Joshua's CISSP Notes

https://www.studynotesandtheory.com/single-post/How-Joshua-Cracked-His-CISSP-Exam

What are you protecting? What controls are you going to apply? How are you going to monitor those controls/ assets?

Remember! Controls and information need a risk assessment for need and cost and need monitoring to see if controls are working properly and not violating security policy. Doesn't matter what kind of controls whether its admin, physical, or logical

All information is not equal in terms of value and risks.

REMEMBER to that policies, DRP/BCP, etc.. all have to be tested and reviewed constantly.

REMEMBER TO PRIORITIZE NEEDS of Organization.

CONTROLS ARE JUST A WAY TO EXECUTE POLICY. How are people or controls and processes going to know what to do without policy?

Be aware of words like "all" or "every" or "always". These words can be associated with high costs or a lot of resources to be used.

Hint: Always ask what's the risk of the activity and the cost of mitigating the risk regarding the CIA and IAAA.

ITIL services = Helps align IT services with business needs. Provides guidance on how to use IT as a strategic tool to help the scalability of businesses.

COBIT = governance. Deals with integrity

Security Professional = evaluate risks against critical assets and deploy safeguards to protect assets. Important to understand the mission and vision of an organization. Also to maintain documentation. They also must ensure that policies and followed are defined based on Senior management expectations to meet information security needs.

Always think about IAAA and CIA

Operations security deals with resources, hardware and information. Not personnel.

Integrity deals with Information and System integrity.

Document Risk Assessment, Vulnerability, and Pen test results. Senior Management will need to review.

Governance (Security and Third party) = making sure security and third party vendors do what they are supposed to do.

Golden rules:

a. **PEOPLE SAFETY FIRST (Physical)**
b. **MANAGEMENT BUY-IN CRITICAL (Endorsement and signature)They initiate. Make sure they understand.**
c. **EVERYONE IS RESPONSIBLE FOR SECURITY (Responsible for understanding and reading policies and procedures and going to training) Including BCP/DRP etc.**
d. **SECURITY AWARNESS TRAINING IS ESSENTIAL (ADMINITRATIVE CONTROL/Deterrent) Modifies behavior**
e. **POLICY (Data, Security, Rention)t SETS THE WHOLE ORGANIZATION UP (WITHOUT POLICY THERE IS NO SECURITY and THERE IS NO RISK MANAGEMENT) IT DEFINES AND DIRECTS (Directive control)!!! YOU CAN"T DO ANYTHING WITHOUT POLICY**
f. **COST IS IMPORTANT and ADMIN OVERHEAD AND RESOURCES.**

Common Criteria seeks to eliminate known vulnerabilities of the product of testing.

Mid-week firings are better.

Awareness training must be tied into all security policies(Ex. Incident response, security policy and DRP)

A threat does not present a risk if there is no vulnerabilities.

Testing a system main purpose is to test the effectiveness of security controls and to see how effective your risk management process is.

As part of the risk mitigation, it is important to prioritize risk based on High to Low

Assigning responsibility is one of the last steps in the risk management.

List of people to implement controls should

Fraud = loss of integrity.

Least Privilege deals with Confidentiality and Integrity

Need to know =Confidentiality

THE most significant cost to a computer program is personnel

Interdependencies = depend on other functional security controls to operate properly. Ex. In order for a control to be successful and secured, it depends on other controls.

Data Handling refers to making sure data isn't lost or stolen when it is being used. Logging, auditing, and monitoring can be used as a recovery/corrective control.

Relating to job positions, it is critical that management define the sensitivity position so that there are no wasted resources or unacceptable risk can be mitigated.

Asymmetric encryption = can be used to verify the server identity. Is used to prove (authentication) an identity to a system. This is important because a system needs to be able to make sure that the right system/user can access another system's information. Protect against authentication attacks.

Separation of duties = separating job roles (ex. Network Admin and System development). Integrity

Least privilege = deals with a users access level. Minimum knowledge to a job. Confidentiality.

Having excessive privileges is dealing with authorization.

If a hacker gains unauthorized access to a system, this can be detected by reviewing accounts frequently. Know which users have access to sensitive information as opposed to users that just have standard access. In addition, if a company is dealing with contractor, know tasks the contractor is responsible for and the systems contractors can access. LEAST PRIVILAGE. Also check for any modifications on a user account. Accounts should only be provisioned by authorized individuals. Of course since these are controls, risk analysis must be conducted by the security professional to determine the cost and risk.

Be careful and read questions. Just because a user has access doesn't mean they have excessive privileges. This could just mean that they are authenticated to the system and nothing more. Review of user accounts can determine inappropriate access.'

Smart Tokens require a lot of user administration due to key management and hardware.

Awareness training (Deterrent) establishes accountability by making user sign that they have attended training. Awareness training can include manuals, guides, events, slides, posters and brochers.

Systems that are available to the public are a concern. Segregate these system to allow the public to access them without damaging organization information.

Automated auditing tools can save money as oppose to manual reviews.

Auditing is a form of due care.

Contractors have high turnover within an organization and costs are high for user administration. Contractors are considered third party. Make sure you monitor(privacy notice) them, properly identify them.

Certification vs evaluation = Certification is a technical evaluation of security controls. Evaluation is used for testing security features of a system.

Keep in mind that continuous monitoring such as Vulnerability and Pen Test also help identify how effect risk management processes are.

PAPA

Protect Society and the commonwealth and the infrastructure (IS systems)

Act honestly, legally, justly, responsibly, and honorable

Provide diligent and competent services to principals

Advance and protect the profession.

Data owner is part of senior management which has the ultimate responsibility of protecting data.

1. Policies are strategic
    a. Standards (tactical) Lower cost of owenership. You scope and tailor standards based on organizational systems.
    b. Guidelines (Tactical)
    c. Procedures (Tactical)

Due Diligence = investigating risks (management) and verification of current controls that are implemented.

Due care = taking action to mitigate risks.

Negligence = lack of due care

Intrusion Detection and Prevention deals with DOS and DDOS.

Return on Investment = how much is saved after mitigating a risk.

Total Cost of ownership = total cost of mitigating a safeguard.

Standards and Policy are considered mandatory controls

Cyber and typo squatting are intellectual Property attacks

Privacy MUST be address in policy and must let people know that they are being monitored and the data being collected!

Personal data must be relevant to the purposes which it is being collected.

Individuals must be able to choose whether they want their information shared or not shared.

Limit the collection of personal data obtain by lawful means

Individual needs to be told and give acknowledgement about how their data will be used.

Personal Data must be kept up to date and accurate and relevent.

People should always know how their data is being used and the type of data that is being stored or if storage changed.

The entity holding onto personal data needs to be accountable for protecting the data.

When it comes to protecting Healthcare information due to privacy. It is recommended (guideline) that encryption is to be used (There are more ways to protect PII). Whole disk is the most secure. This prevents the company from notifying anyone in the event of a breach. When data is not encrypted/unsecured, then the company must alert the individual/public if there is a breach.

If outsourcing services and data remains in another country, it is important to conduct a risk assessment. Also, ensure that laws and regulations are followed since you are the governing (company in charge of data) US company**. It is a must that a contract agreement be developed to account for US laws and regulations (Ex. HIPAA) so that subcontractors or people outside the country must abide by them.**

ISO 17799 = Code of practice for information systems security. Was later renamed to ISO 27002 dealing with techniques. These kinds of standards are treated like guidelines internally.

Third policy governance is making sure that companies you outsource to (ex. Cloud) are in compliance with the primary organizations policies, laws and regulations. This includes:

a. Exchanging and reviewing Documentation by the primary organization to determine if the vendor is compliance with the primary organization security policies (Review how they conduct assessments, incident handling, how they are protecting data, and monitoring)
b. If the documentation is sufficient and complete then an onsite visit can be conducted be a consultant or hire an auditor (Maybe known as a SCA) or go out there yourself to see what security controls are implemented.
c. Any risk that the outsourced organization has will also be the risk of the primary organization.

Bell-lapuda = MAC for government access. Multilevel security.

Cross site forgery = client side attacks and involves 2 sites. Forces an end user to execute unwanted attacks. Does not involve the <Script> tag.

XSS = injection using <Script>

Bluesnarfing = stealing information from you

BlueJacking = Spamming

LOSS OF LIFE AND HUMANS ARE PRIORITY OF PHYSICAL Security

Lighting = 8 feet high and 2 feet candle light = dectective.

Dense vegetation close to buildings must be avoided.

Fencing = minimum = 3-4 ft = deterrent controls

Maximum = 8ft with barbwire

Smart cards = technical control

Proxy Server used to Mask a client's identity

CCTV: (physical controls)

Monitoring (Must let people know because of privacy)

Recording = detective

Windows uses MD4 to hash passwords

Teardrop attack deals with Fragmented packets

Land attack = Layer4 that sets destination and source address to be the same

Fraggle attack = sending large amount of UDP packets instead of ICMP

Promiscuous mode = network devices can intercept and read all network packets.(IDS)s Can be confidentiality violation or can be used for analysis.

Circuit switched = One dedicated line between two companies and only one route to use. Lack of availability.

Packet switched = Packets choose multiple routes to get to destination. VOIP use packet switching are considered low cost.

Wireless LANs are vulnerable to availability attacks.

RFID, Barcoding, and Inventory = Prevents theft and reduces risk. Privacy concerns are also an issue by because of marketing techniques.

Biometrics:

User Acceptability is important. Retina Scan has low Acceptability because it blows puffs of air into the users eye. Also analyzes PII information.

Object Reuse = Space on a disk that is allocated for data and not given back to the OS. This can be a confidentiality problem. Or an object that was previously used and then reused without going through the proper sanitization procedures.

White noise is bad because it can disrupt communications on the wire and scramble or mask an attack.

Crosstalk = effects primary integrity and a little confidentiality. Proper shielding can mitigate it.

Faraday cage blocks radio signals.

TEMPEST protects from electromagnetic and prevents communications from crossing.

TEMPEST attacks is the ability to read screens from a distance.

Identification and authentication requires a lot of admin overhead due to creating, distributing, monitoring accounts, and storing information.

Audit trails can be used with Intrusion detection to provide real time analysis.

Audits = User ID, the program used to execute the event, and the result. They should also be flexible meaning the system owner can choose how much data and which data can be logged based on cost and benefits. Remember! Audits are considered a tech control meaning there are costs associated with it. Also remember that an organization should log and analyze data of high importance (Maybe try sampling). All other data should be logged analyzed based on time and resources. MAKE SURE each LOGGING CLIENT's CLOCK is SYNCHED TO A COMMON TIME SOURCE.

Keep in mind that the more detailed audit records are the more system overhead is required and storage is required. Also, if the system is identifying too many events, then the cost will be high regarding investigations to try to sort through all events. Digital Signatures can also help protect the integrity of audit logs.

SAML = exchanging authentication and authorization data between parties. Used for businesses and organizations. Accessing web services.

OAUTH basically is authorization for third parties accessing certain features on a particular website. For commercial use look general users.

OAUTH 1.0 is more secure because it has native encryption. 2.0 just uses SSL.

AD passwords are stored as hashes

IDP = centralized access. Holds all users credentials information that is sent through SAML. It is a single point of failure

Shrink wrap code attacks = developers packaging their software with bugs and backdoors.

Always have a SLA when contracting out to vendors or buying vendor products. It is not a preventative control though. Due diligence is key to making sure controls are in place. Management can be held responsible if due diligence is not in place because of lack of due care. It is also proper to perform attestation. This means that a 3rd party would review the security posture of the service provider and make sure they can be trusted. This can be in the form of penetration testing or other assessment reports. **Involving security early when acquiring services is a preventative control. Always have due diligence by performing risk assessments (Vulnerability and penetration testing).**

Know where your data is and do a thorough risk assessment to see the dangers of outsourcing data (3rd party governance. Make sure they follow law, policy, and standards.

BCP examines and protects all critical business processes and information areas from natural and manmade disasters and focuses on continuing with no disruption.

The security Professional writes the security policy and **implements**. Make sure to get feedback from different business units. Senior management signs of and endorses. Expresses Senior management goals objectives for security.

Metrics are a management tool that can help identify cost and effectiveness of existing controls.

Policies are strategic (Directive)

Always try to think about laws and privacy when it comes to data.

Objects = Labels

Subjects = clearances

Management roles:

Business owners (senior management) = makes sure of staffing, funding, and all assets are protected.

Data owners = ensures data is protected and labeled. Determines the frequency of backing data up. Authorizes access to who gets to see data.

System owners = ensures hardware and software are protected and secured. Works with Data Owner to ensure that data is protected on the system

Custodians = implements the protections and controls for the system and data. Think of it as custodians are mindless waiting to receive guidance. Day to day operations, maintanence, adherence to policy.

Rights = take actions

Permissions = access a file or write information to files.

When it comes to data classification labels always remember it is the data owner who is responsible for confidentiality; meaning they need to classify and give need to know and least privilege authorizations. Data Custodians implement availability; meaning backups, RAID, etc…

How this all ties in.

In order for an organization to succeed, security must be the at the forefront and support the business and not hinder it. Senior Management is the ultimate decider on what needs to be done and how it needs to be done. Security tasks must be supported by senior management. Since Senior management is ultimately responsible, they are ultimately accountable if security measures are not implemented. It is the goal of Senior management to make sure controls are implemented (due care), and to make sure to follow up on those controls/monitor those controls (due diligence: ensuring, researching, testing, monitoring, and ensuring security/risk assessments are done.).

Let's just say that I have been assigned a **new CISO** position for a company. My first action would be to create a security policy **defining my security goals, the mission, and objectives of the organization.** Also, I would want the security policy to **define roles (Groups of people responsible for certain tasks),** define the type of controls **(Not how to implement them)**, and **define** and **emphasize the importance of the CIA triad as it pertains to our assets**. I would want everyone to understand as the CISO, I will support any security solution that is **cost effective** and that will increase our effectiveness for the CIA triad. We must continue to **monitor and upgrade security** to keep our risk at a minimum. **My support and my signature will be the first step in implementing the policy**. Our **Security professionals will write and continue to implement the policy**.

My next order of business will be to make we define classification system in order to implement security solutions. Then we want to make sure all of our current assets/information are classified and proper security controls are implemented. This way we can fully understand what controls are needed. Next step is to establish a **risk management plan in order to assess the different risks and vulnerabilities/threats involved within the company and to keep risk at a minimum for the assets**. For this plan to work I would need to give my full support and give approval for the security professional/team. **The security professional would need to identify tangible and intangible assets for the organization and state the system characteristics**. From here, the risk analysis will begin in which the security professional establishing a value on assets (Asset Value) based on the cost and overhead, the implementation, maintenance, continual operation, the storage costs, replacement costs, advertisement, offsite storage costs. Then prioritize items based on value. Next would by the threat assessment\vulnerability for each asset in the organization based on confidentiality, integrity, and availability (Viruses, theft, not compliance with policy, break-ins, hacker, software backdoors, malware, brute force/dictionary attacks, data loss, data change, single point of failure, vendor storing the data, etc). The security professional must do a quantitative and qualitative analysis to determine the impact/likelihood(qualitative) and to determine costs of a risk being exposed (quantitative). From there, the security professional can assess different countermeasures\controls\safeguards for that risk and

perform a cost/benefit analysis to find out if the damage the risk generates is higher than the cost of the countermeasure. If so, then you can add the countermeasure to list of recommendations to the CISO. If not, then it is not financially reasonable. **Also make sure when suggesting controls, that they are testable, Accountability, consistent (integrity), have overrides for privileged operators (availability), provide fail-secure (confidentiality), and fail-safe (availability), measurable, consume less resources and labor before and after.** List the recommendations down for the CISO so that I (CISO) can make the choice on whether to implement the countermeasure (Risk mitigation), buy insurance (risk transference), Accept the risk (risk acceptance), or just ignore the risk (risk avoidance – Not recommended). Once The CISO makes the decision on what to do, security professionals MUST monitor (Detective) the safeguards and risk continuously to see if there are any new developments that can violate security policy and document. Keep in mind that sometimes its not about cost. Law and regulations might mandate a security control as well. **In that case, the organization has to comply!**

Now, there could have been a variety of controls recommended by the security professional and selected by the CISO. These controls fall in the category of technical/logical, physical, or administrative. These categories are further divided into sub-categories which are:

1. Directive
2. Deterrent
3. Preventative
4. Corrective
5. Recovery
6. Compensating

For example, let's say one of your assets includes the data for your organization. The risk analysis indicated that there is a high chance (qualitative) that data can be disclosed, tampered, or completely deleted. This can come in many different forms. A security professional makes a recommendation for encryption, hashing, and server backups onsite and offsite. Since data can be invaluable (Could hold a high classification) to an organization, CISO gives the green light based on budget and cost/benefit analysis on doing encryption for data in motion(PKI/SSL/TLS) and at rest (AES, DES). Also gives the green light on providing hashing to protect the integrity. This is where cryptography/networking comes in. Labeling/marking data is also a kind of control that needs to implemented (This should happen after the policy is created). The kind of controls that would be implanted in this situation would be technical/preventative, technical\recovery, administrative\preventative.

Now, after these controls are implemented, they must go through the change management process if the control needs to change or if the system needs changing. This is to ensure:

a. Any changes that happens can be rolled back
b. Any new changes don't effect the current security
c. Must be reviewed and approved by change management board.
d. Changes must be tested
e. Document any changes to the current system.

Once changes are tested then the security professional can implement those changes to the system and continuous monitor, and audit (Detective) to see if the risk has been reduce in terms of violating security policy. Now, the CISO might say I need to perform my due diligence and see if these changes have been or how effect these controls are(Con Mon). This is where testing comes into play such penetration testing(preventive) or vulnerability testing. CISO might hire a penetration tester to see just how secure his system/data is. Of course the penetration tester would need to sign an agreement.

Keep in mind, that as the CISO, you don't want to implement any unnecessary controls due to the fact they might not be compatible or they require extra admin overhead or not cost effective. Or leave unnecessary programs up.

Another example of implementing the approved controls would be Access Controls. If the risk analysis stated that more stringent access controls are necessary then,, CISO would review to see if there is a budget/cost benefit. Once approved, then security professional would implement the access controls. These controls can range from:

A. Two factor authentication (more user admin overhead)
B. Protection against brute force/Dictionary attacks
C. Implementation of non-discretionary/discretionary controls.

Always remember that before controls are sent for recommendation to Senior management, they must be testable, cost effective, Accountability,preferably little not that much resources to implement, compatible, and not hinder the functionality of a system.

Now, what happens if a disaster strikes or a major event impacts our business. I as the CISO will need to make sure we can continue our operations. **This includes gaining my support (convincing me that it will cost more not to have a BCP)** and having a team of business managers (networking, physical, Web administrators) from all areas (including representatives from senior management) of the business to decide which functions are critical in order to keep operations going in case of a manmade or natural disaster. We must keep the availability of the going. I must keep in mind the labor that it takes to implement a BCP and the people it takes. WE don't want to run out the budget or take time away from

other matters at hand. Once we have identified the labor/resources, the business areas, and established my support, the BCP team can get to work establishing what functions/ assets are the most critical to the business so that the that team can identify risks and assign workload to those functions/assets. Now let's do a risk assessment to see what are the possible threats that can threaten the availability of the organization. Let's also do a risk analysis to see how much monetary damage a threat can cause (quantitative) and if the threat can cause damage to a reputation (qualitative). Once the Risk assessment is done the BCP must prioritize the resources based on the risk analysis, The team must also keep in mind to combine the qualitative approach as well. Remember cost effective! The plan should be coming into form and need to see which assets the organization is going to address first. This is called a strategy plan. MTD should be used to help prioritize the each risk. Now let's create the controls that will be used to mitigate the risks that the team felt necessary to fix. Now our policy is complete, I should receive all documented results so that I can make a decision and give my approval. Keep in mind that if you had my support and representatives from the beginning then I should have no problem in signing the document.

As the CISO I need to perform due diligence and make sure that all people receive some kind of training on the BCP in order to instill confidence that the CISO has considered the risks and safety of personnel and business operations.

As the CISO I MUST COMMT TO THE PRESERVATION OF LIFE WHEN IT COMES TO THESE KINDS OF EVENTS.

Also when it comes to acquisition, it is not just referring to hardware and software. It Is also referring to buying the services of Vendors to potentially house the organizations data/systems. Make sure as the CISO you review documentation (SLA, laws and regulations, etc) from the vendor and establish an onsite visit to meet people and to see if security controls are in place according to our organization. If there is any risk then their risk becomes our risk.

Point is Security always comes full circle!!! You always have to perform your due diligence to and always have to keep monitoring. Always remember, EVERYTHING GOES THROUGH SENIOR MANAGEMENT AND THEY HAVE THE FINAL SAY. SECURITY ALWAYS STARTS OFF WITH POLICY(with no policy, there are no controls)AND THEN RISK ASSESSMENT.

Security controls must be effective and consume little resources as possible (Less Admin overhead, People and Labor)

Access control features are the same way. (Ex. Implementing security features such two factor or DAC or ACL). Goes through the same process.

Incident response

Identify = investigating the incident to see if it needs to be elevated

Response = get the incident response team involved. Inform Senior Management so they can make decision.
Mitigate = Contain the incident (Isolate the system)
Report = Report major incidents to Upper management. Then upper management will decide whether to inform law enforcement depending the type of incident.
Recovery = Return the system to full state (This is why configuration management is good)
Remediation = root anaylsis and recommendations to prevent reoccurrence. Have senior management determine whether to implement new controls or not.
Lessons learned = see if there are any lessons to be learned.

REMEMBER! An incident can mean any attempts on a system as well

HoneyPots and Warning banners are considered preventive measures as well disabling unnecessary services.

Active Directory Federated Services: In order to have federated services you need a PKI. As I recall, PKI deals with confidentiality, Integrity, Access Control (Iden, Authoriztion, **Authentication**, preventive), and non-repudiation.

IPS = detect and prevent malicious actions.

IDS = should be designed to detect interesting and abnormal traffic that could lead to an attack based on signature or patterns. SHOULD NOT DETECT INTRUSTIONS
SIEM = IDS

IPS is defense in depth for firewall. Not meant to replace it.

TCP = integrity because of its error free transmission.

Data Loss Prevention = Detect and prevent the exfiltration of data leaving the organization.

EndPoint Security (Defense in Depth) = AntiVirius, Application Whitelisting, Whole Disk Encryption, Host Based Intrustion Detection/Prevention System)

Configuration Management saves time and will increase security for a system by having a harderned version and baseline. Disable unessary services, and remove all applications not needed.

We must set up a SSL certificate to prove (Authentication) who we are (the organization) to other entities in the federation. Now to save COSTS for the organization by not buying a third party certificate (Ex. GoDaddy) we can create our own certificate for our organization so that our Server can prove itself to federation clients trying to connect. In order for clients to trust the server, the clients will have to have the server's public key of the certificate. The public key is stored in the clients Certificate

store of the browser that they will be using. Essentially, this is the same way third party certificates work.

Cryto keys should not last a lifetime due to the frequent use of them.

A federation trust is a one way trust that an organization that maintains resources (such as email services) trusts an organization that maintains accounts to access the resource.

Cold boot = shutting down a computer and refreshing the hardware.

Management can declare a disaster when a critical business unit outage exceeds the MTD.

Difference between data in motion vs transportation. Motion = over networks. Transportation = taking to offsite storage facility.

Grid computing = distributing computing because everything is **not on ONE computer.** Everything is decentralized and spread out towards different computers. Grid computers uses other computer resources.

Internet of things = small internet devices that are difficult to patch and have default credentials.

Malware uses covert channels

Malware (Malicious code) software that attacks applications and systems. Data Loss Prevention protects against this.

Worms = malware that effects availability and integriy. Spreads through network connections.

Client-side attacks = depends on the user downloading malicious content.
Server side attacks = launched directly from a client.

Inference = deduction (polyinstatation) making a decision based on information
Aggregation = mathematical (limit the amount of queries) combination of information.
Mobile devices – make sure before connecting mobile devices that they a patched, and antivirus signatures. Use Layer to 2 802.1X to port **authenticate** before allowing mobile devices to communicate

Math not secrecy is cryto best strength.

Wireless connection lacks availability. Critical functions should use wired networks.
DSSS and FHSS are methods for sending traffic through radio bands. Are there to maximize Availability and less interference.

DSSS uses entire band and spreads the signal throughout the band.

FHSS uses smaller frequencies and hops through them in random order.

MAC filtering is least effective because they are broadcast In clear. Easy to Spoof.

Port isolation = PVLAN = communication only to a certain uplink. Segmentation.

Static protocols are good for small offices. Need to be configured manually.

Routing protocols are more dynamic and can protect the availability of the network. If a network goes down then routing protocols will know where to go next.

Firewalls filters traffic, ports and IP.

Packet filtering firewalls can't stop ICMP and UDP

Proxy Firewall hides the origin. For example a TCP threeway handshake. Rather then a computer sending a SYN to another computer; the firewall terminates it and then sends its own SYN connection and vice-versa.

Circuit switched = One dedicated line between two companies and only one route to use. Lack of availability.

Packet switched = Packets choose multiple routes to get to destination.
MAC = Based on Bell lapada model. (multilevel). System administrator set clearance by administrator but classification set by data owner.

CER = describes the accuracy of biometrics. Used to measure different biometrics systems

If sensitivity increases, FRR rises. If sensitivity is lowered then FAR will rise.

Non-transitive = trust just between 2 partners.
Transitive = trust between 2 partners and any associated partners of the primary partners.

IDAAS = intergrating with cloud identity service providers. Easier deployments, self service password management, and centralization.

Full knowledge testing = easier way to find an insider threat. Least likely to crash a system.
Zero Knowledge = simulate a real attack from outside.

If integrity of system is at risk then the penetration testing should stop.
Penetration testing (Preventive) should be classified at the highest level.

System misconfiguration, outdated software, or lack of patching are all examples of vulnerabilities.
NESSUS should be used to find these vulnerabilities.

Tools like NESSUS are only half of identifying risk. DON't FORGET THAT YOU ALSO NEED TO IDENTIFY THE THREAT! Risk = Threat X Vulnerability.

Security Assessment (due diligence) = are broader and view many controls such as:

- Policies
- Change Management
- Penetration testing
- Real world effectiveness
- Security audits

Goal is to view as many access controls to make sure everything is considered.

Audits make sure standards are met.

Integrity of log files is extremely important. Centralized logging will help with that by saving them in one location. Logging helps with incident response and accountability.

Log rentention policy needs to be created and maintained. Legal and regulatory considerations must be considered as well.

Grahan-Denning Model=There are 8 rules

Harrison – Ruzzo = 6 rules.

Encryt data at rest with symmetric encryption (AES)

Encrpt data in transit (SSL, TLS, VPN)

Data in use make sure there is strong authentication and authorization and accountibility

Always define data classifications. Meaning, always determine the value of the data and the labels used within the organization in the security policy or data policy

Then define the security requirements. Meaning the steps a company should take to protect the confidentiality an integrity of data.

Costs is not a factor in classifying data.

Costs are factor in controls

Forensics vs incident = Forensics focuses on evidence and crimes and incident response is concerned with identifying, recovering from security incidents, and control the cost and damage.

EDiscovery = Electronically stored data...

Identification

Collection

Processing

Preservation

Change Management – Make sure you do a risk assessment on the change after proposing the change to see if it is cost effective. Without change management, vulnerabilities and loopholes can exist in the system. Affects Availability and integrity.

- Identify
- Propose
- **Assess the risk**
- Test change
- Schedule the change
- Notify the parties of change
- Implement
- Report results

The first step towards BCP and DRP is management support. Make them understand the risks for not having one and the cost when a disaster happens.

BCP = umbrella that includes multiple plans including DRP. BCP is focused on long-term and critical business functions or service provided (ex. Service to customers as opposed to email systems).

DRP = short term and is more information systems centric.

If the organization has multiple locations, there needs to be a response plan for each location for DRP.

Documentation is critical for DRP. Must be stored in several secured locations in order to provide availability.

BCPlanner =Maintains relevant documentation, Coordinator for any interruption, responsible for training and backup of all plans.

Keep stakeholders informed since their company is effected by the disaster as well.

BCP determines MTD.

Read through = checklist which means checking to see if all components are available. Cost the least.

IPSEC = VPN which allows to send private data over insecure network.

PPTP = provides authentication by way of CHAP, PAP

PGP = asymmetric encryption confidentiality, integrity, authentication, and nonrepudiation. Used to encrypt emails, documents or entire disks. uses Asymmetric and symmetric. Email uses Asymmetric encryption. There is no certificate authority present because of Web of Trust. Basically, If you trust me that if you trust that my digital, certificate authenticates me then you trust all of my digital certificates.

Grid computing = harnessing resources from other computer resources. It is a form of distributed computing. No confidentiality.

Web 2.0 is more dynamic than its predecessor HTML.. Susceptible to confidentiality attacks. It is the ability to share information and collaboration on the internet.

Smart cards offer accountability due to the chips inside as oppose to regular locks.

Fences = 8 ft = preventive. 3ft = deterrent

POP3 = email protocal that clears email from server after emails have been downloaded.

IMAP4 = Allows emails to be downloaded but they also stay on the server.

SMTP = No authentication and no encryption.

Internal Firewalls block traffic from leaving the network except by proxy server.

Man in the middle = loss of integrity because the attacker can inject his own information in packets and re-route information.

VOIP = uses SIP to protect the integrity of calls.

REMEMBER DATA BACKUPS HELPS WITH INTEGRITY AND AVAILABILITY. They should be verified by restoring tapes at offsite facilities to verify.

Worms, viruses, Trojans, adware, and spyware can be stopped by antivirus.

IPS/IDS inspects network traffic that the firewall passes through to see if there is any suspicious.

HIDS/HIPS inspect logs on the client system

Antivirus = inspects specific files and is endpoint security.

Firewalls filter traffic that comes through (Depending on the type of firewall, it can mask an identity or actually inspect the communication within the firewall).

Multi-tier fire walls depend on how many different segments there are.

Split Knowledge = What each must bring to table. Usually involves combining encryption keys.

Dual Control = Deals with 2 people colluding together to gain access to an asset.

Both deal with integrity just like separation of duties.

Admin controls = Laws/policies that a company makes you agree to in writing. Enforceable by law.

Deterrent (User Awareness Training) = reduce the risk of an attack.

Procedures = Preventive

Policies = directive

Job rotation = detect insider threat.

Mandatory vacation = detect fraud.

Corrective = If something happens, then what is the reactive response and immediate response such as (isolating a network, fail safe/fail safe). Reduce impact.

Recovery = restoring processing back to original state. DRP/BCP

N-DAC = centralized access determined by the administrator. Everything goes through the admin.

Tools that monitor the content of traffic are weak against encryption.