Homework 2

Q1. List three cases of cybercrimes committed by disgruntled employees. Use the web to find the cases and write a brief summary of when, where, and how they happened. (Provide complete citations of where you found the material.)

In March 2022, due to employee negligence and human error a notable amount of Pegasus Airlines sensitive data was left unprotected. Fortunately, no actual breach had occurred which would have resulted in a $183,000 due to it possibly violating Turkish Law on the Protection of Personal Data (LPPD). Because employees PII could've been exposed, and disruption of the flights system software could've possibly occurred.

7 real-life data breaches caused by insider threats | ekran system. (n.d.). https://www.ekransystem.com/en/blog/real-life-examples-insider-threat-caused-breaches

In June of 2006 a system administrator UBS PaineWebber financial firm named Roger Duronio, was charged with disruption of PaineWebber's computer network by implementation of a logic bomb. Duronio was found guilty and received an 8 year and 1 month prison sentence and was required to pay the USB $31. million in restitution.

Disgruntled UBS PaineWebber employee Chardge with allegedly unleashing "Logic bomb" on company computers. (n.d.). https://www.justice.gov/archive/criminal/cybercrime/press-releases/2002/duronioIndict.htm

In 2009, China witnessed the prosecution and sentencing of 11 individuals by the Futian Court in Shenzhen, China for violation of copyright laws. These 11 individuals were involved in a sophisticated counterfeiting operation which enabled them to manufacture and distribute Microsoft software that was pirated worldwide.

Microsoft case shows China's resolve in IPR Protection. (n.d.). https://www.chinadaily.com.cn/china/2009-01/04/content_7363400.htm#:~:text=The%20Futian%20Court%20in%20the%20southern%20city,Chinese%20criminal%20and%20copyright%20laws%20to%20make

Q2. In the context of electric (power) utilities, list three threats and corresponding vulnerabilities that they exploit through information assets. Use the web as a resource. (Provide complete citations of where you found the material.)

I. There's a greater number of threats that are targeting utilities, such as nation-states goal being disruption of the economy and security, the sector's economic value being at risk

because of cybercriminals targeting it, and utility agendas and projects being publicly opposed by hacktivists.

II. The broad attack surface of utilities increasing which is rooted in the sophistication of their geography and organization, such as various organizations cybersecurity leadership being decentralized.

III. The interconnections between the physical and cyber infrastructures in the electric-power and gas sector encounter risks of unique nature. This vulnerability allows for companies to be open to a variety of exploitations such as several wind turbines being stopped due to operational tech systems being intercepted, physical destruction, and wireless "smart meters" being utilized for billing fraud.

Bailey, T., Maruyama, A., & Wallance, D. (2020, November 3). *The energy-sector threat: How to address cybersecurity vulnerabilities*. McKinsey & Company. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities

Q3. Once again, using electric (power) utilities, list three types of risks that they face due to cybercrimes. Use the web as a resource. (Provide complete citations of where you found the material.)

I. Many issues may happen such as power outages, operational failure, etc. due to a malicious actor hacking industrial control systems.

II. Major damage may be inflicted on the power sector due to the concern that is insider threats.

III. Personal and financial data might be stolen because a phishing attack occurred.

Managing cyber risk in the Electric Power Sector. Deloitte Insights. (n.d.). https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/cyber-risk-electric-power-sector.html

Homework 03

Q1. As you are aware, electric power is vital to all aspects of all life. The 2003 Northeast blackout is an example of its criticality. Use web resources and your imagination (state the assumptions) to describe the security services dimension of a desirable IA system for a power company.

Assumptions:

- The power company has employed an IT professional team who have been trained in information assurance.
- The power company possesses the necessary tools to deploy and maintain the IA system.
- The power company is required to comply with regulations mandating certain levels of data protection.

Security services dimensions:

1. Intrusion Detection and Prevention Systems (IDPS):
    a. Maintaining surveillance on the systems and networks identifying any signs of trouble, such as suspicious activities and hacking attempts.
2. Access control Mechanisms:
    a. Ensuring that only authorized personnel are able to access critical systems by utilizing security measures like multi-factor authentication, strong password policies, and role-based access control.
3. Encryption and Data Protection:
    a. Implementing end-to-end encryption protocols to protect communication channels to ensure sensitive data is protected at rest, in transit, and during processing to prevent unauthorized data access and data breaches.
4. Incident response and recovery:
    a. Create a comprehensive incident response plan that thoroughly explains prompt detection procedures, responses, and recovery. Also, perform regular exercises and simulations to ensure preparedness and how effective the incident response plan is.
5. Continuous monitoring for foreign threats:
    a. Utilizing tools such as information sharing platforms and industry partnerships to stay updates on new cyber threats and vulnerabilities in the energy sector. Continuously monitoring system activities in real-time to detect anomalies and prevent security issues.
6. Regulatory Compliance and Record maintenance:
    a. To maintain system's security and safeguard data make sure to adhere to regulations like NERC, CIP, and GDPR. Maintain detailed records of system activities to display that rules are being complied with and aid in investigations if required to.

Q2. You have asked your system administrator to provide you with measures on organization's computer system availability and failures. The administrator reports to you that there were four failures, and that the availability was satisfactory. What is wrong with these metrics? Use the material provided in the metrics papers and slides to critique---don't simply write some English sentences that anyone else could make. Instead, provide a good analytical critique using the material provided.

- The information that was provided by the system administrator is imprecise. Instead of just stating "four failures," we require specifics on what exactly failed, these failures impact on the situation, and the duration of the repair. Also, reporting "availability was satisfactory" does not provide us with a lot of information. It would be preferable to provide a specific number for example, "Over the past month the system had an uptime of 99.9%". This new statement provides a clearer picture of the system's availability. There was no mention from the administrator of any service level agreements or system's performance goals. Without any service agreements or performance standards, it is difficult to identify if the system is operating correctly and meeting expectations.

Q3. Using the web provide a list of ten organizations that are using CVSS to classify/quantify the potential effect of vulnerabilities on their information systems.

1. National Institute of Standards and Technology (NIST)
2. Amazon
3. Security Compass
4. Cisco
5. The U.S National Vulnerability Database (NVD)
6. HP
7. The United States Department of Defense (DOD)
8. Philips Healthcare
9. The European Union Agency for Cybersecurity (ENISA)
10. RWE

Homework 4

Q1. Once again, let us look at the electric power companies. Use web resources to find an information security (or cybersecurity) policy of a utility company and list some of its key features in the context of what you have learned in this module. Make sure to provide a complete citation of the source. Your answer should not exceed a page.

Q2. Look into the security rule of HIPAA and summarize the technical safeguards that it recommends (or enforces) as part of security standards. Once again, use web resources and make sure to provide a complete citation with URL. Your answer should be limited to one page.

Q3. All educational institutions have to comply with FERPA. Use web resources to write a brief summary of the security implications of FERPA from the institution's perspective. Make sure to provide a complete citation with URL. Your answer should be limited to one page.

Homework 5

Q1. Once again, let us look at the electric power companies. Use web resources to find incident reporting requirements for cyber-attacks in this sector. Comment whether or not these are in line with what we discussed in the module. Make sure to provide a complete citation with URLs. Your answer should not exceed a page.

The North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) standards mandates that cybersecurity incidents that compromise critical infrastructure be reported. It is required that establishments report any incident within one of detection that attempts or has compromised physical or electronic security perimeters of important cyber assets. What this report should include is attack vector utilized, level of intrusion, functional impact, level of intrusion, incident's mitigation actions. Also, institutions are required to update incident reports with new information and after the incident occurs to carry out a lessons learned analysis.

These reporting requirements align with what we discussed in the module because they stress the need for timely reporting, understanding the attack's nature, and utilizing incidents to learn from and apply to responses in the future.

Cyber security – incident report - NERC. (n.d.-b). https://www.nerc.com/pa/Stand/Project 201802 Modifications to CIP008 Cyber Secur/CIP_Technical_Rationale_for_CIP-008_Final Ballot_Clean_01152019.pdf

Q2. Old Dominion University has an Information Security Officer. In addition, it has a large team responsible for IT security. From web resources, determine the roles of the IT security team and its process for security incident management. Make sure to provide a complete citation with URLs. Your answer should not exceed a page.

Roles:

- Security Policies and Procedures: Creating and implementing policies and procedures that are aimed to protect Old Dominion's IT resources. This involves protecting the university's I IT system by establishing clear policies to prevent unauthorized access and cyber threats. As well as implementing these rules across the entire university IT system to follow the best practices and comply with necessary regulations and standards.
- Risk Assessment: Detecting and analyzing possible threats and vulnerabilities that may occur in the IT systems of the university. This means actively checking for factors that could harm the security and integrity of the university's IT systems, such as cyber threats, human error, and outdated error. Also, it includes carrying out routine checks to identify any risks and then implementing the appropriate steps to repair and mitigate these risks.
- Incident Response: Addressing security incidents and recovery process management. What this entails is the identification, containment, and mitigation of security breach impact, also restoration of day-to-day operations and disruption minimization by coordination of team efforts.
- Security training and awareness: Offering programs that specialize in information security training and awareness to educate students and staff which aids in the protection of information from cyber threats. These training and awareness programs aid people in developing an understanding of dangers such as malware, data breaches, and phishing. Also, these programs educate students and staff on good habits like being careful with critical information and password protection.
- Compliance: Making sure that the university's IT systems comply with required regulations and laws. This indicates frequently making sure that the university adheres to the laws about keeping data safe and secure. Also, it involves keeping up and updating IT rules so that it adapts to any law changes, and maintaining satisfactory records to prove that the university complies with the requirements and regulations.

Security incident management process:

1. Detection and reporting: The situation is identified and reported to the IT security team.
2. Evaluation and Decision: The incident is evaluated by the IT security team, and they determine an appropriate course of action.
3. Containment and Elimination: The IT security team works toward containment of the situation and removal of the threat.
4. Recovery: The systems that were impacted by the incident are restored and operations are resumed as normal.
5. Post-incident review: A post-incident review is done to identify the key takeaways and improve the responses of future incidents.

Computing security. Old Dominion University. (2023, December 11). https://www.odu.edu/information-technology-services/security

Information Technology Services. https://www.odu.edu/information-technology-services. (2024, March 7). https://www.odu.edu/information-technology-services

Homework 7

Q1. Once again let us look at the electric power companies. The following news report underlines the importance of vulnerability management (VM) in power companies. (U.S. power plants, utilities face growing cyber vulnerabilityLinks to an external site.). Using the material presented in this module and any other web resources, write a two-page report recommending a suitable VM process. Importantly, write the report in your own words, in a cohesive manner.

Your report is addressed a power company executive and may include:

(i) What is VM?

(ii) Why does their utility need it?

(iii) Standard process to follow

(iv) Required personnel

(v) Standard tools, if any.

I assume that you are neither an IT specialist nor a power company executive. Instead, try to put the concepts and processes in the context of electric power companies after reading the material presented and the reports you have read. Make sure to provide complete citations of any references.

Homework 9

(i) One definition of survivability is: "continuing to perform in the face of various kinds of diversity." In the context of ABC, Inc., identify what performance means, and list the types of adversity it is prone to and that should be addressed by its IT team.

(ii) ABC Inc. has two officers COO and CSO. While the COO (chief operations officer) is responsible for the overall operation of ABC Inc., the CSO (chief security officer) is responsible for the security. Both report to CEO who in turn reports to the Board of Directors and the Shareholders.

From what you have learned in this module, and from commonsense knowledge, list ways in which the objactives and goals of COO and CSO have commonalities and differences.

(iii) CEO has asked COO to prepare a list of what-if situation that he is most concerned about regarding the business activities and its survivability. This list will then be passed on to the CSO and to the IT teams for explanation of how the current systems currently address them or how it could be done. Provide five key what-if scenarios that the COO should include in this list.

(iv) Identify and describe one emergent property for this system.

Homework 11

In the context of ABC Inc., which is a large on-line electronic product company, answer the following questions.

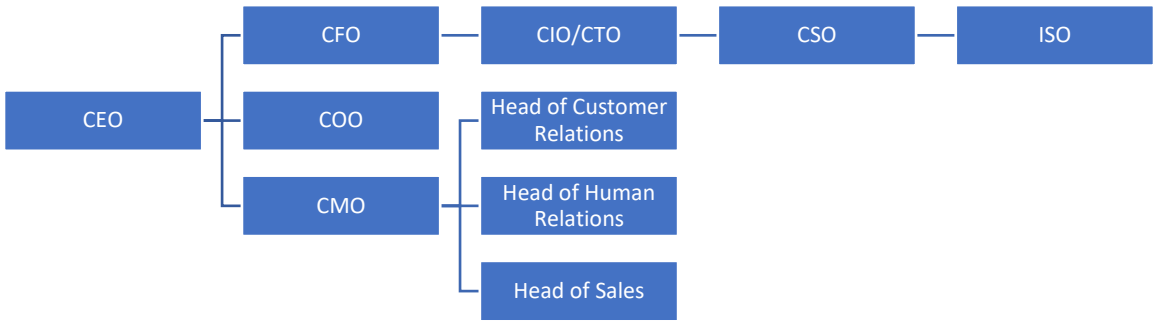
1. State three regulations and standards that it should comply with.
    1. General Data Protection Regulation (GDPR): GDPR needs to be complied with if ABC Inc. handles EU citizens personal data. What GDPR governs is how such data is obtained, stored, and processed, protecting people's privacy and security.
    2. Health Insurance Portability and Accountability Act (HIPAA): ABC Inc must follow HIPAA if the company deals with electronic protected health information (ePHI). HIPAA organizes privacy and security standards for health information, maintains the safety patient data by requiring protections.
    3. Children's Online Privacy Protection Act (COPPA): COPPA must be complied with if ABC Inc. provides online services that's targeted to children under the age of 13 and gathers

their personal data. COPPA requires obtaining parental consent and ensures the security of children's data.

2. List the responsibilities (roles) of the Information Security Officer of ABC Inc.

    1. Policy Development: Creating and implementing security policies, procedures, and guidelines that adheres to industry standards and regulatory requirements.
    2. Security Awareness Training: Training partners and employees about industry standards, security threats, and their duties in keeping a secure environment.
    3. Risk Management: Safeguarding ABC Inc's interests and assets by identifying, evaluating, and mitigating security risks.
    4. Compliance Monitoring: Supervising compliance efforts to important rules and standards, making sure that ABC Inc. meets legal and contractual requirements regarding information security.
    5. Security Incident Response: Reduces damage potential and makes sure that there is adherence with legal requirements by leading the effort to promptly detect, investigate and respond to security incidents.

3. Suggest a reporting structure (as a diagram) for ABC Inc., assuming that it has 2 million customers, 2000 employees, approximately 20000 transactions each day, and $2 billion sales. Give a brief justification.



    1.
    2.

4. Describe an incident response plan for ABC Inc. Write it as a list of steps with a brief description for each

1. Preparation:
    1. Create an Incident Response Team (IRT) with key stakeholders.
    2. Establish an incident response plan that thoroughly explains the roles, responsibilities, and communication methods.
    3. Carry out training and drills regularly so the team is prepared to handle various scenarios.
2. Detection:
    1. To promptly detect security issues, utilize strong monitoring tools.
    2. For suspicious activities put in place alerts and thresholds.
    3. Establish and maintain forensic analysis logs.
3. Containment:
    1. To protect the systems from being damaged any further it is necessary that the affected systems be isolated.
    2. Accounts and services that have been compromised need to be disabled.
    3. And for reduction of immediate risks temporary measures need to be implemented.
4. Investigation
    1. It is necessary to investigate the incident thoroughly and collect evidence.
    2. Make sure that stakeholders that are relevant to the situation whether internal or external are included.
    3. Prepare for any analysis or legal actions by preserving evidence.
5. Communication:
    1. When the incident occurs provide internal stakeholders which includes management with information about the situation.
    2. To adhere to any requirements external parties that are relevant to the incident need to be notified.
    3. Provide all parties regular updates on response and mitigation efforts.
6. Remediation:
    1. Establish a plan to repair the vulnerabilities that were found during the investigation.
    2. Securely restore systems that were affected.
    3. And for prevention similar incidents regularly update security controls.

7. Review and Lessons Learned:
    1. Figure out areas of improvement by analyzing the effectiveness of the response plan.
    2. Lessons that were learned during the investigation need to be documented to aid in future planning and training.
    3. The response plan needs to updated to adapt and address new threats.

Homework 12

In the context of ABC Inc., which is a large on-line electronic product company, answer the following questions.

1. For ABC. Inc., through an example scenario, show how IA, privacy, and individual ethics do not contradict each other.
    a. To improve the user experience on their website ABC Inc. has established a new recommendation system based on artificial intelligence. The system uses AI to provide products based upon a anonymous data they have collected. This system maintains the confidentiality, integrity, and availability of the data by encrypting it and storing it securely. This makes sure the AI-based recommendation system runs without any sensitive information being revealed. Privacy rights are violated if detailed user data is collected without user permission. This is because the users are not informed on what data is being collected and how much of it is being collected. Employees fail to meet ethical standards when they are aware of these practices but do not repair or report them. If this occurs employees are actively involved in the misuse of user data and privacy violations.
2. For ABC. Inc., through an example scenario, show how IA, privacy, and individual ethics do contradict each other.
    a. ABC Inc. decides to enhance its AI-based recommendation system. They plan to carry this out by utilizing detailed user data they have collected which includes purchase history, browsing history, and personal preferences. This user data that was collected was obtained without prior consent from the user and the information was stored without using proper encryption practices.
    b. This violates the confidentiality and proper authorization principles of Information Assurance due to the lack of user permission and adequate encryption. Even though ABC Inc. ensures the user that information that was used is kind of protected and available. A significant privacy breach occurs due to the users of ABC Inc.'s platform not being properly informed on the extent on how much of their information is being used and what exactly is it being used for. Employees fail to uphold ethical standard when they are complacent and do not report any incidents of breach of user privacy and misuse of customer data.

3. Suppose a new employee of ABC Inc., not knowing the privacy rules, reveals the purchase information of a customer to another party, without prior consent of the purchaser, who will be held responsible?
    a. The first one who is directly responsible for this breach is the new employee. This employee may face punishment or possible termination because they released this classified information without prior authorization. The second party responsible for the breach is ABC Inc. because they did not rain this new employee properly on data protection and privacy policies. Due to this malpractice, they may be dealing with legal consequences, fines, and reputation damages. The last part that is responsible is the managers/supervisors because according to how their company policy may be set up they may be responsible for training this employee and making sure this employee was properly informed on the privacy rules.
4. Do you think ABC Inc. is prone to information warfare by other countries? If so, what could be one possible scenario of its involvement?
    a. During an information warfare between other countries the information ABC Inc. holds could be targeted due to it being a massive online electronic product company that collects and stores operational and customer data that others may deem as valuable.
    b. There's a possibility that ABC Inc.'s AI algorithms, sales analytics, and customer data could be stolen by a cyber attack deployed by a foreign country. This information that was stolen could then be utilized to aid a competitor that is state-sponsored compromise ABC Inc.'s market position. Also, ABC Inc.'s reputation and financial stability is at stake due to the distrust that was created when the customer's data was stolen.
5. State two possible codes of ethics that ABC Inc. should enforce/prescribe for its employees.
    a. Data Privacy and Protection
        i. It is required that employees maintain confidentiality and security of customer and company information.
        ii. They must obtain explicit user consent before the collection, storage, or distribution of personal data.
        iii. Employees need to attend mandatory training on data protection laws and internal privacy policies regularly.
    b. Transparency and Accountability
        i. ABC Inc. is dedicated to maintaining transparent operations which means regularly updating their customers on how their information is being used and protected.
        ii. It is encouraged that any unethical behavior or practices that compromises user privacy or data security observed by employees be reported.
        iii. Accountability measures are implemented to effectively and promptly address any ethical guideline breaches.