**IT Security and Risk Management**

**April 2024 Examination**

**1. Malware is intrusive software that is designed to damage and destroy computers and computer systems. Malware is a contraction for “malicious software.” Explain the various types of malware and how is ransomware different from a virus/worm? (10 Marks)**

**Ans 1.**

**Introduction**

Malware, short for malicious software, constitutes a pervasive threat to the integrity and security of computer systems. It encompasses a wide array of intrusive software designed with malicious intent, ranging from viruses and worms to more sophisticated forms like ransomware. Understanding the distinct types of malware is crucial in devising effective strategies for IT security and risk management.

The proliferation of It is only half solved

Buy Complete from our online store

<https://nmimsassignment.com/online-buy-2/>

NMIMS Fully solved assignment available for**session APRIL 2024,**

your**last date is 28th MARCH 2024**.

Lowest price guarantee with quality.

Charges**INR 299 only per assignment.**For more information you can get via mail or Whats app also

Mail id is aapkieducation@gmail.com

Our website [www.aapkieducation.com](http://www.aapkieducation.com/)

After mail, we will reply you instant or maximum

1 hour.

Otherwise you can also contact on our

whatsapp no 8791490301.

Contact no is +91 87-55555-879

**2. The estimated losses due to elder financial abuse range widely, the FBI’s Internet Crime Complaint Center (IC3) 2018 Internet Crime Report shows that people 60 and older submitted more than 62,000 fraud complaints in 2018 with losses totaling nearly $650 million. Some less conservative sources estimate that fraud against seniors, or what’s known as elder financial exploitation (EFE), costs families in the U.S. upwards of $36 billion per year. Research shows that as seniors age, they’re more likely to sustain higher average losses to senior financial scams.**

**Explain the most common types of attacks targeting senior citizens and suggest precautionary measures for them with reference to these attacks? (10 Marks)**

**Ans 2.**

**Introduction:**

Elder financial abuse (EFE) has become a pervasive issue with severe consequences, as evident from the FBI's Internet Crime Complaint Center (IC3) 2018 report, which documented over 62,000 fraud complaints from individuals aged 60 and older, resulting in losses nearing $650 million. The

**3. Case Study: The Equifax Data Breach**

**In 2017, Equifax, one of the three largest credit reporting agencies in the United States, experienced one of the most significant and widely publicized data breaches in recent history. The breach was a massive security incident that compromised the personal and financial information of nearly 147 million individuals. The breach's consequences were far-reaching and included legal and regulatory repercussions, substantial financial losses, damage to Equifax's reputation, and heightened scrutiny of data security practices within the financial industry.**

**Incident Timeline and Impact:**

**i. Undetected Intrusion: The breach began in May 2017 when cybercriminals exploited a vulnerability in Equifax's web application software. They gained unauthorized access to Equifax's systems and started exfiltrating sensitive data. This intrusion went unnoticed for over two months.**

**ii. Scope of Data Compromised: The attackers gained access to a vast amount of sensitive information, including Social Security numbers, dates of birth, credit card details, and other personally identifiable information. The sheer scale of the breach made it one of the most substantial breaches of personal data to date.**

**iii. Delayed Detection and Response: Equifax only discovered the breach in late July 2017, more than two months after the initial intrusion. This delay allowed cybercriminals to continue siphoning off data and led to severe damage to the company's reputation.**

**iv. Public Outcry and Legal Repercussions: The breach triggered a public outcry, legal investigations, and a congressional hearing. Equifax faced multiple lawsuits, regulatory fines, and increased oversight from government agencies.**

**Part a) Discuss the importance of incident response planning, timely notification to affected individuals, and communication with regulatory authorities. What were the shortcomings in Equifax's response to the breach, and what lessons can other organizations learn from this incident? (5 Marks)**

**Ans 3a.**

**Introduction:**

The Equifax data breach of 2017 stands as a stark reminder of the severe consequences a data breach can have on an organization and its stakeholders. With nearly 147 million individuals affected, the incident highlighted the critical importance of incident response planning, timely notification, and effective communication with regulatory authorities in managing such crises.

**Concept and Solution:**

Importance of Incident Response Planning: Incident response planning is fundamental for organizations to

**b) Highlight best practices in vulnerability management, data protection, and cybersecurity governance. How can organizations proactively defend against cyber threats and secure sensitive customer information? Use the Equifax incident as a cautionary example to illustrate the importance of these measures. (5 Marks)**

**Ans 3b.**

**Introduction:**

The Equifax data breach of 2017 serves as a stark reminder of the imperative need for robust practices in vulnerability management, data protection, and cybersecurity governance. Understanding and implementing best practices in these areas are critical for organizations to proactively