**IT Security and Risk Management**

**NMIMS Centre for Distance and Online Education (NCDOE)**

**Internal Assignment Applicable for June 2025 Examination**

**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.**

**Answer:**

**Introduction:**

In today’s digital world, businesses rely heavily on technology to operate, store data, and communicate. While this has led to greater efficiency and innovation, it has also opened the door to various security threats. These threats come in many forms, ranging from cyberattacks and data breaches to internal sabotage and social engineering. A security threat is any potential danger that can exploit a vulnerability to harm a computer system or network. These threats can result in loss of sensitive data, financial damage, legal consequences, and loss of customer trust. Therefore, understanding the different types of security threats and how to protect against them is essential for every organization.

As technology advances, so do the techniques used by attackers. Hackers and cybercriminals constantly look for ways to bypass security systems to steal information, disrupt services, or gain unauthorized access to systems. At the same time, employees may unintentionally create risks through careless behavior or lack of awareness. Hence, it is important not only to use advanced security tools but also to educate staff and establish strong policies. In this answer, we will look at major types of security threats, provide real-world examples, and explain how organizations can use effective countermeasures to defend themselves.

**Concepts and Application:**

**NMIMS June 2025 Assignments Available!**

✅ **Generic/Sample Solutions - Only ₹150 per subject**

**These are sample solutions where you will have to change approximately 30–40% of the content to make it your own.**

**✅ Unique/Customized Solutions – Only ₹500 per subject**

**Ready-to-upload assignments are 100% original and prepared to be submitted directly.**

**Email (Inquiries and Orders): smu.assignment@gmail.com**

**WhatsApp / Call (Seeking immediate help): +919741410271**

**Our website:** [**www.mbaassignmentsolutions.com**](www.mbaassignmentsolutions.com)

**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.**

**Answer:**

**Introduction:**

In a world where cyber threats are increasing every day, both ethical and malicious hackers play very different roles. While both may use similar techniques to access computer systems or networks, their intentions and outcomes are completely different. Ethical hacking, also known as white-hat hacking, is performed by cybersecurity professionals who are hired to find and fix security flaws in systems. Their goal is to improve security and protect sensitive data. On the other hand, malicious hacking, or black-hat hacking, is carried out with the intention of stealing information, damaging systems, or causing financial and reputational harm.

As businesses become more dependent on technology, they often hire ethical hackers to conduct penetration testing. This means simulating cyberattacks to check how strong their security is and to fix weaknesses before real hackers can exploit them. Ethical hacking has become an important part of cybersecurity strategies, especially in industries like banking, healthcare, and e-commerce, where data protection is critical.

In this answer, we will explain how ethical hacking differs from malicious hacking based on intent, methods, and results. We will also evaluate the ethical and legal concerns related to penetration testing and support the explanation with real-world examples.

**Concepts and Application:**

**NMIMS June 2025 Assignments Available!**

✅ **Generic/Sample Solutions - Only ₹150 per subject**

**These are sample solutions where you will have to change approximately 30–40% of the content to make it your own.**

**✅ Unique/Customized Solutions – Only ₹500 per subject**

**Ready-to-upload assignments are 100% original and prepared to be submitted directly.**

**Email (Inquiries and Orders): smu.assignment@gmail.com**

**WhatsApp / Call (Seeking immediate help): +919741410271**

**Our website:** [**www.mbaassignmentsolutions.com**](www.mbaassignmentsolutions.com)

**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.**

**Answer:**

**Introduction:**

A security policy is a formal set of rules that guide how an organization protects its information systems and data. For multinational companies, these policies are essential because they handle vast amounts of sensitive data across various locations. However, even with strong policies in place, the behavior of employees plays a crucial role in ensuring overall security. When employees ignore or bypass these rules—like using weak passwords or sharing credentials—it exposes the company to serious risks such as data breaches, financial loss, and reputational damage. Therefore, security policy guidelines must be both well-communicated and strictly enforced to ensure compliance.

**Concepts and Application:**

**NMIMS June 2025 Assignments Available!**

✅ **Generic/Sample Solutions - Only ₹150 per subject**

**These are sample solutions where you will have to change approximately 30–40% of the content to make it your own.**

**✅ Unique/Customized Solutions – Only ₹500 per subject**

**Ready-to-upload assignments are 100% original and prepared to be submitted directly.**

**Email (Inquiries and Orders): smu.assignment@gmail.com**

**WhatsApp / Call (Seeking immediate help): +919741410271**

**Our website:** [**www.mbaassignmentsolutions.com**](www.mbaassignmentsolutions.com)

**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.**

**Answer:**

**Introduction:**

Security awareness training is a critical component of a company’s strategy to safeguard its information assets. It helps employees understand the importance of security policies and the potential risks posed by ignoring them. Despite having a strong security policy, a company’s success in protecting its assets largely depends on employee behavior. Employees are often the weakest link in security because of lack of awareness or convenience-driven decisions. Security awareness training aims to change risky behaviors, such as using weak passwords or sharing login credentials, by educating employees on security best practices and their significance in maintaining a secure work environment.

**Concepts and Application:**

**NMIMS June 2025 Assignments Available!**

✅ **Generic/Sample Solutions - Only ₹150 per subject**

**These are sample solutions where you will have to change approximately 30–40% of the content to make it your own.**

**✅ Unique/Customized Solutions – Only ₹500 per subject**

**Ready-to-upload assignments are 100% original and prepared to be submitted directly.**

**Email (Inquiries and Orders): smu.assignment@gmail.com**

**WhatsApp / Call (Seeking immediate help): +919741410271**

**Our website:** [**www.mbaassignmentsolutions.com**](www.mbaassignmentsolutions.com)