**Question 1: Answer**

*Phishing is a type of cyber-attack in which adversaries deceive individuals into disclosing private, financial, and sensitive information. This technique has widespread exposure through emails, messages, and phone calls. In the context of the phishing breach at XYZ Corporation, the consequences could include significant financial losses, damage to the company’s reputation, and breaches of privacy. It is crucial for businesses to adhere to a robust cybersecurity framework to ensure a high standard of security and minimize service disruptions.*

**1. Risk Identification**

Identify the specific risks associated with phishing attacks at XYZ Corporation. The following risks are involved due to phishing emails, malware, theft and social engineering.

* **Corporate Data Disclosure:** This could lead to the loss of business plans, financial documents, internal audits, and sensitive information shared within the organization, ultimately resulting in reputational damage.
* **Employee Data Exposure:** Attackers could gain access to employees’ names, positions, titles, Social Security Numbers (SSNs), payroll information, usernames, and passwords.
* **Customer Data Breach:** The breach may expose customer transactions, credit card information, addresses, names, and phone numbers.

**2. Risk Assessment**

Assess the impact and likelihood of these risks. The risk of phishing attacks for XYZ Corporation is **high**, as businesses rely heavily on email, messaging, and phone calls for daily operations. IT security personnel must actively monitor for unauthorized emails, malicious links, and suspicious attachments, as well as oversee network traffic to protect against these threats.

**3. Risk Mitigation**

Top three propose strategies to reduce or eliminate the risks:

* **Recommendation 1: Encrypt All Data**  
  Customer data should always be encrypted when stored on servers. Plain text storage, especially of usernames and passwords, should be avoided.
* **Recommendation 2: Data Masking**  
  Data masking should be applied to information that is not necessary for specific roles. For example, IT staff should only see the last four digits of Social Security Numbers when relevant. Similarly, customer transaction details can be masked by default and revealed only upon user request.
* **Recommendation 3: Deploy an Email Filtering Platform**  
  Implement a filtering system that scans emails for content, attachments, senders, and checks the legitimacy of websites. This platform should also conduct regular campaigns to educate users about phishing tactics.

**4. Risk Acceptance**

Employees may use personal devices to access company emails, which presents a BYOD (Bring Your Own Device) risk. While this risk can be accepted, implementing two-factor authentication can help lower the chances of unauthorized access. Additionally, obtaining insurance can protect XYZ Corporation from significant financial losses and aid in rebuilding infrastructure.

**5. Risk Transfer**

* Designate a professional responsible for communicating security breaches to the public and engaging law enforcement when necessary.
* Third party involvement to conduct vulnerability scans can help identify weaknesses in the network like penetration testing and framework.

**6. Risk Monitoring and Review**

* This can be achieved through regular audits of assets, data, users, and roles. All findings and research should be documented for future reference.
* Employee should have education on phishing tactics and receive feedback on it.
* Implement incident response plan to investigate each risk.

**Question 2: Answer**

*Ransomware is a type of cyber-attack in which adversaries encrypt data and demand a financial payment to restore access. This attack vector is on the rise, particularly in the banking sector, where threats such as Distributed Denial of Service (DDoS) attacks, compromised credentials, spoofing, and phishing is increasingly common. Below is a cybersecurity strategy for ‘SafeBank Corp’. aimed at mitigating risks associated with ransomware attacks.*

**Risk Identification**

The risks and vulnerabilities that SafeBank Corp. faces regarding ransomware attacks are:

* **Social Engineering:** Attackers can exploit social engineering techniques to gather information about customers and employees from online sources like Facebook and LinkedIn. If a data breach occurs, sensitive credential information such as names, emails, and passwords may be leaked on the dark web.
* **Malware Infection:** Employees may inadvertently download malware through adware or browser extensions while surfing the internet, compromising their devices.
* **Outdated Systems:** Ensuring that all software and hardware meet current security standards is essential to mitigate vulnerabilities.

**Risk Assessment**

The impact and likelihood of these risks occurring is **high**:

* **Tampering of Bank ATM Systems:** There is a significant risk that adversaries could manipulate ATM systems.
* **Insider threat:** The like hood of leaking the confidential is high because of access to confidential data like bank balance, deposits, social security number, etc.
* **Un managed asset:** Since the banking network is huge the asset, including IoT devices, software, servers, and hardware, need to be updated to the latest security standards.

**Risk Mitigation**

We can follow these strategies and controls to reduce or eliminate the risks:

* **Periodic Testing:** Implement regular testing and tabletop exercises with stakeholders to prepare for potential ransomware incidents.
* **Advanced Technologies:** Utilize artificial intelligence (AI) and machine learning (ML) to enhance ransomware detection and secure the infrastructure.
* **Multi-Factor Authentication (MFA):** Implement MFA to add an additional layer of security beyond traditional password protection.
* **Least privilege:** Making sure the access to data is only allowed to perform the necessary duties.

**Risk Response**

The appropriate response actions in case of a ransomware attack, including incident response and recovery plans:

* **Isolation:** Disconnect infected systems from the external network and place them in an isolated environment to prevent further spread.
* **Notification Protocol:** Immediately notify security professionals to assess the situation.
* **Playbook:** Follow the predefined instruction and guidelines for handling the incident.
* **Incident Playbook:** Follow a detailed playbook that outlines procedures for responding to ransomware incidents.
* **Documentation :** Document all interactions with internal and external contacts during the ransomware incident.
* **Communication Channels:** Never agree to a ransom payment. Instead, redirect all communications to appropriate higher-level channels.
* **Preservation of Evidence:** Protect devices, logs, and any evidence to maintain the chain of custody.
* **Lesson learned:** Review the steps taken and make necessary changes as needed. Also, discuss the post incident review with the team

**Risk Monitoring and Review**

Continuously monitor and review the risk management strategies to ensure they remain effective and adapt to evolving threats:

* **Stay Informed:** Keep up to date with current tactics used by threat actors by following industry news and collaborating with other cybersecurity professionals.
* **Monitor User Activity:** Regularly monitor employee and user activities for anomalies in data usage.
* **Security Information and Event Management (SIEM):** Integrate SIEM solutions to analyze network traffic coming into and leaving the organization.
* **Policy update:** Review the lesson learned section and make new guidelines as necessary.

**Question 3: Answer**

*The Internet of Things (IoT) refers to devices that are connected to the internet, allowing users to access and control them through wired or wireless connections. Here are the following measures for ‘TechSecure Inc’ to follow:*

**Asset Identification**

Assets within the IoT ecosystem that need protection are:

* **Smart Devices:** Examples include remote car starters, smart speakers (like Amazon Alexa and Google Home), and smart thermostats.
* **Network Devices:** This category includes routers, switches, CCTV cameras, servers, and gateways.
* **Intangible Assets:** These encompass software applications and cloud storage solutions.

**Threat Identification**

Potential threats and vulnerabilities that could exploit the IoT devices:

* **Open Ports:** Unsecured open ports can serve as entry points for attackers.
* **Outdated Firmware:** Devices that are not regularly updated may have vulnerabilities that can be exploited.
* **Unknown Manufacturers:** Devices from untrusted or unknown manufacturers may lack adequate security measures.
* **Denial of Service:** Getting too many requests from the traffic.

**Attack Vectors**

The possible attack vectors through which threats can compromise the IoT devices:

* **Shodan:** Hackers can use tools like Shodan to find unsecured devices, such as CCTV cameras, that are accessible without authentication.
* **Physical Tampering:** Attackers may physically manipulate devices to establish unauthorized connections.
* **Phishing:** If the phishing attack is successful, if might downgrade the firmware of IoT devices.
* **Brute force attack:** Attackers might have access through the device if weak and default password are used.

**Risk Assessment**

The impact and likelihood of the identified threats is **medium**-**high**:

* **Security Mechanisms:** IoT devices often come with minimal security features by default. It is essential to adjust settings to make it more challenging for outsiders to breach the network.
* **Location Vulnerability:** Devices that are not securely placed can be easily accessed. If breached, IoT devices could serve as backdoors for attackers to execute malicious code.
* **Weak credentials:** Likelihood of getting attack is high with default and weak credentials

**Mitigation Strategies**

Propose effective mitigation strategies to address each identified threat:

* **Firmware Updates:** Regularly upgrade the firmware of IoT devices to protect against known vulnerabilities.
* **Trusted Brands:** Only purchase devices from reputable manufacturers that provide reliable security features.
* **Use of VPN:** Implement Virtual Private Networks (VPNs) to secure data during transmission and when accessing shared resources.
* **User education:** Educating the user on how to update and secure the network is important.

**Continuous Monitoring**

Implement continuous monitoring to detect and respond to potential threats in real-time:

* **Device Monitoring:** Continuously monitor connected devices and scan for any new additions to the network.
* **Vulnerability Scanning:** Regularly conduct vulnerability scans and review reports from reputable antivirus platforms to identify and mitigate potential risks.
* **Logging:** A detail log of users, process and access records should be maintained to audit purpose.
* **Technology Investment:** Invest in lates IoT devices that have better hardware security protocols.

**Question 5: Answer**

*To address the challenges ‘TechSavvy Solutions’ faces in tracking and managing IT assets, I propose implementing the IT Asset Management platform, ServiceNow. This solution will significantly enhance the company's ability to manage its IT assets effectively.*

**Step 1: Asset Identification**

We will categorize ‘TechSavvy Solutions' assets into three primary groups: software, hardware, and cloud services. Examples include:

* **Software**: Microsoft Word, Python, Adobe Premiere Pro
* **Hardware**: Printers, workstations, telephones
* **Cloud Services**: Azure platform, virtual machines
* **Licenses**: OS, warranties, privacy

**Step 2: Asset Inventory**

We will implement the ServiceNow platform in this step to have all the asset in our centralized environment. This will allow for continuous tracking and improvements of infrastructure.

**Step 3: Risk Mitigation**

* This asset data will be imported into ServiceNow, which will provide detailed information such as version numbers, manufacturing dates, and warranty details.
* Additionally, ServiceNow will enable operations analysts to monitor the lifecycle of each device, ensuring compliance with ISO standards.

**Step 4: Monitoring and development**

* We will establish a systematic method for creating and maintaining an accurate inventory of all IT assets, including hardware, software, and licenses. This inventory will also include tracking the decommissioning of IT assets when necessary.
* For software and application-related issues, users can easily create tickets within ServiceNow to initiate updates or patches for resources.
* The platform will include reporting mechanisms to monitor the status and performance of IT assets in real time via an accessible dashboard.
* This approach ensures compliance with various regulations, including ISO, PCI DSS, and GDPR.

Citation:

Castelly, John. “ServiceNow Platform Compliance.” *ServiceNow*, www.servicenow.com/company/trust/compliance.html#certifications. Accessed 22 Oct. 2024.

**Question 4: Answer**

*As the Supply Chain Manager for "Global Electronics Inc.," a multinational company that manufactures electronic components, you are tasked with developing a risk management plan to mitigate disruptions caused by natural disasters, geopolitical tensions, and supplier insolvencies. Below is a comprehensive risk mitigation strategy for Global Electronics Inc.*

**Risk Management Techniques**

1. **Diversification**

*Mitigates natural disasters which have high impact.*  
Establishing relationships with multiple vendors for manufacturing and supply will reduce dependence on any single source. Outsourcing is essential to maintain service continuity for our customers, especially when a particular vendor faces risks from natural disasters or other unforeseen events.

1. **Redundancy**

*Mitigates geopolitical tensions which have medium impact.*  
Create a stockpile of essential supplies and actively track inventory levels to meet demand during peak periods. We will implement automated systems to provide an overview dashboard for the organization.

1. **Risk Assessment and Monitoring**

*Mitigates supplier insolvencies which have low impact.*  
Engaging third-party experts to conduct penetration testing will help identify vulnerabilities in our network. It is crucial to ensure that our partners and vendors comply with their respective countries' laws and regulations. Additionally, as a manufacturing company, adherence to OSHA guidelines is essential.

1. **Collaboration and Communication**

*Mitigates geopolitical tensions which have medium impact.*  
We will host secure conferences and meetings where all business plans are documented and accessible only to authorized users. Corporate email addresses will be used for communication, and resources will be shared in a secure cloud environment.

1. **Technology Integration**

*Mitigates supplier insolvencies which have low impact.*  
Implementing automated infrastructure will enhance the efficiency of our manufacturing processes. Regular maintenance and the use of the latest equipment are vital to keeping operations running smoothly.

1. **Contractual Agreements**

*Mitigates geopolitical tensions which have medium impact.*  
All policies, guidelines, protocols, and rules must be signed by all stakeholders. These agreements will cover penalties, profits, loss mitigation strategies, and associated risks.

1. **Scenario Planning and Simulation**

*Mitigates natural disasters, geopolitical tensions and supplier insolvencies which have high impact.*  
Regular tabletop exercises, meetings, and training sessions will prepare the organization for real-life scenarios. For example, we will develop a legal playbook outlining the steps to take during a ransomware attack.

1. **Flexibility and Agility**  
   To enhance flexibility, the company will maintain backup plans and options. Regular audits of devices, applications, and software will be conducted. Any identified vulnerabilities will be promptly patched, and a lifecycle management plan will be established for all devices.
2. **Insurance**

*Mitigates financial burden upon attacks which have high impact.*  
Adequate insurance coverage will protect the business from financial losses and reputational damage. It is crucial to maintain an industry-standard security posture to support valid claims. This approach will provide peace of mind, allowing the business to thrive without excessive worry about risks.

1. **Continuous Improvement**  
   To outperform competitors, Global Electronics Inc. must prioritize diversification, implement redundancy for availability, and continuously enhance infrastructure through ongoing improvements.

**Question 6: Answer**

*Based on (Data Lifecycle Management) DLM principles, here is a detailed plan for ‘HealthTech Solutions’:*

**Step 1: Data Creation and Capture**

* Policies should be established for collecting various types of information, such as names, dates of birth, addresses, and phone numbers.
* Patients can provide this information through verbal communication, registration forms, online sign-ups, or entries on the website.
* All collected data must comply with HIPAA regulations to ensure that unauthorized individuals do not access these records.
* Login credentials should encrypt, and data masking should be applied wherever possible.

**Step 2: Data Storage**

* Data can be stored on-premises or using cloud technology.
* Regardless of the storage method, it is crucial to encrypt the data and implement effective data protection and recovery strategies.
* Given the vastness of the healthcare industry, a hybrid infrastructure may be beneficial.
* Regular security audits and access review should be done.

**Step 3: Data Maintenance**

* Data should not be alterable by unauthorized personnel.
* Servers must sanitize data before storage, necessitating the use of robust database systems such as Oracle or MySQL.
* Patient information should be verified using government-issued IDs, and any updates to health information must be accurately reflected in their profiles.
* Using of encryption methods to check the integrity of data.

**Step 4: Data Usage**

* Access to data should be limited to authorized stakeholders, including insurance representatives, doctors, healthcare professionals, and patients.
* Data must be reusable and readable without including information irrelevant to the current user.
* The insights gained from this data should be meaningful, actionable and options to present as report.

**Step 5: Data Sharing**

* Health information should only be shared with authorized individuals. If another party requires access, a legally signed release should be obtained.
* Stored data must be encrypted, and data masking techniques should be employed wherever possible.
* Use secure communication channels like encrypted mails, secure file sharing and https.

**Step 6: Data Archival**

* Medical histories, treatments, and patient information should be preserved for future reference. The retention period for this data will depend on healthcare industry and the state.
* Even in archival storage, proper security measures must be implemented to protect this data.
* Data should be categorized as active and inactive that meets archival policy.

**Step 7: Data Disposal**

* Once the archival period has elapsed, patient information should be permanently deleted from the database.
* No access to the disposed data should be possible to prevent leaks and maintain security.
* The organization must follow established disposal protocols to ensure compliance and provide audit report.

**Step 8: Monitoring and Review**

* Establish protocols to ensure that no data leaves the network without authorization. Continuous monitoring of servers and regular audits of user access (both read and write) are essential.
* Frequent audits should also assess compliance with ISO, GDPR, and HIPAA regulations.
* Additionally, creating an IT security department dedicated to safeguarding healthcare data is crucial.
* Throughout these processes, adherence to governance regulations such as HIPAA and GDPR is imperative.