

INFO5990: Professional Practice in IT

Week 9: Security Management

“Whether greater cybersecurity requires a greater sacrifice of our digital freedoms is an important debate that we should be having, preferably with all the facts in front of us”.

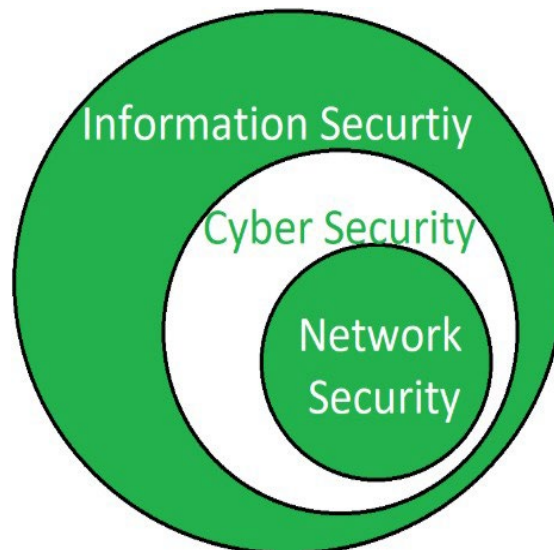
Evgeny Morozov



THE UNIVERSITY OF
SYDNEY

Information security

Information Security (InfoSec) refers to the practice of protecting information, in any form, from unauthorized access, disclosure, disruption, modification, or destruction. It ensures the confidentiality, integrity, and availability (the **CIA triad**) of data, whether it is stored, processed, or transmitted.



The General Data Protection Regulation (GDPR)

The Importance of Data Protection:	Data protection, especially personal data, is now a global priority for governments and organizations.
	With the rise of internet data and privacy risks, there's a growing need for robust regulations.
Introduction of the GDPR:	In 2016, the European Union (EU) recognized the need to update its data protection laws.
	The outdated 1995 Data Protection Directive was replaced with the General Data Protection Regulation (GDPR).
Key Features of the GDPR:	Effective from May 25, 2018, the GDPR sets new, uniform standards for data protection across the EU.
	It aims to enhance privacy rights and address risks associated with data processing.
Impact and Enforcement:	The GDPR imposes enforceable requirements on organizations handling personal data.
	Non-compliance can result in significant penalties, driving organizations to prioritize data protection.

How does it affect Australian businesses?

- Australian businesses are **subject to** GDPR if they:
 - have a presence in the EU; **or**
 - “offer” products or services to EU residents; **or**
 - monitor the behavior of EU residents (e.g. analytics on your website)

GDPR Key Aspects – 1

Scope and Applicability: The GDPR applies to all organizations that process personal data of individuals residing in the European Union (EU), regardless of the organization's location.

Consent and Lawful Basis for Processing: Organizations must obtain clear and explicit consent from individuals before processing their personal data. Additionally, they must have a lawful basis for processing data, such as contractual necessity or legitimate interests.

Enhanced Rights of Individuals: GDPR grants individuals various rights, including the right to access, rectify, erase, restrict processing, and data portability. Individuals also have the right to object to the processing of their personal data.

Data Protection by Design and Default: Organizations are required to implement data protection measures from the outset of any data processing activity (Privacy by Design) and ensure that only necessary data is processed (Privacy by Default).

GDPR Key Aspects – 2

Data Breach Notification: Organizations must report data breaches to the relevant supervisory authority within 72 hours of becoming aware of them. Individuals must also be notified without undue delay if the breach is likely to result in a high risk to their rights and freedoms.

Data Protection Officer (DPO): Some organizations are required to appoint a Data Protection Officer responsible for overseeing GDPR compliance, particularly for larger organizations or those processing sensitive data.

International Data Transfers: The GDPR imposes restrictions on the transfer of personal data outside the EU to ensure that such transfers meet certain standards of protection.

Accountability and Penalties: Organizations are accountable for complying with the GDPR and must be able to demonstrate their compliance. Non-compliance can result in fines of up to 4% of annual global turnover or €20 million, whichever is higher.

Individual Right – 1



Informed Consent: It requires demonstrating that data subjects have been informed about their right to consent, ensuring consent is freely given, specific, and unambiguous.

Example: A healthcare app must provide users with clear information about how their medical data will be used, and users must actively agree (consent) before their data is collected and processed for medical research purposes.



Access to Information: Organizations must provide a copy of collected data upon request, explain its usage, list any third-party access, and specify storage duration within a month of the request.

Example: Suppose an individual requests access to their social media account data from the platform. In that case, the platform must provide them with a copy of their profile information, posts, comments, and any other data collected, along with explanations on how this data is used and shared with third parties.



Anonymity or Pseudonymization: When necessary, organizations must transform identifying data to prevent unauthorized tracing back to individuals.

Example: An online survey platform may collect demographic information from respondents but removes their names and email addresses before analyzing the data to ensure respondents' identities are protected while still providing valuable insights.



Rectification: Compliance is required with requests to correct inaccurate data.

Example: If a customer's address is incorrectly recorded in an e-commerce database, they can request rectification, and the e-commerce company must promptly correct the address to ensure accurate shipping of goods.

Individual Right – 2



Objection or Restriction of Data Processing: Organizations must provide a legal reason for continuing data processing if objected by individuals, or demonstrate processing under limited circumstances with explicit consent.

Example: A marketing company must stop sending promotional emails to a customer who has opted out of receiving marketing communications or restrict the processing of their personal data for marketing purposes unless explicit consent is provided.



Data Portability: Compliance is mandatory with requests from data subjects to transfer their personal data to another organization.

Example: If a user decides to switch to a new cloud storage provider, they can request their personal data from their current provider to be transferred to the new provider in a commonly used and machine-readable format.



Erasure or Right to be Forgotten: Data subjects have the right to withdraw consent, necessitating permanent removal of their personal data from organizational records upon request.

Example: If a user closes their online account with a social media platform, they can request the permanent deletion of their account data, including all posts, comments, and personal information, from the platform's records.

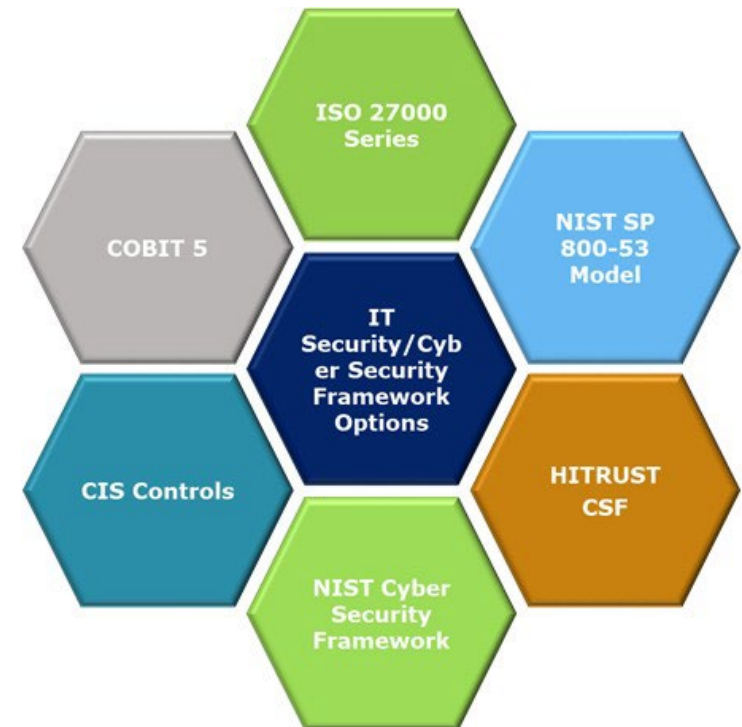


Breach Notification: Immediate notification to affected individuals and relevant supervisory authorities within 72 hours of becoming aware of a data breach deemed likely to compromise individuals' rights.

Example: If a healthcare provider experiences a data breach compromising patients' medical records, they must promptly notify the affected patients and relevant supervisory authorities within 72 hours of becoming aware of the breach.

Common Cybersecurity Standards

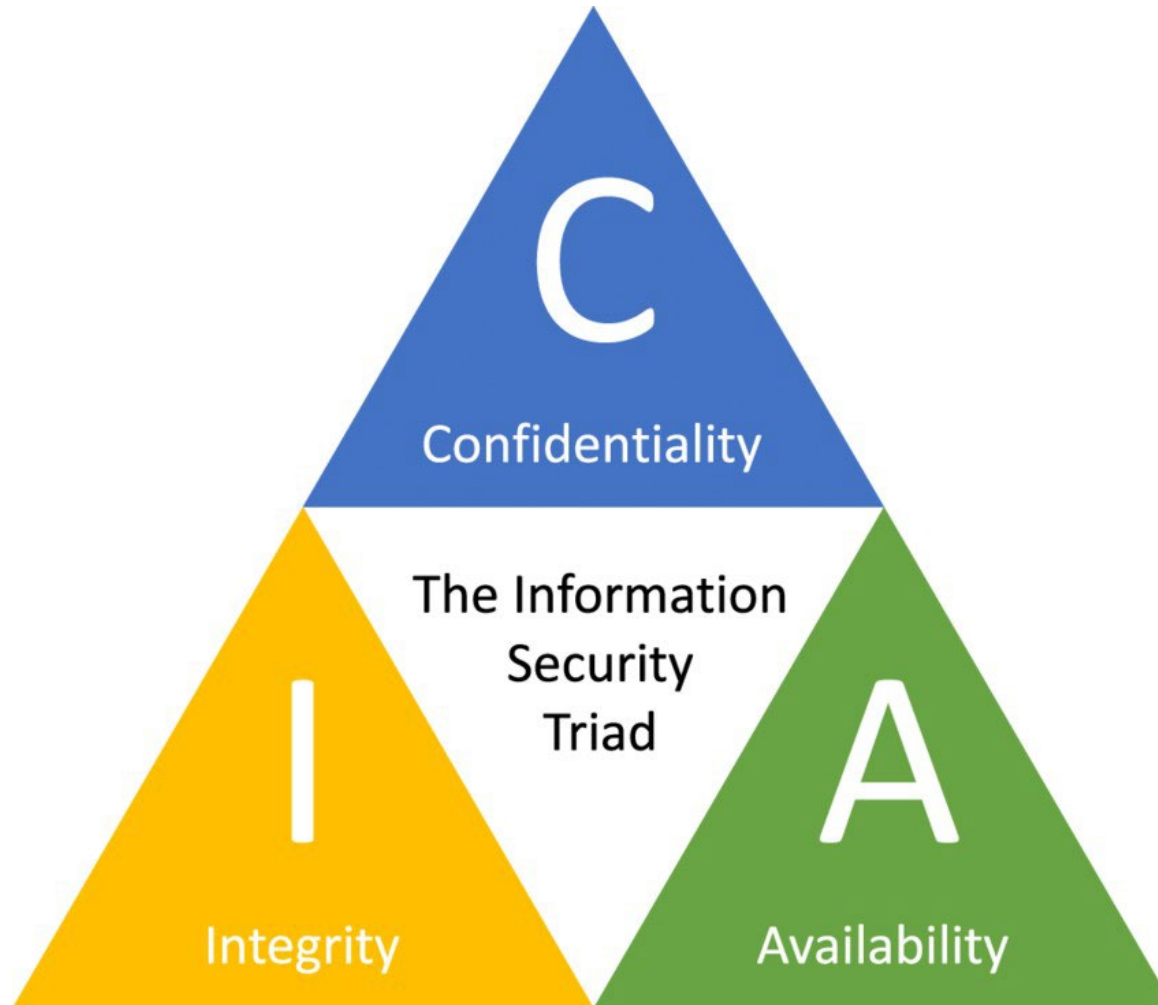
- ISO / IEC 27001: Establishes information security management systems (ISMS) for comprehensive security controls.
- NIST Cybersecurity Framework: Offers guidelines to manage and reduce cybersecurity risks across critical infrastructure sectors.
- PCI DSS: Focuses on secure payment card data handling for merchants and payment processors.
- HIPAA: Addresses security and privacy of healthcare information.



Types of Cyber Threats

- Malware, short for malicious software, includes viruses, worms, trojans, and spyware.
- Ransomware encrypts data and demands a ransom for its release.
- Phishing involves tricking individuals into revealing sensitive information, often through deceptive emails.
- Distributed Denial of Service (DDoS) attacks overwhelm systems with traffic to disrupt services.

Threats leading towards CIA Triad



Technical, Physical, and Administrative Controls

Security Controls	Technical Controls	Physical Controls	Administrative Controls
Focus	Technology-based measures for system, network, and data protection.	Measures to safeguard physical assets, facilities, and information.	Policies, procedures, and practices for security management.
Examples	Access control systems, firewalls, encryption, intrusion detection systems.	Perimeter security, surveillance systems, access badges.	Security policies, employee training, risk assessments, incident response.
Purpose	Manage access, prevent unauthorized use, ensure data integrity.	Prevent unauthorized access, tampering, and theft.	Set foundation for security framework, guide implementation.
Implementation	Utilizes technology and software to enforce controls.	Requires physical infrastructure, hardware, and facilities.	Involves policy creation, training programs, regular assessments.
Benefits	Protects digital systems, data, and information integrity.	Safeguards physical assets, deters unauthorized entry.	Educates personnel, identifies vulnerabilities, ensures compliance.





Best Practices

- Use Strong Passwords
- Enable Multi-Factor Authentication (MFA)
- Keep Software Updated
- Beware of Phishing
- Secure Web Browsing (HTTPS)
- Encrypt Sensitive Data
- Regular Data Backups
- Apply Least Privilege
- Employee Training
- Incident Response Plan

Password

- Use complex passwords with a mix of letters, numbers, and symbols.
- Avoid using easily guessable information like birthdays or names.
- Consider using a password manager to securely store and manage passwords.

Passwords Attacks

Brute-force attack		Attacker tries every possible combination of characters until they find the correct password
Dictionary attack		Attacker uses a prebuilt list of common passwords to guess the password
Rainbow table attack		Attacker uses a precomputed table of hashes to find the plaintext to a particular hash
Social engineering attack		Attacker uses psychological manipulation to trick the victim into revealing their password

Multi-Factor Authentication (MFA)

- Multi-Factor Authentication (MFA) enhances security by requiring multiple forms of verification. It adds an extra layer of defense against unauthorized access and cyber threats.
- How MFA Works:
 - Something You Know: Typically, a password or PIN.
 - Something You Have: A physical device like a smartphone, security token, or smart card.
 - Something You Are: A biometric factor like a fingerprint, facial scan, or iris scan.

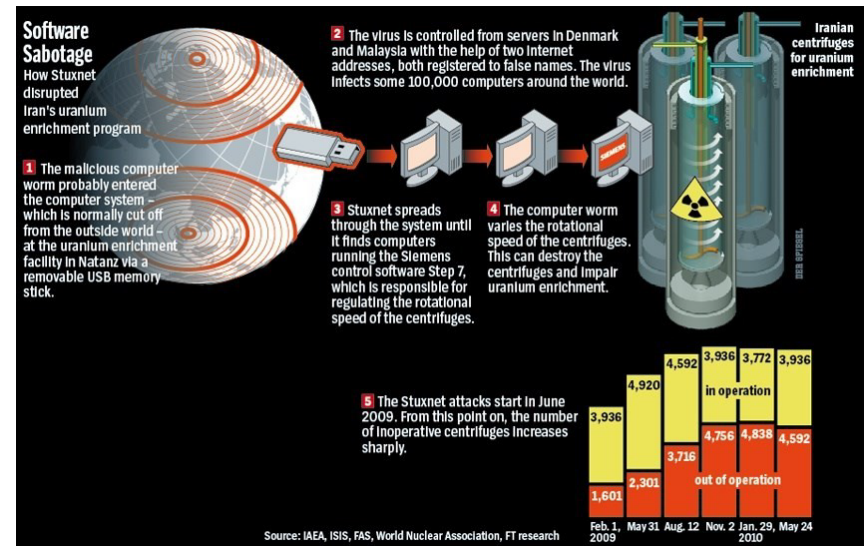
Social Engineering

- Definition: Social engineering is psychological manipulation that tricks people into revealing sensitive information or taking actions, aiding cyberattacks.
- Tactics:
 - Phishing: Fake emails seeking personal data or credentials.
 - Pretexting: Crafting false scenarios to extract information.
 - Baiting: Offering something enticing to trigger an action.
 - Quid Pro Quo: Providing something for data or access.



Advanced Persistent Threat (APT)

- Definition: APT is a sophisticated, prolonged cyberattack led by skilled actors with strategic intent.
- Characteristics:
 - Sustained Effort: Long-term planning, research, and execution.
 - Stealthy Operations: Evade detection using advanced techniques.
 - Customized Attacks: Tailored to target's vulnerabilities and industry.
 - Multi-Stage: Phases from initial compromise to data exfiltration.
- Examples:
 - Stuxnet: Damaged Iran's nuclear centrifuges.



STRIDE threat modelling

- Created by Microsoft
- STRIDE threat model has been widely adopted throughout the industry
- Provides a standardised way of describing threats by their attributes
- Developers can use this model to attempt to discover flaws and vulnerabilities in the software they're creating

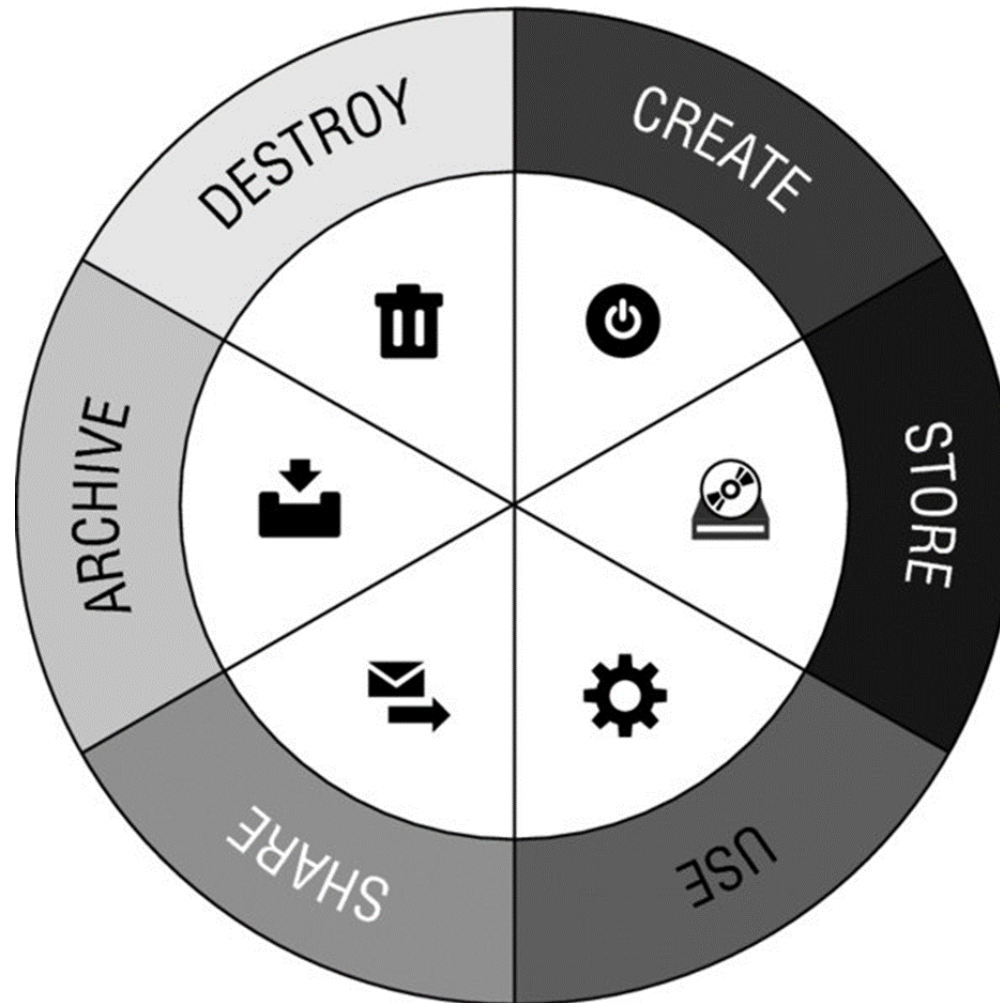
STRIDE

Letter	Threat Type	Description
S	Spoofing	Impersonating something or someone else.
T	Tampering	Modifying data or system components maliciously.
R	Repudiation	Denying performing an action without others being able to prove otherwise.
I	Information Disclosure	Exposing information to unauthorized individuals.
D	Denial of Service	Disrupting or degrading service availability.
E	Elevation of Privilege	Gaining unauthorized access or higher-level permissions.

STRIDE

Tool	Description
Microsoft Threat Modeling Tool	The official tool designed specifically to implement STRIDE-based threat modeling easily through diagrams.
OWASP Threat Dragon	An open-source, web-based and desktop tool for threat modeling — supports STRIDE methodology.
IriusRisk	A powerful threat modeling and risk management tool that supports STRIDE and integrates with DevOps pipelines.
Threagile	Open-source YAML-based threat modeling tool — supports STRIDE threats.
ThreatModeler	Enterprise-grade tool for automated threat modeling, uses STRIDE among other frameworks.
Pytm (Python Threat Modeling)	Code-based threat modeling using Python, supports STRIDE threat identification.

Data Lifecycle



Contingency Strategies

- Incident Response Plan (IRP)
- Disaster Recovery Plan (DRP)
- Business Continuity Plan (BCP)

Incident Response

- Even with a secure infrastructure, incidents can still happen due to various reasons such as human error, system vulnerabilities, or external attacks.
- Incident response is the process of **identifying, analysing, and responding** to security incidents, breaches, or other disruptions that impact the confidentiality, integrity, or availability of an organisation's information assets.
- Incident response is important because it helps organisations quickly and effectively respond to and recover from security incidents, minimising the impact on the organisation, its customers, and stakeholders.

Log vs Alert vs Metric

Log	Alert	Metrics
A record of a specific thing that happened	A type of event where the system decides it's worth notifying someone	A set of numbers that give information about something
Generated in response to an event	Generated in response to a predetermined threshold or condition	Collected on a time-based basis
Provides detailed information about an event	Signals a potential problem or significant event	Measures the performance or state of a system or component
Can be used for investigation, troubleshooting, or compliance purposes	Requires immediate attention or action	Used for monitoring, trend analysis, or capacity planning
Examples: authentication logs, web request logs, system logs	Examples: intrusion detection alerts, antivirus alerts, network anomaly alerts	Examples: CPU usage, memory usage, network bandwidth, response time
Avoid including passwords, API keys, sensitive personal information, protected health information, or any other sensitive data in logs.		

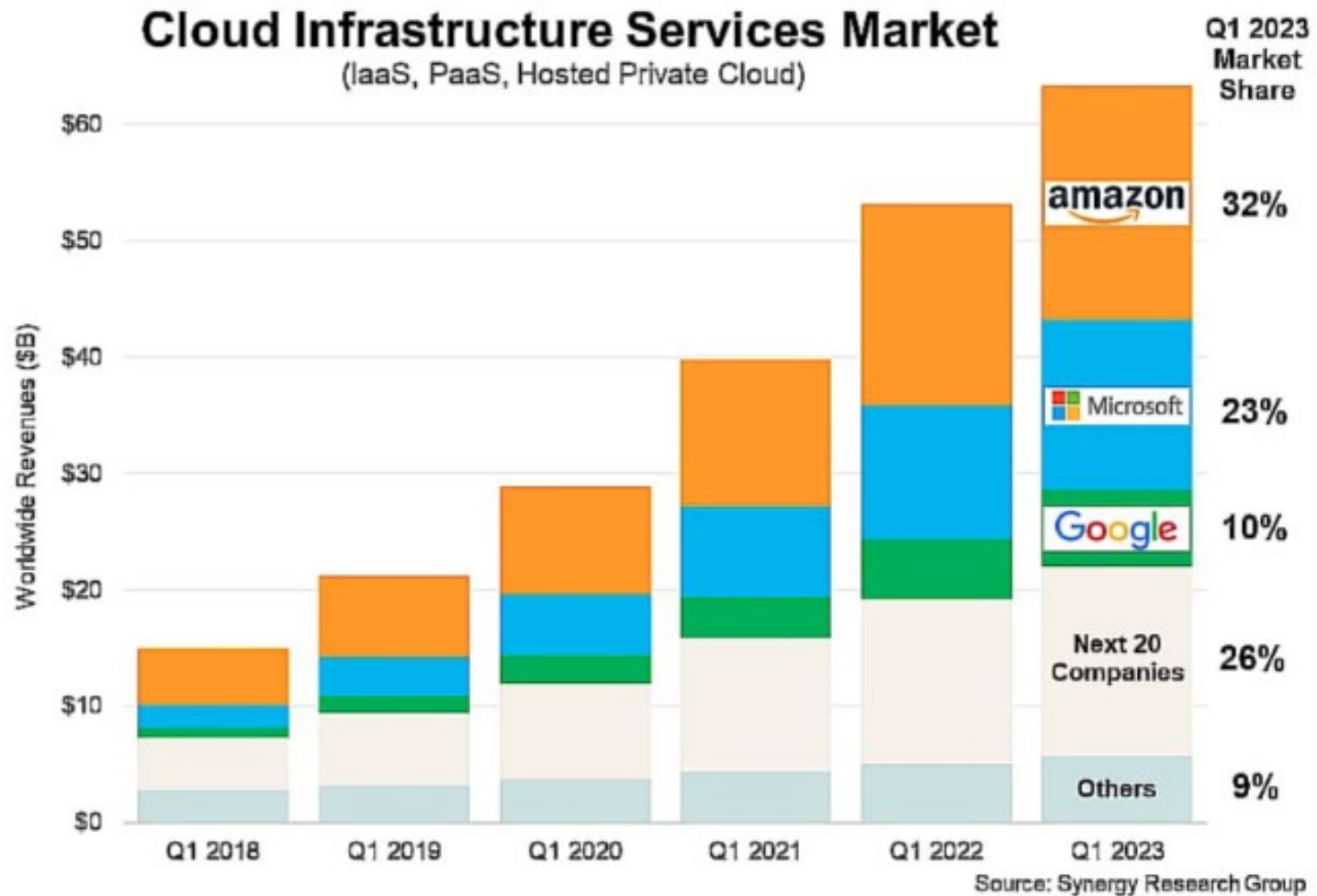
Incident Response Testing

Exercise type	Description	Participants	Focus
Tabletop exercises	Scenario-based discussion led by a facilitator to analyse response to a simulated incident	Team members	Analysis of response
Functional exercises	Simulated incident scenario where team members simulate their roles and responsibilities in response to an incident	Team members	Simulation of roles and responsibilities
Full-scale exercises	Comprehensive simulations of an incident response involving a broad range of team members, systems, and procedures	Broad range of team members	Comprehensive testing of incident response
Red teaming	Testing where a team of experts simulate an attack to identify vulnerabilities and test the effectiveness of the organisation's defenses	Experts	Identification of vulnerabilities and testing effectiveness of defenses

DRP Vs BCP

	Disaster Recovery (DR)	Business Continuity (BC)
Focus	IT systems and data recovery	Overall business operations
Objective	Minimize IT downtime	Ensure business continuity
Scope	Limited to technology	Holistic, including people, processes, technology
Timeframe	Short-term recovery	Long-term sustainability
Components	Data recovery, backup	Crisis management, planning
Testing	IT systems and data	Comprehensive business plans
Dependency	Subset of Business Continuity	Encompasses Disaster Recovery

Cloud Adoption



<https://www.cloudzero.com/blog/cloud-computing-market-size/>

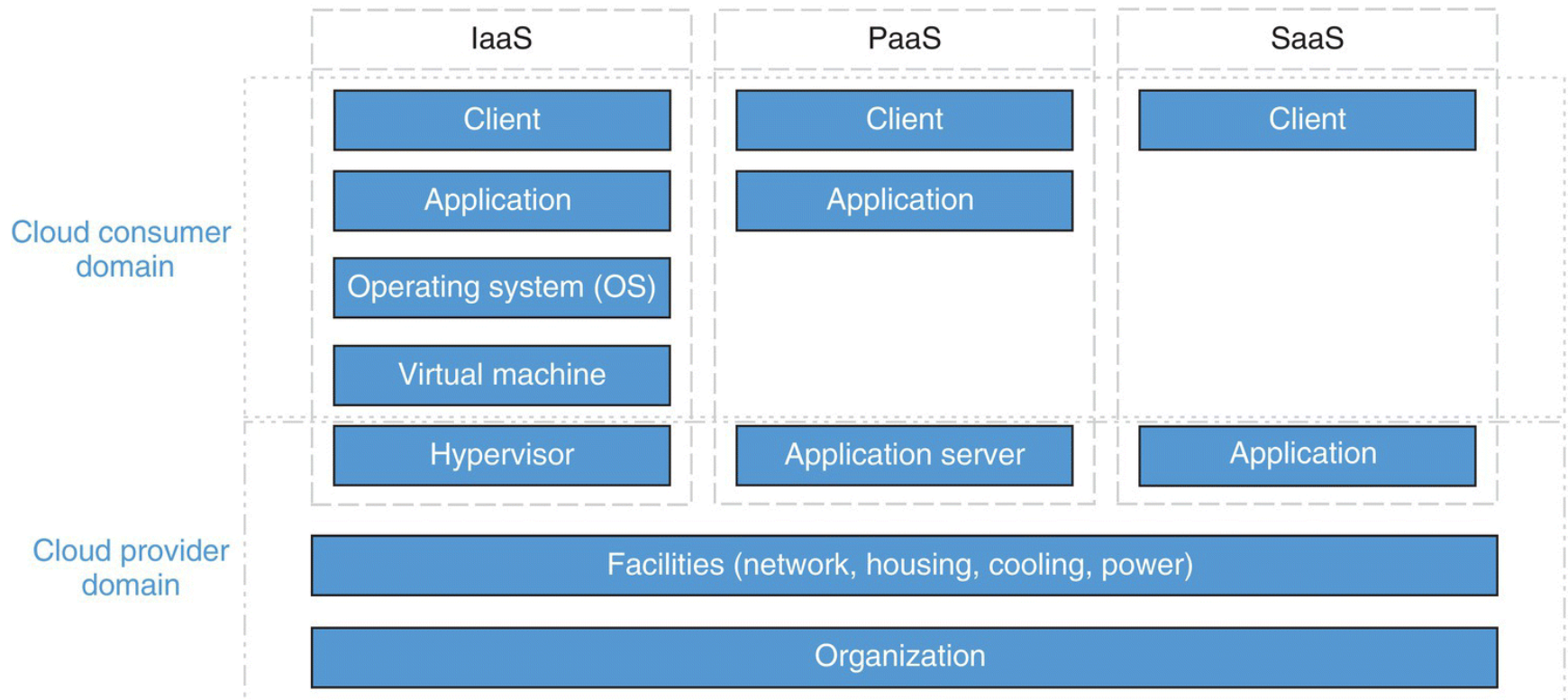
Deployment Models

- **Public cloud:** The infrastructure is owned and managed by the service provider and is located in the provider's facilities. It provides services to the public.
- **Private cloud:** It is dedicated entirely for a single organisation. It resides in the organisation's facilities or hosted and managed by a third-party provider.
- **Community cloud:** Multiple organisations share resources and services based on common requirements.
- **Hybrid cloud:** This is a combination of the private, public, or community clouds.

Virtualisation

- Virtualisation allows multiple virtual machines (VMs) to run on a single physical machine by partitioning the resources of the physical machine into multiple virtual environments
- Components include:
 - Hypervisor
 - Guest OS
 - Host OS
 - Virtual network
 - Virtual storage

Cloud Service Models



Exam Questions for Discussion

Question. Please read the scenario carefully and answer the questions:

CIA Failures in Remote Development Project

Scenario:

An Australian tech company outsources development to remote freelancers. During a version control sync, they discover that:

- **Source code was leaked publicly** (confidentiality breach),
- **A core script was altered maliciously** (integrity breach),
- **The central server crashed due to an untested update** (availability issue).

Weak access policies and no centralized oversight led to a **triple failure across the CIA triad**. The BCP only addressed server hardware failures and not insider or operational risks.

Exam Questions for Discussion

Q1. How were all three CIA principles violated in this scenario?

A1.

- **Confidentiality:** Source code was published to a public repository or shared externally, exposing intellectual property.
 - **Integrity:** The core logic in a script was modified without authorization, affecting functionality and reliability.
 - **Availability:** The server crashed due to unapproved updates, making the system unavailable to users.
- These breaches reveal poor governance over codebase, access rights, and change management in a remote setting.

Q2. What secure development practices could prevent such issues?

A2.

- Use of **enterprise-grade version control systems** like GitHub Enterprise with granular access control.
- Mandatory **pull request reviews and approvals** before merging code.
- **Automated CI/CD pipelines** with testing and validation before deployment.
- Use of **secrets management tools** to avoid credential exposure.
- **Secure communication protocols** (e.g., VPN, SSH) for all remote contributors.

Exam Questions for Discussion

Q3. Why is centralized version control critical in remote projects?

A3. Centralized version control provides:

- **Traceability** of every code change and its origin.
- **Access control enforcement**, ensuring only authorized users commit to production branches.
- **Branch protection rules** and auditing of merge histories.
- Easier **recovery and rollback** if changes cause issues.

In remote teams, this becomes crucial for maintaining oversight and quality.

Q4. What BCP improvements can address multi-dimensional CIA breaches?

A4. The BCP should be enhanced to include:

- **Role-based access and onboarding/offboarding protocols** for developers.
- **Activity monitoring tools** to track code changes and access patterns.
- **Incident playbooks** for code leak, tampering, or server crashes.
- **Backup repositories and version snapshots** to ensure code integrity and availability during outages.
- **Periodic CIA audits** across infrastructure and repositories.

Exam Questions for Discussion

Question. Please read the scenario carefully and answer the questions:

Compromised Remote Device in Government Project

Scenario:

A student intern working on a smart city project accesses internal systems using a personal laptop. The device is unknowingly infected with a keylogger. It captures credentials and provides an external attacker access to sensitive internal resources. The organization's BCP did not include endpoint protection or Bring Your Own Device (BYOD) threats. The breach halted progress on the project and triggered a full internal review.

Exam Questions for Discussion

Q1. What are the dangers of using personal devices in sensitive projects?

A1. Personal devices often lack enterprise-grade security tools, meaning they are more likely to be unpatched, outdated, or unmonitored. They provide no centralized control for security teams and increase the attack surface, especially when accessing critical infrastructure.

Q2. How could this malware have been detected before spreading?

A2. Endpoint Detection and Response (EDR) tools would have flagged anomalous behavior such as credential dumping, unknown processes, or data exfiltration. Also, enforcing mandatory security checks before remote connection could have prevented device access altogether.

Exam Questions for Discussion

Q3. What should the updated BCP include after such an incident?

A3. The revised BCP should include BYOD policies, device health checks, and remote isolation protocols. It should also define procedures for quickly revoking compromised credentials and limiting device access.

Q4. How can a Zero Trust model reduce risks in remote environments?

A4. Zero Trust continuously verifies each access request based on user identity, device health, and location. Even if a device connects, its permissions are tightly scoped, and access to sensitive resources is conditional and monitored, which reduces the blast radius of such attacks.