

Cyber Security

Lesson 3



Labs



Assignments

Užduotis - Create Risk register

Due April 4, 2025 5:30 PM

Instructions

Remiantis Teorines paskaitos Nr.02 medžiaga, sukurti Rizikų registrą su ne mažiau kaip 10 skirtingų rizikų (teigiamų ir neigiamų - santykis nesvarbus). Rizikas įvertinti kokybiniu analizės metodu. Bonus taškai (respect), jeigu ir kiekybiniu bus pvz.

Rizikų registre, kiekvienai rizikai, turi būti pateikta tokia informacija:

1. Cause/priežastis.
 2. Event (Risk)/įvykis (rizika).
 3. Effect / padariniai (efektas).
 4. Probability/tikimybė (1-8).
 5. Impact/poveikis (1-10).
 6. Value (Probability x impact) / Vertė (tikimybė x poveikis).
 7. Risk Tolerance / Rizikos tolerancija.
- Praktinį darbą atlikti remiantis pateiktu rizikų registro šablonu ir pavyzdžiu.

Turite laiko iki 2025-04-04.

Įkelti failus, dokumentus, reikia, paspaudus apačioje:

"Užduotis - Create Risk register (25 03 26 Kiber NF OV)"

Rekomenduojama PDF formatu.

[illegible]

Risk register with qualitative analysis

Cause/priežastis	Event (Risk)/įvykis (rizika)	Effect / padariniai (efektas)	Probability/tikimybė (1-8)	Impact/poveikis (1-10)	Value (Probability x impact) / Vertė (tikimybė x poveikis)	Risk Tolerance / Rizikos tolerancija
Įmonė neturi Cyber Security specialisto	Nėra laiku fiksuojami kibernetiniai įvykiai ir incidentai	Įsilaužimas į serverius ir kompiuterius	4	7	28	25
Įmonė neturi teisininko	Teisės aktų pažeidimai	Finansiniai nuostoliai, įmonės veiklą ribojančios kardomosios priemonės	3	5	15	
Nerakinama serverinės patalpa	Įmonės turto praradimas	Darbo prastovos ir finansiniai nuostoliai	5	8	40	
Pasenusios operacinės sistemos naudojimas įmonės kompiuteriuose	Pažeidžiamumų išnaudojimas	Užšifruoti įmonės dokumentai	3	4	12	
Verslo modelio keitimas (perėjimas prie internetinės prenumeratos)	Klientų praradimas	Nuolatinės pajamos ir klientų lojalumas	3	3	9	
Didesnis produktų kiekio užsakymas tiesiogiai iš gamyklos už žemesnę nei rinkos kainą	Sandėlio perpildymas	Išauga pardavimai, didesnis pelnas	2	5	10	

Risk register with qualitative analysis

Probability	Impact					
	Insignificant 1	Minor 2	Moderate 3	Major 4	Severe 5	
	5 - Very likely	5	10	15	20	25
	4 - Likely	4	8	12	16	20
	3 - Possible	3	6	9	12	15
	2 - Unlikely	2	4	6	8	10
	1 - Very unlikely	1	2	3	4	5

Risk level



Low



High



Moderate



Severe

In the previous lesson...

Positive and negative risks



Positive and negative risks

NEGATIVE RISK RESPONSES		POSITIVE RISK RESPONSES	
AVOID	Eliminate and use new process. Communication important.	EXPLOIT	Remove uncertainty so opportunity is sure to happen.
MITIGATE	Reduce size of risk through internal controls.	ENHANCE	Focus on root causes and the likelihood of it happening.
TRANSFER	Pass ownership to third party, ie insurance	SHARE	Partnership needed
ACCEPT	Impact is small enough to handle actively or passively. Develop contingency plans	ACCEPT	Impact is handled actively or passively when it happens

Threats – negative risks

AVOID	Eliminating the threat.
MITIGATE	Reduce the probability or impact of a threat.
TRANSFER	Shifting the responsibility and impact of the threat to a third party
ESCALATE	Passing the responsibility for managing a specific risk to a higher authority
ACCEPT	Acknowledge and tolerate a risk without taking immediate action.

Positive and negative risks



POSITIVE RISKS

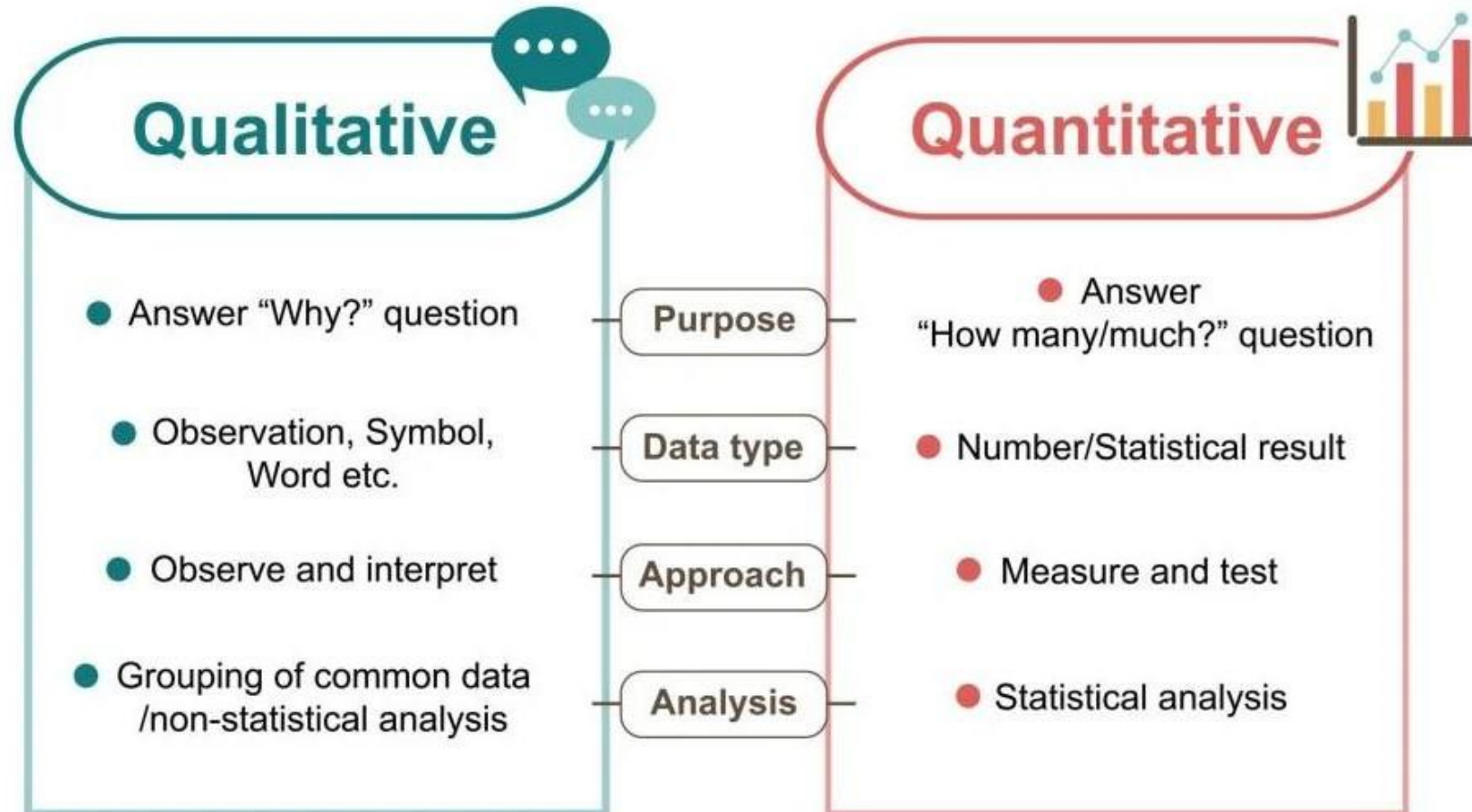
- ✦ Something that can help you
- ✦ Expands one's opportunity
- ✦ Helps you grow and meet goals
- ✦ Pushes you forward
- ✦ Turns out good for you... not dangerous/ unsafe
- ✦ "good outcome"



NEGATIVE RISKS

- ✦ **Restricts your opportunities**
- ✦ **Pushes you backwards**
- ✦ No gain
- ✦ Something bad or destructive happens
- ✦ "risky risk"
- ✦ **Can get you in trouble or hurt (unsafe)**
- ✦ Dangerous
- ✦ Life threatening

Qualitative ir Quantitative analysis



Risk register with qualitative analysis

Cause	Event (risk)	Effect	Probability (1-8)	Impact (1-10)	Value (probability x impact)
Because there are no team lead	Module will be developed poorly with many security issues	More time for testing and bug fixing, more possibilities and time to use for hacking	2	7	14

Risk Mitigation

- The key to control selection is the implementation of cost-effective controls that reduce or mitigate risks to levels that are conventional to the organisation
- With the implementation of the controls on the basis of this accept, organisations will reduce risk but not eliminate it
- Controls can be categorised in:



Introduction

- Understanding Core Security Goals DONE
- Introducing Basic Risk Concepts DONE
- Understanding Security Controls
- Using Command-Line Tools
- Understanding Logs

Understanding Security Controls

Understanding Security Controls

- Overview
 - Managerial controls are primarily administrative in function
 - Operational controls help ensure that the day-to-day operations of an organization comply with the security policy
 - Technical controls use technology

Understanding Security Controls

- Managerial Controls
 - Risk assessments
 - Vulnerability assessments
- Operational Controls
 - Awareness and training
 - Configuration management
 - Media protection
 - Physical and environmental protection

Understanding Security Controls








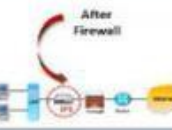
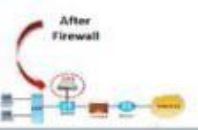
- Managerial Controls
 - Risk assessments
 - Vulnerability assessments
- Operational Controls
 - Awareness and training
 - Configuration management
 - Media protection
 - Physical and environmental protection

Understanding Security Controls

- Technical Controls
 - Encryption
 - Antivirus software
 - IDSs and IPSs
 - Firewalls
 - Least Privilege



Firewall vs IPS vs IDS

IDS vs IPS vs Firewall						
Parameter	FIREWALL		IPS		IDS	
						
Abbreviation For	-		Intrusion Prevention System		Intrusion Detection System	
Philosophy	Firewall is a network security device that filters incoming and outgoing network traffic based on predetermined rules		IPS is a device that inspects traffic, detects it, classifies and then proactively stops malicious traffic from attack.		An intrusion detection system (IDS) is a device or software application that monitors a traffic for malicious activity or policy violations and sends alert on detection.	
Principle Of Working	Filters traffic based on IP address and port numbers		Inspects real time traffic and looks for traffic patterns or signatures of attack and then prevents the attacks on detection.		Detects real time traffic and looks for traffic patterns or signatures of attack and them generates alerts.	
Configuration Mode	Layer 3 mode or transparent mode		Inline mode , generally being in layer 2		Inline or as end host (via span) for monitoring and detection	
Placement	Inline at the Perimeter of Network		Inline generally after Firewall		Non-Inline through port span (or via tap)	
Traffic Patterns	Not analyzed		Analyzed		Analyzed	
Placement w.r.t Each Other	Should be 1 st Line of defense		Should be placed after the Firewall device in network		Should be placed after firewall	
Action On Unauthorized Traffic Detection	Block the traffic		Preventing the traffic on Detection of anomaly		Alerts/alarms on detection of anomaly	
Related Terminologies	<ul style="list-style-type: none">Stateful packet filteringpermits and blocks traffic by port/protocol rules		<ul style="list-style-type: none">Anomaly based detectionSignature detectionZero day attacksBlocking the attack		<ul style="list-style-type: none">Anomaly based detectionSignature detectionZero day attacksMonitoringAlarm	

H+ and N+

- **HIDS (Host-based Intrusion Detection System):** An IDS installed on a host or virtual machine that identifies threats, but does not block them.
- **HIPS (Host-base Intrusion Prevention System):** An IPS installed on a host or virtual machine that blocks activity it identifies as malicious.
- **NIDS (Network-based Intrusion Detection System):** An IDS that inspects network traffic often at the packet level to identify threats but does not block it.
- **NIPS (Network-based Intrusion Prevention System):** An IPS that inspects network traffic often at the packet level and blocks traffic containing activity it identifies as malicious.

W+

- WIDS, WHIDS, WNIDS, WIPS, WHIPS, WNIPS
- Wireless local area network (WLAN) protection
- Used to continuously protect a wireless network and in some cases, a wired network, from unauthorized users.
- In a WIDS, a system of sensors is used to monitor the network for the intrusion of unauthorized devices, such as rogue access points.
- In a WIPS, the system not only detects unauthorized devices, but also takes steps to mitigate the threat by containing the device and detaching it from the wireless network.

Malicious content types

- Statics content remains unchanged
- Polymorphic content involves changing each copy of its code to bypass anti-malware protection.
- Metamorphic content with each iteration rewrites its own content to bypass anti-malware protection.

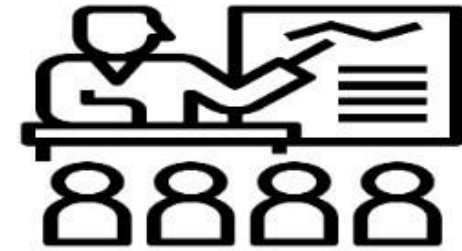
Detection of threat

- Signature-based detection catches threats by their known 'signature' of malicious content unique to specific content.
- Behavior-based cyber threat detection looks for malicious actions or behaviors that are typical of malware, threats can be identified through heuristics.

Control Types

- Preventative Controls

- Hardening
- Training
- Security guards
- Change management
- Account disablement policy
- Intrusion prevention system (IPS)



Control Types

- **Detective Controls**

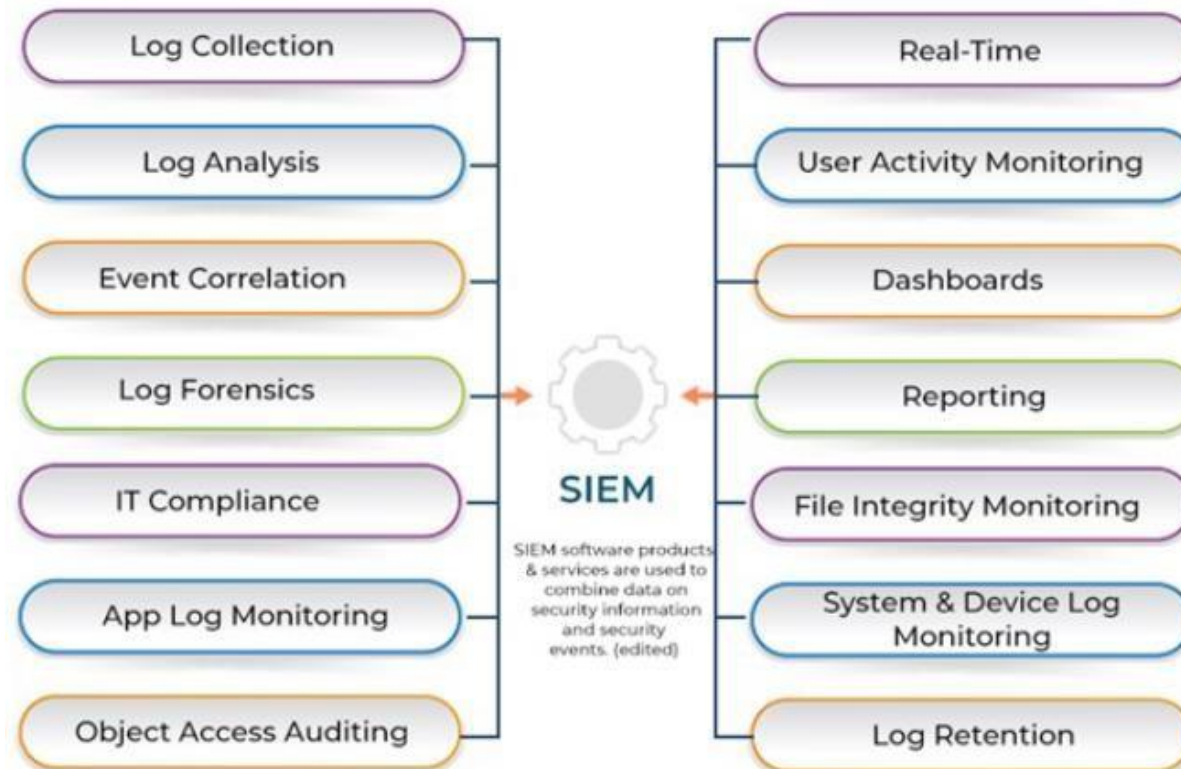
- Log monitoring
- SIEM systems
- System audit
- Video surveillance
- Motion detection
- Intrusion detection system (IDS)



SIEM



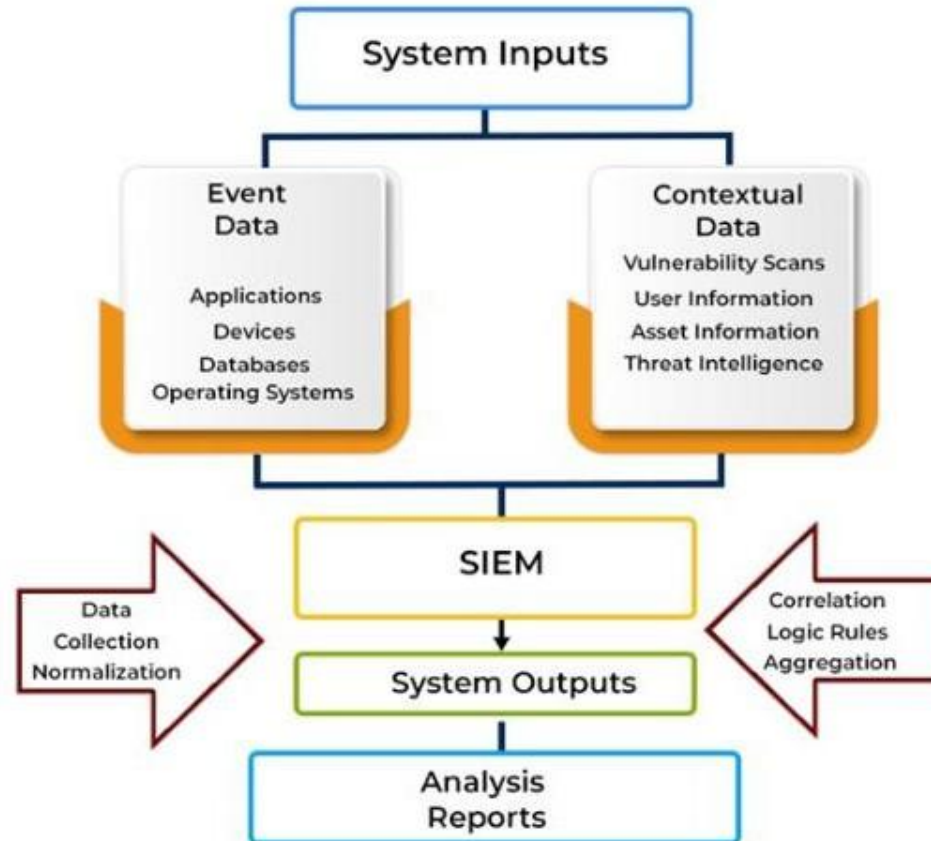
SECURITY INFORMATION AND EVENT MANAGEMENT



SIEM architecture



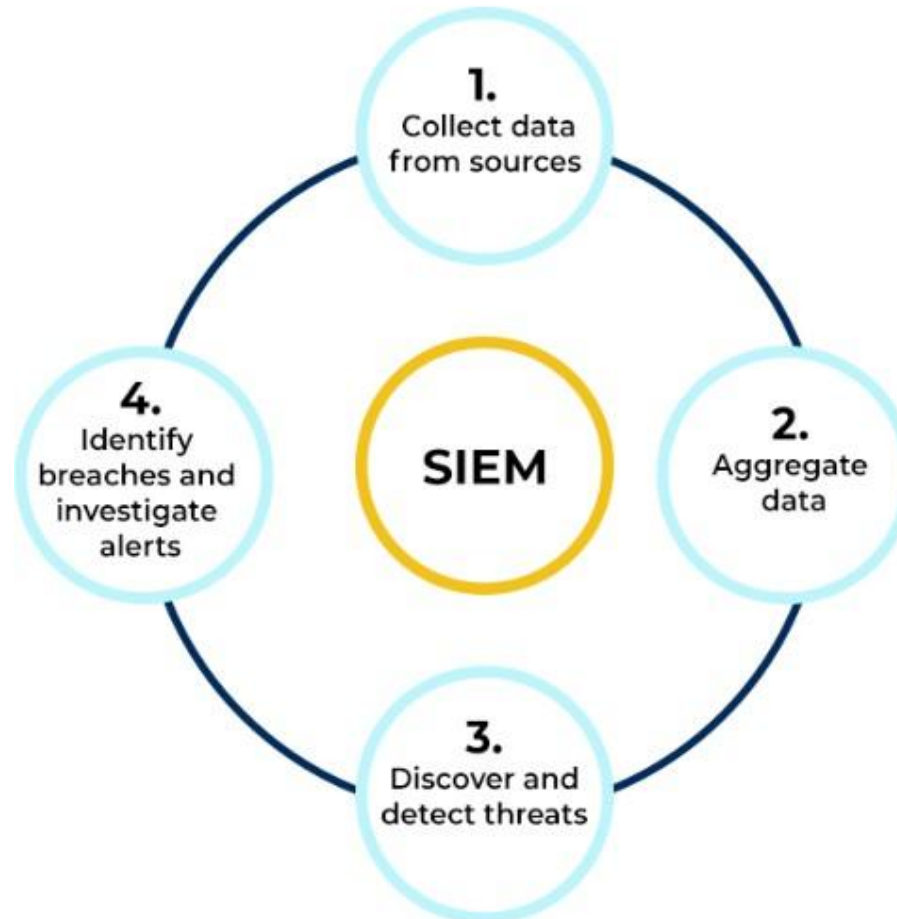
UNDERSTANDING THE SIEM ARCHITECTURE



SIEM process flow



SIEM PROCESS FLOW



Video surveillance use

- **Remote video monitoring:** to protect against theft, burglaries, and dishonest employees.
- **Facility protection:** to protect the perimeter of the property or the perimeter of buildings.
- **Monitor operations:** to monitor day-to-day operations and as a tool to streamline operations.
- **Loss prevention:** to protect assets.
- **Vandalism deterrence:** visible cameras may be a deterrent to vandals because of the possibility that they can be identified on the video. High-definition cameras with facial recognition in a durable, vandal-proof housing can be used.
- **Employee safety:** for compliance with safety regulations and also to protect the employer in civil proceedings.
- **Parking lots and asset drop places:** to monitor for theft or damage to assets as well as accidents.
- **Event video surveillance:** for crowd control as well as crime prevention.
- **Public safety:** routinely used for city streets, parks, communities, and neighbourhoods to help deter crime and enhance public safety.
- **Traffic monitoring:** commonly used to improve the flow of traffic and monitor for accidents.
- **Outdoor perimeter security:** security can be maintained in different ways by utilizing video surveillance with security/protection officers on patrol, fences, vehicle, and pedestrian gates and intrusion detection.

Motion detection

Process of detecting a change in the position of an object relative to its surroundings or a change in the surroundings relative to an object.

Motion detection can be :

- **Mechanical**

The most basic forms of mechanical motion detection utilize a switch or trigger.

- **Electronic**

The principal methods by which motion can be electronically identified are optical and acoustic.

- **Motion perception**

When it is done by natural organisms

Motion can be detected by monitoring changes in:

- Infrared light
- Visible light
- Radio frequency energy
- Sound
- Kinetic energy
- Magnetism
- Wi-Fi Signals

Control Types

- Corrective and Recovery Controls
 - Backups and system recovery
 - Incident handling processes
- Physical Controls
- Compensating Controls
- Response Controls

Control Goals

- **Deterrent**
 - Attempt to discourage individuals from causing an incident
 - Cable locks, hardware locks
- **Compare to prevention**
 - Deterrent encourages people to *decide* not to take an undesirable action
 - Prevention stops them from taking an undesirable action
 - Security guard can be both



Access Control Defensive Categories and Types

- **Access Control Categories:**
 - **Administrative (Directive) Controls:**
 - ◆ Organizational policies and procedures.
 - ◆ Regulation.
 - ◆ Training and awareness.
 - **Technical Controls:**
 - ◆ Hardware/software/firmware – Firewalls, routers, encryption.
 - **Physical Controls:**
 - ◆ Locks, fences, guards, dogs, gates, bollards.
- **Access Control Types** (Many can be multiple types – On the exam look at question content to see which type it is).
 - **Preventative:**
 - ◆ Prevents action from happening – Least privilege, drug tests, IPS, firewalls, encryption.
 - **Detective:**
 - ◆ Controls that Detect during or after an attack – IDS, CCTV, alarms, anti-virus.
 - **Corrective:**
 - ◆ Controls that Correct an attack – Anti-virus, patches, IPS.
 - **Recovery:**
 - ◆ Controls that help us Recover after an attack – DR Environment, backups, HA Environments .
 - **Deterrent:**
 - ◆ Controls that Deter an attack – Fences, security guards, dogs, lights, Beware of the dog signs.
 - **Compensating:**
 - ◆ Controls that Compensate – other controls that are impossible or too costly to implement.

Summary + Bonus info

Information Security Governance

- **Security governance principles.**
 - **Values:**
 - ♦ What are our values? Ethics, Principles, Beliefs.
 - **Vision:**
 - ♦ What do we aspire to be? Hope and Ambition.
 - **Mission:**
 - ♦ Who do we do it for? Motivation and Purpose.
 - **Strategic Objectives:**
 - ♦ How are we going to progress? Plans, goals, and sequencing.



Summary + Bonus info

- **Personnel Security – Users often pose the largest security risk:**
 - **Awareness** – Change user behavior - this is what we want, we want them to change their behavior.
 - **Training** – Provides users with a skillset - this is nice, but if they ignore the knowledge, it does nothing.
 - **Hiring Practices** – We do background checks where we check: References, degrees, employment, criminal, credit history (less common, more costly). We have new staff sign a NDA (Non-Disclosure Agreement).
 - **Employee Termination Practices** – We want to coach and train employees
- **Outsourcing and Offshoring** - Having someone else do part of your (IT in our case) work.
 - ◆ This can lower cost, but a thorough and accurate Risk Analysis must be performed. Offshoring can also pose problems with them not having to comply with the same data protection standards.

Risk Identification, Assessment, Response, Monitoring and Reporting

- **Risk Management - Identification:**

$$\text{Risk} = \text{Threat} * \text{Vulnerability}$$

- **The Risk Management lifecycle is iterative.**

Identify our Risk Management team.

- What is in and what is out of scope?
- Which methods are we using?
- Which tools are we using?
- What are the acceptable risk levels, which type of risk appetite do we have in our enterprise?
- Identify our assets.
 - ◆ Tangible: Physical hardware, buildings, anything you can touch.
 - ◆ Intangible: Data, trade secrets, reputation, etc.

- **Risk Assessment.**

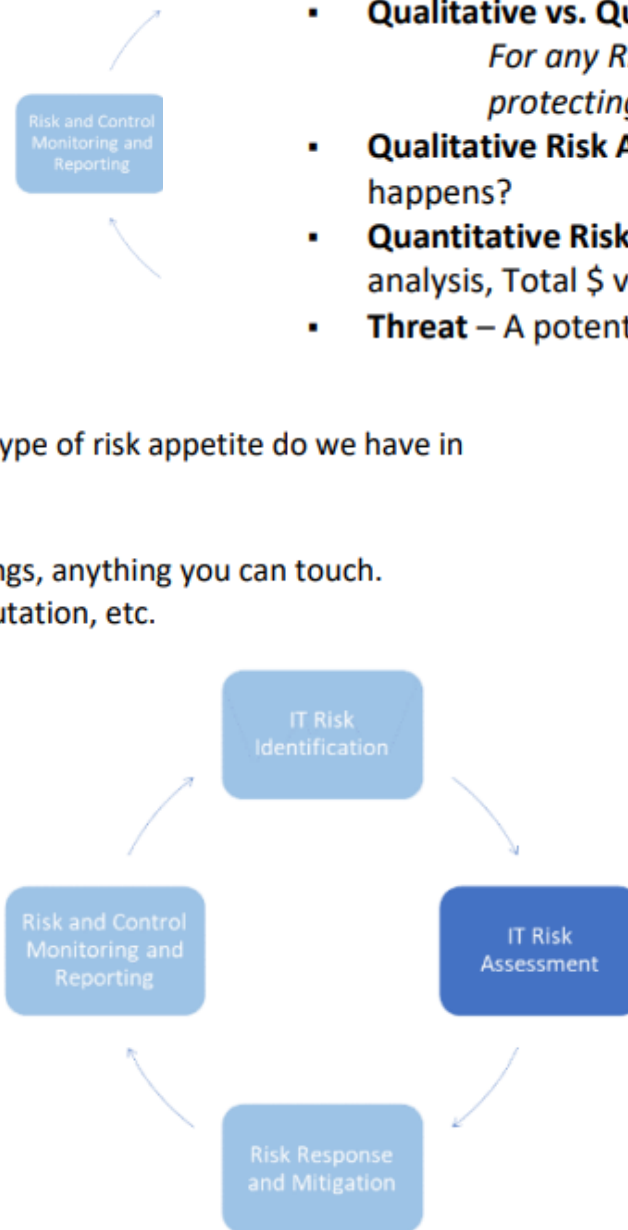
- Quantitative and Qualitative Risk Analysis.
- Uncertainty analysis.
- Everything is done using cost-benefit analysis.
- Risk Mitigation/Risk Transference/Risk Acceptance/Risk Avoidance.
- Risk Rejection is **NEVER** acceptable.
- We assess the current countermeasures.
 - ◆ Are they good enough?
 - ◆ Do we need to improve on them?
 - ◆ Do we need to implement entirely new countermeasures?

- **Risk Analysis:**

- **Qualitative vs. Quantitative Risk Analysis.**

For any Risk analysis we need to identify our assets. What are we protecting?

- **Qualitative Risk Analysis** – How likely is it to happen and how bad is it if it happens?
- **Quantitative Risk Analysis** – What will it actually cost us in \$? This is fact based analysis, Total \$ value of asset, math is involved.
- **Threat** – A potentially harmful incident (Tsunami, Earthquake, Virus, ...)



Summary

- **Vulnerability** – A weakness that can allow the Threat to do harm. Having a data center in the tsunami flood area, not earthquake resistant, not applying patches and anti-virus, ...
- **Risk** = Threat x Vulnerability.
- **Impact** - Can at times be added to give a fuller picture. Risk = Threat x Vulnerability x Impact (How bad is it?).
- **Total Risk** = Threat x Vulnerability x Asset Value.
- **Residual Risk** = Total Risk – Countermeasures.

- **Qualitative Risk Analysis with the Risk Analysis Matrix.**

Pick an asset: A laptop.

- How likely is one to get stolen or left somewhere?
I would think possible or likely.
- How bad is it if it happens?
That really depends on a couple of things:
 - ♦ Is it encrypted?
 - ♦ Does it contain classified or PII/PHI content?

		Consequences				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Almost Certain	H	H	E	E	E
	Likely	M	H	H	E	E
	Possible	L	M	H	H	E
	Unlikely	L	L	M	H	E

Where the L, M, H, E is for your organization can be different from this.
L = Low, M = Medium, H = High, E = Extreme Risk

- Let's say it is likely and a minor issue, that puts the loss the high risk category.
- It is normal to move high and extreme on the quantitative risk analysis. If mitigation is implemented, we can maybe move the risk level to "Low" or "Medium".

Bonus

- **Types of attackers**
 - **Hackers:**
 - ♦ **Now:** Anyone trying to get access to or disrupt any leg of the CIA Triad (Confidentiality, Integrity, Availability).
 - ♦ **Original use:** Someone using something in a way not intended.
 - ♦ **White Hat hackers:** Professional pen testers trying to find flaws so we can fix it (Ethical hackers).
 - ♦ **Black Hat hackers:** Malicious hackers, trying to find flaws to exploit them (Crackers – they crack the code).
 - ♦ **Gray/Grey Hat hackers:** They are somewhere between the white and black hats, they go looking for vulnerable code, systems or products.
 - ♦ **Script Kiddies:**
 - They have little or no coding knowledge, but many sophisticated hacking tools are available and easy to use.
 - **Outsiders:**
 - ♦ Unauthorized individuals - Trying to gain access; they launch the majority of attacks, but are often mitigated if the organization has good Defense in Depth.
 - ♦ Interception, malicious code (e.g. virus, logic bomb, trojan horse), sale of personal information, system bugs, system intrusion, system sabotage or unauthorized system access.
 - ♦ 48-62% of risks are from outsiders.

Bonus

- **Insiders:**
 - ♦ Authorized individuals - Not necessarily to the compromised system, who intentionally or unintentionally compromise the system or data.
 - ♦ This could be: Assault on an employee, blackmail, browsing of proprietary information, computer abuse, fraud and theft, information bribery, input of falsified or corrupted data.
 - ♦ 38-52% of risks are from insiders, another reason good Authentication and Authorization controls are needed.
- **Hackivism/Hacktivist (hacker activist):** Hacking for political or socially motivated purposes.
 - ♦ Often aimed at ensuring free speech, human rights, freedom of information movement.
- **Governments:**
 - ♦ State sponsored hacking is common; often you see the attacks happening between the hours of 9 and 5 in that time zone; this is a day job.
 - ♦ Approximately 120 countries have been developing ways to use the internet as a weapon to target financial markets, government computer systems and utilities.
 - ♦ Famous attacks: US elections (Russia), Sony websites (N. Korea), Stuxnet (US/Israel), US Office of Personnel Management (China), ...

Bonus

- **Types of Attacks**
 - **Phishing, spear phishing and whale phishing** (Fisher spelled in hacker speak with Ph not F).
 - ♦ **Phishing** (Social engineering email attack):
 - ☐ Click to win, Send information to get your inheritance ...
 - ☐ Sent to hundreds of thousands of people; if just 0.02% follow the instructions they have 200 victims.
 - ♦ **Spear Phishing:** Targeted phishing, not just random spam, but targeted at specific individuals.
 - ☐ Sent with knowledge about the target (person or company); familiarity increases success.
 - ♦ **Whale Phishing (Whaling):** Spear phishing targeted at senior leadership of an organization.
 - ☐ This could be: "Your company is being sued if you don't fill out the attached documents (with trojan in them) and return them to us within 2 weeks".
 - ♦ **Vishing (Voice Phishing):** Attacks over automated VOIP (Voice over IP) systems, bulk spam similar to phishing.
 - ☐ These are: "Your taxes are due", "Your account is locked" or "Enter your PII to prevent this" types of calls.



Labs

- Add to risk register information about deterrent and preventative actions or tools



Labs

Cause	Event (risk)	Effect	Probability (1-8)	Impact (1-10)	Value (probability x impact)	Preventative actions (tools)	Deterrent actions (tools)
Because there are no team lead	Module will be developed poorly with many security issues	More time for testing and bug fixing, more possibilities and time to use for hacking	2	7	14		

Preventative Actions: Regular Cybersecurity Trainings, Phishing simulations, Password change policy, Security Audits, Policies renew, OS and Software updates, Allow only VPN connection

Deterrent: Firewall, 2FA activation, Trainings about sensitive data, Monetary losses, Penalties, Activity Monitoring

Tools: Firewall, Antivirus>Security, VPN client, CTV, DLP, IPS, IDS, Access Control System, PAM