**Contingency plan exercise**

*By*

**Mehnaz Afrose**

**Contingency Plan 1:**

This exercise is based on creating two contingency plans for one software asset and one system asset. I decided to do it by using my real-life experience in asset management. First one is for software asset, I decided to make a contingency plan for an identified threat I faced from my Facebook application software. A couple of months ago I received a text message from one of my Facebook friends via messenger. The text message contained a link claiming that a famous apparel brand is giving a huge discount. Unfortunately, that brand was my favorite one, and I was a regular customer of theirs. It was hard to ignore the temptation at first. I just wanted to check whether it is real. I clicked the link, and there were consequences. Although the attack happened couple of months ago, I decided to do the assignment because there could be more phishing attacks like this, not only with me, but also with my family members and friends.

|  |
| --- |
| **RISK MANAGEMENT PLAN 1**  Revision 1 Date:11/16/23  **Software Asset Name: Facebook** |
| **Risk Description and Consequences:**  Threats: Phishing Attack via Messenger.  Description: The risk involves receiving a deceptive link through a familiar platform, together with Facebook Messenger, purportedly offering significant discount offers from a famous apparel brand. The link leads to a website mimicking the logo of the valid website, urging customers to interact in a game and share the hyperlink considerably.  Consequence: Engaging with that tricky link could expose personal info, block chats, and spread it to more folks. It might make people doubt messages from friends and even risk stealing private stuff or money.  **Mitigation Strategies:**   1. Raising awareness: Raising concerns and awareness about sneaky phishing links 2. Tools for Safety: Using antivirus stuff and browser blocks to stop bad websites. 3. Double-Checking: Checking deals directly from real sources before clicking anything. 4. Better Platform Security: Making sure our messaging apps spot and stop these tricky links.   **Contingency Actions and Trip Wires:**  Trip Wires/Indicators that the risk is happening:   1. Surge in Suspicious Links: When there's suddenly a bunch of unusual links floating around in messages or posts. 2. Abnormal Account Behavior: Unexpected changes in profile information, such as name, profile picture, or added contacts. 3. Friends Complaining About Chat Blocks: Receiving reports from friends stating their inability to engage in chats after interacting with a link. 4. Strange Account Activity: Getting alerts about login attempts user didn’t make or changes in user’s account settings user didn’t do. 5. Unsolicited Messages: Receiving messages from unknown contacts or messages containing suspicious content without any prior interaction. 6. Unexplained Account Restrictions: Being suddenly restricted from performing usual actions on the platform without any clear reason. 7. Unrecognized Posts or Activities: Seeing posts or actions made from user’s account that user didn't initiate. 8. Unrecognized Transactions: Noticing unexpected financial transactions or purchases linked to user’s account. 9. Unusual Network Activity: Observing a surge in network traffic or unusual activity on the internet or home network while using the platform. 10. Unexplained Account Deactivation: Finding user's account suddenly deactivated or inaccessible without user's initiation. 11. Spam or Phishing Messages: Receiving multiple unsolicited messages asking for personal information or promising rewards/prizes. 12. Massive Increase in Friends/Contacts: Noticing a sudden surge in new friend requests or contacts from unknown profiles.   Actions to take upon identification that the risk is happening:   1. Alert Everyone ASAP: Send out a message through trusted channels like texts or calls to warn family/friends/other related person who can be affected about the possible risk. 2. Block and Warn About the Link: Immediately stop that sneaky link from causing more trouble and let everyone know to steer clear. 3. Hold Off Sharing Temporarily: Pause sharing for a bit to stop the link from spreading any further. 4. Ramp Up Security Measures: Activate extra safety tools and keep an eye out for more of these tricky links to keep everyone safe.   **Resources needed:**  List all that are needed including: training, backups, software/hardware:   1. Antivirus programs, firewalls, and anti-malware tools to prevent and detect threats. 2. Reliable communication sources, such as text message, phone, email. 3. Reliable devices with updated security features: cell phone, computer 4. Awareness re   **Notifications**  List contacts needed to be made should risk happen:   1. Platform Support or Help Desk: Contacts for the platform (social media support, app support) to report incidents. 2. Immediate Family Members (Parents, siblings, spouse, or children), or trusted close friend who has technical IT knowledge. 3. Work Colleagues or Manager: Especially if the risk affects work-related accounts or data. 4. Financial Institutions: Banks, credit card companies if financial information might be compromised.   **Subject Matter Expert/Person Responsible for implementing plan**  User himself/herself of this Facebook account. In addition, if the user may have a trusted tech-savvy friend or family member who's particularly skilled in cybersecurity or technology matters, then user might designate them as a consultant or advisor to assist with implementing specific technical measures or providing guidance when needed.  **Date Plan Must be Ready**  Within one week from 11/16/2023 (depends on user’s urgency).  **Approvals**  User himself. If necessary, then trust family members, mentor/advisor. |

**Contingency Plan 2:**

The second contingency plan is about the risk of losing a laptop, one of the system assets. A couple of months ago, I was walking through the street hanging my backpack on my shoulder. The backpack was carrying my personal laptop and other valuable belongings. A passerby was cycling beside me. Suddenly, he grabbed my backpack and stanched it. I fell down the street. It was very sudden that before realizing anything about what was happening, the snatcher eloped from out of reach. All files, documents, pictures, movies, and other valuable data were lost along with the laptop itself. It was a crestfallen moment. Later, I was able to recover most of my data from my google drive. I also keep backup everything in an external hard drive. It also helped me to recover a portion of the data I lost with the laptop. Although external hard disk is a reliable platform to keep backup data, it can be lost too. Compared with the situation, for backing up data in online drives is steadier platform, while secured with a strong password and other secured authentication for logging in. This laptop was my personal property. If it were official property, then the consequences would have been more catastrophic.

|  |
| --- |
| **RISK MANAGEMENT PLAN 2**  Revision 1 Date: 11/16/2023  **System Asset Name: Laptop** |
| **Risk Description and Consequences:**  Threats: Unauthorized laptop theft  Description: Thieves grab laptops without permission, usually in public spots or by sneaking into personal stuff. They do it quickly, hoping to make money or mess with personal info. They might snatch it in public or sneak into bags or places where laptops are left alone, all because they're valuable and easy to take.  Consequence: Loss of important data, files, documents, other important assets stored in the memory, and the laptop itself. Other consequences can be privacy breach, identity theft, misuse of personal information. The incident can disrupt the system of daily routine, work and responsibilities, and cause inconvenience.  **Mitigation Strategies:**   1. Enhanced Security Measures: Use laptop locks or secure bags when out and about to prevent theft. 2. Data Encryption and Backups: Keep important stuff safe by regularly backing up files on an external drive or in the cloud. 3. Stay Alert: Be aware of surroundings and avoid leaving laptop unattended in public places. 4. Remote Tracking and Locking: Set up tools like “Prey”, or other tracking software so it can be tracked or locked remotely if it goes missing. 5. Insurance Coverage: Obtaining insurance coverage for laptops to mitigate financial losses in case of theft.   **Contingency Actions and Trip Wires:**  Trip Wires/Indicators that the risk is happening:   1. Unusual Behavior: Observing someone showing excessive interest in laptop or loitering suspiciously near the belongings. 2. Unfamiliar Approaches: Noticing unfamiliar individuals trying to engage in distracting conversations or attempts to get close to the bag or belongings. 3. Unexplained Distractions: Sudden distractions or commotions in public spaces that might serve as a cover for theft attempts. 4. Physical Contact: Feeling an unexpected touch or bump that could indicate an attempt to snatch laptop or personal belongings. 5. Unattended Belongings: Recognizing instances where the bag or laptop is left unattended, even momentarily, in a public area. 6. Unfamiliar Individuals: Noticing strangers or unfamiliar individuals wandering in or around the premises, especially near areas where laptops are kept. 7. Tampering or Damage: Signs of forced entry, broken locks, or tampering with windows or doors leading to areas where laptops are stored. 8. Unexplained Inventory Changes: Unexpected discrepancies or changes in the inventory of laptops or electronic devices kept in storage or office spaces. 9. Missing Security Measures: Sudden absence or malfunctioning of security systems, such as cameras, alarms, or access control systems. 10. Unattended Doors or Windows: Finding doors or windows left open or unlocked in restricted areas where laptops are usually stored. 11. Unusual Behavior: Witnessing suspicious behavior such as individuals carrying bulky bags or items leaving the premises without authorization.   Actions to take upon identification that the risk is happening:   1. Alert Authorities: Notify law enforcement or security personnel about the suspected theft, providing details of the observed indicators or suspicious activities. 2. Secure the Premises: If safe to do so, secure the area by locking doors and windows to prevent further unauthorized access. 3. Activate Security Measures: Initiate security protocols, such as activating alarm systems or surveillance cameras, to monitor and record any ongoing activities. 4. Limit Access: If feasible, restrict access to the area where the laptops are stored to prevent additional unauthorized entries. 5. Document the Incident: Record details of the observed indicators or suspicious behaviors for future reference and reporting purposes. 6. Inform Relevant Parties: Notify appropriate personnel within the organization or household about the suspected theft and coordinate actions for further investigation or security reinforcement.   **Resources needed:**   1. Training and Education: Sessions or materials educating individuals on theft prevention, security protocols, and recognizing suspicious behavior. 2. Physical Security Measures: Laptop locks, secure bags, or safes for storing laptops securely. 3. Backup Systems: Reliable external drives or cloud storage for regularly backing up important data and files. 4. Software Tools: Anti-theft software, encryption tools, or remote tracking applications to protect and track devices. 5. Hardware Devices: Security cameras, alarms, or access control systems for home or office security. 6. Insurance Coverage: Laptop insurance policies to mitigate financial loss in case of theft. 7. Security Updates: Regular updates and patches for software security, ensuring devices have the latest protection. 8. Emergency Communication Channels: Clear channels or contacts for reporting theft incidents promptly.   **Notifications**   1. Law Enforcement: Local police or emergency services to report the theft. 2. Building Security or Office Manager: If a theft occurs in an office or building premises, notify the security personnel or office manager. 3. IT or Security Department: Within an organization, inform the IT or security team to activate necessary security measures or track the device. 4. Home or Office Insurance Provider: Inform the insurance company about the theft to initiate the claims process if applicable. 5. Family Members or Roommates: Notify family members or individuals sharing the living space about the incident. 6. Colleagues or Coworkers: If the laptop belongs to a workplace, inform colleagues or supervisors about the incident. 7. Bank or Financial Institutions: If any financial information was stored on the laptop, inform relevant financial institutions to monitor for suspicious activity. 8. Online Account Providers: Change passwords or inform online service providers if the laptop was used for accessing sensitive accounts. 9. Device Manufacturer or Retailer: Report the theft to the laptop manufacturer or retailer, especially if it's a company-owned device. 10. Credit Reporting Agencies: Consider informing credit reporting agencies to place a fraud alert on user’s accounts in case of potential identity theft.   **Subject Matter Expert/Person Responsible for implementing plan**  For personal contingency plan: The user/owner of the laptop himself.  For organizational contingency plan: Chief Information Security Officer (CISO) or Security Manager, Facility or Operations Manager, Human Resources (HR) Representative, Risk Management Committee, IT Security Team (depends on the organization system)  **Date Plan Must be Ready**  Within one week from 11/16/2023 (Depends on the urgency of the user or organization)  **Approvals**  In personal contingency plan: User himself.  In organizational contingency plan: Depends on the hierarchy of the organizational settings. |