Case study security officer

Business

Look up “ the paper that started the study of computer security.

” Prepare a summary of the key points. What in this paper specifically addresses security in areas previously unexamined? B) Consider the information stored on your personal computer. For each of the terms listed, find an example and document it: threat, threat agent, vulnerability, exposure, risk, attack, and exploit.

Question 2 ere next day at SSL found everyone in technical support busy restoring computer yester to their former state and installing new virus and worm control software. Amy found herself learning how to install desktop computer operating systems and applications as SSL made a heroic effort to recover from the attack of the previous day.

Questions: a) Do you think this event was caused by an insider or outsider? Why do you think this? B) Other than installing virus and worm control software, what can SSL do to prepare for the next incident?) Do you think this attack was the result of a virus or a Norm? Why do you think this? Chapter 2 (40)) Consider the statement: an individual threat agent, like a hacker, can be a factor in more than one threat category. If a hacker hacks into a network, copies a few files, defaces the Web page, and steals credit card numbers, how many different threat categories does this attack fall into? A. Overall, I believe this attack falls into four major threat categories: deliberate acts of trespass, compromises to intellectual property, technical failures, and managerial failure.

Furthermore, I believe this attack would be categorized as a deliberate act of heft/trespass which compromises intellectual property due to technical and managerial failures. B.

It seems as this hacker was deliberately causing harm (I. E. Copying files, vandalizing the web page, and theft of credit card numbers); due to their method of entry – hacking into a network – it leaves me to believe there were some technical failures, such as software vulnerabilities or a trap door. However, that is Just one possibility as to what could have occurred.

This could have also been a managerial failure; say the unknown hacker used social engineering to obtain the information to gain access to the network – proper planning and procedure execution could have potentially thwarted this hacker’s attack. 2.

Using the Web, research Motivators exploit TTS When and now did he compromise sites? How was nee caught? C. Michael Demon Scale, also known as Mafioso, was a high school student from West Island, Quebec, who launched a series of highly publicized Dos (denial-of-service) attacks in February 2000 against large commercial websites including: Yahoo! Fife. Com, Amazon. Com, Dell, Inc.

, E*Trade, Ebay, and CNN. Scale also attempted to launch a series of simultaneous attacks against nine of the thirteen root name servers. D. On February 7th, 2000, Scale targeted Yahoo! With a project he named ‘ Ravioli” -.

.. B) The chapter discussed many threats and vulnerabilities to information security. Using the Web, find at least two other sources of information on threat and ‘ limitlessness. Begin with www. Security’s.

Com and use a keyword search on ‘ threats. ” Soon after the board of directors meeting, Charlie was promoted to Chief Information

Security Officer, a new position that reports to the CIO, Gladys Williams, and that was created to provide leadership for Sol’s efforts to improve its security profile. A) How do Fred, Gladys, and Charlie perceive the scope and scale of the new information security effort? B) How will Fred measure success when he evaluates Gladys’ performance for this project? How will he evaluate Charlie’s performance? C) Inch of the threats discussed in this chapter should receive Charlie’s attention early in his planning process?