Dalton Murray

**Chapter 11 questions**

**Question 2: Briefly outline the steps required to complete a risk assessment**

There are many different ways to complete a risk assessment and it may depend on one of the three risk assessment frameworks, or potential other frameworks, the three listed risk assessment frameworks are: Operationally Critical Threat, Asset, and Vulnerability Evaluation, or OCTAVE, and it is from the Computer Emergency Readiness Team, Control Objectives for Information and Related Technology, or COBIT, and it is from the Information Systems Audit and Control Association, and Risk Management Guide for Information Technology Systems or the NIST guide, and it is from the National Institute of Standards and Technology (FitzGerald, J. p. 296).

The general steps which are shared within these frameworks to complete a risk assessment are:

Develop risk measurement criteria – These are the measurements which are used in order to evaluate the way in which a security threat would be able to affect the organization and have an impact such as on their financial, productivity, reputation, safety and legal areas (FitzGerald, J. p. 297). On top of this, it is important to be able to prioritize impact areas of importance. (FitzGerald, J. p. 297).

Inventory IT assets – Firstly what is an asset? An asset is something which has a value and can be multiple different things such as hardware, software, data or even an application. It is important to take an inventory of all IT assets, especially mission-critical applications which would requirement immediate response if it were to be taken down (FitzGerald, J. p. 298). It is also important to rate all assets in importance. (FitzGerald, J. p. 298).

Identify threats – You must be able to identify threats, threats are any potential occurrence which is able to do harm, interrupt the systems using the network or even cause any monetary loss to the organization (FitzGerald, J. p. 299). On top of identifying threats, you should create threat scenarios (FitzGerald, J. p. 300).

Document existing controls – In this you are documenting existing controls, creating a risk control strategy, or how you address a risk, you can generally either accept, mitigate, share, or defer a risk and then continue from what you have picked (FitzGerald, J. p. 301). Controls are also generally referred to as antivirus software, firewalls, security training, or any other controls which your company has in place (FitzGerald, J. p. 301).

Identify improvements – This is the final step, and it is to identify where you are able to make improvements or where they are needed at such as additional controls (FitzGerald, J. p. 304). This also includes focusing on threat scenarios which the mitigation has a low level of adequacy (FitzGerald, J. p. 304).

**Question 5: What are the most common security threats? What are the most critical? Why?**

The most common security threats fall under two categories which is business continuity and preventing unauthorized access (FitzGerald, J. p. 294 - 295). The most common security threats are malware, information theft, equipment theft, device failure, denial of service attacks, sabotage, and natural disasters (FitzGerald, J. p. 300).

The most critical security threats are the ones which your company determines to have the highest impact score. This is because different companies will have different most critical security threats depending on their structure. However, the most common most critical/major security threats to business continuity are viruses, theft, DoS attacks, device failure, and disasters (FitzGerald, J. p. 339). This is because they may pose the most amount of damage.

**Question 10: What is the purpose of a disaster recovery plan? What are the five major elements of a typical disaster recovery plan?**

A disaster recovery plan is a plan which addresses various levels of response to multiple different disasters and is able to provide partial or complete recovery of data, applications, network components, as well as physical facilities (FitzGerald, J. p. 310).

The five major elements of a typical disaster recovery plan are as follows:

* “The name of the decision-making manager who is in charge of the disaster recovery operation. A second manager should be indicated in case the first manager is unavailable” (FitzGerald, J. p. 311).
* “Staff assignments and responsibilities during the disaster” (FitzGerald, J. p. 311).
* “A preestablished list of priorities that states what is to be fixed first” (FitzGerald, J. p. 311).
* “Location of alternative facilities operated by the company or a professional disaster recovery firm and procedures for switching operations to those facilities using backups of data and software” (FitzGerald, J. p. 311).
* “Recovery procedures for the data communication facilities (backbone network, metropolitan area network, wide area network, and local area network), servers and application systems. This includes information on the location of circuits and devices, whom to contact for information, and the support that can be expected from vendors, along with the name and telephone number of the person at each vendor to contact” (FitzGerald, J. p. 311).

**Question 11: What is a computer virus? What is ransomware?**

Although not directly defined in the book, a computer virus is a piece of malicious code designed to do something specific, such as cause a disruption in your computer, to spread to other files and programs, and perform actions without your knowledge or consent, it operates by inserting or attaching itself to a potentially legitimate/real program and then executing its code, this code it has may cause damage to your computer (FitzGerald, J. p. 304 & Johnson, A.).

Ransomware can be harmless, and its purpose is to cause an annoyance rather than real damage, however, it can also be very serious (FitzGerald, J. p. 304). Ransomware can completely destroy a system to make it unusable (FitzGerald, J. p. 304). The idea behind ransomware is that they attack a system and encrypt all the data on it and then make the person who owns the system pay money, a ransom, to get their files back. However, there isn’t even a guarantee that after paying they will unlock your system for you and could just delete everything permanently now that they have your money too.

**Question 13: How does a denial-of-service attack differ from a distributed denial-of-service attack?**

A denial-of-service attack is when a single attacker tries to disrupt their target by flooding it with messages, or packets, so that the server/target is unable to process or respond to messages from regular people (FitzGerald, J. p. 305).

A distributed denial-of-service attack has the same end hopes of a DoS attack, however, is not from a single attacker and is from many if not thousands of attackers/computers which are trying to disrupt the service (FitzGerald, J. p. 306).

**Question 17: There are many components in a typical security policy. Describe three important components.**

Three important components of a typical security policy are as follows:

* “The name of the decision-making manager who is in charge of security” (FitzGerald, J. p. 314).
* “An incident reporting system and a rapid-response team to respond to security breathes in progress” (FitzGerald, J. p. 314).
* “A risk assessment with priorities as to which assets are most important” (FitzGerald, J. p. 314).

**Question 26: What is a NAT firewall, and how does it work?**

NAT or Network Address Translation is the process of which you are converting between a set of public IP addresses and a set of private IP addresses which are hidden from outside of an organization (FitzGerald, J. p. 316). A NAT is also transparent, so no computer knows what is happening (FitzGerald, J. p. 316). It is most commonly used for security and for IPv4 address conservation and means if an external intruder somehow gets into your network, they won’t be able to see the private IP addresses and thus cannot attack your computers (FitzGerald, J. p. 316).

A NAT firewall has an address table which it uses so it can translate the private IP addresses from within the organization into a proxy IP address which is used on the Internet (FitzGerald, J. p. 317). When there is a computer inside the network/organization which is trying to access a computer on the Internet the firewall changes the source IP address in its outgoing IP packet to its own, further it sets the source port number in the TCP segment to its own unique number which is then used as an index for the address table so it can find the real IP address of the sender within the internal network (FitzGerald, J. p. 317). When the computer which the internal one was contacting to outside finally responds the message goes to the firewall which makes sure that the packet is permitted within the network and then changes the destination IP address to the internal/private IP address as well as changes the TCP port to the correct one (FitzGerald, J. p. 317). This allows systems outside of the network to never see the true IP and port of the internal computers (FitzGerald, J. p. 317).

**Question 28: Explain how a Trojan horse works.**

Trojan horses work are remote access management consoles, also sometimes called a rootkit, and it enabled the person who is controlling the trojan horse to access a computer and manage it remotely (FitzGerald, J. p. 322). Trojan horses are usually concealed in other software, which is why it is called a trojan horse, which runs when the software it is concealed under runs (FitzGerald, J. p. 322). When the overarching software gets ran the trojan horse silently installs and allows the attacker to take over (FitzGerald, J. p. 322). When the trojan horse is installed, it allows the attacker full control over the system and allows themselves to be able to do quite a few things such as immediately disable firewalls, antivirus software or other defensive software, on top of this they can change the trojan horse so it can be ran with a specific port, software name, as well as run during specific times (FitzGerald, J. p. 322).

**Question 30: Describe how symmetric encryption and decryption work.**

Symmetric encryption and decryptions works by using a key to encrypt a message, and the same key is used to decrypt it, having one key in total (FitzGerald, J. p. 323).

One of the more commonly used symmetric encryption techniques is called DES, or Data Encryption Standard and uses a 56-bit key and can be more easily cracked (FitzGerald, J. p. 324). 3DES, or Triple DES, is a newer standard which uses a 168-bit key, however, there is an even newer and better technique, the AES or Advanced Encryption Standard, which uses 128, 192, and 256-bit keys (FitzGerald, J. p. 323).

**Question 31: Describe how asymmetric encryption and decryption work.**

Asymmetric encryption and decryptions works by having a key to encrypt a message, and then a different key is used to decrypt the message, having two keys in total. (FitzGerald, J. p. 323 & 325).

An example of asymmetric encryption is RSA, which was invented by MIT in 1977 (FitzGerald, J. p. 325). With public key encryption, keys are often in the 512, 1024, and 2048 bit length (FitzGerald, J. p. 325).

**Question 36: What is PKI, and why is it important?**

PKI, or Public Key Infrastructure is formed by RSA and is what allows the use of public key cryptography for many different things ranging from digital signatures through data encryption and integrity (FitzGerald, J. p. 325). It often uses 512, 1024, and 2048 bit lengths for their keys (FitzGerald, J. p. 325). PKI is important because it allows the usage of encryption more easily by everyone, and reduces key management problems (FitzGerald, J. p. 325). Additionally, public key encryption allows the usage of digital signatures (FitzGerald, J. p. 326).

**Question 38: How does PGP differ from SSL?**

PGP stands for Pretty Good Privacy and is a freeware public key encryption package, most often used to encrypt emails (FitzGerald, J. p. 328). With PGP a user posts their public key on web pages which anyone who wants to send an encrypted message can use to send an encrypted message (FitzGerald, J. p. 328).

SSL stands for Secure Sockets Layer and is an encryption protocol very widely used on the Internet (FitzGerald, J. p. 328). SSL works between the application layer software and the transport layer (FitzGerald, J. p. 328). It works by encrypting outbound packets coming out of the application layer before they can even reach the transport layer, it also decrypts inbound packets coming out of the transport layer before they can reach the application layer (FitzGerald, J. p. 328). When using SSL, the client and the server begin by performing a handshake for its PKI authentication, during this the server provides its public key and their preferred encryption techniques, after receiving this the client generates a key for the encryption technique which is then sent to the server encrypted with the server’s public key (FitzGerald, J. p. 328).

The main differences here is how the communication occurs and the usages between PGP and SSL.

**Question 39: How does SSL differ from IPSEC?**

SSL, Secure Sockets Layer, is an encryption protocol. SSL also focuses on web applications (FitzGerald, J. p. 328). SSL works between the application layer software and the transport layer (FitzGerald, J. p. 328). It works by encrypting outbound packets coming out of the application layer before they can even reach the transport layer, it also decrypts inbound packets coming out of the transport layer before they can reach the application layer (FitzGerald, J. p. 328). The client and the server begin by performing a handshake for its PKI authentication, during this the server provides its public key and their preferred encryption techniques, after receiving this the client generates a key for the encryption technique which is then sent to the server encrypted with the server’s public key (FitzGerald, J. p. 328).

IPSec, or IP Security Protocol, is also a widely used encryption protocol. However, IPSec can be and is used for a larger variety of application layer protocols (FitzGerald, J. p. 328). IPSec is between IP at the network layer and TCP/UDP at the transport layer (FitzGerald, J. p. 328). IPSec can also use a large variety of encryption techniques (FitzGerald, J. p. 328). The first step when using IPSec is for the sender and receiver to determine the technique used for the two of them, once the key and technique has been established, they can transmit data (FitzGerald, J. p. 328).

The main difference between the two is also where they are used and where they sit between such as application layer and transport layer and network layer and transport layer.

**Question 40: What are the three major ways of authenticating users? What are the pros and cons of each approach?**

The three major ways of authenticating users is based on something you know, something you have, or something you are (FitzGerald, J. p. 330).

With something you know, an example is a password, and is the most common use of something you know (FitzGerald, J. p. 330). When using passwords, you must enter in your password before you can log in (FitzGerald, J. p. 330). One of the cons of using this technique is that often passwords are poorly chosen, which is why using something you know may not be the best way (FitzGerald, J. p. 330). A pro of using this is that they can be very easy to manage with tools such as a password manager and can be beneficial as a first layer of security (FitzGerald, J. p. 330).

With something you have it often refers to two-factor authentication, for example having an ATM card while knowing your PIN (FitzGerald, J. p. 331). The pros of this is that it may add a second layer of security, and isn’t something easily guessed (FitzGerald, J. p. 331). Unfortunately, a con of this system is that a lot of people think of it as just adding something extra they have to do, and a lot of places do not require having this extra layer of authentication (FitzGerald, J. p. 331).

With something you are, this often refers to biometrics, such as a fingerprint or retina or face scanning (FitzGerald, J. p. 332). The pros of this is that it is often fast, and does not require much effort (FitzGerald, J. p. 332). Unfortunately, the cons with this is that it may not always be entirely accurate as more and more low-quality systems enter the market (FitzGerald, J. p. 332).

**Question 45: What techniques can be used to reduce the chance that social engineering will be successful?**

One of the best techniques which can be used to reduce the chance of social engineering being successful is simply by giving proper training to all employees of a company (FitzGerald, J. p. 332). Intrusion detection systems can also be useful when preventing social engineering as they may find anomalies which wouldn’t have been figured out before, on top of this is misuse detection (FitzGerald, J. p. 334).

**Chapter 12 questions**

**Question 3: Why is combining voice and data a major organizational change?**

Combining voice and data is a major organizational change because they are usually handled by two separate departments, voice being a communications department who typically would have a switchboard and older technology to be able to handle phone calls/voice, and data usually an IT/technology related department. When combining the two departments, you’ll also likely be redoing all the voice department, changing it to VoIP, Voice over Internet Protocol, allowing voice to be transmitted by digital signal instead of analog. With this change, it may require a lot of additional changes to be put in place such as new hardware and software to handle everything.

**Question 6: What is desktop management, and why is it important?**

Desktop management, also called electronic software delivery, or automated software delivery, is a potential solution to configuration problems (FitzGerald, J. p. 362). It allows the ability to install software on client computers over a network despite not physically at each client (FitzGerald, J. p. 362). It is important so you can mass-deploy software to clients instead of going to each client individually to install software or other things on it, it also reduces the cost of configuration management, and can automatically produce and maintain documentation of all software on each client computer (FitzGerald, J. p. 362).

**Question 14: What are the primary functions of end user support?**

The primary functions of end user support are to resolve problems such as with user equipment like failed hardware, helping with a lack of user knowledge, and for providing software support such as if there are settings/configuration, or incompatibility issues (FitzGerald, J. p. 371).

**Question 18: What do network management software systems do and why are they important?**

Network management software systems are used to help store, organize, and analyze the reports and alerts given by a managed network which monitors, collects and transmits traffic reports (FitzGerald, J. p. 354). They are important because they help manage the network, on top of this the network manager would be able to access the data it stores and organizes and can see the reports which it has analyzed so they are able to see what is wrong with a network or see if an error is occurring so they can fix it (FitzGerald, J. p. 354).

**Question 19: What is SNMP and RMON?**

SNMP, or Simple Network Management Protocol, is the most commonly used network management protocol, and it each SNMP device has an agent which collects information about itself and its messages it processes and stores into a database which is called the MIB, or management information base (FitzGerald, J. p. 355). The network manager which has access to the network management software also has access to the MIB and using software can send messages to each device or group of devices (FitzGerald, J. p. 355).

RMON is something which an SNMP device may have, and stands for remote monitoring (FitzGerald, J. p. 355). RMON with SNMP allows the device to store all MIB information on the device instead of sending it constantly to a central location (FitzGerald, J. p. 356).

**Question 20: Compare and contrast device management software, system management software, and application management software.**

Device management software – Device management software is sometimes called point management software, and it is designed so that it will provide information about specific devices on the network (FitzGerald, J. p. 354). Device management software also allows someone, usually the network manager, to view this information and to see configuration information, traffic volumes as well as error conditions for each individual device (FitzGerald, J. p. 354).

System management software – System management software is also sometimes called enterprise management software or also a network management framework, what this does is provide the same error information, traffic, and configuration information as device management software, however, it also analyzes the device information in order to diagnose patterns (FitzGerald, J. p. 354). With this it also sends out alarm storms which can make it difficult to pinpoint an exact root cause, however, there is also root cause analysis which makes this easier (FitzGerald, J. p. 354).

Application management software – Application management software builds on top of device management software too, however, instead of monitoring systems it monitors applications (FitzGerald, J. p. 354).

**Question 21: How does a load balancer work?**

A load balancer, or also a virtual server, works as a traffic manager which is at the front of the server farm (FitzGerald, J. p. 357). Requests are directed to the load balancer, at its IP, which then forwards it to a specific server using the servers IP (FitzGerald, J. p. 357). There are also different formulas which a load balancer can use such as a round-robin formula and more complex ones (FitzGerald, J. p. 357). When load balancing, if a server crashes, it will direct traffic away from that server (FitzGerald, J. p. 357).

**Question 22: What is server virtualization?**

Server virtualization is more on the opposing side of server farms and load balancers (FitzGerald, J. p. 204). Server virtualization creates multiple logically separate servers on the same physical computer (FitzGerald, J. p. 204). With the different virtual servers, they all are able to appear on the network as separate servers, despite all being on same computer (FitzGerald, J. p. 204).

The example given in the book I really like, picture there’s a company with a lot of servers running at low capacity, having server virtualization can reduce the number of physical servers they need and combine the capacity onto one computer with multiple virtual servers (FitzGerald, J. p. 204 - 205).

**Question 23: What is policy-based management?**

Policy-based management is sometimes called application shaping or traffic shaping and allows a network manager or another person with access to use special software in order to set priority policies for network traffic on different conditions, such as if the network becomes very busy (FitzGerald, J. p. 357). These policies allow them to set different things to have a higher or lower policy, such as saying videoconferencing, such as Zoom, has a higher priority than traffic which has the domain YouTube or other similar policies (FitzGerald, J. p. 357). Policy-based management can be done through hardware and software, an example of the hardware used is a traffic shape (FitzGerald, J. p. 357).

**Question 24: What is capacity management?**

Capacity management uses capacity management devices which are sometimes called bandwidth limiters or bandwidth shapers, these devices monitor traffic and are able to slow down traffic/devices from users who are using up a large amount of bandwidth/network capacity (FitzGerald, J. p. 358).This relates to policy-based management but is more simple in that it looks at sources of traffic instead of the nature of the traffic (FitzGerald, J. p. 358).

References:

FitzGerald, J., Dennis, A., & Durcikova, A. (2021). *Business data communications and networking* (Fourteenth). Wiley.

Johnson, A. (n.d.). What is a computer virus? Norton. Retrieved from [https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html#](https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html)

I pledge that on all academic work that I submit, I will neither give nor receive unauthorized aid, nor will I present another person's work as my own.

Dalton Murray