**Exercise 1 of 3: Windows Updates (Hypothetical)**

Lin is going on vacation and decides to set up Windows Updates to run automatically while she’s out, just in case there are any critical vulnerabilities. The next week, as Lin is basking on the beach, users all over the company are unable to access their Email because the server isn’t responding

1. What happened:

* Lin's decision to enable automatic Windows Updates caused an unintended consequence, where the server became unresponsive, resulting in users being unable to access their email.

1. What assets were impacted:

* The company's email server was impacted, which is a critical asset for business communication.

1. Who was the threat actor:

* There was no specific threat actor in this scenario. However, the incident was caused by an internal action (Lin's decision to enable automatic updates).

1. How would you describe the risk level:

* The risk level in this scenario is moderate to high because the email server is a critical asset, and the unavailability of email can disrupt business operations and cause financial loss.

1. What sorts of controls might have prevented or mitigated this risk:

* To prevent or mitigate this risk, several controls could have been implemented, such as:
  + Conducting a thorough risk assessment before making any changes to the system.
  + Testing any changes on a non-production environment before implementing them on the production system.
  + Implementing a change management process to review and approve all changes to the system.
  + Implementing a backup and recovery process to quickly restore the system in case of any issues.
  + Having a monitoring and alerting system to quickly detect and respond to any system issues.

**Exercise 2 of 3: Ukrainian IT Army (Current Event)**

During the early stages of the Russian / Ukrainian conflict, there was an unprecedented response from the global cybersecurity community. Individuals and even hacktivist groups all over the world “volunteered” to serve as champions of one side of the cause or another (although majoritively the out-pouring was in support of Ukraine). These volunteers then carried out malicious activities against nation-level targets. As an example, a group of volunteers launched a DDoS attack (denial of service) against Russian utility company services.

1. What Assets were impacted?

* The assets impacted were the Russian utility company services that were targeted in the DDoS attack.

1. Who were the Threat Actors?

* The threat actors in this scenario were the group of volunteers who carried out the DDoS attack against the Russian utility company services.

1. How would you describe this activity?

* This activity can be described as a form of hacktivism, where individuals or groups use hacking and other cyberattacks to promote a political or social cause. In this case, the volunteers were supporting Ukraine and carried out the DDoS attack against a Russian utility company as a form of protest.

1. Was this ethical? Moral? Legal?

* This activity raises several ethical, moral, and legal concerns. From an ethical perspective, the use of cyberattacks against nation-level targets raises questions about the appropriateness of using technology to achieve political goals. From a moral perspective, the volunteers' actions may be viewed as justifiable by some as they were supporting a political cause, but others may see it as an unjustifiable form of aggression against a foreign entity. From a legal perspective, the use of cyberattacks is illegal and could result in severe consequences if caught, such as fines or imprisonment. Therefore, this activity was not legal.

**Exercise 3 of 3: SolarWinds (Current Event)**

In 2020, it came out that malicious actors had broken into a major network and server monitoring company known as SolarWinds. As the news unfolded, we discovered that not only had SolarWinds been breached, but the malicious actors had used SolarWinds as a launch point to penetrate a huge (untold) number of other companies and even US agencies including Microsoft, Cisco, Intel, parts of the Pentagon, and even the Department of Homeland Security.

1. How would you describe what happened?

* Malicious actors were able to breach SolarWinds, a major network and server monitoring company, and use it as a launch point to penetrate other companies and US government agencies.

1. What Assets were impacted?

* The assets impacted were the networks, systems, and data of the various companies and US government agencies that were penetrated through SolarWinds.

1. Who was the Threat Actor?

* The threat actor in this scenario was a group of malicious actors that were able to breach SolarWinds and use it as a launch point to carry out further attacks.

1. How would you describe the Risk level?

* The risk level in this scenario was high, given the number and significance of the companies and US government agencies impacted. The attack compromised sensitive data and could have had far-reaching and damaging consequences.

1. What sorts of Controls do you think might have prevented or mitigated this risk?

* To prevent or mitigate this risk, several controls could have been implemented, such as:
  + Conducting regular security assessments and penetration testing to identify and address vulnerabilities in the system.
  + Implementing multi-factor authentication and access controls to restrict unauthorized access to the system.
  + Regularly updating and patching software to address known vulnerabilities.
  + Implementing intrusion detection and prevention systems to detect and block malicious traffic.
  + Implementing a security information and event management (SIEM) system to monitor and respond to security incidents in real-time.