SECURITY+ EXAM CRAM

THE COMPLETE COURSE

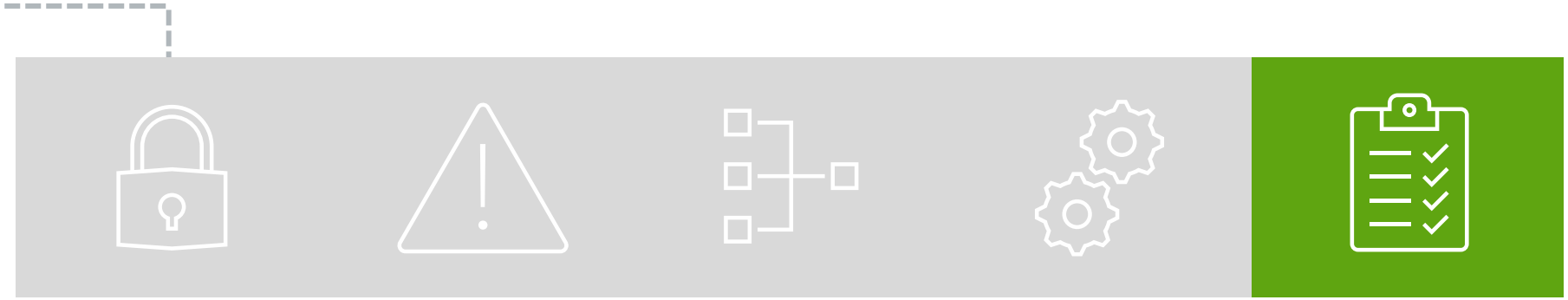
2024 EDITION

DOMAIN 5

Coverage of every topic in the official exam syllabus!

Series playlist in video description

with **Pete Zerger** vCISO, CISSP, MVP



- 5.0 Security Program Management and Oversight

line-for-line review of the official exam syllabus!

5.0 SECURITY PROGRAM MANAGEMENT AND OVERSIGHT

5.1 Summarize elements of effective security governance

- **Guidelines**
- **Policies**
  - Acceptable use policy (AUP)
  - Information security policies
  - Business continuity
  - Disaster recovery
  - Incident response
  - Software development lifecycle (SDLC)
  - Change management
- **Standards**
  - Password
  - Access control
  - Physical security
  - Encryption
- **Procedures**
  - Change management
  - Onboarding/offboarding
  - Playbooks
- **External considerations**
  - Regulatory
  - Legal
  - Industry
  - Local/regional
  - National
  - Global
- **Monitoring and revision**
- **Types of governance structures**
  - Boards
  - Committees
  - Government entities
  - Centralized/decentralized
- **Roles and responsibilities for systems and data**
  - Owners
  - Controllers
  - Processors
  - Custodians/stewards

Security Policy
Sets the overall vision and goals for information security.

Security Standards
Translate the policy into specific technical requirements and best practices.

Security Procedures
Provide detailed instructions on how to implement the standards.

Security Guidelines
Offer additional recommendations and best practices that can be adopted to further enhance security.

Security Guidelines

Function: Offers recommendations and best practices for achieving security objectives but are not mandatory.

They provide the "could" for additional security measures.

Specificity: Least specific, offering recommendations that can be adapted to specific situations.

Example:
“Employees are encouraged to take advantage of security awareness training programs.”

Security Policies

Function: Provide the overall high-level direction and objectives for information security within an organization.

It defines the "why" behind security measures.

Specificity: General statements and principles, often broad in scope.

Example:
“The organization is committed to protecting the confidentiality, integrity, and availability of its information assets.”

Security Policies

Function: Provide the overall high-level direction and objectives for information security within an organization.

It defines the "why" behind security measures.

Specificity: General statements and principles, often broad in scope.

Policies are a major input to procedures

POLICIES

Acceptable Use Policy

Defines allowed/appropriate uses of the organizations IT resources (computers, software)

Prohibits activities that could compromise security

(e.g., downloading unauthorized software, using social media during work hours)

Information Security

Sets the overall direction for information security within the organization

Outlines the organization's commitment to protecting data, security practices, and user responsibilities

POLICIES

Business Continuity

a high-level document that outlines the organization's commitment to maintaining critical business functions during disruptions

Defines the organization's overall strategy for business continuity

Disaster Recovery

Focuses on recovery from disasters (natural disasters, major outages)

Can guide the IT/Security efforts in designing and implementing systems and services

POLICIES

Incident Response

Sets the high-level direction for how the organization will identify, contain, eradicate, and recover from security incidents

Software Development Lifecycle

High-level guidance that software development teams must follow in creating software

Acts as a roadmap, ensuring quality, security, and efficiency during development.

Security Standards

Function: Defines mandatory technical specifications and best practices for implementing the security policy.

It provides the "what" and "when" for achieving security goals.

Specificity: More detailed than policies, specifying technical requirements for systems, configurations, or processes.

Example:
“Credit card data must be encrypted at rest, in transit, and in use, using a compliant encryption algorithm.”

Password

Defines password complexity and password management practices (frequent changes, avoiding reuse).

Entities such as NIST and CIS maintain guidance in this area

Access Control

Specify who has access to specific systems, data, and resources based on the principle of least privilege.

ISO 27001 offers guidance on ISMS requirements that can guide orgs

Physical Security

Outline measures to protect physical access to IT systems and data centers

(e.g., access badges, security cameras, fire suppression, HVAC).

ANSI, NFPA, ISO, and NIST offer guidance, and many industry-specific entities exist.

FIPS 140-2/3 is a mandatory standard for protection of sensitive data within Federal systems.

Encryption

Specify the algorithms and key management practices for encrypting sensitive data at rest and in transit to ensure confidentiality.

Evolve over time, will be impacted by quantum computing

Security Procedures

Function: Provides step-by-step instructions on how to perform specific tasks related to security controls.

It defines the "how" for implementing standards.

Specificity: Highly detailed, outlining the exact actions to be taken in specific situations.

Example: Procedure for Incident Response: Upon discovering a security incident, follow these steps:

1. Isolate the affected system.
2. Notify the security team.
3. Document the incident.

How Policies Affect Procedures

Derive from Policies: Procedures are directly derived from the specific requirements outlined in corporate policies.

Ensure Consistency: Procedures ensure consistent implementation of policies across the organization.

Provide Clarity: Procedures translate broad policy statements into clear, actionable steps for employees to follow.

Facilitate Training: Procedures serve as a reference point for training employees on how to comply with policies

An analogy

Policy is the recipe:

The recipe would state inputs and outputs

- ingredients (data, resources)
- desired outcome (secure environment, efficient operations).

Procedures are the cooking instructions:

They would detail the steps (how-to) for

- mixing ingredients (data handling)
- cooking temperature (security protocols)
- cooling time (incident response protocol).

PROCEDURES

Change Management

Detail the steps involved in proposing, reviewing, approving, implementing, and documenting changes to IT systems and infrastructure.

Ensures security risks are assessed and mitigated.

Onboarding/Offboarding

Outline processes for granting access to new employees and revoking access for terminated employees.

Ensure appropriate access controls are maintained.

Playbooks

Detailed step-by-step instructions for responding to specific security events, ensuring a consistent and efficient response.

In the SOC, playbooks are automated as runbooks in SOAR

EXTERNAL CONSIDERATIONS

Regulatory

Compliance with data privacy regulations like GDPR, HIPAA, and PCI DSS may dictate specific security controls and reporting requirements.

Will influence corporate policies, processes, and procedures.

Legal

Laws concerning data breaches, electronic discovery, and intellectual property can influence security practices.

Industry

Industry best practices and standards relevant to your sector may provide additional security guidance.

Most impactful to regulated industries and high-risk areas

Local/Regional/National/Global

Local, regional, national, and international laws and regulations can all impact security requirements.

Policies, processes and procedures should address all of these

MONITORING AND REVISION

Effective security governance is a **continuous process**, not a one-time task.

Monitoring

Security audits, regular reviews of access logs, periodic vulnerability scans, and analysis of incident response metrics.

Can highlight areas where the security measures are working and where improvement is needed

Revision

Process of updating security governance documents and practices

Changes are based on the insights gained from monitoring

Changes in corporate strategy may trigger need for revision

TYPES OF GOVERNANCE STRUCTURES

Security governance is a process for overseeing the cybersecurity teams who are responsible for mitigating business risks.

Security governance leaders make the decisions that allow risks to be prioritized

This ensures security efforts are focused on business priorities rather than their own

The different **security governance structures** include:

- Boards
- Committees
- Government Entities
- Centralized/Decentralized

The most effective security governance structure depends on organization's size, complexity, and risk profile

TYPES OF GOVERNANCE STRUCTURES

Security governance is a process for overseeing the cybersecurity teams who are responsible for mitigating business risks.

Boards

Typically, a Board of Directors, holds the highest level of authority within an organization.

Their decisions are binding on the entire organization.

Committees

Subgroups within an organization that focus on specific areas or tasks, often created by and reporting to the board.

Authority is limited to the specific area they are assigned to oversee and focus may vary

TYPES OF GOVERNANCE STRUCTURES

Security governance is a process for overseeing the cybersecurity teams who are responsible for mitigating business risks.

Government Entities

Government agencies, such as the National Institute of Standards and Technology (NIST) in the US.

These entities may issue security regulations, standards, and best practices that organizations must comply with.

In some cases, only providing oversight to government entities, but in other cases to regulated industries

FedRAMP only applies to government agencies, but U.S. Government provides oversight to banking & healthcare

TYPES OF GOVERNANCE STRUCTURES

Security governance is a process for overseeing the cybersecurity teams who are responsible for mitigating business risks.

Centralized

Security decisions and controls are managed by a central security team.

Sets policies and standards for the entire organization

Decentralized

Delegates security decisions and controls to some extent to business units or departments.

A central security team typically provides guidance and oversight in this model.

KNOW THESE TWO ROLES!

The most likely to show up on the exam?

Data Owner

Holds the legal rights and complete control over a single piece of data.

Usually a member of **senior management**. Can delegate some day-to-day duties. CANNOT delegate total responsibility!

Data Custodian

Responsible for safe custody, transport, and storage of data, and implementation of business rules, technical controls. (CIA, audit trails, etc)

Usually someone in the **IT department**. Does not decide what controls are needed, but does implement controls for data owner

TIP: if question mentions "day-to-day" it's custodian!

GDPR Data Roles and Concepts

Two roles that appear in GDPR regulations

Data Processor. A natural or legal person, public authority, agency, or other body, which processes personal data solely on behalf of the data controller.

Data Controller. The person or entity that controls processing of the data (is responsible for the data).

In the OSG - may appear on the exam!

OTHER ROLES

Data Subject

Refers to any individual person who can be identified, directly or indirectly, via an identifier.

Identifiers may include name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity.

Data Steward

Data owners often delegate some duties to this role

Ensure the data's context and meaning are understood, and business rules governing the data's usage are known and followed.

Use that knowledge to ensure the data they are responsible for is used as intended.

5.0 SECURITY PROGRAM MANAGEMENT AND OVERSIGHT

5.2 Explain elements of the risk management process

- **Risk identification**
- **Risk assessment**
  - Ad hoc
  - Recurring
  - One-time
  - Continuous
- **Risk analysis**
  - Qualitative
  - Quantitative
  - Single loss expectancy (SLE)
  - Annualized loss expectancy (ALE)
  - Annualized rate of occurrence (ARO)
  - Probability
  - Likelihood
  - Exposure factor
  - Impact
- **Risk register**
  - Key risk indicators
  - Risk owners
  - Risk threshold
- **Risk tolerance**
- **Risk appetite**
  - Expansionary
  - Conservative
  - Neutral
- **Risk management strategies**
  - Transfer
  - Accept
    - o Exemption
    - o Exception
  - Avoid
  - Mitigate
- **Risk reporting**
- **Business impact analysis**
  - Recovery time objective (RTO)
  - Recovery point objective (RPO)
  - Mean time to repair (MTTR)
  - Mean time between failures (MTBF)

IMPORTANT TERMS

Important risk management concepts you should know for the exam:

Risk Identification

The process of identifying the threats and vulnerabilities that exist in an operating environment.

May come from a variety of sources, including cyber threats, system failures, and natural disasters

Risk Assessment

This is the broader process of identifying, analyzing, evaluating, and prioritizing potential risks.

Encompasses the entire lifecycle of risk management, from initial identification to developing mitigation strategies

RISK ASSESSMENT

Types of risk assessment to identify, analyze, and prioritize potential risks

Ad hoc Often performed to address a change in the environment
Informal, one-time assessments conducted in response to a specific event or concern.

Recurring Used to track the evolution of risks over time
Assessments conducted periodically, at predetermined intervals (e.g., annually, quarterly).

One-time In response to a security incident or management request
A more formal version of one-time assessment as compared to ad hoc.

Continuous Often automated, such as recurring system scans
An ongoing process where risk identification and analysis are integrated into daily operations.

RISK ASSESSMENT vs RISK ANALYSIS

Risk assessment vs **risk analysis**; what's the difference?

Feature	Risk Assessment	Risk Analysis
Scope	Broader process encompassing risk identification, analysis, evaluation, and mitigation.	Specific step within risk assessment focused on analyzing identified risks.
Activities	Identifying, analyzing, prioritizing, and mitigating risks.	Evaluating likelihood and impact of identified risks.
Focus	Overall risk management lifecycle.	Detailed examination of risk characteristics.

RISK ANALYSIS

Two ways to evaluate risk to assets:
qualitative and **quantitative**

QUANTITATIVE

Assigns a dollar value to evaluate effectiveness of countermeasures

QUANTITATIVE

Assigns a **dollar value** to evaluate effectiveness of countermeasures

OBJECTIVE, uses formulas

QUANTITATIVE

Assigns a **dollar value** to evaluate effectiveness of countermeasures

To prioritize, sometimes initially calculated using "impact x probability" score

QUALITATIVE

Uses a scoring system to rank threats and effectiveness of countermeasures

QUALITATIVE

Uses a **scoring system** to rank threats and effectiveness of countermeasures

SUBJECTIVE

QUALITATIVE

Uses a **scoring system** to rank threats and effectiveness of countermeasures

typically uses low/med/high or number scale

Stated simply...

Quantitative measurements use numbers, such as asset values and security control costs.

Qualitative measurements use judgments.

Both methods aim to help management make educated risk decisions based on priorities.

RISK ANALYSIS

An important note on **quantitative risk formulas** from the OSG

> Be prepared to explain the terminology of quantitative risk analysis...
>
> and perform these calculations when you take the Security+ exam.

This means you need to know the QRA formulas!

Important Terms & Concepts

Impact. Potential consequences or negative effects that could occur if the risk materializes.

Asset Value (AV). Monetary value of the asset for which we are making calculations.

Safeguard Evaluation. Answers the question "Is this safeguard cost effective?".

Organizations will not spend more than an asset's value to protect the asset!

Important formulas:

Important elements in quantifying potential loss

exposure factor (EF)

single loss expectancy (SLE)

annualized rate of occurrence (ARO)

annualized loss expectancy (ALE)

Exposure Factor (EF)

Percentage of loss that an organization would experience if a specific asset were violated by a realized risk

$30,000 loss on $100,000 valuation is EF of 30%

Single Loss Expectancy (SLE)

Represents the cost associated with a single realized risk against a specific asset

Single Loss Expectancy (SLE)

SLE = Asset Value (AV) X Exposure Factor (EF)

EF of 30% on $100,000 valuation, SLE = $30,000

Single Loss Expectancy (SLE)

AV **EF** **SLE**

$100,000 X .3 (30%) = $30,000

Annualized Rate of Occurrence (ARO)

The expected frequency with which a specific threat or risk will occur within a single year.

Risk occurs 2 times in a year? 2÷1 = 2

Annualized Rate of Occurrence (ARO)

The expected frequency with which a specific threat or risk will occur within a single year.

Risk occurs once every 2 years? 1÷2 = **0.5**

Annualized Rate of Occurrence (ARO)

The expected frequency with which a specific threat or risk will occur within a single year.

Risk occurs once every 5 years? 1÷5 = 0.2

Annualized Loss Expectancy (ALE)

The possible yearly cost of all instances of a specific realized threat against a specific asset.

Annualized Loss Expectancy (ALE)

ALE = single loss expectancy (SLE) x annualized rate of occurrence (ARO)

ALE Example

Office Building = **$200,000**
Hurricane damage estimate **50%**
Hurricane probability is one every 10 years **10%**

(AV x EF = SLE) $200,000 x .50 = **$100,000**

(SLE x ARO = ALE) $100,000 x .10 = **$10,000**

value of the safeguard (annually)

Formulas and Terms

Exposure Factor (EF) . The percentage (%) of value an asset lost due to an incident.

Single Loss Expectancy (SLE). How much would it cost you if it happened just ONE time?

SLE = Asset Value x Exposure Factor (SLE = AV x EF)

Annualized Rate of Occurrence (ARO). How many times does it happen in one year? Watch for AROs longer than 1 year!

Annualized Loss Expectancy (ALE). How much you will lose per year? ALE = SLE x ARO or AV x EF x ARO

Formulas and Terms

Annualized Rate of Occurrence (ARO). How many times does it happen in one year?

Watch for AROs longer than 1 year, which will be represented as a fraction.

One occurrence every 5 years? 1÷5 = 0.2

Remember, the Official Study Guide suggests these formulas may come up on the Security+ exam!

QUANTITATIVE RISK ANALYSIS

JUST THE FORMULAS!

real-world example!

Available on YouTube

CISSP

EXAM

CRAM

RISK ANALYSIS

There are two terms that refer to the ***possibility*** of a risk event occurring that you should know for the exam.

Probability

Refers to the chance of an event happening, often expressed as a numerical value between 0 (impossible) and 1 (certain).

Represents a 'quantitative' approach

Likelihood

Expresses the chance of a risk occurring using descriptive terms such as "high," "medium," "low," or "rare."

Represents a 'qualitative' approach

RISK REGISTER

Risk Register

A tool in risk management and project management.

Sometimes used to fulfill regulatory compliance but often to track potential issues that can derail intended outcomes.

Typically includes several details, including:

- Risk ID
- Description
- Probability
- Impact
- Severity
- Response
- Owner

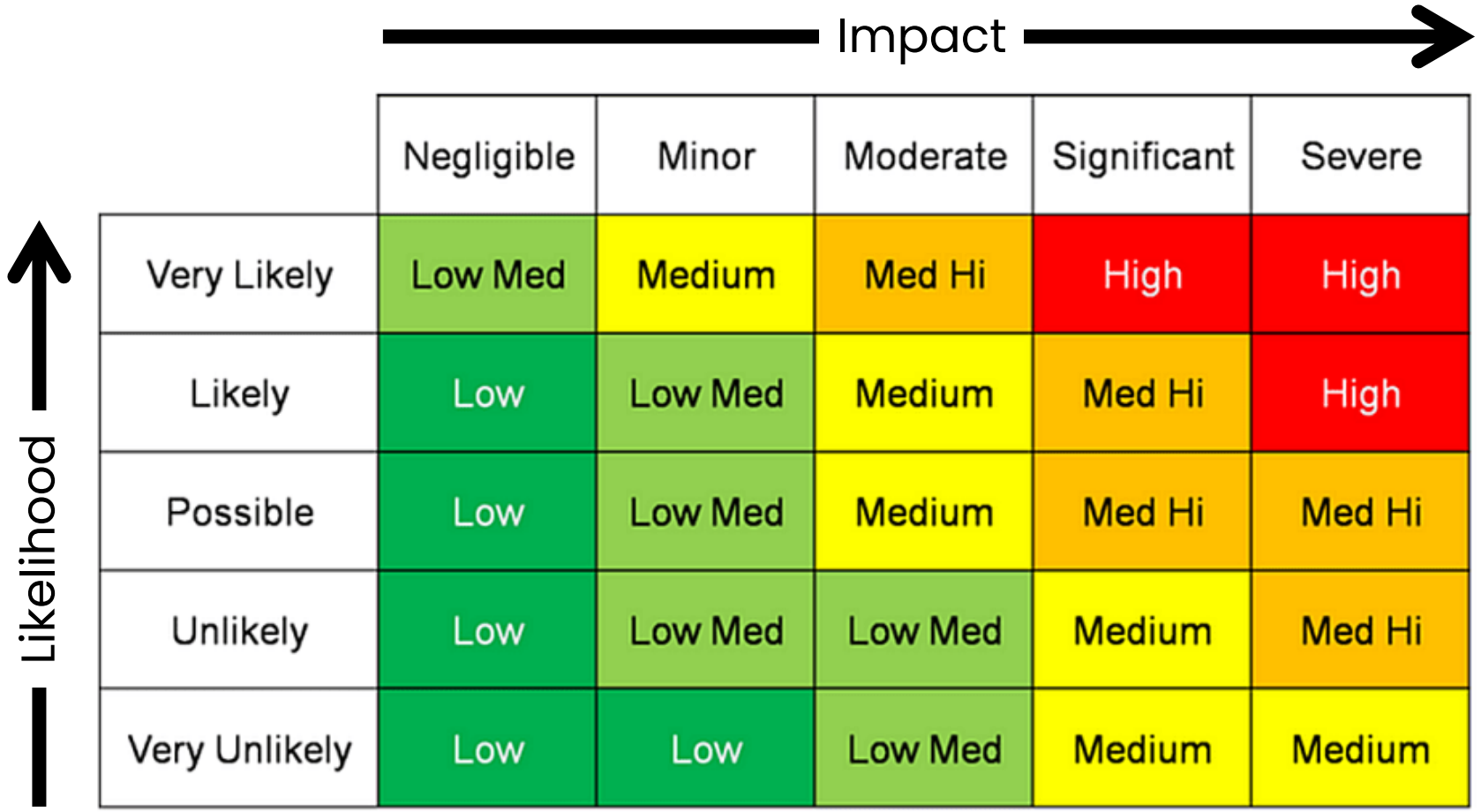
Metrics in a risk register will vary from company to company.

Should be considered a living document and updated periodically (at least annually).

RISK MATRIX/HEAT MAP

A **risk matrix** is used to a provide visual representation of risks affecting a company.

A **heat map** shows the severity of the situation, with the most severe risks being in red.



	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

RISK MATRIX/HEAT MAP

Here are some key concepts associated with a risk register:

Key Risk Indicators (KRIs):

These are measurable metrics that signal potential changes in the likelihood or impact of a risk.

Monitoring KRIs allows for early detection, escalation, and mitigation

Risk Owners:

Each risk should be assigned a designated owner, typically a person or department responsible for managing and mitigating the risk.

This ensures accountability for addressing specific risks.

Risk Threshold:

This refers to the level of risk tolerance established by the organization.

The risk register may be **qualitative** (using low/med/high) or **quantitative** (using numeric scoring)

RISK APPETITE

Risk appetite and risk tolerance; what's the difference?

Risk Appetite

Risk appetite describes the amount of risk an organization is **willing** to accept without mitigating.

Organization use its risk appetite to determine its **risk threshold**

This is level of risk that a situation must rise to ***before*** the organization chooses to take action to manage that risk.

Risk Tolerance

It refers to the organization's **ability** to take on risk.

For example, an organization with more cash on hand has a greater ability maintain stability through financial risk.

It's important that an orgs appetite and tolerance are aligned

RISK APPETITE

Risk appetite refers to the amount of risk an organization is willing to accept.

There are three levels of risk appetite. Organizations with:

Expansionary risk appetites are willing to take on a high level of risk in pursuit of high rewards.

Neutral risk appetites take a balanced approach to risk-taking.

Conservative risk appetites prefer low-risk investments and prioritize preserving their current security posture

This varies across organizations based on their goals, strategic objectives. Start-ups and orgs investing in cutting edge tech have greater appetite.

Response to Risk

Risk Acceptance. Do nothing, and you must accept the risk and potential loss if threat occurs.

Risk Mitigation. You do this by implementing a countermeasure and accepting the residual risk.

The act of reducing risk

Risk Transference. Transfer (assign) risk to a 3rd party, like by purchasing insurance against damage.

Risk Avoidance. When costs of mitigating or accepting are higher than benefits of the service.

EXCEPTION vs EXEMPTION

There are two flavors of risk acceptance you should be familiar with for exam day; ***exception*** and ***exemption***.

Exception

A temporary deviation from a security policy or control due to specific circumstances.

It's a documented and approved decision to accept a higher level of risk for a defined period.

Exemption

A permanent deviation from a security policy or control.

It's a formal decision to permanently accept a risk because mitigation is deemed impractical or infeasible.

RISK REPORTING

Will detail risks discovered, and generally recommendations for remediation as well.

Organizations leadership uses this to decide which controls to implement and which risks to accept.

Reporting is the last phase of the risk assessment process

Risk reports contain sensitive information and should be restricted to those with a need-to-know.

BUSINESS IMPACT ANALYSIS

BIA

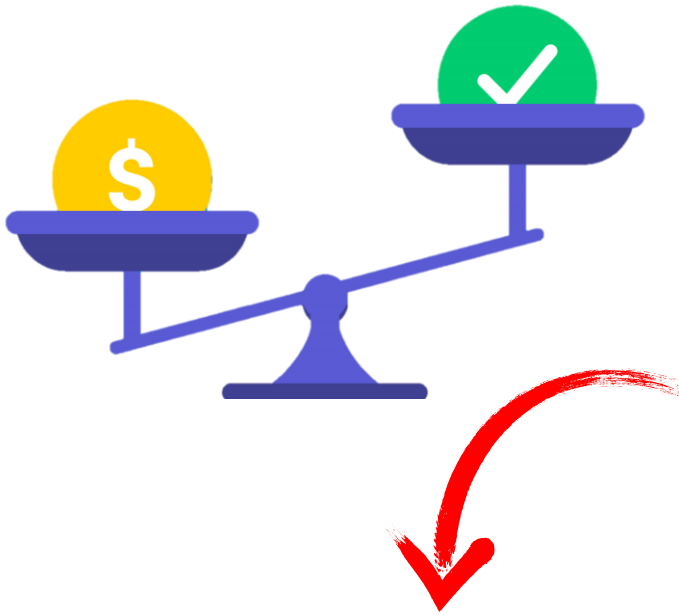
Business Impact Analysis

Identifies mission-critical functions and critical systems that are essential to the organization's success.

Also identifies maximum downtime limits for these systems and components...

as well as scenarios that can impact these systems and components, and the potential losses from an incident.

BUSINESS IMPACT ANALYSIS



A **business impact analysis (BIA)** contains two important items:

✓ a cost-benefit analysis (CBA) AND

✓ a calculation of the return on investment (ROI)

A **cost-benefit analysis** lists the benefits of the decision alongside their corresponding costs.

CBA can be strictly quantitative: adding the financial benefits and subtracting the associated costs to determine whether a decision will be profitable.

A thorough cost-benefit analysis will consider intangible benefits (those you cannot calculate directly).

BUSINESS IMPACT ANALYSIS

Recovery Point Objective (RPO)

is the **age of data** that must be recovered from backup storage for normal operations to resume if a system or network goes down

Max tolerable data loss between last backup and a disaster

Recovery Time Objective (RTO)

is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity.

SLAs between a company and customers will influence RPO and RTO

BCP DEFINITIONS

Important BCP-related definitions for the exam

MTBF (Mean Time Between Failures)
a time determination for how long a piece of IT infrastructure will continue to work before it fails.

MTTR (Mean Time to Repair)

a time determination for how long it will take to get a piece of hardware/software repaired and back on-line.

5.0 SECURITY PROGRAM MANAGEMENT AND OVERSIGHT

5.3 Explain the processes associated with third-party risk assessment and management

- **Vendor assessment**
  - Penetration testing
  - Right-to-audit clause
  - Evidence of internal audits
  - Independent assessments
  - Supply chain analysis
- **Vendor selection**
  - Due diligence
  - Conflict of interest
- **Agreement types**
  - Service-level agreement (SLA)
  - Memorandum of agreement (MOA)
  - Memorandum of understanding (MOU)
  - Master service agreement (MSA)
  - Work order (WO)/statement of work (SOW)
  - Non-disclosure agreement (NDA)
  - Business partners agreement (BPA)
- **Vendor monitoring**
- **Questionnaires**
- **Rules of engagement**

VENDOR ASSESSMENT

Vendor assessment focuses on understanding the security posture and risk profile of potential and existing vendors.

Common methods include:

Penetration Testing: Simulating a cyberattack to identify vulnerabilities in the vendor's systems and data security measures.

Right-to-Audit Clause: Including a clause in the contract that allows your company to audit the vendor's security practices at designated intervals.

Evidence of Internal Audits: Requesting proof that the vendor conducts regular internal audits of their security controls.

Independent Assessments: Utilizing audit reports from independent external security firms that have evaluated the vendor's security posture.

Supply Chain Analysis: Mapping your vendor ecosystem to identify potential risks introduced by their subcontractors or suppliers.

Supply Chain Analysis

Today, most services are delivered through a chain of multiple entities

Supply Chain Analysis

A secure supply chain includes **vendors** who are secure, reliable, trustworthy, reputable

Due diligence should be exercised in assessing vendor security posture, business practices, and reliability

Supply Chain Analysis

A secure supply chain includes **vendors** who are secure, reliable, trustworthy, reputable

May include periodic attestation requiring vendors to confirm continued implementation of security practices

Supply Chain Analysis

A secure supply chain includes **vendors** who are secure, reliable, trustworthy, reputable

A vulnerable vendor in the supply chain puts the organization at risk

VENDOR ASSESSMENT

Organizations need strong project *and* people management to effectively perform vendor management activities, including:

Assess vendor viability:

This is often a process that is not conducted by the security team, as it deals with operational risk.

Assessing the viability of vendors may involve reviews of public information like:

- financial statements
- vendors performance history and reputation
- or even formal reports like a SOC 1

All of these identify potential weaknesses that could impact the vendors ability to continue operations.

RIGHT-TO-AUDIT

Customer rights and capabilities to perform forensic investigation varies in the cloud versus on-premises.

Right-to-Audit Clauses

written into supply chain contracts, allow an auditor can visit the premises to inspect and ensure that the contractor is complying with contractual obligations.

This would help an auditor identify:

- Faulty or inferior quality of goods
- Short shipments
- Goods not delivered
- Kickbacks
- Gifts and gratuities to company employees
- Commissions to brokers and others
- Services allegedly performed that were not actually necessary

Supply Chain Analysis

When evaluating 3rd parties in the chain, consider:

On-Site Assessment . Visit organization, interview personnel, and observe their operating habits.

Document Exchange and Review . Investigate dataset and doc exchange, review processes.

Process/Policy Review . Request copies of their security policies, processes, or procedures.

Third-party Audit. Having an independent auditor provide an unbiased review of an entity's security infrastructure.

CONTRACT MANAGEMENT

Right to audit

The customer can request the right to audit the service provider to ensure compliance with the security requirements agreed in the contract.

Contracts often written to allow the CSP's standard audits (e.g., SOC 2, ISO 27001 certification) to be used in place of a customer-performed audit.

You will never audit a public cloud service provider (CSP), such as Microsoft, Amazon or Google.

SECURITY+ EXAM CRAM

THE COMPLETE COURSE

DEMO

Retrieving audit reports on-demand from a CSP

EXAMPLE FOR CONTEXT - The Security+ exam is vendor-agnostic.

INSIDE CLOUD AND SECURITY

DUE DILIGENCE

Process/effort to collect and analyze information before making a decision, signing a contract, or transacting.

Involves a comprehensive review of a prospective vendor's:

- financial health
- reputation
- security practices
- compliance with relevant regulations

Due diligence supports **due care** efforts, which are the actions taken by the organization based on due diligence

CONFLICT OF INTEREST

In vendor selection it is important that there are no circumstances that may unfairly influence results the selection process

Financial Interests

Vendor Ownership. A customer employee (or someone close to them) has a financial stake in the vendor company.

Could influence their decision-making process during vendor selection or contract negotiations

Kickbacks or Bribes A vendor offers gifts, trips, or other incentives to a customer employee in exchange for preferential treatment

e.g. inflated contract prices or relaxed quality standards

CONFLICT OF INTEREST

In vendor selection it is important that there are no circumstances that may unfairly influence results the selection process

Information Sharing

Confidentiality Breaches. A vendor with access to a customer's confidential information might misuse it for their own gain or sell it to a competitor.

(e.g., trade secrets, customer data)

Unequal Information Sharing. Customer might not receive all the necessary information from the vendor about their product or service limitations.

Potentially leads to biased decision-making or unexpected problems later

CONFLICT OF INTEREST

In vendor selection it is important that there are no circumstances that may unfairly influence results the selection process

Professional Relationships

Pre-existing Relationships. A customer employee has a close personal or professional relationship with a vendor representative.

May impact objectivity during vendor selection or issue resolution

"Revolving Door" Problem. employee leaves their position and takes a job with a vendor they previously worked with.

Can create a conflict if they possess sensitive customer information or knowledge

SERVICE-LEVEL AGREEMENTS

Stipulate performance expectations such as maximum downtimes and often include penalties if the vendor doesn't meet expectations.

Generally used with vendors

Memorandum of Understanding (MOU)

A formal agreement between two or more parties indicating their intention to work together toward a common goal.

Similar to an SLA in that it defines the responsibilities of each party.

More formal alternative to handshake but lacks the binding power of a contract.

Less formal than an SLA, no monetary penalties

Memorandum of Agreement (MOA)

Similar to an MOU but serves as a legal document and describes terms and details of the agreement.

MOA is a legal contract, MOU is not

MSA

Master Service Agreement

Provides structure to the agreements for vendors that you will work with repeatedly.

Contract with general terms between two or more parties enter into as a service agreement.

MSA should address compliance and process requirements the customer is passing along to provider.

MSA comes before statement of work (SOW) and spans projects throughout life of the relationship

MSA should include breach notification and vendor duty to inform the customer of a breach within a specific time period after detection.

STATEMENT OF WORK (SOW)

Legal document usually created after an MSA has been executed and governs a specific unit of work.

MSA may document services and prices, and SOW requirements, expectations, and deliverables for a project.

MSA focus is "overall, ongoing", SOW is "limited & specific"

NDA

NON-DISCLOSURE AGREEMENT

Contract with vendors and suppliers that prohibits disclosure of the company's confidential information.

Also used by companies to prohibit employees from sharing proprietary data.

Duration and terms may vary, so an NDA should be entered into with care

Business Partners Agreement (BPA)

is used between two companies or individuals who want to participate in a business venture to make a profit.

Details include

Each partner's contributions, rights, and responsibilities

Details of operations, decision-making, and sharing of profits.

Rules for the partnership ending either at a given point or if one of the partners dies or moves on.

MONITORING & QUESTIONNAIRES

Continuous monitoring is essential to keep track of evolving risks

Vendor Monitoring. Continuous monitoring of vendors to identify the emergence of new vulnerabilities is essential.

Vulnerabilities of one vendor can impact the entire supply chain, and validation of vendor security reduces risk

Questionnaires. Sending periodic questionnaires to vendors to gather updates on their security controls and risk management practices.

This is a form of self-attestation, and should elicit lower confidence versus an external vendor assessment

RULES OF ENGAGEMENT

To establish clear boundaries in vendor monitoring, it is necessary to establish **rules of engagement**.

Define the purpose of any tests, and what the scope will be for the people who are performing this test.

Establishing a clear agreement outlining expectations for data security, incident response, and communication protocols.

Ensure everyone is aware of what systems will be considered, date and time, and any constraints all should be aware of.

Should also include clear processes for issue resolution in the event of findings or disputes

5.0 SECURITY PROGRAM MANAGEMENT AND OVERSIGHT

5.4 Summarize elements of effective security compliance

- **Compliance reporting**
  - Internal
  - External
- **Consequences of non-compliance**
  - Fines
  - Sanctions
  - Reputational damage
  - Loss of license
  - Contractual impacts
- **Compliance monitoring**
  - Due diligence/care
  - Attestation and acknowledgement
  - Internal and external
  - Automation
- **Privacy**
  - Legal implications
    - o Local/regional
    - o National
    - o Global
  - Data subject
  - Controller vs. processor
  - Ownership
  - Data inventory and retention
  - Right to be forgotten

COMPLIANCE REPORTING

Reporting ensures organizations **meet regulatory requirements** and **maintain transparency** with internal and external stakeholders

Internal Reporting

Regularly informing internal stakeholders / management about the organization's compliance posture.

Demonstrates transparency and keeps leadership informed about potential compliance risks for which they are ultimately accountable.

External Reporting

Submitting reports to external entities, such as regulatory bodies or auditors, as required by specific regulations, to demonstrate compliance with regulations

e.g. GDPR, PCI, HIPAA require either annual or on-request reporting

CONSEQUENCES OF NON-COMPLIANCE

Reputational Damage

effects may last for years!

Can result in loss of customer trust and loss of revenue.

Sanctions

Legal repercussions that can be harsher than fines, including restrictions on operations or even criminal charges.

Contractual Impacts

Failure to comply with regulations might lead to contractual breaches, resulting in penalties or termination of partnerships.

Fines

Failing to report a breach can result in fines that can reach into the millions of dollars. and may lead to lawsuits

Loss of License

In some cases, non-compliance can lead to the revocation of a business license or permit to operate.

COMPLIANCE MONITORING

due diligence

due care

Due Diligence/Care

Taking reasonable steps to assess and mitigate security risks associated with vendors, systems, and data handling practices.

Attestation and Acknowledgement

Obtaining formal confirmation from relevant parties (e.g., employees) that they understand and will comply with security policies and procedures.

Internal and External Audits

Regular assessments conducted by internal or external auditors to evaluate the effectiveness of security controls and identify areas for improvement.

Internal auditors reveal issues to correct before external audit

Automation

Utilizing SIEM and SOAR tools, vulnerability scanners, and other automated solutions to streamline compliance monitoring activities.

Can automate investigation, incident response, and reporting

PRIVACY vs CONFIDENTIALITY

What is the difference between **privacy** and **confidentiality**?

Privacy

Focuses on the **rights of individuals** to control their personal information.

It's about giving people ownership and control over their data

Confidentiality

Ensures that **data** is only accessed and disclosed to authorized individuals or entities.

It's about keeping data protected from unauthorized access

PRIVACY

What is the source of our privacy rights?

Privacy (US). The basis for privacy rights is in the Fourth Amendment to the U.S. Constitution.

The "Stored Communication Act (SCA) of 1986" extends the Fourth Amendment to the electronic realm

Privacy (EU). General Data Protection Regulation (GDPR) protects subjects in the EU but applies to US companies.

Considered the gold standard of data privacy laws.

Applies to every company with customers in the EU!

PRIVACY

Cybersecurity professionals are responsible for protecting **confidentiality**, **integrity**, and **availability** of all sensitive information under their care.

Legal Implications

Navigating privacy regulations that apply to the organization, considering local, regional, national, and international data protection laws.

Requires constant monitoring/oversight to ensure compliance

Data Subject

The individual to whom personal data belongs.

Compliance practices should respect the rights of data subjects, such as the right to access, rectify, or erase their data.

Controller vs. Processor

Covered in section 5.1

Distinguishing between data controller (*determines purpose and means of processing*) and data processor (*processes data on behalf of controller*)

JURISDICTIONAL DIFFERENCES IN DATA PRIVACY

Different laws and regulations may apply depending on the **location** of

- data subject
- data collector
- cloud service provider
- subcontractors processing data
- company headquarters of the entities involved

Legal concerns can:

- prevent the utilization of a cloud services provider
- add to costs and time to market
- drive changes to technical architectures required to deliver services

Never replace compliance with convenience when evaluating services, as this increases risks

Many privacy frameworks impose fines or other action for noncompliance.

PRIVACY

Cybersecurity professionals are responsible for protecting **confidentiality**, **integrity**, and **availability** of all information under their care.

Data Ownership

Determining who has ultimate control and decision-making authority over specific data sets within the organization.

Data Inventory and Retention

Maintaining a comprehensive and accurate record of all personal data collected and processed.

Must be accompanied by data retention policies that specify how long data will be stored before secure disposal.

Right to be Forgotten

A data subject's right to request the deletion of their personal data under certain circumstances, as mandated by regulations like GDPR

Orgs must have processes in place to handle subject requests

DATA INVENTORY

As a first step, organizations should develop a **data inventory** containing the following types of sensitive information.

- Personally identifiable information (PII)
- Protected health information (PHI)
- Financial information
- Intellectual property
- Legal information
- Regulated information

These sensitive info types are covered in-depth in section 3.3

5.0 SECURITY PROGRAM MANAGEMENT AND OVERSIGHT

5.5 Explain types and purposes of audits and assessments

- **Attestation**
- **Internal**
  - Compliance
  - Audit committee
  - Self-assessments
- **External**
  - Regulatory
  - Examinations
  - Assessment
  - Independent third-party audit

- **Penetration testing**
  - Physical
  - Offensive
  - Defensive
  - Integrated
  - Known environment
  - Partially known environment
  - Unknown environment
  - Reconnaissance
    - o Passive
    - o Active

The 'WHAT' and 'WHY'

AUDIT vs ASSESSMENT

Security AUDIT vs Security ASSESSMENT; what's the difference?

Feature	Security Audit	Security Assessment
Focus	Compliance with standards/regulations	Identifying and prioritizing risks
Purpose	Verification	Evaluation and analysis
Formality	Formal, often by external auditors	Formal or informal
Outcome	Report on compliance gaps	Report on identified risks and recommendations

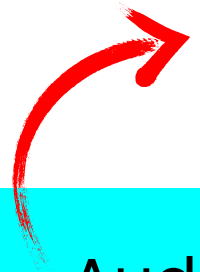
The exam

Studying for the exam

Attestation

An independent verification of an organization's adherence to specific controls or standards.

Attestation engagements can be **internal** or **external**.



For an internal auditor, independent means "free to report results without fear of punishment or retaliation"

Auditors, whether internal or external, should always be **independent**

INTERNAL

Internal audits and assessments are performed within the organization itself, usually by a dedicated team.

Compliance Audits

These audits assess an organization's internal controls against industry standards or regulatory requirements.

They ensure compliance with policies and procedures.

Audit Committee

A committee reporting to the board of directors that is responsible for overseeing the internal audit function and ensuring its independence.

Self-Assessments

Internal evaluations conducted by an organization's own staff to identify areas for improvement in controls or processes.

EXTERNAL

External audits and assessments are performed by entities outside of the organization.

Regulatory Audits

Auditor/auditing often an appointed third-party firm

Audits required by government agencies or regulatory bodies to ensure compliance with specific regulations.

(e.g., SOX for publicly traded companies)

Examinations

A broader term encompassing various types of external reviews, including compliance audits and security assessments.

Independent Third-Party

An external, unbiased entity that conducts the audit or assessment, free from conflicts of interest within the organization.

PENETRATION TESTING Categories

Penetration testing *actively assesses* deployed security controls, trying to exploit vulnerabilities by simulating or performing an attack.

Physical

Evaluates the physical security measures of a facility, assessing the possibility of unauthorized physical access to systems or data.

Offensive

Focuses on the technical security of computer systems and networks, attempting to exploit vulnerabilities to gain unauthorized access.

Defensive

Focuses on evaluating the effectiveness of existing security controls to withstand attacks.

Integrated

Physical + Offensive + Defensive

Combines physical, offensive, and defensive techniques for a more comprehensive evaluation.

PENETRATION TESTING

Types

Known environment

white box test

penetration tester is given a map of target systems and networks. They go into the test with substantial/full information of the target systems and networks.

Unknown environment

black box test

penetration tester knows nothing about target systems and networks. They go into the test completely blind and build out the database of everything they find as they go.

Partially known environment

grey box test

Limited information is shared with the tester, sometimes in the form of login credentials.

Simulate knowledge level of a hacker with long-term access to a system would achieve through research and system footprinting.

Rules of engagement

Rules of engagement define the purpose of the test, and what the scope will be for the people who are performing this test on the network.

They ensure everyone will be aware of what systems will be considered, date and time, and any constraints all should be aware of

PASSIVE AND ACTIVE RECONNAISSANCE

Passive reconnaissance. one is not interacting directly with the target and as such, the target has no way of knowing, recording, or logging activity.

This involves gathering data from publicly available sources.

EXAMPLES

Searching the internet. searching for information about the target organization, its employees, and its systems.

Reviewing media. Examining social media posts, news articles, and public records that might reveal details about the target's security posture.

Analyzing DNS records to understand the target's network infrastructure.

Using search engines with advanced operators to find specific information about the target.

PASSIVE AND ACTIVE RECONNAISSANCE

Active reconnaissance interacts directly with the target in some way and as such, the target may discover, record, or log these activities.

Involves using tools and techniques to probe and scan the target for vulnerabilities and potential entry points

EXAMPLES

Using port scanners to identify open ports on the target network and the services running on those ports.

Sending ping sweeps to identify active devices on the network.

Utilizing vulnerability scanners to identify known weaknesses in the target's systems and software.

Employing social engineering techniques to trick employees into revealing information about the target's security practices.

NEVER do these without a written, signed contract!

5.0 SECURITY PROGRAM MANAGEMENT AND OVERSIGHT

5.6 Given a scenario, implement security awareness practices

- **Phishing**
  - Campaigns
  - Recognizing a phishing attempt
  - Responding to reported suspicious messages
- **Anomalous behavior recognition**
  - Risky
  - Unexpected
  - Unintentional
- **User guidance and training**
  - Policy/handbooks
  - Situational awareness
  - Insider threat
  - Password management
  - Removable media and cables
  - Social engineering
  - Operational security
  - Hybrid/remote work environments
- **Reporting and monitoring**
  - Initial
  - Recurring
- **Development**
- **Execution**

Principles of social engineering success

Authority

Citing position, responsibility, or affiliation that grants the attacker the authority to make the request.

Intimidation

Suggesting you may face negative outcomes if you do not facilitate access or initiate a process.

Consensus

Claiming that someone in a similar position or peer has carried out the same task in the past.

Scarcity

quantity

Limited opportunity, diminishing availability that requires we get this done in a certain amount of time, similar to urgency.

Principles of social engineering success

Familiarity

aka 'liking'

Attempting to establish a personal connection, often citing mutual acquaintances, social proof.

Trust

Citing knowledge and experience, sometimes assisting the target with an issue to establish a relationship.

Urgency

Time sensitivity that demands immediate action, similar to scarcity

All attempts to get users to circumvent standard security policies and procedures

CLASSIFYING SOCIAL ENGINEERING ATTACKS

At a high level, two categories of social engineering attacks:

Physical Attacks

- ✓ Tailgating
- ✓ Shoulder surfing
- ✓ Dumpster diving

Virtual Attacks

- ✓ Phishing
- ✓ Spear Phishing
- ✓ Whaling
- ✓ Vishing
- ✓ Hoax
- ✓ Watering hole attack

SOCIAL ENGINEERING TECHNIQUES

Best defense for both is security awareness training (user education)

Social Engineering

an attempt by an attacker to convince someone to provide info (like a password) or perform an action they wouldn't normally perform (such as clicking on a malicious link)

Social engineers often try to gain access to the IT infrastructure or the physical facility.

Phishing

commonly used to try to trick users into giving up personal information (such as user accounts and passwords), click a malicious link, or open a malicious attachment.

Spear phishing targets specific groups of users

Whaling targets high-level executives

Vishing (voice phishing) phone-based

Smishing uses sms(text) messaging on mobile

phishing is #1 cyber attack!

An entry point for ransomware!

Know all these variants!

SPAM AND SPIM

SPAM

Unsolicited email, generally considered an irritant

defeat with strong spam filtering

SPIM

SPAM over instant messaging, also generally considered an irritant

IM and mobile providers providing some protection here

Create cryptic usernames and do not list your ID in the IM service public directory

Not always just an irritant! Both are delivery channels for ransomware!

WHAT IS DUMPSTER DIVING

Gathering important details (intelligence) from things that people have thrown out in their trash.

Often legal, and may target individuals or organizations

SOCIAL ENGINEERING TECHNIQUES

Tailgating

when an unauthorized individual might follow you in through that open door without badging in themselves.

Usually not an accident!

Eliciting Information

aka 'elicitation'

strategic use of casual conversation to extract information without the arousing suspicion of the target

Can involve complex cover stories and co-conspirators!

SOCIAL ENGINEERING TECHNIQUES

Shoulder Surfing

a criminal practice where thieves steal your personal data by spying over your shoulder

Can happen anywhere with any device

Pharming

an online scam where a website's traffic is manipulated thru DNS, redirects a user to a different (malicious) website.

a portmanteau of the words "phishing" and "farming",

PHISHING

Phishing is a deceptive attempt to steal sensitive information, by masquerading as a trustworthy entity in an electronic communication.

Campaigns

Conduct simulated phishing campaigns to test employee awareness and preparedness.

Can help identify knowledge gaps requiring additional training.

Recognizing a Phishing Attempt

Train employees on red flags associated with phishing emails.

e.g. generic greetings, typos, urgency, suspicious attachments/links

Responding to Reported Suspicious Messages

Establish a clear procedure for employees to report suspicious emails to the IT security team.

Should include instructions on how to forward the email without compromising security

ANOMALOUS BEHAVIOR RECOGNITION

Employees should be trained to recognize when **risky**, **unexpected**, and **unintentional behavior** takes place.

Risky

Downloading files from untrusted websites

Clicking on suspicious links in email

Sharing passwords or other sensitive info

Leaving work devices unattended in public

Unexpected

Sudden increase in failed login attempts for a user

User accessing sensitive info outside their normal duties

Working unusual hours outside of normal schedule

Transferring large amounts of data to personal devices

Unintentional

Using weak passwords and same PW repeatedly

Falling victim to a phishing attack and entering creds

Printing sensitive docs and leaving them unattended

Oversharing sensitive documents (data leak)

USER GUIDANCE & TRAINING

There are several important topics that should be included in end-user security training programs include (per the OSG).

Policy/Handbooks

The company's security policy handbook should include a section with guidance on phishing awareness.

Should include guidance on reporting suspicious messages

Situational Awareness

Train employees on the evolving threat landscape, emphasizing the increased risk of phishing attacks in a remote work environment.

and to open emails from unknown senders with caution

Insider Threat

Educate employees about the dangers of insider threats, such as disgruntled coworkers, who may attempt to steal data or interrupt business operations.

USER GUIDANCE & TRAINING

There are several important topics that should be included in end-user security training programs include (per the OSG).

Password Management

Train employees on strong password creation and management practices.

Advise against password reuse and encourage the use of password managers

Removable Media and Cables

Remind employees about the security risks associated with using removable media (USB drives, external hard drives) and public charging cables.

Training should guide use of authorized devices and data encryption

Social Engineering

Educate employees on different social engineering techniques commonly used in phishing attacks.

Train users on "The 7 principles of social engineering"

USER GUIDANCE & TRAINING

There are several important topics that should be included in end-user security training programs include (per the OSG).

Operational Security (OpSec)

Train employees on OpSec principles, such as being mindful of the information they share online or in public places.

and risks of unsecured Wi-Fi networks or public computers

Hybrid/Remote Work Environments

Develop specific security guidelines for remote work setups .

Include guidance on home wi-fi and work data on personal devices

DEVELOPMENT and EXECUTION

Development

Develop training materials that are engaging, informative, and tailored to the specific needs of the organization and its employees.

Consider using a variety of training methods, such as online modules, interactive workshops, or video presentations.

Execution

Launch the security awareness training program across the organization, ensuring all employees participate, regardless of location.

Hybrid training sessions (onsite and remote users) are common

Promote the training program internally and encourage employees to actively participate and ask questions.

Regularly measure the effectiveness of the training program through assessments and reporting, and make adjustments as needed

REPORTING and MONITORING

Initial

Conduct an initial assessment to gauge employees' current level of security awareness regarding phishing and related threats.

This can be achieved through surveys or knowledge-based tests.

Recurring

Schedule regular security awareness training sessions to reinforce best practices and keep employees updated on the latest phishing tactics.

Monitor reporting trends to identify areas where employees might need additional training or support.

Regular updates to training material are necessary to address evolving threats and employees' weak areas

THANKS

FOR WATCHING!