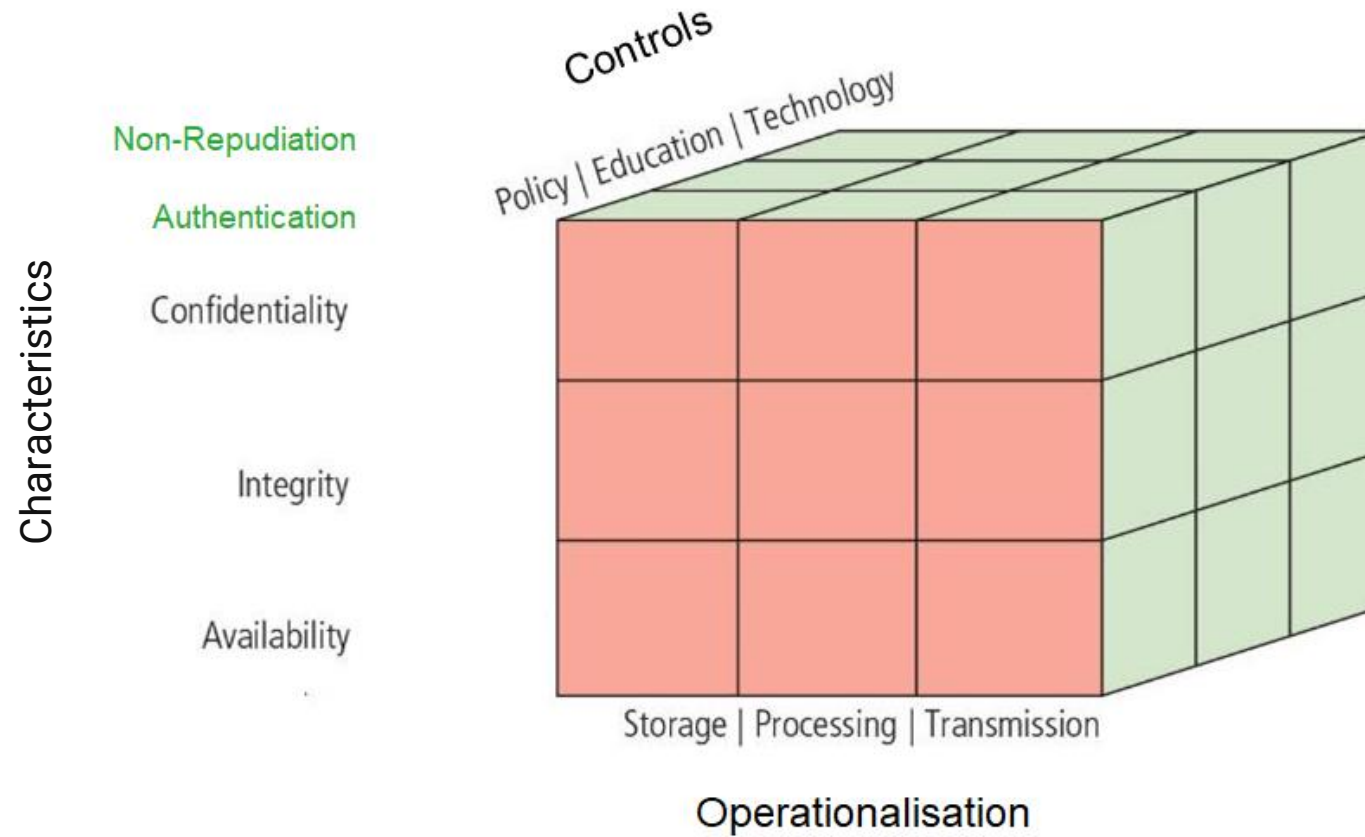
Availability: This means that information and systems should be available for operation and use when required.



Discuss this in relation to your use of email!

CNSS Security Model

(U.S. Committee on National Security Systems - CNSS)



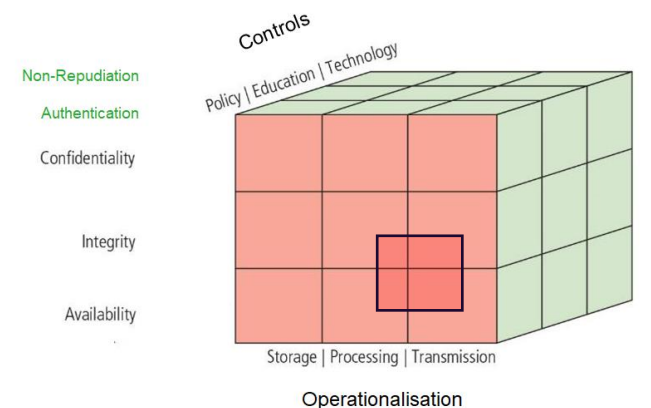
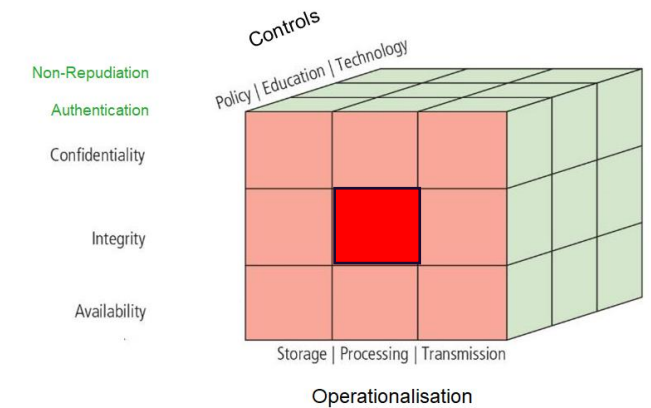
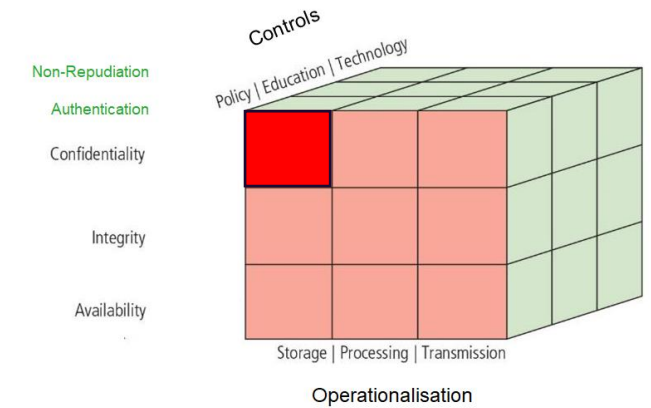
Repudiation:

Denial of the truth or validity of something.

Abstraction of security

Example

Confidentiality/Policy/Storage	<p>This component combination shows the intersection of the factors Confidentiality, Policy of Security, and Data Storage.</p> <p>Security Policy:</p> <ul style="list-style-type: none"> The registered student only accesses the course related material. The student discussion posts are for students only. The assignments/homework's must be viewable by the student and assigned instructor.
Integrity/Policy/Processing	<p>This component combination shows the intersection of the factors Integrity, Policy, and Processing.</p> <p>Security Policy:</p> <ul style="list-style-type: none"> The submitted work should be original. All the resources must be properly cited. The references must be included. The instructor must be able to see the work of assigned students.
Availability/Education/Processing	<p>This component combination shows the intersection of Availability, Education, and Processing cells.</p> <p>Security Policy:</p> <ul style="list-style-type: none"> The website of university should have minimum downtime. The students must be aware of all the policies to do the assignment.



Finding the right balancing between security and access



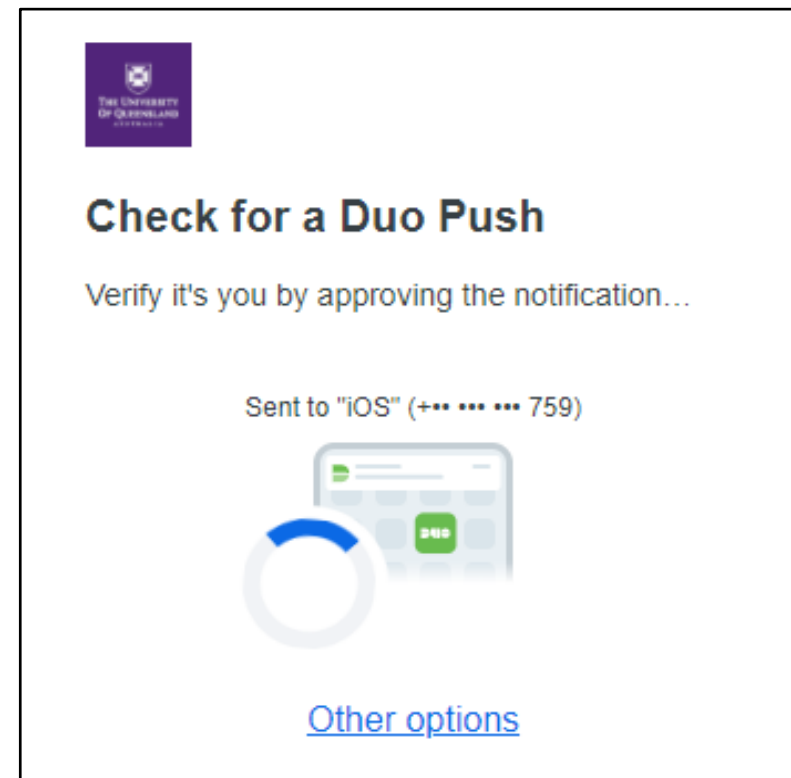
How much is too much?



Balancing information security and access

- **Impossible to obtain perfect security** – it is a process, not an absolute.
- Security is a **balance between protection and availability**.
- To achieve balance, the level of **security must allow reasonable access, but protect against threats**.

Example: UQ Two-Factor Authentication:



Another layer has been added recently!



Verified push added to MFA



ITS Service Desk <noreply@uq.edu.au>

To: Alex Pudmenzky



Thu 02-Feb

If there are problems with how this message is displayed, click here to view it in a web browser.

[View online](#)



Dear Alex,

You may have noticed an additional step when using UQ's multi-factor authentication (MFA).

What has happened?

An additional step has been added to the Duo MFA process. Once you are prompted to MFA, you will have to add a pin to authenticate. This process is called 'verified push'.

This was added to some applications in January 2023, and will now be enabled for all instances.

How does verified push work?

The MFA process remains the same, with the additional step of adding a PIN.

After signing in to UQ Authenticate, a three digit pin will appear on your device.

When you open the Duo application, a screen will appear asking '*Are you logging in to UQ Authenticate*' where you will need to enter the three digit pin to verify.

Why has verified push been added to MFA?

Verified push has been enabled as we are experiencing increased fraudulent attempts to gain access to our networks. It uses the Duo mobile app, and offers an extra layer of protection, requesting a passcode in addition to the usual notification. This is particularly relevant for applications that access the UQ network, safeguarding against fraudulent requests.

Security professionals in the organization



Senior
management
support is the
key
component.

Information security implementation is initiated by upper management (top-down)

- Issue policy, procedures, and processes – describe policy process.
- Ensure adequate resourcing for security process and allocation of roles.
- Dictate goals and expected outcomes of project
- Determine accountability for each required action.
- The most successful involve formal development strategy referred to as systems development life cycle.

Security professionals in the organization



Senior management support is the key component.

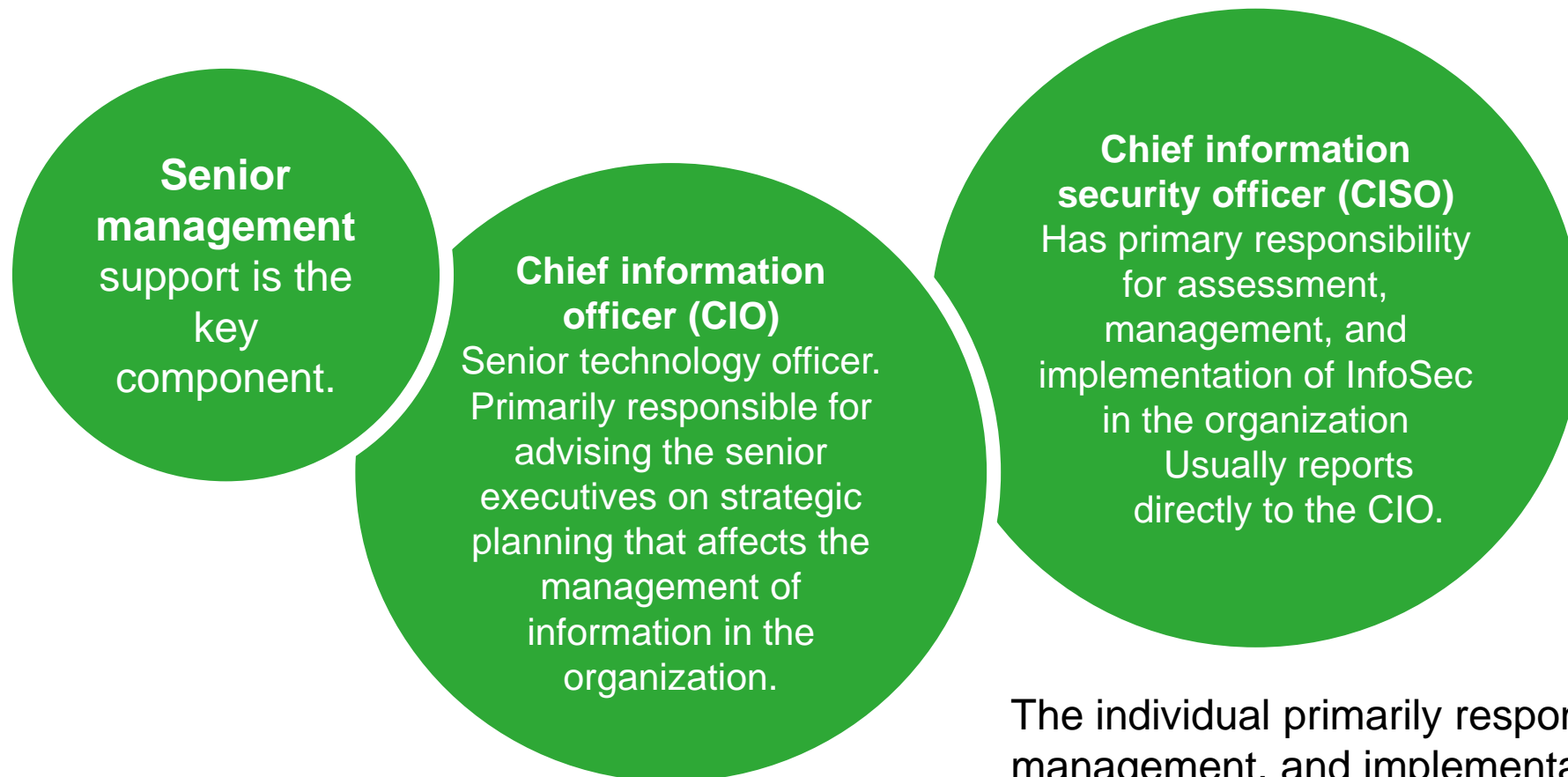
Chief information officer (CIO)

Senior technology officer. Primarily responsible for advising the senior executives on strategic planning that affects the management of information in the organization.

The senior technology officer, although other titles such as Vice President of Information, VP of information technology, and VP of systems may be used.

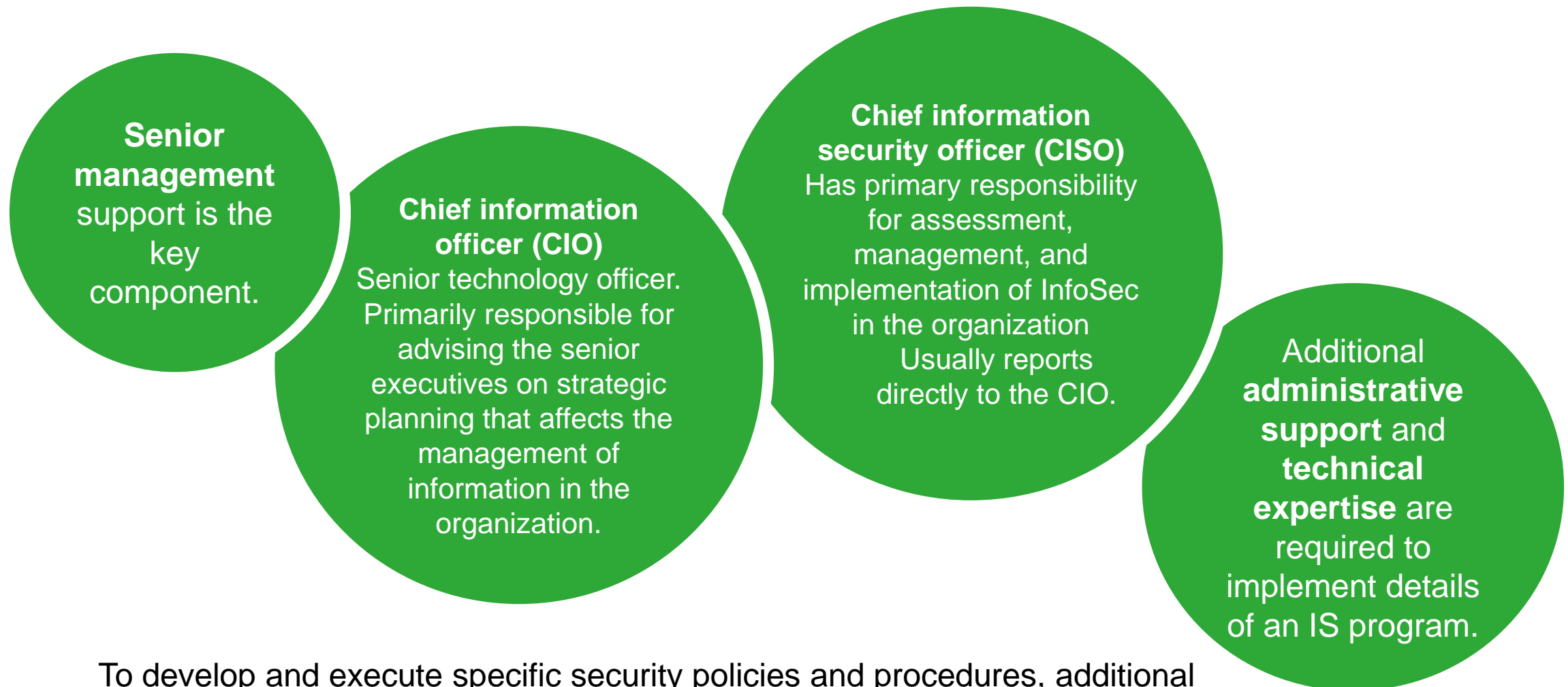
The CIO is primarily responsible for advising the chief executive officer, president, or company owner on the strategic planning that affects the management of information in the organisation.

Security professionals in the organization



The individual primarily responsible for the assessment, management, and implementation of securing the information in the organization. The CISO may also be referred to as the manager for security, the security administrator, or a similar title.

Security professionals in the organization



To develop and execute specific security policies and procedures, additional administrative support and technical expertise is required.

Security professionals in the organization

Senior management support is the key component.

Chief information officer (CIO)

Senior technology officer. Primarily responsible for advising the senior executives on strategic planning that affects the management of information in the organization.

Chief information security officer (CISO)

Has primary responsibility for assessment, management, and implementation of InfoSec in the organization
Usually reports directly to the CIO.

Additional administrative support and technical expertise are required to implement details of an IS program.

Information security project team

A small functional team of people who are experienced in one or multiple facets of required technical and nontechnical areas.



Champion: A senior executive who promotes the project and ensures its support, both financially and administratively, at the highest levels of the organization.

Information security project team

A small functional team of people who are experienced in one or multiple facets of required technical and nontechnical areas.

Champion: A senior executive who promotes the project and ensures its support, both financially and administratively, at the highest levels of the organization.

Team leader: A project manager, who may be a departmental line manager or staff unit manager, who understands project management, personnel management, and information security technical requirements.

Information security project team

A small functional team of people who are experienced in one or multiple facets of required technical and nontechnical areas.

Champion: A senior executive who promotes the project and ensures its support, both financially and administratively, at the highest levels of the organization.

Team leader: A project manager, who may be a departmental line manager or staff unit manager, who understands project management, personnel management, and information security technical requirements.

Security policy developers: Individuals who understand the organizational culture, policies, and requirements for developing and implementing successful policies.

Information security project team

A small functional team of people who are experienced in one or multiple facets of required technical and nontechnical areas.

Champion: A senior executive who promotes the project and ensures its support, both financially and administratively, at the highest levels of the organization.

Team leader: A project manager, who may be a departmental line manager or staff unit manager, who understands project management, personnel management, and information security technical requirements.

Security policy developers: Individuals who understand the organizational culture, policies, and requirements for developing and implementing successful policies.

Risk assessment specialists: People who understand financial risk assessment techniques, the value of organizational assets, and the security methods to be used.

Information security project team

A small functional team of people who are experienced in one or multiple facets of required technical and nontechnical areas.



Information security project team

A small functional team of people who are experienced in one or multiple facets of required technical and nontechnical areas.



Information security project team

A small functional team of people who are experienced in one or multiple facets of required technical and nontechnical areas.

End users: Those whom the new system will most directly impact. Ideally, a selection of users from various departments, levels, and degrees of technical knowledge assist the team in focusing on the application of realistic controls applied in ways that do not disrupt the essential business activities they seek to safeguard.

Champion: A senior executive who promotes the project and ensures its support, both financially and administratively, at the highest levels of the organization.

Team leader: A project manager, who may be a departmental line manager or staff unit manager, who understands project management, personnel management, and information security technical requirements.

Systems administrators:
People with the primary responsibility for administering the systems that house the information used by the organization.

Security professionals:
Dedicated, trained, and well-educated specialists in all aspects of information security from both technical and nontechnical standpoints.

Risk assessment specialists: People who understand financial risk assessment techniques, the value of organizational assets, and the security methods to be used.

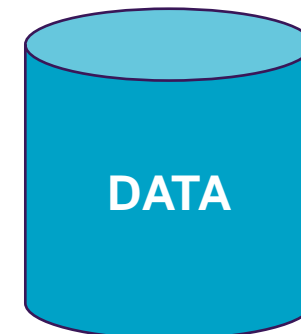
Security policy developers:
Individuals who understand the organizational culture, policies, and requirements for developing and implementing successful policies.

Data responsibilities

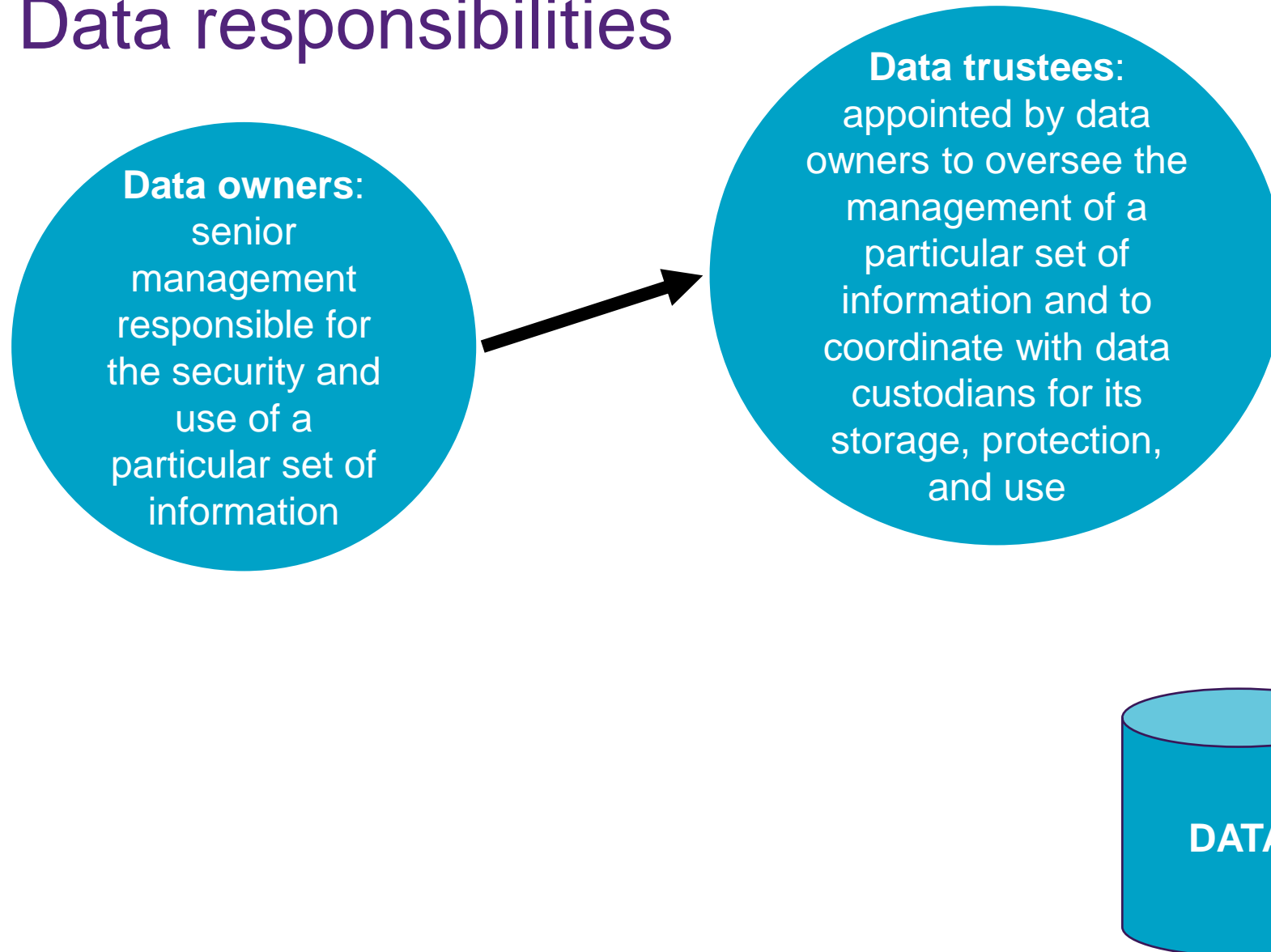


Data owners:
senior
management
responsible for
the security and
use of a
particular set of
information

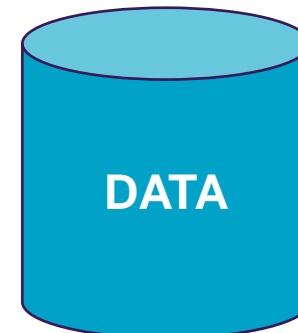
Members of senior management who are responsible for the security and use of a particular set of information. The data owners usually determine the level of data classification (discussed later), as well as the changes to that classification required by organizational change.



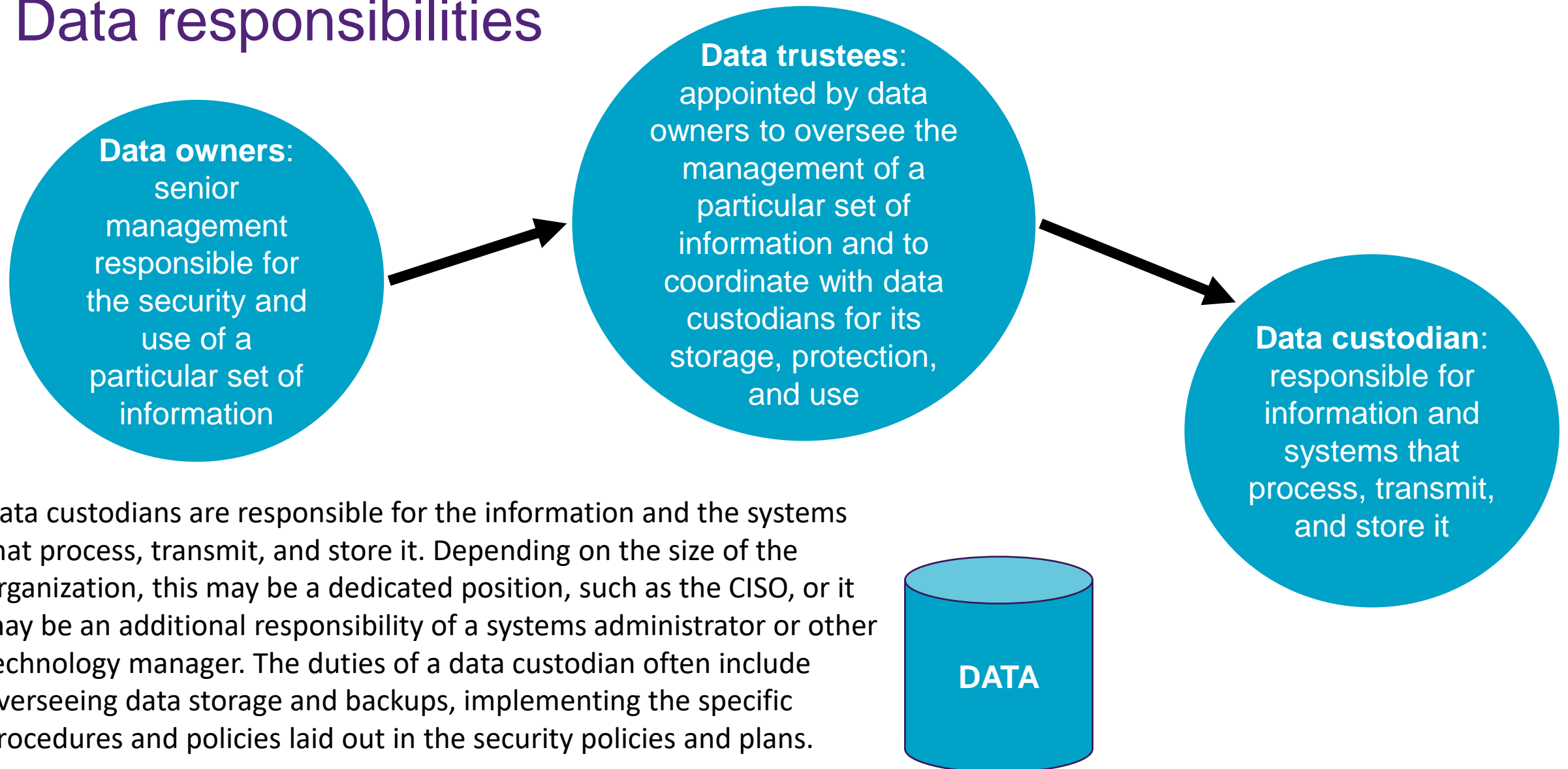
Data responsibilities



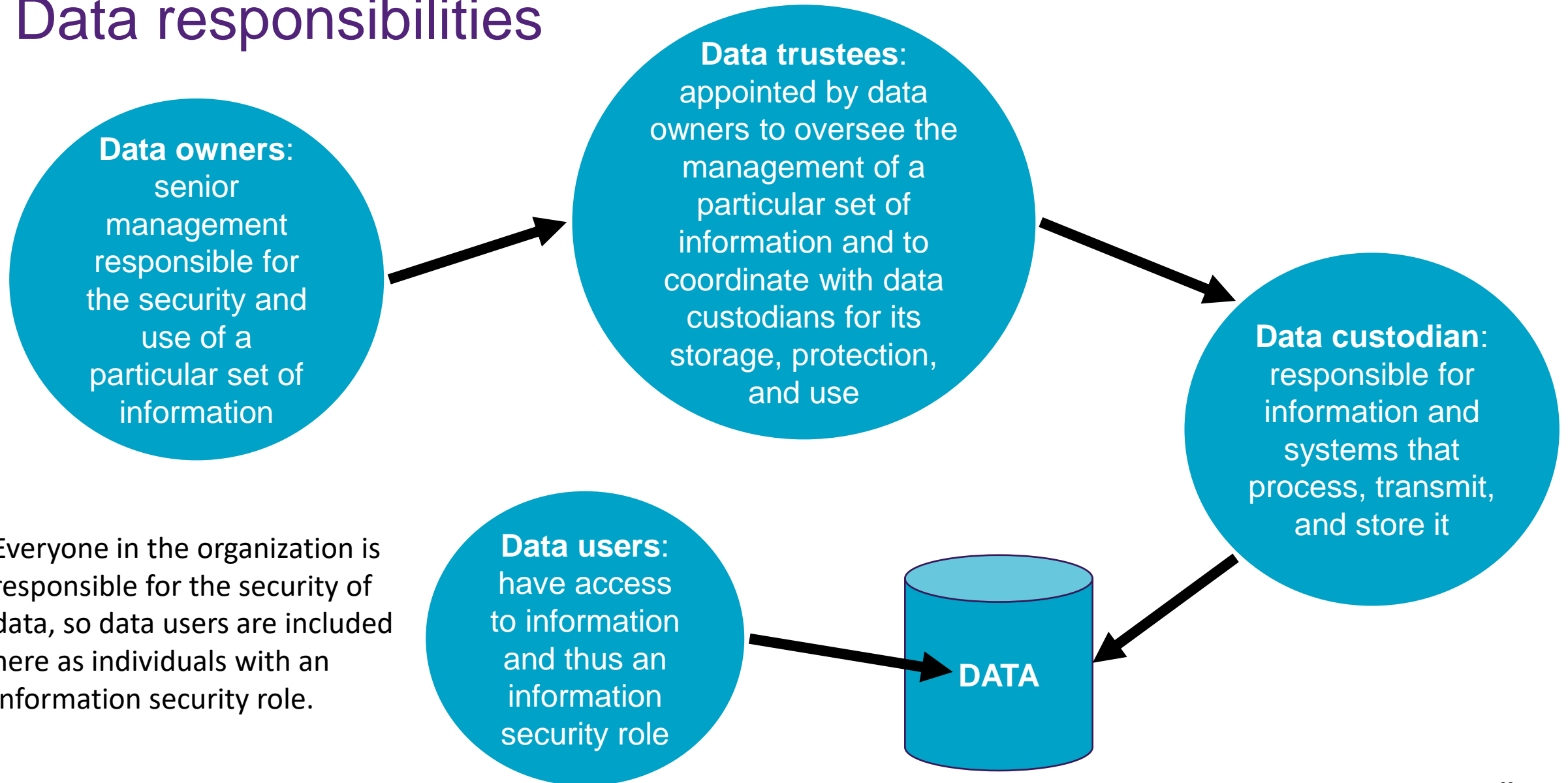
The data owners work with subordinate managers to oversee the day-to-day administration of the data.



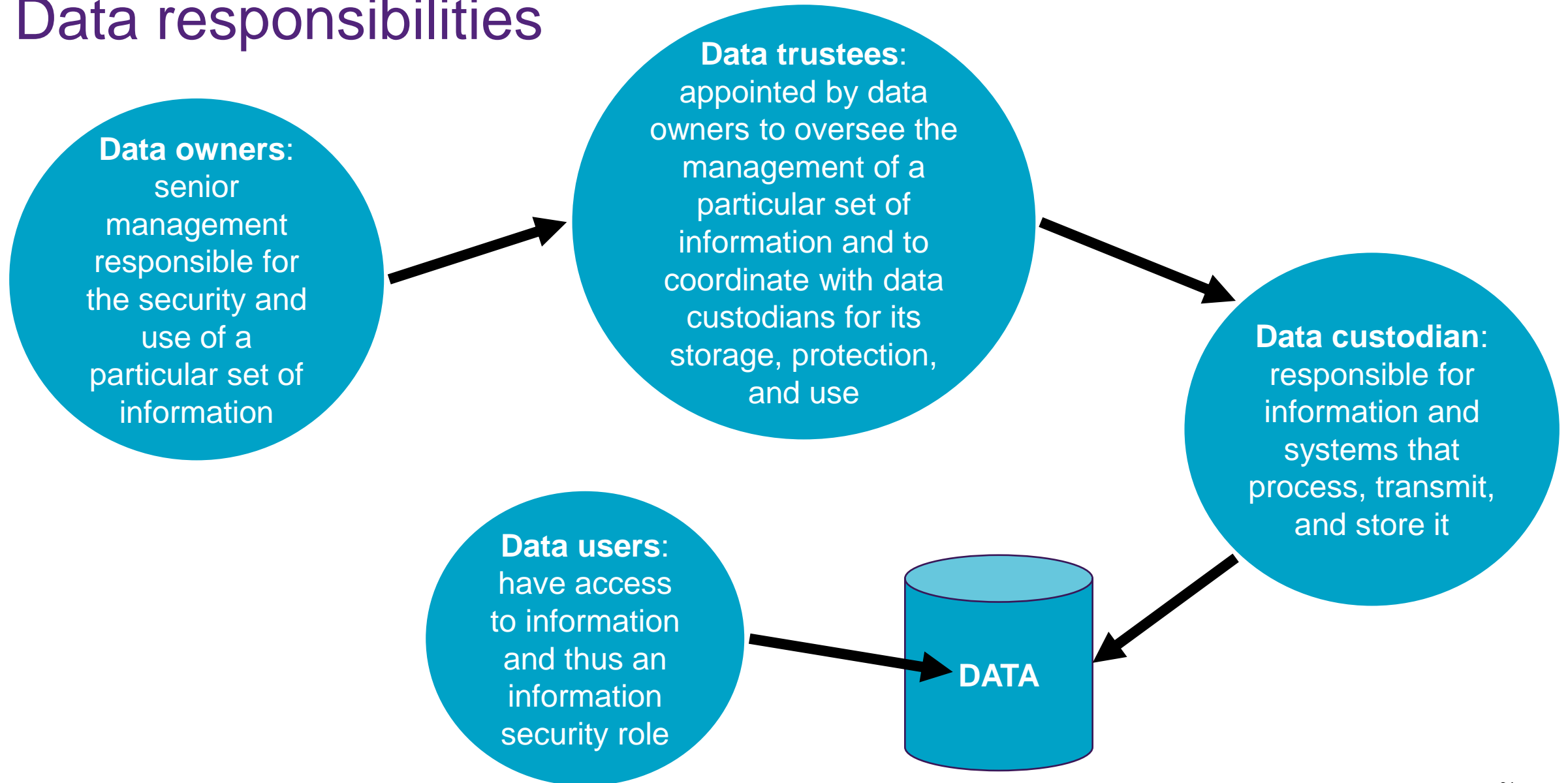
Data responsibilities



Data responsibilities



Data responsibilities



Summary

- Information security is a “**well-informed sense of assurance that the information risks and controls are in balance**”.
- Computer security has evolved into information security.
- **Successful organizations have multiple layers of security in place:** physical, personal, operations, communications, network, and information.
- **Security should be considered a balance between protection and availability.**
- Information security must be managed similarly to any major system implemented in an organization.



Copyright 2004 by Randy Glasbergen,
www.glasbergen.com



"The boss is worried about information security,
so he sends his messages one alphabet letter
at a time in random sequence.'

```
end;
func, std::vector<int>

write(Endtext);
end.
CREATE TABLE product(
class MultinomialNB(object):
def __init__(self):
2))
self.X = None
self.y = None
def __loading(self):
self.list_labels = cl.Counter(s
int acc(std::function<int(int, int)> fun
auto it = operands.begin();
int result = func(*it, *(++it));
if (operands.size() > 2) {
for (++it; it!=operands.end(); ++it)
result = func(result, *it);
}
}
return result;
CDog& operator=(C
```

Thank you