Nicholas Catani

ISM6331 Information Security
Final Exam Winter 2023 - Gerhard Steinke

Answer all the following 7 questions. **I expect about 300 words for your response to each question**. In all cases, your response is going to an executive of the organization (who needs a clear explanation!). (Add a word count at the end of each question.)

You may not communicate with or discuss these questions with anyone – not even have someone proofread your response. Please add a statement to the end of your exam confirming that you completed this exam completely on your own!

Nicholas Catani

1. Explain the difference between single key (symmetric) and public/private key encryption. What are the two main disadvantages of single-key (symmetric) encryption? (Not the issue of losing the key!) What are the two main benefits of public/private key encryption? What is the purpose of calculating a hash of a file? What is a digital signature? How is the hash used in creating a digital signature?

As far as I am concerned, both encryption methods use keys to encrypt and decrypt data. The main difference is that symmetric encryption uses the same key to encrypt and decrypt data. Whereas asymmetric encryption uses a pair of keys – a public one to encrypt data and a private key to decrypt information. I think the biggest disadvantage of symmetric encryption is its use of a single, secret cryptographic key to encrypt and decrypt information. Because if this key is stored in an insecure location on a computer, then a hacker could gain access to it using software attacks, allowing him to decrypt the encrypted data and thereby defeating the entire purpose of symmetric encryption. Another one would be if one user is encrypting at one location and a separate user decrypting at a second, then the key will need to be transmitted, leaving it vulnerable to interception if the transmission channel is compromised. With asymmetric encryption, private keys should remain stored in a secure location and thus private to the entities using them. The keys needed to decrypt sensitive information are never exchanged over a potentially compromised communication channel. Also, senders can use their private keys to digitally sign and verify that a message or file originated from them and not an untrusted third party.

Hashing allows a user to compare two files for equality - without opening two documents to compare them word-for-word. The calculated hash value of these files will allow the creator to know immediately if they are different.

A digital signature is a mathematical technique used to validate the authenticity and integrity of a digital document, message, or software. It is the equal of a handwritten signature or stamped seal, but it offers far more inherent security. It can provide evidence of the origin, identity, and status of electronic documents, transactions, or digital messages.

To create a digital signature, the software provides a one-way hash of the electronic data to be signed by the creator. An algorithm generates a fixed-length string of letters or numbers called a hash. Then, the private key is used to encrypt the hash. The so-called "Encrypted Hash" with additional information forms the digital signature. You want to encrypt the hash rather than the message because the hash function may convert an arbitrary input into a fixed-length value.

WORD COUNT: 390

Nicholas Catani

2. Suggest two reasons why it might be more secure for Swedish hospital to host their patient data in the cloud. Suggest two reasons it might be less secure for Swedish hospital to host their patient data in the cloud. Explain.

A cloud-based server seems to be secure by default. Only authorized users can have access to certain services. By relying on third parties, the hospital could relieve the burden of data storage and management while having at its disposal technical expertise that otherwise would not be possible to recruit in the healthcare industry. These cloud professionals conduct penetration testing and employ preventive measures such as encryption, or proactively monitoring, to endure that the hospital system is "always" secure. Third parties allocate more time and budget to monitor vulnerabilities, assist in automatic backups, and disaster recovery and improve cloud security – something that is less unlikely to happen in a hospital, because of its busy schedule. However, by migrating to the cloud, is assured that the hospital delegates sensitive responsibilities to the vendor – in a software as a service, for instance. It could raise concerns about patient data which the hospital has little control over it. Sometimes clouds can experience downtimes. Thus, the hospital must rely on a traditional system which might be time-consuming.

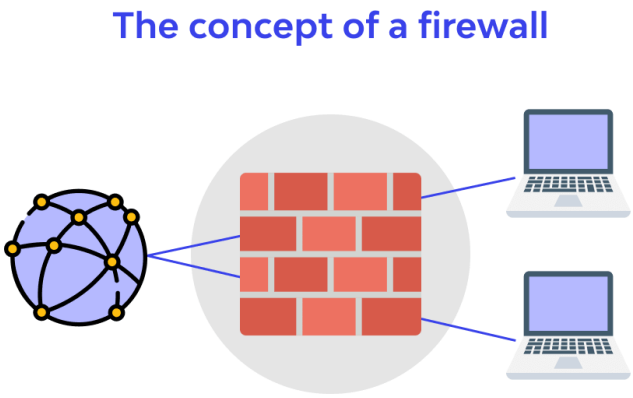
Nowadays, cloud-based servers are implemented with cloud security, a set of policies, strategies, controls, procedures, and practices designed to safeguard the data, resources, and applications hosted on the cloud by the hospital. It provides multiple levels of protection within the network infrastructure against data breaches, unauthorized access, or DDoS attacks (a distributed denial-of-service attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers). Thus, cloud computing security solutions typically have built-in redundancies to ensure that the applications are always available. The Content Delivery Networks used have distributed global networks of edge servers that deliver content optimally, accelerate application performances, and minimize access to the server. However, even though cloud security seems hacker or malware-proof, some threats may come from employees themselves. A data leak can be caused by unintentional, erroneous actions and often deliberate wrecking by the staff.

WORD COUNT: 350

Nicholas Catani

3. A firewall is an important part of an organization's security measures. Describe some of the functions of a firewall appliance. Where would you physically find the firewall in an organization such as SPU? Explain part of the process of setting up and installing a firewall. Suggest two reasons/scenarios where the firewall may not provide the expected security.

A firewall is a system specifically designed to prevent suspicious access from entering a private network. It can be hardware, software, or a combination of both. To function properly, a firewall must meet certain standards, be able to establish a "secure fence" around a private network, and prevent unauthorized access and various disruptions to documents or files on the user's computer.



A firewall has several functions to protect computer networks that can be clustered as follows:

Network Security Post. All traffic that enters or exits the network must go through a firewall as a security post that will conduct an inspection. Every time traffic occurs, the firewall will try to filter the traffic under the security that has been determined.

It prevents valuable information from being leaked without notice. Many firewalls are installed for File Transfer Protocol so that every data traffic is controlled. As such, it minimizes the traffic of confidential data from users to other parties.

Record User Activity. Every time a user access data, he/she goes through a firewall which then records it as documentation – log files. The firewall can access log data while providing statistics on network usage, concurrently.

Also, it prevents modification of other party data. Using the hospital example, the facility may have confidential data such as patients' records, medical research, or other secrets, that might have a negative impact if known by unauthorized parties. Hence, a firewall prevents modifications and places a hedge in between so that the data remains safe.

Firewall works by limiting personal computers to the internet. It is like a security guard in front of the house gate and identifying visitors who come while filtering intruders whose intention is to have access to confidential data. Logically, a firewall should be placed between the internet and the network. A basic configuration would be a router that connects to a wide area network (WAN), then a firewall that connects to the router, filtering all traffic before distributing it throughout the network.

There are four primary steps in installing a firewall system in a network.

Secure access to the firewall by giving administrator access to only the people who are trusted and need it. Then secure their logins with strong passwords. Also, it is possible to create users with limited privileges as well.

It is important to define network architecture after setting the access controls, by placing the resources with sensitive data deep in the network with limited inbound traffic from the internet.

Configure the firewall and set rules for "access control lists" to control the traffic in the network. It is possible to filter the data based on different rules to manage going traffic into different network zones.

Lastly, the firewall must be tested to validate that it is blocking the traffic which is intended to be filtered as per the rules configured.

As far as I am concerned, a firewall faces some shortcomings. The first I recall is that a firewall operates based on predetermined rules. It is not a problem until you realize that it can be outsmarted. Once the hacker figures out what the rules are, it is possible to circumvent them; in fact, phishing or ransomware are just a few instances of developed threats to get around a firewall. The second one is about foreseeing a threat. A firewall is unable to predict which menace is coming down the pipeline. Unfortunately, it is a reactive system, not a proactive one. If by any chance, the right rule is not in place, the firewall can't block the threat because it does not know how to defend against it.

WORD COUNT: 600

4. “I promised everyone they can work from home or while on the road", said the CIO of the Good Coffee Company. Provide a summary of the security issues and concerns of working from home or while traveling. Provide an overview of a remote access policy for the organization. Then describe some of the technology needed to securely carry out the promise.

Working remotely is convenient, but remote employees may unintentionally put the company's data and networks at risk. Remote work means an employer has less control and visibility over employees' data security. In Europe, the General Data Protection Regulation mandates that companies protect personal information and reduce the security risk of data breaches through various security measures by outlining which employees have access to corporate servers, what data they can use, and how they can use it as part of their daily tasks.

Most malware and other hacks are delivered via phishing email attacks. They often rely on topical stories to exploit people’s fears and emotions to get them to open malicious attachments or click links to spoof sites. The scams are designed to fool people into handing over login details or downloading malicious software that gives criminals access to the computer. These emails have become so sophisticated that it is increasingly difficult for employees to detect them, especially if hackers make it past the corporate email filters into their inboxes.

Even with VPNs, firewalls, and regular training, people are the biggest security risk to a corporate network – especially when it comes to passwords. Employees are stormed by passwords to remember today that they often store them in unsecured places, such as sticky notes on their monitors or digital note on their smartphones. These actions put the employer's entire network at risk. Hackers know that remote employees are laxer in their security practices outside of the office and use these methods to crack passwords to get past sophisticated security software and access corporate information.

The last concern I may recall is that when employees work remotely, they are usually using their devices to access the corporate network. Most are not given corporate laptops and other devices, which can cause vulnerabilities and security risks. Companies with good cybersecurity usually have VPNs and SSO solutions with encrypted tokens that keep everything secure, no matter the device that's accessing the corporate network. Unfortunately, people do not think to encrypt their phones or use a VPN to access the internet at home, even if they are checking their work voicemails.

A remote access policy is a written document containing the guidelines for connecting to an organization’s network from outside the office. It is one way to help secure corporate data and networks amidst the continuing popularity of remote work, and it is especially useful for large corporations with geographically dispersed users logging in from unsecured locations such as their home networks. Generally, IT management and staff are jointly responsible for ensuring policy compliance. It should cover everything, from the types of users who can be given network access from outside the office to device types that can be used when connecting to the network. Once written, employees must sign a remote access policy acceptance form. Thus, employees are made aware of the need to safeguard the network using best practices. Couple that with effective enforcement, and threats from unsafe employee behavior can be virtually eliminated.

Nicholas Catani

The first implementation I recommend for protecting remote workers is to deploy a VPN as it allows to provide secure connectivity between devices, such as computers or smartphones, and the corporate network. A VPN usually encrypts data in transit, so hackers cannot steal data as it travels across an untrusted network. Also, it provides another layer of remote working data security against misconfigured or unpatched devices since most people do not keep their devices updated. It can help the security team to monitor and filter employees' traffic for legal and security reasons.

A second implementation when assigning corporate computers to remote employees is to add a login app or lock screen triggered after a time delay can make it harder for third parties to access. Perhaps using a password manager solution to support employees storing their passwords securely while reducing the number they need to remember is a safe bet.

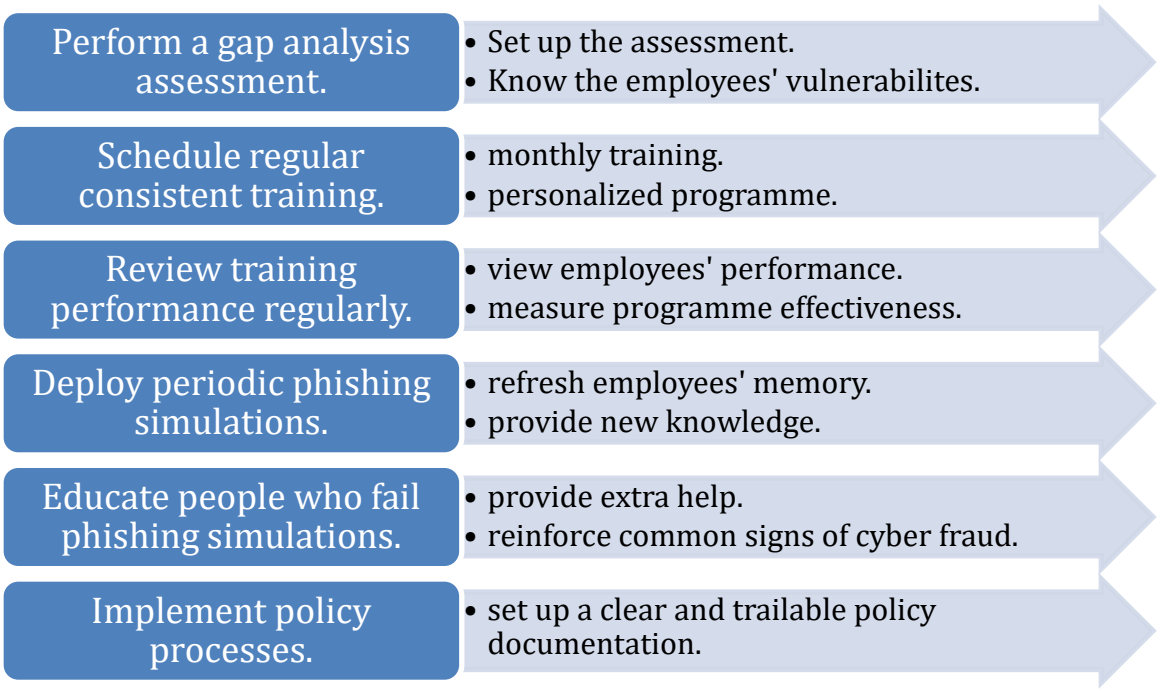
A third one is to ensure share files and data securely via file-sharing services with built-in security such as Dropbox or OneDrive. For encrypted emails, the company can use Proton Mail or Hush Mail.

Finally, I STRONGLY RECOMMEND extensively training employees on cybersecurity and how to detect any attempt of intrusion. It should be implemented for both existing and new hires to ensure that everyone is aware. Scheduling regular training and refresher courses might do the trick in keeping up-to-date employees on the latest risks.

WORD COUNT: 750

Nicholas Catani

5. The CIO of Golf Bank is interested in hiring you to create and implement a security awareness program for all 50 employees in the organization. Respond with an outline of such a program, along with a description of the process you would follow to implement the security awareness program. You will be awarded the contract based on the thoroughness, effectiveness, and creativity of your response.



It is critical to perform a gap analysis to assess potential human risk and security awareness vulnerabilities in the organization. For instance, we would like to know why employees kept falling for phishing emails, or better if no staff fell for phishing emails, how much would the company be able to save every year? Another example would be to determine the most effective and efficient way to fix things. By doing a gap assessment, the company will get an in-depth understanding of which employees are the top priority for training and which improvement areas should be considered. It is possible to identify the current state and devise a plan of action to achieve the desired future state.

I think monthly security awareness training is the most effective approach for educating all staff on new threats whilst maximizing their knowledge retention. There are hundreds of choices on the market for security awareness training software at a cheap price. However, what I would recommend is to pick the most suitable one by looking at the software that allows the company to choose and set personalized training.

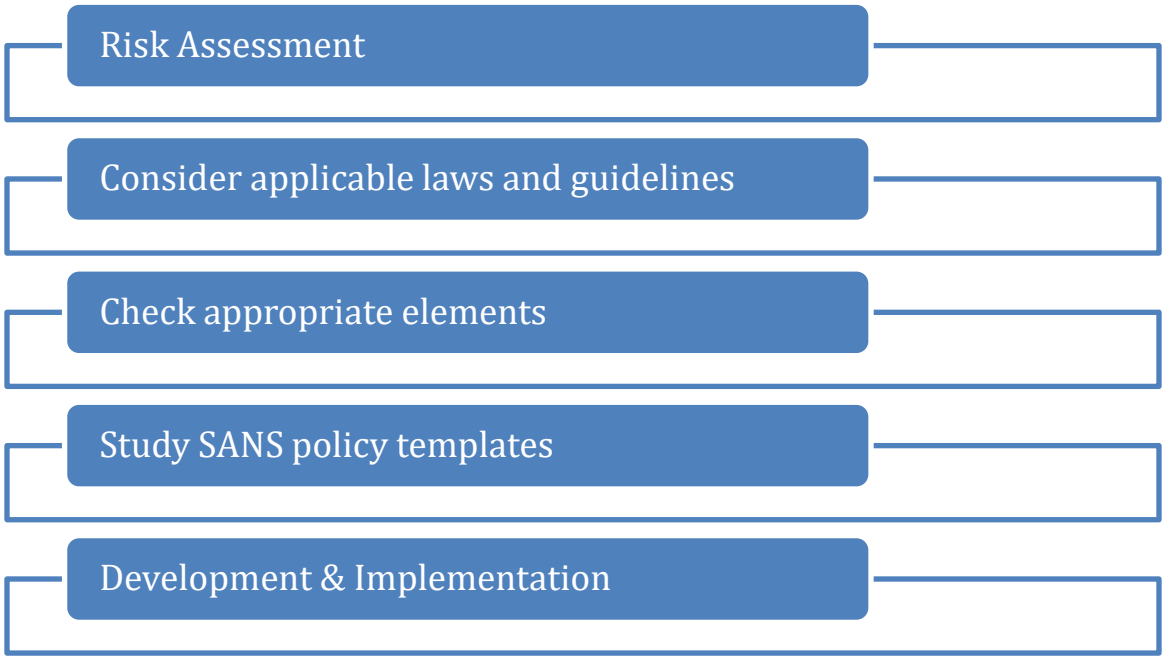
Regardless of what type or frequency of training the company is providing for its employees, it is important to regularly review their performance. It helps to understand exactly where each one of them stands and what they should do to improve. Most software on market has a set of criteria to help managers define every employee's learning effectiveness. Also, some provide short tests or assessments to evaluate employees' performance and determine where they should go next.

I think that every skill requires regular practice, otherwise, mastery is unattainable. This is especially true in today's ever-changing cybercrime landscape; one-off employee training is not enough and periodic phishing simulations should be deployed regularly. They serve as refresher courses that not only help employees sharpen their skills already learned but also enable the organization to measure the improvement the employees have made along the training journey.

Finally, rather than having managers send out different types of documentation to employees, some security programs offer a wide range of readily made policy templates, such as email policy, password policy, or encryption policy. These kinds of software with a tracking function provide managers with a clear overview of employees' progress in responding to policies. Some advanced ones allow managers to set automatic rules and send policies to specific employees at a specific time, to make sure no targeted employee is being left behind.

WORD COUNT: 450

6. The CEO of Good Tea Co. (~100 employees) is concerned because the organization doesn't have a security policy—none of the board members can remember seeing one. Put together a proposal, describing how you would go about creating a security policy for Good Tea Co. Provide a potential outline and list of some components in the resulting security policy.



I would start with a risk assessment. We go through the entire operation and identify all confidential data. It could be customer data, corporate records, financial documents, or other information that is proprietary and private. Once the check is complete, we need to create a record of all systems, devices, and technology. For instance, where and how do users access data? What are the weak points that hackers will target? And what security systems do we already have in place? Then, an evaluation of what are and are not acceptable risks. Because the policy must balance getting work done effectively and efficiently while providing the organization with an appropriate amount of protection against security threats.

The next step is to look at all local, state, and federal laws, and applicable industry standards, that covers information security. For instance, in the hospital case in the previous question, the provider should consult HIPAA standards to make sure the IT security efforts meet what is required.

Then the process of developing an actual policy can begin. Looking at several security policies, a company can tailor-made one by drawing from a list of elements that appear in standard policies as guidelines. For example: Bring your one device or (BYOD), delineates how and when employees can use their technology to conduct company business and access company information. Auditing and Policy Review underscores how and how often we monitor and review the IT security policy. Because threats are constantly changing, the policy needs to be a living document that is regularly reviewed to ensure it

stays up to date. Access Control Policy (ACP), outlines who has access to what information within the company and how it is monitored and controlled. Antivirus Software, the policy emphasizes whether or not antivirus software is required on each employee's computer and explains why or why not. Also, we might want to include additional policy components depending on our circumstances such as Monitoring, Intrusion Detection, Disaster Recovery, and Security Profiles.

I would recommend looking up other companies' security policy templates, even though is not mandatory, to learn from others' mistakes and see how other companies have approached the work.

Once we have the policy in place, it is VITAL to implement it with minimal disruption to the workflow – by keeping in mind that the policy will impact employees and their work. To achieve this result, we think that employees need to understand the reasons behind the changes. Through internal communication channels, we should address why the company needs these policies, clearly stating what is the risk without them, and their role in protecting the company and its assets. Then, write a report in an easy-to-understand language and in a way that shows how these policies impact their daily routines. Create a repository and store it safely. Finally, employees need to know where to go to find these policies when they have a question.

WORD COUNT: 491

7. You want to get **one** of the following security certifications: CISSP, CISA, CompTIA Security+, CISM, or CEH. Write a memo to your boss making the case for your organization paying for you to get this certification. Why is this the best certification for you? What can you do with it? What do you have to do to prepare for the exam? What are some of the benefits and limitations of you having this certification?

Mr. Smith

Hoping this email finds you well.
I'm reaching out because I've heard that the company makes at disposal of its employees, a certain budget for pursuing one of the many security certifications available on the market. With that in mind, I would like to use such an opportunity to advance my security skills to the next level. I've reason to believe that the CISSP is extremely valuable for an employee like me by testing my ability to manage security risks, design security architectures, and security postures and vulnerability testing. I looked up on the internet and collected some pieces of information regarding who qualifies for it, the total cost, and exam preparation. As far as I am concerned, the registration fee ranges from $699 to $749 and the candidate undergo a three-hour English exam consisting of 100 to 150 questions for the computerized adaptive testing. The certification requires a candidate to have completed either five years of full-time employment (which I'll complete next month) or four years plus an undergraduate degree in Cybersecurity.
Having said all of that, let me introduce to you some benefits and limitations that come with possessing this certificate. One of the benefits is tied to being a more competitive job candidate by granting the chance to be among the top candidates in the information security industry. Plus, it proves that I have at least four or five years of hands-on experience in the field. By obtaining the certificate, I become an (ISC)2 member and get granted access to network opportunities with more than a hundred thousand cybersecurity professionals around the world. However, once obtained, to maintain a good standing through ISC, I have to earn at least 120 credits every three years in a mixture of attending security conferences, vendor presentations, or even viewing a security webcast.

Thank you so much for your time and consideration.
Hopefully, the company will allow me to enhance my knowledge even further.

All the Best
Nicholas Catani

WORD COUNT: 328

I HAVE COMPLETED THIS EXAM ON MY OWN **NICHOLAS CATANI**