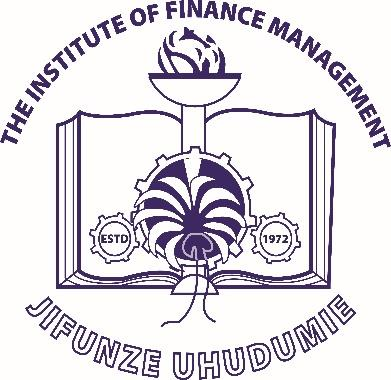
**THE INSTITUTE OF FINANCE MANAGEMENT**



|  |  |
| --- | --- |
| **Module Name:** | Information System Security and Risk Management |
| **CODE Number:** | ITU 08115 |
| **Department:** | Computer Science and Mathematics |
| **Class:** | BAIT\_3B |
| **Student Name** | GODFREY ERNEST MAPUNDA |
| **Registration Number** | IMC/BAIT/2123823 |

**Individual Assignment 1**

As a cybersecurity researcher, analyze and present a report on emerging cyber threats and

trends. Discuss how these threats might impact businesses in the next five years and

propose proactive security measures to mitigate these potential risks.

**Cyber threat** refers to the malicious act or event that could have a negative impact on a computer system, network, or data. Cyber threats can take many forms, including malware, phishing attacks, denial-of-service attacks (DoS), Distributed Denial of Service attack (DDoS), and man-in-the-middle attacks(MITM).

**Emerging cyber threats** encompass a range of evolving risks that pose challenges to the security of digital systems, networks, and sensitive information. These threats often leverage new technologies, attack vectors, or exploit vulnerabilities in innovative ways. The following are the key explanation bout the emerging cyber threats in the modern word, as follows;

**Geopolitical Threats Loom Large:** Geopolitical threats have gained prominence, with events like Russia's invasion of Ukraine showcasing the intersection of cyberattacks and physical warfare. This form of hybrid warfare, combining cyber and physical realms, presents a significant challenge. Global geopolitical conflicts, such as trade bans and sanctions, can spill over into cyberspace, with nation-states leveraging cyberattacks against private enterprises for various motives, including espionage, negotiation leverage, resource control, or showcasing technological prowess. For example: **Cyber Influence on Democratic Processes:** Geopolitical events like democratic elections can become flashpoints for cyber conflicts. Nation-states may use cyber tactics to influence or interfere with election processes in other countries, aiming to shape outcomes in favour of their geopolitical interests, but also ***Russia's actions in Ukraine*** (2014 and 2022)involved a combination of conventional military operations and cyberattacks. Cyberattacks targeted Ukrainian government sites, critical infrastructure, and banking systems, demonstrating the integration of cyber and physical warfare in hybrid conflicts.

**Cloud Computing Threat is Increasing:** The increasing complexity of cloud computing poses challenges for organizations relying on cloud services. Common threats include insecure configurations of infrastructure as a service (IaaS), malware and privilege escalation in guest operating systems, and configuration drift in software as a service (SaaS) applications. Cloud security governance becomes crucial, necessitating security instrumentation and tooling within cloud workloads. Organizations must leverage native security capabilities, cloud security posture management, and infrastructure as code (IaC) scanning to detect and remediate threats effectively. For example: One of the notable incident related to cloud computing and cybersecurity is the ***Capital One data breach***that occurred in 2019. While the breach itself was not a direct compromise of cloud services, it involved the exposure of sensitive customer data stored on the Amazon Web Services (AWS) cloud platform. In this incident, a former employee of Amazon Web Services exploited a misconfigured web application firewall on a cloud server hosted by AWS. This misconfiguration allowed the attacker to gain unauthorized access to the Capital One server and exfiltrate a large amount of customer data, including names, addresses, credit scores, and Social Security numbers.

**AI Deployment Emerges as a Top Cybersecurity Threat:** The rise of artificial intelligence (AI) deployments introduces new challenges in defending against attacks on machine learning models. Generative AI tools, like ChatGPT, bring AI into mainstream enterprise applications, enabling adversaries to scale attacks. Threats include data poisoning to cause algorithmic drift, impacting the efficacy of AI models. Organizations must prioritize understanding how AI vendors protect their models, as vulnerabilities in AI tools could have cascading effects on cybersecurity.

**Ransomware Continues to Batter Organizations:** Ransomware remains a persistent and evolving threat, with threat actors adopting double extortion tactics. Beyond encrypting files, attackers now extort additional payments to prevent the disclosure of stolen data. Critical infrastructure and supply chain companies are prime targets. Global collaboration through initiatives like the Counter Ransomware Initiative highlights the severity of the issue. Organizations should prioritize comprehensive ransomware defense, incorporating external threat intelligence services and following established guidelines for developing a robust strategy. Consider the following:

In the realm of escalating cyber threats, the **8Base ransomware group** has emerged as a formidable adversary, notably deploying the sophisticated Phobos variant. **Cisco Talos'** recent analysis sheds light on the group's modus operandi, revealing that 8Base utilizes **SmokeLoader, a backdoor trojan**, as a means of distributing its Phobos variants. Unlike conventional methods, 8Base incorporates the ransomware component directly into encrypted payloads, enhancing its evasive tactics. The Phobos ransomware, as dissected by Talos, exhibits a range of capabilities, including a **user access control** (UAC) bypass technique and a mechanism for reporting victim infections to an external URL. Particularly concerning is the group's strategic targeting of critical infrastructure and supply chain companies. Talos' findings underscore the evolution of ransomware beyond mere file encryption, with the added threat of data disclosure, exemplifying the need for organizations to fortify their defences comprehensively. As global collaboration initiatives like the Counter Ransomware Initiative gain prominence, the imperative for organizations to prioritize comprehensive ransomware defence becomes even more pronounced. The analysis unravels the intricacies of 8Base's Phobos variant, providing a deeper understanding of the group's tactics and emphasizing the critical importance of robust cybersecurity strategies in the face of evolving cyber threats.

**BEC Social Engineering Tops Ransomware in Insurance Claims:** Business email compromise (BEC) social engineering attacks have surpassed ransomware in insurance claims, combining tactics like phishing and fraudulent wire transfers. Successful BEC attacks often exploit human vulnerabilities, relying on employees' courtesy and helpfulness. Traditional security awareness and training programs are deemed insufficient. Organizations need to adopt advanced protocols like DMARC, focus on positive behaviour change, and employ human risk quantification solutions to effectively combat the growing threat of BEC social engineering.

**HOW THESE THREAT CAN BE MITIGATED**

**MITIGATING GEOPOLITICAL THREATS**

**Understanding and Monitoring:** Stay informed about geopolitical events that could impact your organization. Regularly monitor news and updates related to potential conflicts or sanctions.

**Enhanced Security Measures**: Implement advanced cybersecurity measures, especially if your business operates in regions prone to geopolitical tensions. This may include investing in advanced threat detection, intrusion prevention systems, and encryption technologies.

**Incident Response Plan:** Develop and regularly update an incident response plan that specifically addresses geopolitical cyber threats. This plan should outline steps to be taken in the event of a cyber-physical attack.

**Collaboration and Information Sharing:** Collaborate with industry peers, government agencies, and cybersecurity organizations to share threat intelligence. This can help in staying ahead of emerging threats and preparing appropriate defences.

**MITIGATING CLOUD COMPUTING THREATS:**

**Security Best Practices:** Adhere to security best practices for cloud services. Regularly audit and update configurations, enforce the principle of least privilege, and conduct regular security assessments.

**Cloud Security Tools:** Leverage native security tools provided by cloud service providers. Implement cloud security posture management (CSPM) solutions to continuously monitor and remediate security issues.

**Employee Training:** Provide comprehensive training to employees regarding cloud security risks and best practices. Human error is often a factor in cloud security incidents, so educating the workforce is crucial.

**Incident Response and Recover:** Develop and test an incident response and recovery plan specifically for cloud-related incidents. This includes having a backup and recovery strategy in place.

**MITIGATING AI DEPLOYMENT THREATS:**

**Vet AI Vendors:** Prioritize AI vendors with robust security measures in place. Ensure that the AI tools deployed in your organization undergo thorough security assessments.

**Regular Audits:** Conduct regular audits of AI systems to identify and patch vulnerabilities. This includes assessing the security of data used to train machine learning models.

**Employee Training:** Educate employees about the risks associated with AI deployments. Human factors, such as social engineering, can still play a role in AI-related cyber threats.

**Algorithmic Security:** Implement measures to secure machine learning algorithms, such as monitoring for data poisoning attempts and ensuring the integrity of training data.

**MITIGATING RANSOMWARE THREATS:**

**Backup and Recovery:** Regularly backup critical data and ensure that the backup systems are isolated from the primary network. Test the backup and recovery processes periodically.

**User Training:** Train employees on recognizing phishing attempts and suspicious links. User awareness is a key factor in preventing ransomware infections.

**Endpoint Security:** Implement robust endpoint protection solutions that can detect and prevent ransomware infections. This may include advanced antivirus software and behavior-based detection tools.

**Incident Response Plan:** Develop a detailed incident response plan for ransomware attacks. This should include steps for containing the infection, communicating with stakeholders, and reporting the incident to authorities.

**MITIGATING BEC SOCIAL ENGINEERING THREATS:**

**Advanced Email Security Protocols:** Implement advanced email security protocols, such as DMARC (Domain-based Message Authentication, Reporting, and Conformance), to prevent email spoofing and phishing attempts.

**Employee Training:** Provide ongoing training to employees about the risks of social engineering attacks, specifically BEC. Teach them to verify email requests for sensitive information or financial transactions.

**Human Risk Quantification:** Use human risk quantification solutions to assess and measure the potential impact of human vulnerabilities in your organization. This can help tailor security training to address specific weaknesses.

**Multi-Factor Authentication (MFA):** Enable multi-factor authentication for sensitive systems and transactions to add an extra layer of security, making it harder for attackers to gain unauthorized access.

In all cases, a holistic cybersecurity approach that combines technology, employee training, and proactive monitoring is crucial for effective threat mitigation. Regularly reassess and update mitigation strategies to adapt to evolving cyber threats. Additional issues includes the following:

### ****Regulatory Compliance:**** Emphasizing the importance of staying compliant with data protection regulations, such as GDPR (General Data Protection Regulation) and HIPAA (Health Insurance Portability and Accountability Act), is crucial for businesses. Non-compliance not only leads to legal consequences but also exposes organizations to reputational damage. As cyber threats evolve, regulatory frameworks are adapting to address emerging challenges. For instance, GDPR includes provisions for data breach notifications, ensuring organizations promptly report incidents, fostering transparency, and enhancing overall cybersecurity.

### ****Supply Chain Security:**** In recent years, there's been a growing focus on the cybersecurity posture of supply chain partners. Third-party vendors can introduce significant risks, and it's essential for businesses to assess and monitor their cybersecurity practices. The SolarWinds cyberattack in 2020 exemplifies the potential dangers, where threat actors exploited a software supply chain vulnerability. Businesses must implement stringent cybersecurity requirements for suppliers, conduct regular audits, and col laborate with partners to enhance collective security.

### ****Incident Response Testing:**** Emphasizing the importance of regularly testing incident response plans through simulations and exercises is crucial. These tests help organizations identify gaps in their response capabilities and improve their ability to address cyber incidents effectively. For instance, running a simulated ransomware attack can reveal weaknesses in communication protocols, allowing organizations to refine their incident response procedures and ensure a swift and coordinated reaction to real threats.

### ****Threat Intelligence Integration:**** Suggesting the integration of threat intelligence feeds into the cybersecurity infrastructure is vital. Real-time threat intelligence enhances the ability to detect and respond promptly to emerging cyber threats. By aggregating data from various sources, organizations can proactively identify potential threats. For example, integrating threat intelligence feeds may reveal patterns of malicious activity, allowing businesses to adjust their security measures accordingly and fortify defence against evolving threats

### ****Blockchain and Zero Trust Architecture:**** Blockchain technology has the potential to enhance cybersecurity by ensuring the integrity of data and transactions. It provides a decentralized and tamper-resistant ledger, reducing the risk of data manipulation. Additionally, introducing the concept of Zero Trust Architecture, which assumes that no user or device should be automatically trusted, adds an extra layer of security. By verifying every user and device accessing the network, businesses can mitigate the risk of unauthorized access and lateral movement within their systems.

### ****Continuous Security Training:**** Stressing the need for ongoing and adaptive cybersecurity training for employees is essential. Cyber threats are dynamic, and regular training ensures that employees are aware of the latest tactics used by threat actors. For example, phishing simulations can help employees recognize and avoid falling victim to social engineering attacks. Continuous training fosters a cybersecurity-aware culture within the organization, making employees a proactive line of defense against evolving threats.

### ****Collaboration and Information Sharing:**** Encouraging collaboration between businesses, industries, and government agencies for sharing threat intelligence is critical. A collective effort is more effective in combating sophisticated cyber threats. For instance, the Financial Services Information Sharing and Analysis Center (FS-ISAC) facilitates collaboration within the financial sector, allowing organizations to share threat intelligence and collectively strengthen their cybersecurity defenses.