**Cyber Security Quick Revision**

**UNIT 1: INTRODUCTION TO CYBER SECURITY**

**General Cyber Security Concepts**

1. **What is cyber security, and why is it important?**  
   **Solution:** Cyber security is the practice of protecting systems, networks, and data from cyber threats. It is crucial to safeguard sensitive information, maintain privacy, and ensure business continuity.
2. **Define the CIA triad in cybersecurity.**  
   **Solution:** The CIA triad consists of Confidentiality (protecting data from unauthorized access), Integrity (ensuring data accuracy and reliability), and Availability (ensuring authorized users have access when needed).
3. **How does risk management play a role in cyber security?**  
   **Solution:** Risk management involves identifying, assessing, and mitigating risks to protect systems and data from potential cyber threats.
4. **What are the key differences between cyber security and information security?**  
   **Solution:** Cyber security focuses on protecting digital assets and networks, while information security encompasses the protection of all forms of information, including physical and digital data.
5. **Explain the role of cryptography in cyber security.**  
   **Solution:** Cryptography secures communication and data through encryption, ensuring confidentiality, integrity, and authentication of information.

**Internet Governance – Challenges and Constraints**

1. **What is internet governance, and why is it necessary?**  
   **Solution:** Internet governance refers to the rules, policies, and standards governing the internet’s development and use, ensuring security, privacy, and accessibility.
2. **What are some key challenges in internet governance?**  
   **Solution:** Challenges include jurisdictional conflicts, privacy concerns, cybercrime enforcement, and balancing regulation with innovation.
3. **How do different governments regulate cyber security policies?**  
   **Solution:** Governments implement laws and regulations like GDPR, CCPA, and cybersecurity frameworks (NIST, ISO 27001) to safeguard national and organizational cybersecurity.
4. **Discuss the role of international organizations in internet governance.**  
   **Solution:** Organizations like the UN, ITU, and ICANN help create policies, set standards, and foster international cooperation on cyber security.
5. **Why is achieving a global consensus on cyber regulations challenging?**  
   **Solution:** Differences in national laws, varying enforcement priorities, and geopolitical tensions make global cybersecurity standardization difficult.

**Cyber Threats: Warfare, Crime, Terrorism, and Espionage**

1. **Define cyber warfare and provide an example.**  
   **Solution:** Cyber warfare involves nation-state attacks on another country’s infrastructure, such as the Stuxnet attack on Iran’s nuclear program.
2. **How does cyber crime impact businesses and individuals?**  
   **Solution:** Cyber crime leads to financial loss, identity theft, reputational damage, and operational disruptions.
3. **Differentiate between cyber terrorism and cyber espionage.**  
   **Solution:** Cyber terrorism aims to create fear and disrupt critical infrastructure, while cyber espionage involves unauthorized access to confidential data for intelligence purposes.
4. **What are some common tactics used in cyber espionage?**  
   **Solution:** Methods include phishing, social engineering, malware deployment, and network infiltration.
5. **How can nation-states defend against cyber warfare?**  
   **Solution:** By implementing cyber defense strategies, intelligence-sharing, critical infrastructure protection, and international cooperation.

**Need for a Nodal Authority and International Conventions**

1. **Why is a centralized nodal authority necessary for cyber security?**  
   **Solution:** It ensures coordinated responses to cyber threats, policy enforcement, and national cyber resilience.
2. **What are the responsibilities of a national cyber security agency?**  
   **Solution:** Monitoring cyber threats, enforcing regulations, incident response coordination, and cyber awareness programs.
3. **Why do we need an international convention on cyberspace?**  
   **Solution:** To establish global norms, facilitate cooperation, and combat cybercrime effectively across borders.
4. **How can international cooperation improve cyber security enforcement?**  
   **Solution:** By information sharing, coordinated investigations, and aligning regulatory frameworks.
5. **What are the challenges in forming an international cyber security agreement?**  
   **Solution:** Differing national interests, lack of trust, and enforcement challenges.

**UNIT 2: CYBER SECURITY VULNERABILITIES**

**General Overview of Cyber Vulnerabilities**

1. **What are the main types of cyber security vulnerabilities?**  
   **Solution:** Software flaws, weak authentication, misconfigurations, insider threats, and social engineering attacks.
2. **How does outdated software contribute to cyber risks?**  
   **Solution:** It contains unpatched vulnerabilities that attackers can exploit.
3. **Explain the impact of human error on cyber security.**  
   **Solution:** Mistakes like weak passwords, misconfigurations, and falling for phishing scams can compromise security.
4. **How do supply chain vulnerabilities affect organizations?**  
   **Solution:** Attackers can exploit third-party vendors with weaker security to infiltrate the main organization.
5. **What are the risks of not patching security vulnerabilities?**  
   **Solution:** Unpatched systems remain exposed to known exploits and cyberattacks.

**Software Vulnerabilities**

1. **What are the most common software vulnerabilities?**  
   **Solution:** Buffer overflow, SQL injection, cross-site scripting, and remote code execution.
2. **How does buffer overflow create a security risk?**  
   **Solution:** It allows attackers to overwrite memory and execute malicious code.
3. **What is SQL injection, and how can it be prevented?**  
   **Solution:** A technique where attackers manipulate SQL queries; prevent it using prepared statements and input validation.
4. **Discuss the security risks associated with zero-day exploits.**  
   **Solution:** They target unknown vulnerabilities before patches are available, making them highly dangerous.
5. **How can organizations minimize software vulnerabilities?**  
   **Solution:** Regular updates, secure coding practices, and vulnerability scanning.

**System Administration Vulnerabilities**

1. **What are the biggest cyber security risks in system administration?**  
   **Solution:** Poor patch management, default credentials, and lack of access controls.
2. **How does misconfiguration lead to security vulnerabilities?**  
   **Solution:** It exposes systems to unauthorized access and exploitation.

**Cyber Security Safeguards**

1. **What are the best practices for cybersecurity?**  
   **Solution:** Strong authentication, encryption, network monitoring, security awareness training, and incident response planning.
2. **How can organizations prevent data breaches?**  
   **Solution:** Implementing access controls, encryption, and regular security audits.

**Sample Scenario Based Questions**

**UNIT 1: INTRODUCTION TO CYBER SECURITY**

**1. Internet Governance & Challenges**

1. A multinational company operating in different countries faces conflicting data privacy laws (e.g., GDPR in Europe, CCPA in the U.S.). As the company’s Chief Information Security Officer (CISO), how would you ensure compliance with varying regulations while maintaining operational efficiency?

**2. Cyber Threats: Warfare, Crime, Terrorism, and Espionage**

1. A government agency detects an ongoing cyber-espionage campaign targeting its classified information. The attackers are using sophisticated phishing techniques. As a cyber security expert, outline the steps you would take to mitigate this threat and prevent future attacks.
2. A major banking institution experiences a Distributed Denial-of-Service (DDoS) attack, disrupting online banking services. How would you identify the source of the attack, mitigate the impact, and prevent future occurrences?

**3. Need for a Nodal Authority & International Cybersecurity Conventions**

1. A country is considering setting up a national nodal authority for cyber security. You have been invited as an expert to advise on its structure and key responsibilities. What recommendations would you give, and how should it collaborate with international cyber security organizations?

**UNIT 2: CYBER SECURITY VULNERABILITIES**

**4. Software Vulnerabilities & System Administration**

1. A company’s internal database was compromised due to a SQL injection attack. Analyze the possible reasons for this vulnerability and suggest a strategy to prevent such attacks in the future.
2. A healthcare organization experiences a ransomware attack that encrypts patient records, demanding a ransom for decryption. Discuss the immediate response measures and long-term security strategies to prevent such incidents.

**5. Complex Network Architectures & Open Access to Organizational Data**

1. A cloud service provider hosts multiple clients, including financial institutions and healthcare organizations. Recently, a misconfiguration in access control led to unauthorized access to sensitive data. What security measures should be implemented to prevent such issues?
2. An e-commerce platform allows employees to access critical systems remotely. Due to weak authentication, an attacker gains unauthorized access and alters transaction records. How would you redesign the authentication system to improve security while ensuring user convenience?

**6. Weak Authentication & Unprotected Broadband Communications**

1. A university uses a public Wi-Fi network for students and faculty, but security researchers discover vulnerabilities that allow attackers to intercept login credentials. What recommendations would you give to enhance the security of this network?
2. A financial firm allows employees to use personal devices to access company resources remotely. However, weak authentication mechanisms have led to multiple unauthorized access incidents. Propose a security framework that balances security and usability for remote access.

**Scenario:**

A **global financial institution** with branches across multiple countries relies on **complex network architectures**, including cloud-based services, IoT devices, and remote access systems. The company recently experienced a **cyber attack** that exploited **software vulnerabilities** and **weak authentication mechanisms**, leading to a **data breach** of sensitive customer information.

**Attack Details:**

* The attackers exploited an **unpatched software vulnerability** in the bank’s online transaction system.
* They launched a **SQL Injection attack** to gain unauthorized access to the database.
* Using **stolen credentials** obtained through phishing emails, they accessed critical financial records.
* The attack was executed using a **botnet-driven DDoS attack** to divert attention from the data exfiltration process.
* **Poor internet governance policies** led to a **lack of coordination** between branches across different countries, delaying the response to the attack.
* Due to **unprotected broadband communications**, attackers intercepted customer login credentials via **public Wi-Fi hotspots** at various banking centers.
* **Insider threats** were also suspected, as an employee with high-level access had recently resigned under suspicious circumstances.
* The attack raised concerns about **cyber warfare** and **cyber espionage**, as some indicators suggested involvement from an advanced persistent threat (APT) group with ties to a foreign nation.
* Due to the international nature of the attack, legal complexities arose, highlighting the **need for an international cybersecurity convention** and a **centralized nodal authority** to manage such incidents effectively.

**Solution:**

This scenario highlights multiple cybersecurity challenges, from **technical vulnerabilities** to **governance issues**. A **multi-layered security strategy** is essential, incorporating **advanced security solutions**, **strict regulatory compliance**, and **global cooperation** to protect financial institutions from evolving cyber threats.

**Immediate Response & Containment:**

1. **Incident Response Activation**:
   * Deploy the **Cyber Incident Response Team (CIRT)** to contain the breach and analyze attack patterns.
   * Isolate affected systems to prevent further data exfiltration.
2. **Threat Mitigation Measures**:
   * Patch the **SQL Injection vulnerability** and enforce **input validation** on all database queries.
   * Implement **Multi-Factor Authentication (MFA)** to prevent unauthorized access.
   * Disable compromised accounts and enforce password resets for all employees and customers.
   * Deploy **DDoS mitigation tools**, such as rate limiting and Web Application Firewalls (WAF).

**Long-Term Security Measures:**

1. **Network Security Enhancements:**
   * Strengthen **network segmentation** to limit access between different banking operations.
   * Implement **Zero Trust Architecture (ZTA)** to enforce strict access control policies.
   * Deploy **intrusion detection and prevention systems (IDPS)** to monitor and block malicious activities.
2. **Cyber Governance & Compliance:**
   * Strengthen **internal cybersecurity policies** across all branches to align with global regulations (e.g., GDPR, ISO 27001, NIST).
   * Establish a **centralized cybersecurity authority** to oversee security measures across branches.
   * Advocate for an **international cybersecurity convention** to facilitate global cooperation on cyber threats.
3. **Employee & Customer Awareness:**
   * Conduct **cybersecurity training programs** for employees to recognize phishing attacks.
   * Educate customers on **safe banking practices**, such as avoiding public Wi-Fi for transactions.
4. **Cyber Threat Intelligence & Partnerships:**
   * Partner with **international cybersecurity agencies** to track threat actors involved in cyber warfare or espionage.
   * Strengthen **collaborations with law enforcement agencies** for rapid legal actions.