**IT Security and Risk Management**

**Jun 2025 Examination**

**PLEASE NOTE: This assignment is application based, you have to apply what you have learnt in this subject into real life scenario. You will find most of the information through internet search and the remaining from your common sense. None of the answers appear directly in the textbook chapters but are based on the content in the chapter**

**Q1 Discuss different types of security threats and explain how organizations can mitigate these threats using appropriate countermeasures. Provide real-world examples to support your answer. (10 Marks)**

**Ans 1.**

**Introduction**

In today's digitally driven world, organizations face a multitude of IT security threats that can disrupt operations, compromise sensitive data, and damage reputations. As businesses increasingly rely on interconnected networks, cloud computing, and digital platforms, cyber threats have become more complex and frequent. These threats are not limited to external hackers but can also arise from internal sources, human errors, or system vulnerabilities. Failure to address these security issues can lead to financial losses, regulatory penalties, and loss of customer trust. Hence, understanding the different types of threats and implementing effective risk management strategies has become a critical need for organizations. This answer explores major categories of IT security threats and the countermeasures companies can adopt,

Its Half solved only

Buy Complete assignment from us

**Price – 290/ assignment**

**NMIMS University Complete SolvedAssignments session JUNE 2025**

buy cheap assignment help online from us easily

we are here to help you with the best and cheap help

**Contact No – 8791514139 (WhatsApp)**

**OR**

**Mail us-** **bestassignment247@gmail.com**

**Our website -** [**www.assignmentsupport.in**](http://www.assignmentsupport.in)

**Q2 Analyze how ethical hacking differs from malicious hacking in terms of intent, methodology, and impact. Evaluate the ethical and legal considerations in conducting penetration testing on corporate networks. Provide real-world examples to support your answer. (10 Marks)**

**Ans 2.**

**Introduction**

In the digital age, cybersecurity has become a critical component of organizational resilience. As cyber threats continue to grow in sophistication, companies have increasingly turned to ethical hackers to proactively identify and fix security vulnerabilities. Ethical hacking, also known as penetration testing or white-hat hacking, is conducted with permission and clear intent to improve system defenses. In contrast, malicious hacking, or black-hat hacking, is unauthorized and aims to exploit or damage systems for personal or political gain. While both use similar technical methods, the key distinction lies in the intent and impact of their actions. This answer explores the differences between ethical and malicious hacking, followed by an evaluation of the ethical and legal aspects of penetration testing on corporate networks,

**Q3A. A multinational company has developed a comprehensive security policy to safeguard its information assets. However, some employees frequently bypass security controls, such as using weak passwords and sharing login credentials.**

**A) Assess the importance of Security Policy Guidelines in ensuring compliance among employees. Provide recommendations for enforcing adherence. (5 Marks)**

**Ans 3a.**

**Introduction**

Security policy guidelines are a foundational part of an organization’s overall information security framework. They define acceptable behavior, outline access control procedures, and set clear expectations for all employees. Despite having comprehensive policies in place, many organizations face non-compliance due to lack of awareness or disregard for rules. This behavior can lead to vulnerabilities and data breaches. Therefore, ensuring that employees not only understand but also follow these guidelines is critical for maintaining the confidentiality,

**Q3B. A multinational company has developed a comprehensive security policy to safeguard its information assets. However, some employees frequently bypass security controls, such as using weak passwords and sharing login credentials.**

**B) Discuss the role of security awareness training in changing employee behavior and reducing policy violations. (5 Marks)**

**Ans 3b.**

**Introduction**

Security awareness training is a strategic initiative designed to educate employees about cybersecurity risks and best practices. Human error is one of the leading causes of data breaches, and even the most secure systems can be compromised by negligent user behavior. Employees who are not aware of the implications of weak passwords, phishing emails, or data sharing are more likely to violate security policies. Therefore, awareness training is a crucial