INFO 6027 - W2023 Assignment 2

Gihan Shamike Liyanage

1142109

Information Security Management

06/03/2023



1. What in the article tells you that Mr. Oh has planned for Business Continuity Planning (BCP)?

Oh’s team sat all the surviving servers that powered some basic services, such as Wi-Fi and the internet-linked TVs, to bypass the dead gatekeeper machines. By doing so, they managed to bring those bare-minimum systems back online just minutes before the end of the ceremony. Other than that staff of the stadium had started distributing Wi-Fi for reporters and security had started check badges manually within few minutes. This indicates the importance of BPC and how they already identified critical business functions that must be maintained during a cyberattack. Furthermore, Article declares Pyeongchang organizing committee's cybersecurity advisory group had met 20 times since 2015. They'd conducted drills as early as the summer of the previous year, simulating disasters like cyberattacks, fires, and earthquakes. This indicates BCP has been regularly updated to ensure it is effective. Apart from that almost 12 hours after the cyberattack, Oh and his staffers finished reconstructing their servers from backups and began restarting every service and these indicates team already has been prepared for this kind of cyberattack. Provide training to employees on how to recognize and respond to a cyberattack is another major point of BCP and this statement illustrates how nicely Oh's team had technical knowledge to respond and overcome the attack. Within few minutes they had started working according to their respond plan and within 12 hours they managed to overcome the situation.

1. List the steps that Mr. Oh and team took to subdue the malware.

* Isolation: To stop the infection from spreading, the first step was to isolate the infected systems.
* Analysis and Identification: Examined the malware to comprehend its characteristics, intent, and source. And identified domains associated with the malware.
* Control: Restricted malware and prevented it from communicating with the other servers.
* Removal: Start removing the malware from the affected systems.
* Monitoring: Continuously monitored the systems to ensure that the malware had been fully removed and that there were no further signs of infection.
* Improving security: Took necessary action to enhance cyber security to prevent future attacks.

1. In your opinion, do Mr. Oh and his team follow an Incident Response Plan or a Disaster Recovery Plan?

It appears that Mr. Oh and his team followed an Incident Response Plan (IRP) rather than a Disaster Recovery Plan (DRP). It is stated that Mr. Oh's staff discovered the malware immediately, found the source and worked to contain it. These actions are typical points of an IRP, which concentrates on quickly locating and containing a security incident to reduce damage. Furthermore, his team members worked to improve system security and took precautions to prevent future attacks and these points align more closely with the IRP.

1. Create a BIA by listing, prioritizing the asset inventory and providing an estimated cost of downtime for each listed asset.

|  |  |  |
| --- | --- | --- |
| **Asset** | **Rank** | **COD** |
| Servers | 1 | $2.2 million per hour |
| Hotels and Accommodations | 2 | $2 million per hour |
| Transportation systems | 3 | $2 million per hour |
| Broadcasting systems such as internet-linked TVs | 4 | $1 million per hour |
| Advertising systems | 5 | $500,000 per hour |
| Ticketing and payment systems | 6 | $400,000 per hour |
| Security systems such as RFID-based security gate | 7 | $300,000 per hour |
| Timing and scoring systems | 9 | $200,000 per hour |
| Athlete data | 10 | $100,000 per hour |

1. What in your mind would have been the consequences if Mr. Oh and his team had been unsuccessful?

The cyberattack may have prevented the entire event from taking place, resulting in enormous financial losses and harm to South Korea's reputation as a safe and secure nation for hosting international events. The participants' and attendees' personal information might have been compromised, opening the door to identity theft and other cybercrimes. Also, it might have put the athletes' and spectators' safety in danger, putting them at risk of harm or injury. The cyberattack might have had larger repercussions, such as harming diplomatic ties between South Korea and other nations, especially if it became out that a foreign government was behind it.

# References

Greenberg, A. (2019). *The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History*. Retrieved from Wired: https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/

Perlroth, N. (2018). *Cyberattack Caused Olympic Opening Ceremony Disruption*. Retrieved from The New York Times: https://www.nytimes.com/2018/02/12/technology/winter-olympic-games-hack.html