CASE STUDY SET 3

VIKRAMADITYA REDDY VARKALA

Z1973679

**CASE STUDY 6:FBI New Haven Field Office-CART**

**Q1)What should the Connecticut company have done to prevent the computer intrusion described in this case? What should it have done to detect this computer intrusion?**

The vulnerability existed in BoatingCT.com's shopping cart software.The GET command allowed users to open the order.log file (home/boatingct/cgi-bin/Web\_store/Admin\_files/ order.log) and copy the file from BoatingCT.com's machine to their own machines.Intruders from around the world had gained unauthorized access to BoatingCT.com's daily order file, and to its customer order and credit card information.

The company should have upgraded its shopping cart software to the latest version of WebStore (version 2.0) in order to prevent intrusion, which was immune to this vulnerability. This patch had been available since October 2000, six months before the company's customers began to receive the suspicious e-mail confirmation messages requesting their credit card verification numbers and bank account information.

To detect this computer intrusion the company should have followed a few simple measures like:

* Input validation:checks if input data is acceptable or not.If a user wants to enter an email address in the web form , he / she should not be allowed to enter any data unless it is in expected form .
* access control list (ACL): restricts file access to authorized users and ensures that users cannot access files outside of their permissions.
* web application firewall (WAF).
* Keeping software up-to-date.

**Q2)What security controls should be implemented by any organization to prevent, detect, and recover from a computer intrusion?**

To prevent, detect, and recover from a computer intrusion organizations should :

* Educate their employees about the risks of computer intrusion and how to identify and report suspicious activity.
* Test their systems regularly for vulnerabilities and weaknesses that could be exploited by attackers. Vulnerability assessments and penetration testing helps to identify potential weaknesses before they are exploited.
* Implement encryption for data at rest and in transit to ensure that sensitive data is protected from unauthorized access.
* Regularly back up their critical data and systems and implement a disaster recovery plan to ensure that systems can be restored in the event of an intrusion or other catastrophic event.
* Implement security monitoring tools and techniques to detect and respond to potential threats.
* Develop an incident response plan to ensure that they can respond quickly and effectively in the event of a security breach.
* Implement anti-virus and anti-malware software to protect against malicious software that can compromise systems and steal sensitive information.
* Implement access controls to ensure that only authorized individuals have access to sensitive information and systems.
* Implement firewalls, intrusion detection and prevention systems, and other network security measures to protect against external threats.

**Q3)Why would someone want to use a forged e-mail address? Explain how this worked to the intruder's advantage in this case.**

Forged email address can be advantageous for an intruder in several ways:

* Intruder can send an email that appears to come from a trusted source, such as a bank or a popular websites, in an attempt to trick the recipient into giving out sensitive information, sending money or clicking on a malicious link.
* It can be used for spamming or mass-mailing, where the intruder wants to send a large volume of unsolicited email without being traced back to their actual address.
* By using a forged email address, the attacker can avoid detection and potentially continue their activities for a longer period of time.
* By forging email addresses intruder can bypass spam filters and other email security measures. Many email providers use authentication protocols such as SPF, DKIM, and DMARC to verify the authenticity of incoming emails.
* Forged emails can also be used for distributing malware, where the attacker sends an email containing an attachment or a link that, when clicked, infects the recipient's computer with malware.

**Q6)When the FBI New Haven field office requested the log files from the University of Akron, none were available. Do you think it is typical for universities not to retain log files? What is the impact of this on the security of university computing environments?**

It is not typical for universities to not retain log files especially in the context of cyber security ,as log files are an important tool for monitoring and maintaining the security of computing environments.This information can also be critical in identifying and investigating security incidents and can help organizations take steps to prevent future incidents.It is important for universities to establish policies and procedures for log retention and to ensure that these policies are followed consistently across all systems and networks.

The impact of not retaining log files on the security of university computing environments can be significant.Without log files,

* It will be difficult or impossible to detect unauthorized access or suspicious activity on the network.
* It is Difficult to determine the cause or extent of the breach.
* Universities may be unable to comply with regulatory requirements for data retention and security.

**Q7)The FBI New Haven CART field examiners imaged the hard drive and worked off of that. They did not use the original drive or the original evidence. Why?**

FBI New Haven CART field examiners did not use the original drive or the original evidence because originally The computer had two hard drives. The master drive and the imaged drive.The master drive, which had been partially destroyed, was sent to an outside vendor for data recovery but the vendor's efforts were unsuccessful.

So the FBI New Haven CART field examiners imaged the slave drive and used ILook to analyze its contents.Among the tests that were conducted using ILook was acsearch for the keywords "boatingct" and "boatinget.com", which was conducted on the free space and the slack space of the imaged hard drive. Data related to the intrusion at BoatingCT.com were recovered from the free space on the imaged hard drive.

**Q10) What types of Internet-related crimes should be reported to the FBI? At what point should a computer crime be reported to law enforcement?**

Types of internet-related crimes that should be reported to the FBI are:

* Cyber terrorism
* Internet fraud
* Computer intrusion
* Identity theft
* Internet extortion
* Cyberstalking
* Malware and ransomware attacks
* Phishing and spear-phishing scams
* Cyberbullying and harassment
* Money laundering or other financial crimes conducted online

These types of crimes or any other serious computer crime that involves theft, fraud, or threats of violence. one should report it to law enforcement as soon as possible. The longer you wait, the harder it can be to gather evidence and track down the perpetrator. If you're not sure whether a particular incident should be reported, it's a good idea to contact law enforcement anyway. They can help you determine whether the incident rises to the level of a crime and what steps you can take to protect yourself.

**CASE STUDY 7:AETNA**

**Q1). Many organizations have tried, but have not been able, to implement a successful information security awareness program. How was Aetna able to succeed with its program?**

Aetna succeeded in establishing a cost-effective program that measurably improves its users security behaviors where as Many other organizations have tried, but have not been able, to implement a successful information security awareness program because Its security awareness program is based on realistic goals, ties security with the business environment, reflects the corporate culture, uses multiple delivery mechanisms to reinforce the security message, ensures that all users are exposed to information security training provides the ability to measure the knowledge being transferred, and receives continued support from senior-level managers and executives.

**Q2)Most companies tend not TO fund security awareness programs during financially difficult times. When Aetna implemented its first InfoSec exam in 1999, the company's stock price was $99.87 per share. By February 2000, Aetna's stock price had fallen to $40.75. Despite rising costs and declining profits, the company continued to support its internal security awareness program. What reasons might Aetna have had for doing this?**

Aetna continued to support its internal security awareness program despite rising costs and declining profits because :

* The InfoSec exam is updated annually to incorporate security topics that are relevant to Aetna's environment.
* Each exam builds on the strengths of the previous exam and attempts to correct obvious weaknesses
* The 2000 InfoSec exam focused on confidentiality. The 2001 and 2002 InfoSec exams emphasized different aspects of the Health Insurance Portability and Accountability Act (HIPAA). The 2003 and 2004 InfoSec exams were integrated within the company's Business Conduct and Integrity training program and they addressed various facets of information security.
* In addition to the exams redesign, improvements were made in the way it was targeted to employees.
* Improvements were also made in the way it was targeted to employees. Role-based exams were introduced, enabling the security topics to be focused more directly toward different groups of users.

**Q4)Most of the eight to ten users who are selected for usability testing have an entry-level understanding of computers and tend to be uncomfortable with Web-based applications. Why aren't more experienced users chosen for testing?**

The users who aren’t experienced are chosen for testing because:

* The purpose of usability testing is to ensure that the content of each module is acceptable to the users and the exam is easy to navigate.
* The ISPP group selects users to participate in the testing drawn from variety of work groups at the same location.
* The users are chosen on the basis of their willingness to participate and the level of their technological capability.
* Most of the eight to ten users who are selected have an entry-level understanding of computers and tend to be uncomfortable with Web-based applications.
* so,Entry-level users who have limited experience with technology, since they are more likely to encounter the same problems and challenges that the actual users would face.

**Q5)Research at least five security awareness solution providers. Summarize their similarities and differences.**

* **MediaPRO**: MediaPRO provides a security awareness training program that includes customizable modules, interactive quizzes, and analytics to measure the effectiveness of the training. This program is available in multiple languages to support global organizations. mediaPRO also offers a range of compliance solutions to help organizations comply with various regulations related to data privacy and security.
* **CybeReady**: CybeReady founded in 2015, provides a security awareness training program that uses AI and machine learning to personalize the training experience for each employee. Their platform includes interactive modules, simulated phishing attacks, and analytics to measure the effectiveness of the training.
* **Mimecast**: Mimecast founded in 2003, provides a security awareness training program that includes interactive modules, phishing simulations, and assessments to measure the effectiveness of the training. Their program is customizable to meet the specific needs of an organization.
* **KnowBe4**: KnowBe4 is a security awareness solution provider that offers a comprehensive training program that includes phishing simulations, interactive modules, and assessments. This platform also includes a range of reporting and analytics features to help organizations measure the effectiveness of the training.
* **Cofense**: Cofense(previously PhishMe founded in 2011, is a provider of security awareness training that offers an immersive training experience, gamification elements, and real-world simulations to educate employees on how to detect and avoid phishing attacks. Their platform includes a range of reporting and analytics features to help organizations measure the effectiveness of the training.

**Similarities:**

Above mentioned security awareness solution providers mentioned above offer comprehensive security awareness training programs to help organizations educate their employees about cyber threats and build a security-conscious culture.

They use customized training modules, interactive simulations, and assessments to measure the effectiveness of the training. Some provide training experiences using AI and machine learning technology and using real world simulations.

They all offer reporting and analytics features to measure the effectiveness of the training.

**Differences:**

The differences among the providers mainly lie in their unique approach to training and the features they offer, but they all share a common goal of improving an organization's security by educating its employees.

* Cofence provides offer gamification elements to make the training more engaging and interactive to the users.
* MediaPRO and KnowBe4 offers their training programs in multiple languages.
* CybeReady uses AI and machine learning to provide personalized training experience for employees.
* Mimecast utilizes assessments as part of their training program.

**Q6)Why is it important for a company officers to be able to demonstrate due care? How is due care related to negligence?**

* Due care refers to taking reasonable steps to secure and protect your company's assets, reputation, and finances
* Negligence refers to failure to exercise due care. In legal terms, negligence occurs when someone breaches their duty of care, resulting in harm or loss to others.
* If a company officer fails to exercise due care, and this leads to harm or loss to the company or its stakeholders, they may be found liable for negligence so It is important for company officers to demonstrate due care because it shows that they are taking reasonable steps to protect their organization's assets and stakeholders from harm, as well as avoid legal and financial losses.
* Therefore Demonstrating due care is therefore necessary to prevent negligence claims against company officers which involves taking reasonable steps to avoid harm or loss, such as doing proper research before implementing appropriate risk management strategies, and ensuring compliance with laws and regulations.

**Q9)What factors should be considered in the development of any information security awareness program?**

A successful information security awareness program requires careful planning, ongoing monitoring, and continuous improvement to ensure that it meets the organization's needs and objectives.The following factors should be considered during the development of the program:

* Identify the potential security threats, vulnerabilities, and risks that the organization faces. This can help prioritize the awareness program's focus and content.
* Have clear objectives for the awareness program that align with the organization's overall goals and strategies.
* Compliance with legal and regulatory requirements can help mitigate risks, reduce potential losses.
* Provide training and education programs that are interactive, practical, and hands-on.
* Establish metrics and evaluation methods to measure the program's effectiveness and impact.
* Develop a communication strategy that ensures the program's messages reach the target audience effectively.

**Q10)It is often difficult to cost-justify an information security awareness program. What quantitative and qualitative factors should be considered when justifying the program's expense?**

It is important to consider both quantitative and qualitative factors when justifying the expense of an information security awareness program

**Quantitative factors:**

* The larger the organization the bigger the size of employees and higher the potential risk. hence, more cost to implement a security awareness program.
* The cost and resources required to train employees.
* The cost of data loss during a security breach.
* Cost of non-compliance with regulations.
* Potential cost savings from reduced IT support costs.
* Reduced premiums for organizations that have well executed comprehensive security awareness program.
* Return of investment of a security awareness program by comparing the program costs to potential cost savings and benefits.

**Qualitative factors:**

* A thought out and well executed security awareness awareness program will make employees more aware of security risks and how to handle them.
* The potential damage to the organization's if a security breach were to occurs.A security awareness program increases the customer trust.
* Implementing culture of security among the employees through security awareness program.
* Security Awareness program can help prevent security incidents and increase productivity.
* These programs reduces human risk which can be a leading cause for data breaches and hence can avoid it.
* Organizations can reduce legal actions incase of data breaches or customer information leakage through proper security regulations.
* Increased business for organizations from customers that has strong security practices.