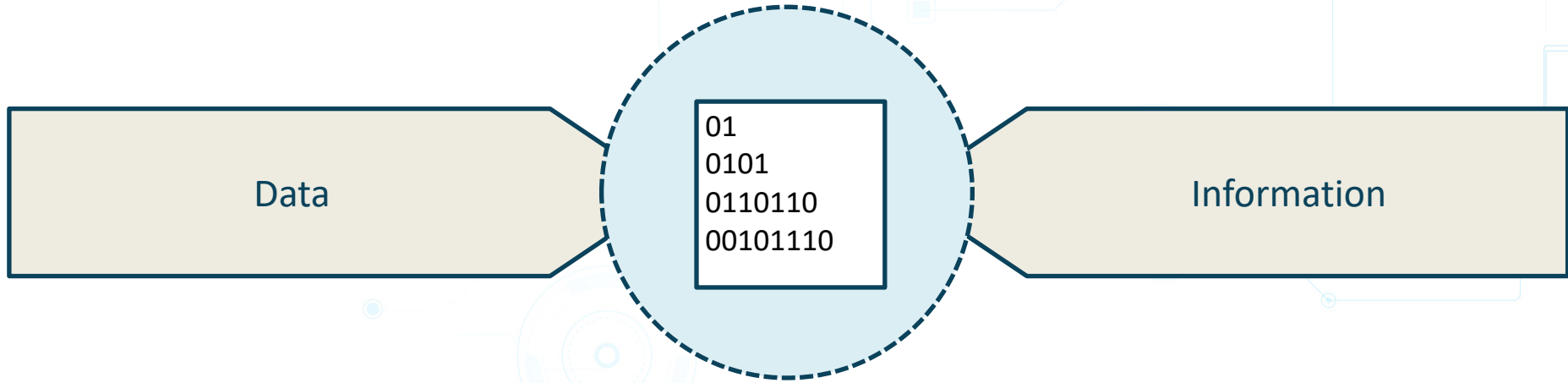



Data and Information



Data and Information



```
01
0101
0110110
00101110
```

Data

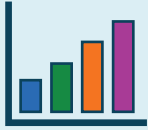
- Raw numbers, text, and dates
- Not organized
- Example
 - Details regarding antimalware scans on individual hosts



Information

- Results from processed data
- Insights
- Example
 - How often specific malware types cause security incidents within the organization

Data and Information

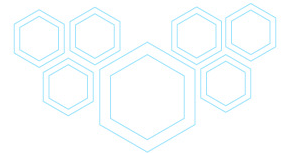


- Reliability of data
 - Confidentiality and integrity of processing systems and data
- Data transformation
 - Formatting and dissimilar processing systems
- Solid information = informed decision making

Data Analytics



- Can involve large volumes of data (big data)
- Technology and automation can process big data quickly



Data Analytics



- Performance insights
 - Placement of database servers to increase performance
 - Reduction in amount of time to complete a transaction with a customer
- Security insights
 - Patterns or abnormal network, host, and app usage
 - Indications of wrong-doing
- Cost efficiencies
 - Removal of duplicate job roles and systems
 - Streamline, remove, and replace processes

Data Analytics



- Supports informed decision making
 - Overall summaries
 - Hidden patterns
 - Prediction modeling
- Data analytics technology solutions
 - Cluster nodes working together
 - E.g. Apache Hadoop

Storage Area Networks



- Dedicated network for storage communications
- Storage consumers access shared storage over the network
- Storage consumer can also use local storage
 - Direct attached storage (DAS)
- IS auditors may need to audit backup procedures
 - Backup agents may not be needed on storage consumers

Storage Area Networks



iSCSi

- Standard network equipment
 - Switches
 - NICs
- SCSI disk commands are embedded within IP packets

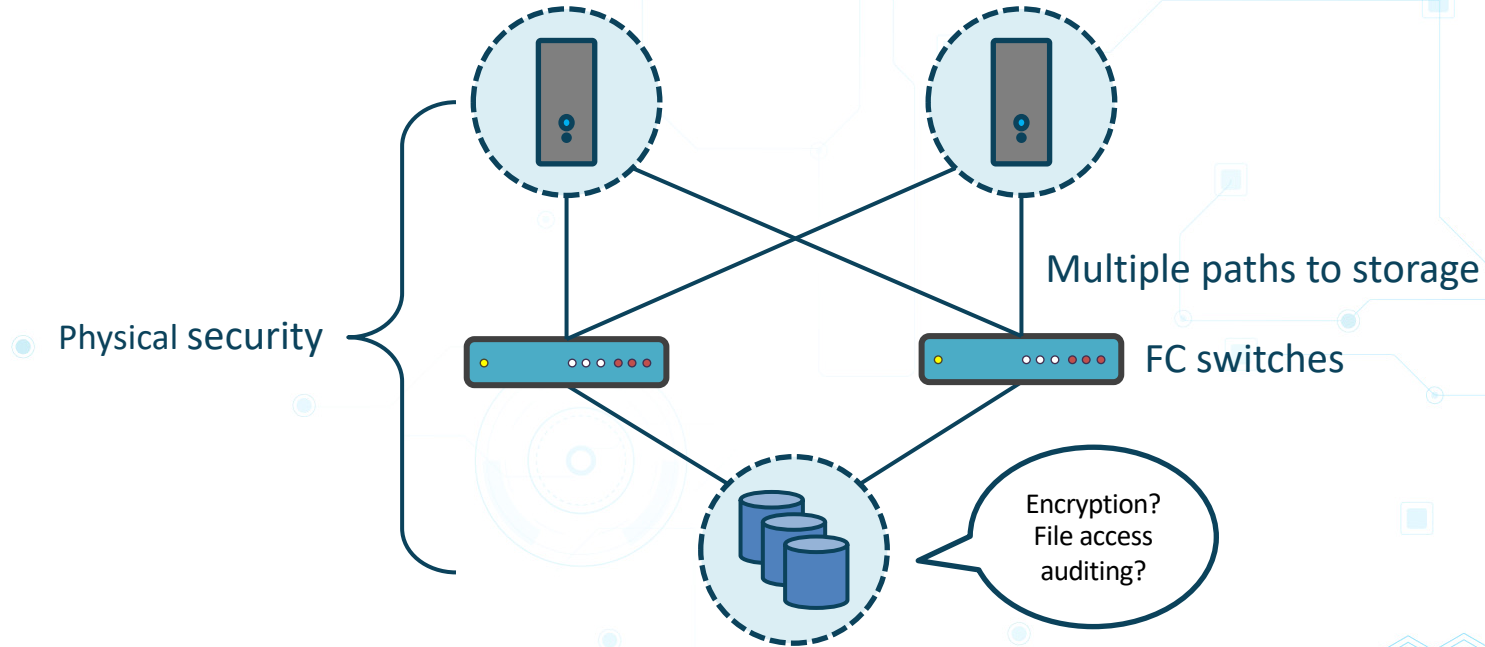


Fibre Channel

- Specialized equipment
 - Host bus adapters (HBAs)
 - Fibre channel (FC) switches

Fibre Channel SAN

Servers, each with an HBA



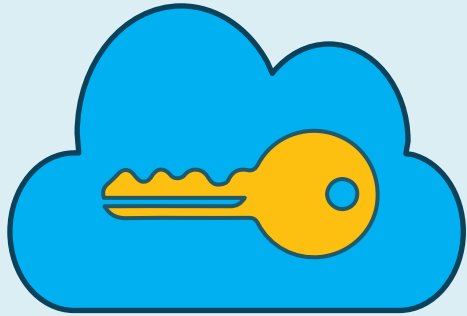
Storage arrays (LUN masking), backup units

Cloud Storage Security



- Laws and regulations
 - Is cloud storage allowed?
 - Location of cloud provider datacenters within national boundaries?
 - Nationality of cloud data center technicians

Cloud Storage Security

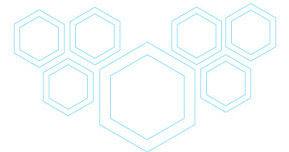


Cloud provider security compliance

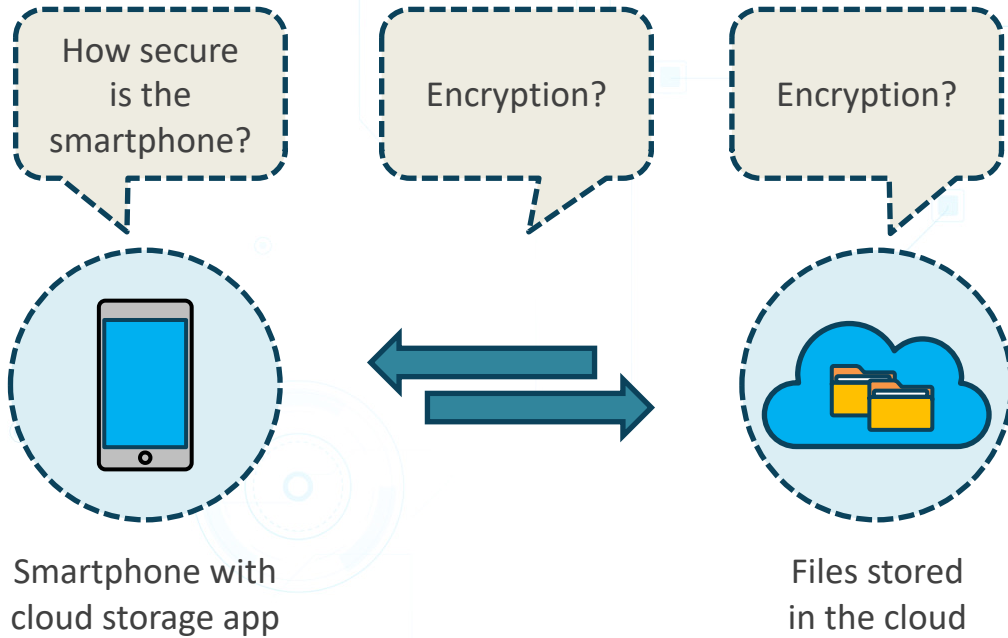
Encryption of data at rest (AES 256)

Data retention policies

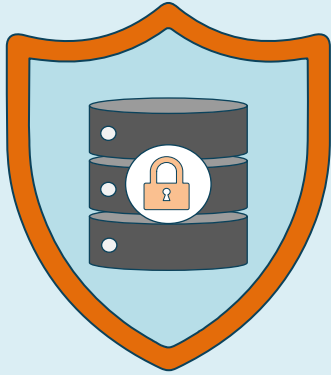
Data wiping practices



Cloud Storage Security



Database Security



- On-premises and cloud
 - Database servers
 - Databases
- Mobile devices
 - SQLite

Database Security



- Network security
 - Isolated from other network hosts
 - Never placed in the DMZ
- Server security
 - Hardened OS
 - Patches applied
 - Server firewall rules
 - Multi-factor user authentication

Database Security



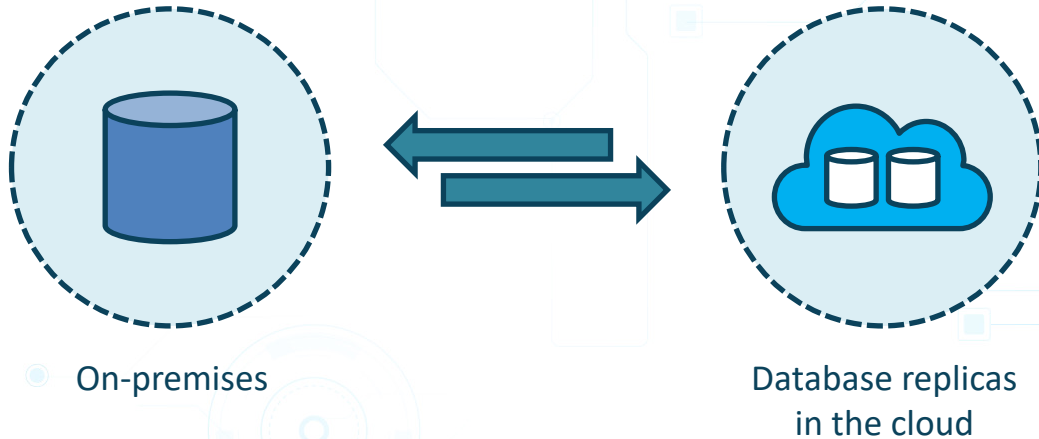
Encryption of data at rest

Data masking

Queries: secure coding and input validation

Database object, row, and column security

Database Availability

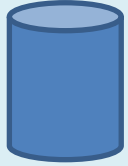


On-premises

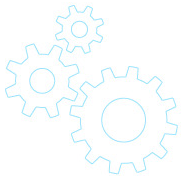
Database replicas
in the cloud

Always consider programmatic database access

Backup and Restore



- On-premises backup
- Cloud backup
- Backup schedule and tape rotation
- Data retention policies
- Data immutability
- Restored data and ACLs



Backup Types



The diagram features a central light blue circle with a dashed dark blue border containing two yellow folder icons. A dashed dark blue line extends from this circle to a large, light beige rounded rectangle with a dashed dark blue border. This rectangle is divided into three columns, each representing a backup type. The background is decorated with light blue line art, including a cloud, a target, a smartphone, a tablet, and gears.

Full
All data

Incremental
New and
modified data
since last full or
incremental

Differential
New and
modified data
since last full
backup

Malware

Malicious software



Malware authoring
tutorials and toolkits

Malware Infections

Reconnaissance



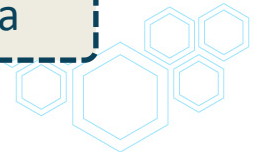
Trick user



Malware infects device



Stolen, encrypted, or
deleted systems and data



Malware Types



Trojan

- Wolf in sheep's clothing
- Appears benign
- Often used to deliver other types of malware



Virus

- Attaches itself to files
 - Office productivity
 - App installation
 - Media
 - Illegal downloads of music, movies, and TV shows

Malware Types



Worm

- Does not need to be attached to a file
- Self-propagating over the network
- Scans for vulnerable file sharing hosts



Ransomware

- Prevents system start-up
- Encrypts data files
- Demands ransom payment in the form of Bitcoin
 - There is never a guarantee that decryption keys will be provided

Social Engineering



- Trickery and deception
- Goal is the disclosure of sensitive information from unsuspecting victims

Social Engineering - Fear

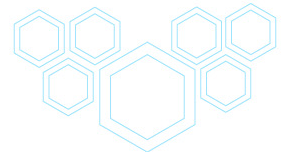


Impersonating government departments

Impersonating law enforcement

Phishing

Extortion, sextortion, and blackmail



Social Engineering Without Malware

Impersonation of communications provider technician over phone



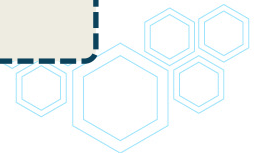
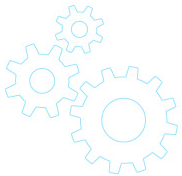
Attacker shows up dressed appropriately



Victim allows attacker into server room or wiring closet



Attacker now has physical access to equipment



Phishing Example

Legitimate looking e-mail



Link to reset user password



Victim clicks link



The link downloads and installs malware or the user credentials are sent out

Phishing E-mail Message



Commonwealth Bank <W63lLuR.RPz7P2TAHn.yZl@clutt.sheldegis.org.uk>

Sat 2018-11-17 3:24 AM

You ✓



CommonwealthBank



Why you received this email.

Your Account has been Locked due to several unsuccessful login attempts.

Date: 17/11/2018

Activity: 3 failed login attempts.

Unlock Account

Notice : It is necessary to validate your netcode after having checked your information .

If you have questions about your account you will find additional helpful information under [CommBank Help & Contact](#).

You received this email to let you know about important changes to your account and services.

© 2018 Commonwealth Banking group.

Social Engineering Mitigation Controls



Administrative

- User training and awareness
- Security documentation easily accessible to users
- Periodic e-mail reminders about security
- Security posters in workplace

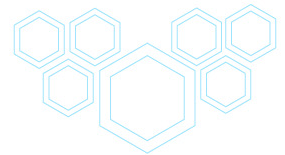
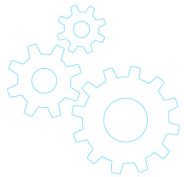


Technical

- E-mail spam filtering
- Antimalware up-to-date
- Network firewall rules
- Host firewall rules
- Intrusion detection and prevention systems

In this exercise, you will

- List ways to secure a storage area network
- List ways to secure a database server
- Define social engineering
- Describe ways to prevent malware infections



Storage Area Network Security

- Isolated network
- LUN masking
- Separate SAN management interface on protected network
- Separation of duties

Database Server Security

- Isolated network
- Network, host, and database firewall rules
- OS hardening
- Principle of least privilege
- Database object, row, and column security
- Data masking
- Encryption of data in transit and data at rest

Social Engineering



- User deception
- Sensitive information disclosure
- Does not have to use technology

Malware Prevention

- User awareness and training
- Up-to-date antimalware solution
- Intrusion detection and prevention systems