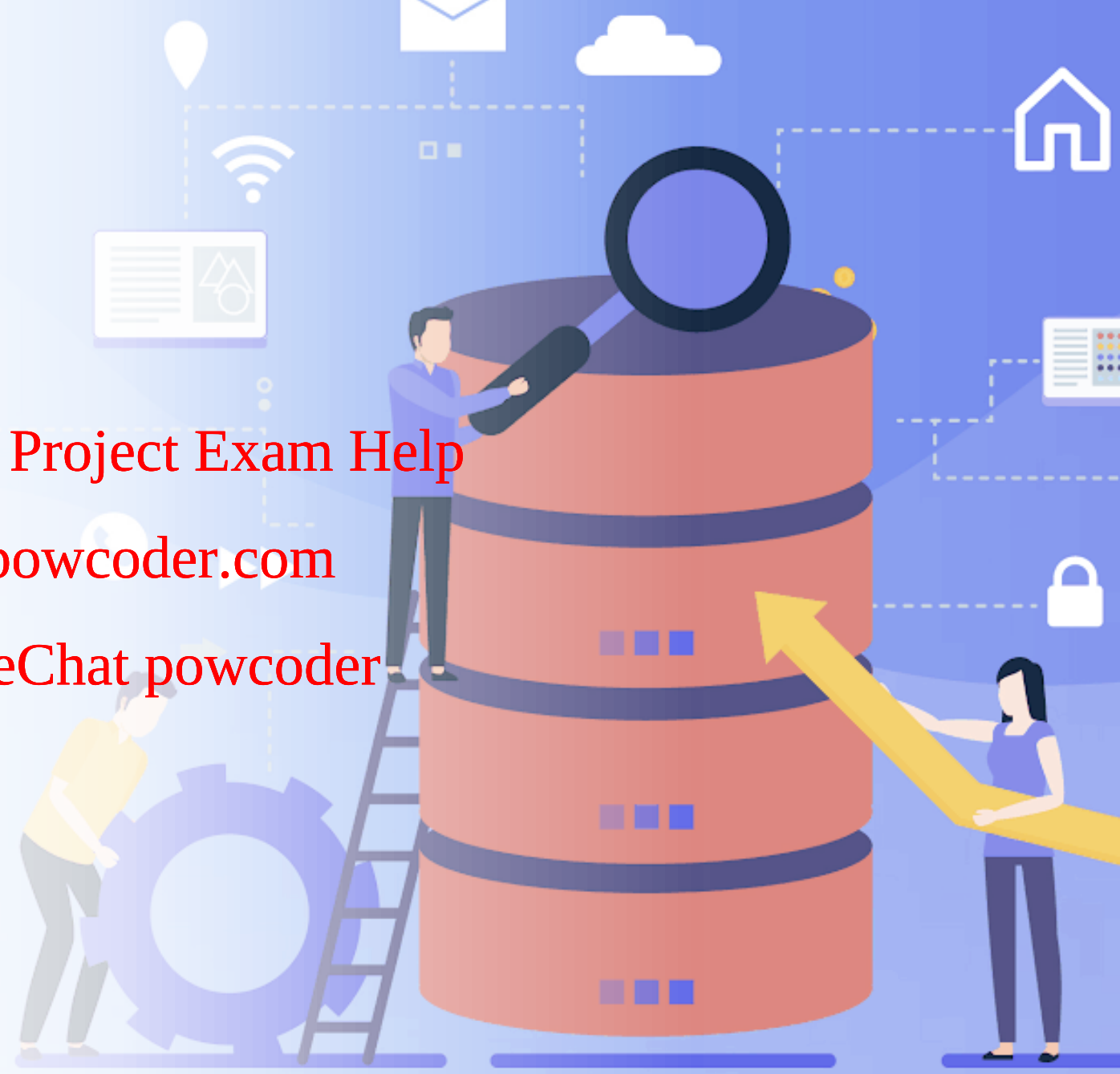
Database Security

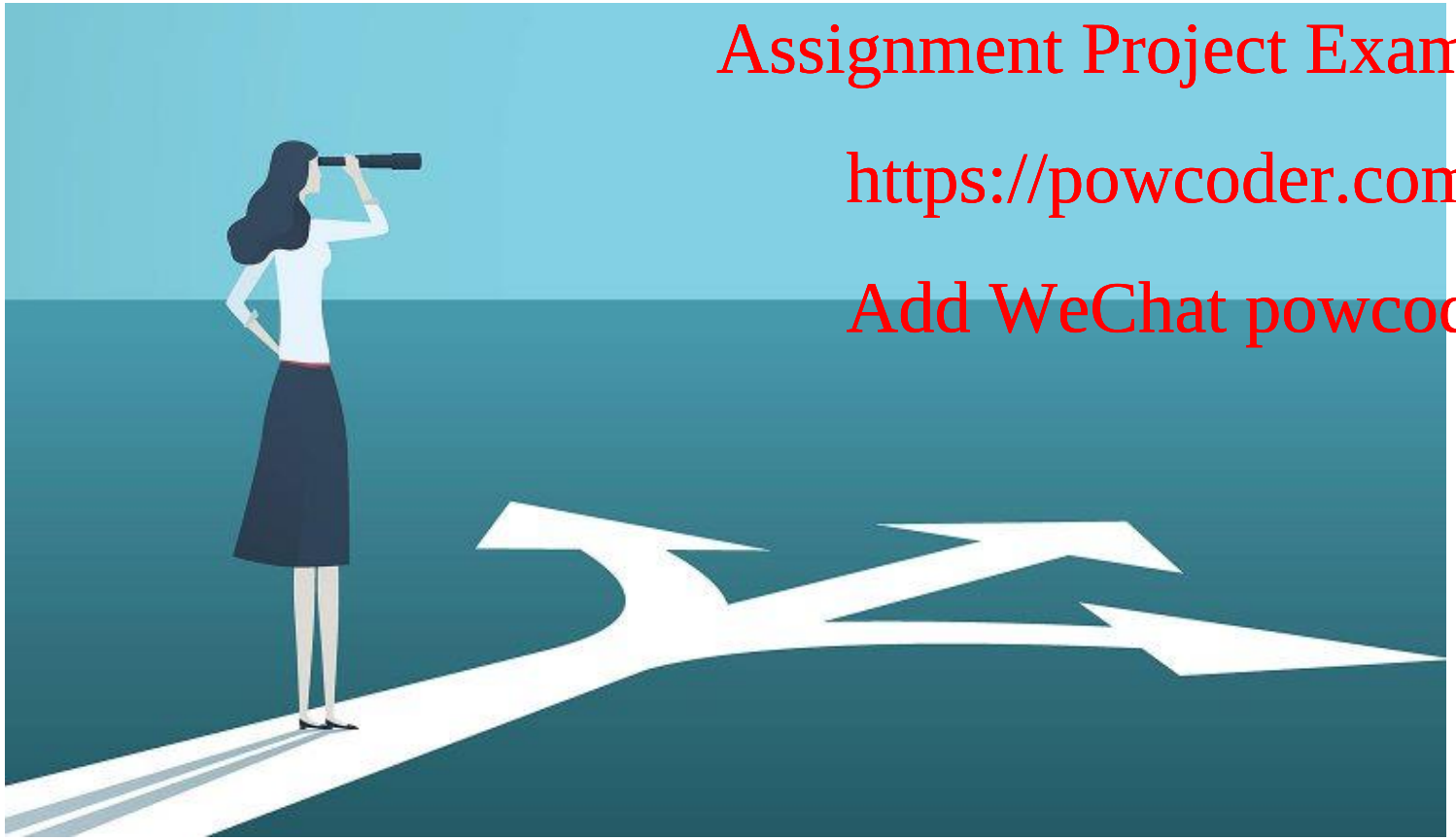
Shesha M.

Agenda

- Security 101
- Database Security?
- Its importance
- Attacks
- Mitigation



A bit about me.



- Education
- Industry

Security 101

- Security is about protecting assets
  - Systems
  - Devices
  - Networks
  - Data
- Information security, Information systems security, computer security, cybersecurity
- *Measures used to protect the confidentiality, integrity and availability of systems and information* (ACSC)

How do we protect our assets?

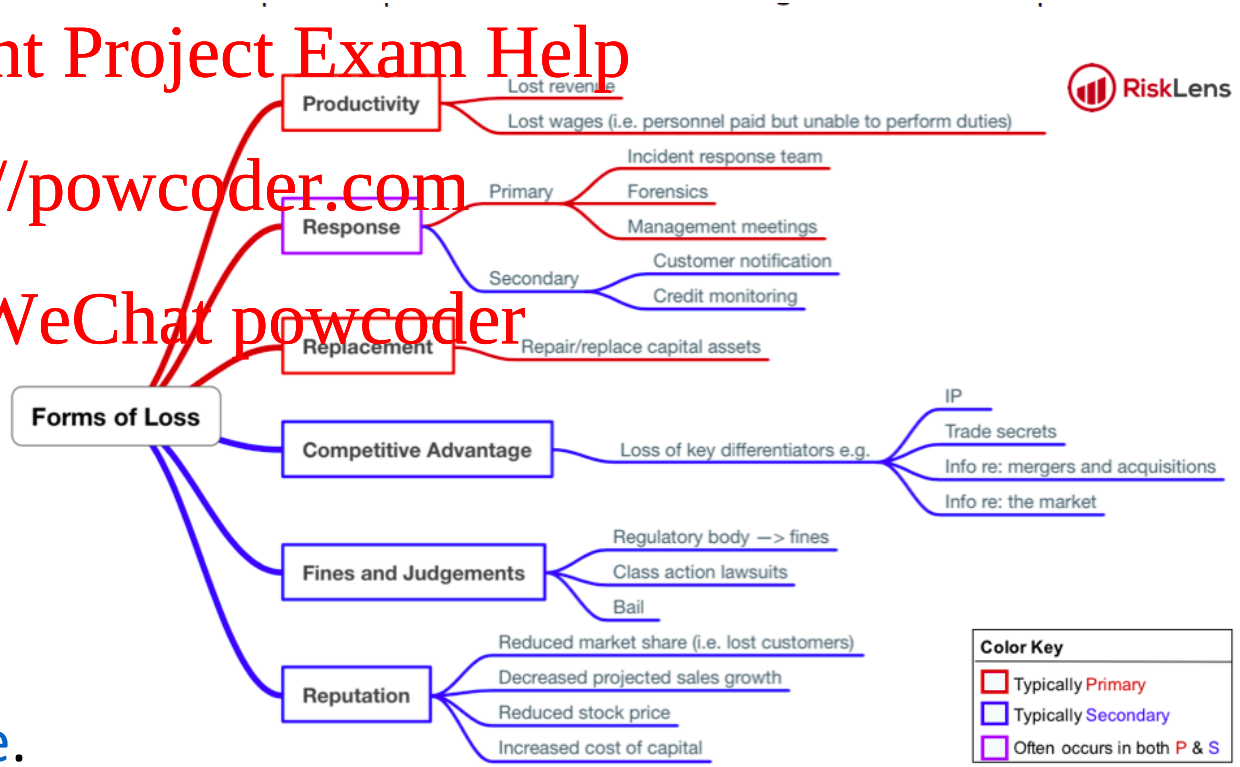
- By protecting:
  - Confidentiality
  - Integrity
  - Availability
- One may be more important than the other
  - E.g. Information Tech vs Operational Tech
  - Corporate Systems vs Industrial Control Systems (ICS)
- Implement countermeasures to assure the above

Who do we need to protect the assets from?

- Threat actors
  - *An entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact – an organisation's security* (ACSC)
- Each have their own motive
  - ACSC detail a lot more threats
  - FireEye have threat reports
- Risks can be:
  - Internal/External
  - Natural/Man-made
    - Man-made can be: Malicious/Accidental

Why do we need to protect our assets?

- Because vulnerabilities exist:
  - Technical
  - Process
  - People
- Humans are the “weakest” link – NO.
- Consequences and Loss
  - FAIR Framework’s Six Forms of Loss
  - You can read more about these here.



Source: FAIR Institute

Source: NIST Cybersecurity Framework

How do we protect the assets?

- Risk Management – understand the risk appetite
  - Identify the risks
  - Analyse and prioritise
  - Action and monitor
  - Residual Risk
- Qualitative vs Quantitative
- Risk Management Strategies (CompTIA)
  - Mitigation
  - Avoidance
  - Transference
  - Acceptance

Database security

- *Database security refers to the range of tools, controls, and measures designed to establish and preserve database confidentiality, integrity, and availability* (IBM)
- Purpose is to protect:
  - Data in databases
  - Database Management System
  - All applications connected to database
  - Database Server and associated infrastructure

Why is Database Security important?

- Data → Information
  - Reveal insights
  - Intellectual property
  - Trade secrets
  - Reputation
  - Compliance
- Threats and vulnerabilities exist

Threats and Vulnerabilities

- Database configurations
- Data itself
  - Sensitive data in DEV., TEST, PROD. environments
- Passwords
- User Access
- Human error
- Cloud – deployment model
- Third parties/Suppliers

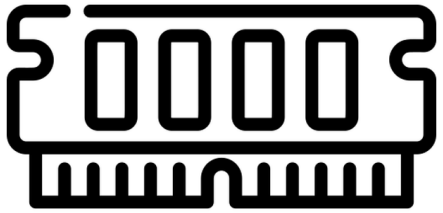
Exploiting the vulnerabilities

- SQL injection
- Buffer overflow
- DoS/DDoS
- Malware
- Ransomware
- Data breach

Deep dive – SQL Injection Attacks

- SQL Injection
  - Inserting SQL query via the input data from the application to database
  - Access and read sensitive data from the database
  - Modify data – insert, update, delete
  - Extract data
  - Execute administration operations/commands – e.g. shutdown
- Consequences:
  - Compromised confidentiality, integrity
- Example: SQL Injection
- Can read more here.

Deep dive – Buffer Overflow Attacks



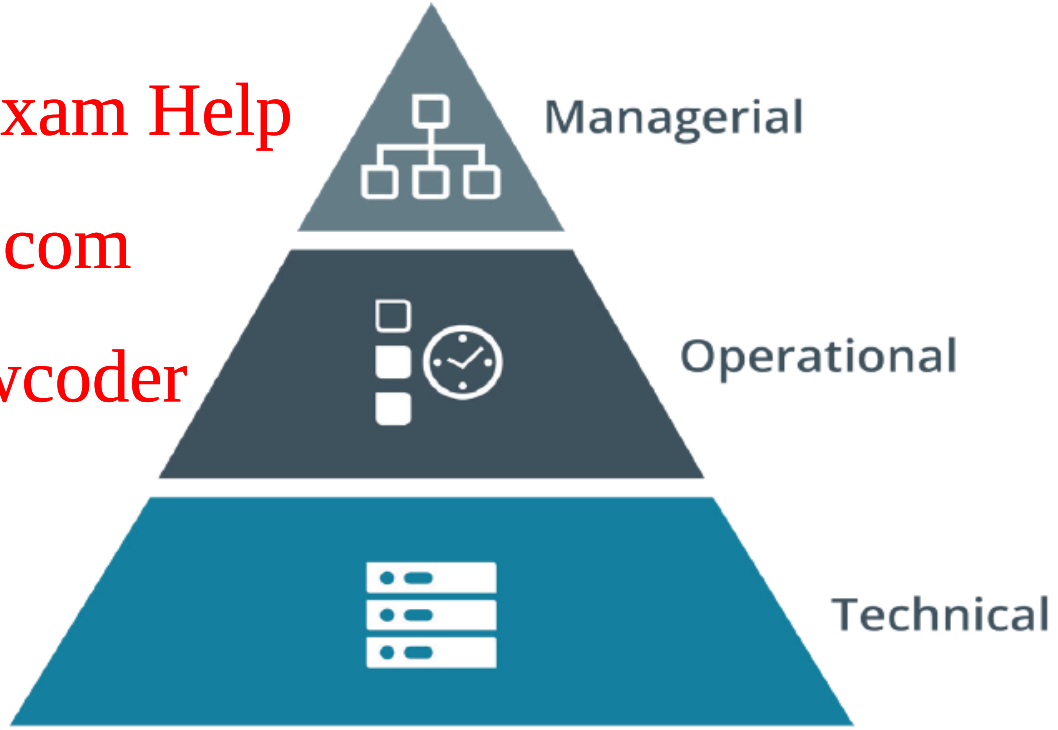
- Buffer – temporary storage to store data for a short time – generally in RAM
- Overflow – program/application tries to write more data to a buffer that it can hold – so the data leaks into adjacent buffers
- Consequences:
  - Compromised availability – application crashes
  - Data corruption
  - Can lead to corrupted back-up copies too
- Example: Buffer Overflow
- Can read more here.

Other attacks

- DoS/DDoS
  - Denial of Service/Distributed Denial of Service
  - Disrupting systems/applications in a way that they become inaccessible to intended users
- Malware
  - Malicious Software
  - Designed to harm systems/devices/applications/networks
  - E.g. Virus, Worms, Trojan, Spyware, Adware
- Ransomware
  - Type of malware
  - Encrypts files and data, and a ransom is demanded
- Data breach
  - Confidential/Sensitive/Personal data is accessed without authorisation by an untrusted user

Mitigations

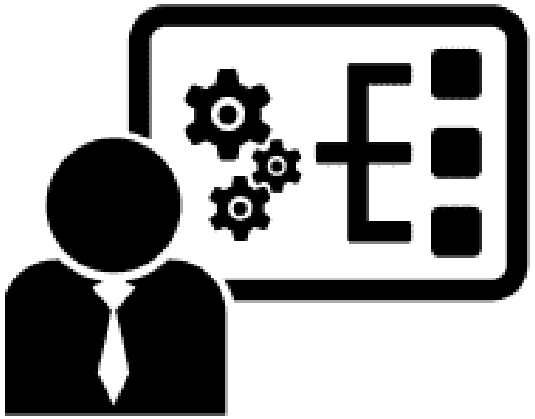
- Managerial
  - Controls that give an oversight of the information system
  - E.g. Tool to identify and manage cyber risks
- Operational
  - Controls implemented by people
  - E.g. Training and awareness programs
- Technical
  - Aka Logical Controls
  - Controls implemented as a system
  - Can be hardware, software, firmware
  - E.g. Firewalls, or Anti-virus
- Function: Preventive, Detective, Corrective



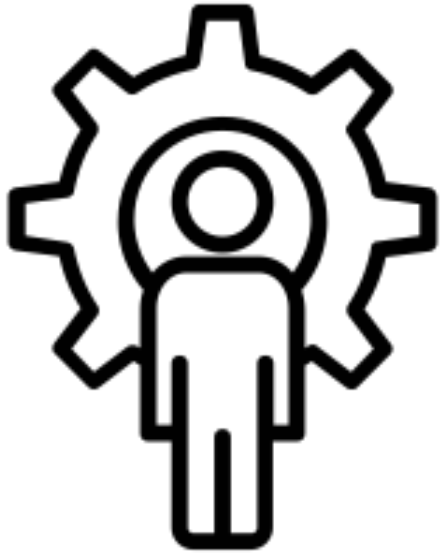
Categories of Security Controls (CompTIA)

Managerial Controls

- Defence in depth
- Risk assessments and management
  - Risk Owner? Actions?
  - Cloud vs On-premise solutions
- Compliance
  - Frameworks
  - Standards
  - Policies
  - Regulations
  - E.g. Payment Card Industry Data Security Standard (PCI DSS)
- Audit
  - Regular auditing
  - Implement recommendations based on audit findings
- Password Policies
  - Need to be enforced – via various operational and technical controls
- DevSecOps
  - Integrating security in the development phases



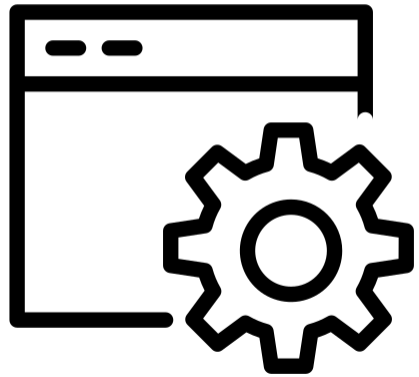
Operational Controls



- User Training and Awareness
  - Security culture
- Physical security for data centres
  - Data centres are where servers sit – on which databases are
  - CCTV monitoring
  - Guards
  - Locked doors/cabinets
- Separation of duties
  - E.g. for financial or HR functions
- Backup
  - Differential vs Incremental
  - Offline vs Offsite
  - 3-2-1 rule
- Patch Management
  - Test the patches in TEST environment
- Documentation
  - Development – e.g. requirements
  - Configuration – e.g. network diagrams, IP schema
  - Decisions and justification

Technical Controls

- Database configuration
  - Access Control – Lock down user accounts – need to know basis
  - Strengthen database authentication to reduce risk of compromised credentials
  - Anonymisation of data in PROD environments
  - Data masking
  - Vaults – data, database, key
- Encryption
  - Data in use – even if you encrypt data at rest, you must decrypt at some point for the data to be usable
  - Data at rest; Data in transit
- Logging and monitoring
  - Activate alerts and notifications – false positives vs false negatives
  - On database SQL traffic, user access, user activity
- Database firewalls - Rules
  - Host-based vs Network-based
- Cloud Configuration
  - Understand risks associated with cloud solutions
  - Access to data
  - Security updates and patches
- Data Loss Prevention solutions



Further reading

- Oracle
  - http://www.oracle.com/au/database/technologies/security.html