Case Study A : “ One Sony Strategy Simplifies Global Collaborations”

Sony Corporation is a leading manufacturer of audio, video, and communications products for customers and professional markets. Its motion picture, television, computer entertainment (games), music, and online business make Sony one of the most comprehensive entertainment and technology companies in the world. The corporation is headquartered in Tokyo, Japan, and has over 700 total network sites and 141,000 employees worldwide.

In the early 2000s, Sony Corporation followed a strategy of mergers and acquisitions to strengthen itself against intensifying competition. By 2007, Sony’s enterprise (internal) networks had become too complex and incapable of supporting communication, operations and further business growth. A key problem was that its enterprise network was based on IPv4, which could not provide real-time collaboration among its business units and group companies. Expanding the business was being delayed because of the networks’ complicated outdated architecture. The network’s total cost of ownership (TCO) was increasing as its business value decreased.

To solve its networks weaknesses and the threat of running out of IPv4 addresses, Sony launched an IPv6 implementation in 2008. They had to upgrade Cisco Switches at the corporate data centre and remote offices to handle both IPv4 and IPv6 traffic. With a virtually unlimited IP addresses, IPv6 would support Sony’s long-term, next-generation information and communication technology (ICT) infrastructure strategy and improve collaboration and productivity.

Source: page 90 – 91 of the prescribed textbook

Case Study B : The Sony Pictures Hack Explained

Hackers broke into the computer systems of Sony Pictures entertainment in October 2014. The attackers stole huge swaths of confidential documents from the Hollywood studio and posted them online in the following weeks -- exposing them to everyone from potential cybercriminals to journalists who have been poring through the documents and reporting everything from the details of recent film productions to the extent of the employee data laid vulnerable on the Internet.

Multiple reports suggest U.S. government officials believe the attack is tied to the North Korean government, who expressed outrage over the Sony-backed film "The Interview," an action-comedy centered on an assassination plot against North Korean leader Kim Jong Un.

Sony Pictures canceled the theatrical release of the film Wednesday, responding to a vague threat against theaters showing the film supposedly posted by the hackers. Here's what we know so far:

What happened?

The Monday before Thanksgiving, Sony Pictures employees who tried to log into their computers were greeted with a graphic of a neon red skeleton featuring the words "#Hacked by #GOP," and a threat to release data later that night if an unspecified request was not met. Over the coming weeks multiple statements purported to be from GOP, short for "Guardians of Peace," were posted online -- many to a text-sharing site called PasteBin, which is also used by some hactivist groups. The messages were often accompanied by links to download huge amounts of what appears to be data from Sony Pictures' internal networks. In a memo shortly after the first leaks were obtained by the Hollywood Reporter, Sony Pictures executives Michael Lynton and Amy Pascal acknowledged the theft of a " large amount of confidential" data:

While we are not yet sure of the full scope of information that the attackers have or might release, we unfortunately have to ask you to assume that information about you in the possession of the company might be in their possession.

The same day as the attack, the FBI released a flash memo warning about a destructive type of malware. As late as this week there are reports that that Sony employees are still unable to use their old computers due to concerns that code left by the hackers may not have been completely removed from the system.

Who was responsible?

Attribution is really hard when it comes to cyberattacks because it can be difficult to tie the digital forensics left behind to real-world actors, but the leading theory is that the attack is tied in some way to the North Korean government. On Wednesday The Washington Post, the New York Times and others reported that anonymous U.S. officials were pointing the finger at the secretive nation.

One official briefed on the investigation told The Post that intelligence officials believe with "99 percent certainty" that hackers working for the North Korean government were behind the attack. But the administration is reportedly unsure what to do with that information -- fearing no good outcome could come from pointing figures at the secretive state: North Korea is diplomatically isolated, and there are already significant sanctions in place.

North Korean officials have officially denied involvement in the attack but did call it a "righteous" deed and suggested it may have been the work of supporters of the regime.

Because of the difficulty of positively identifying cyber actors, the United States rarely names nation-state actors it suspects of being behind cybersecurity incidents. An exception occurred earlier this year, when the Department of Justice announced indictments against several Chinese military employees it said were tied to cyberespionage activities against American companies. Officials are also said to be concerned about the diplomatic fallout for Japan -- Sony is based in Japan, and the nation is much closer to North Korea geographically than the United States.

The North Korean link was speculated early on, when tech news site re/Code reported that investigators were looking into the possibility of a link. After that report, messages purported to be from the hackers alluded to "The Interview" -- first saying that Sony needed to stop "the movie of terrorism," and later explicitly mentioning the film while invoking the Sept. 11, 2001, terrorist attacks and threatening theaters that planned to show the film.

Technical details about the cyberattack are reported to bear similarities to previous attacks on South Korean media institutions that some cybersecurity experts attributed to North Korea. But some remain skepticalabout the connection, noting that much of the publicized evidence linking the attacks is circumstantial.

How has Sony Pictures responded?

The studio canceled plans to release "The Interview" theatrically on Wednesday, after a string of major theater chains had indicated they planned not to show the film. It's unclear if the film will receive any distribution at all.

Earlier this week, a lawyer representing Sony Pictures sent a letter to media outlets covering documents leaked by the hackers demanding that they not download future leaks and that they destroy stolen data already in their custody. It appears unlikely that this will stop outlets from reporting on the content of the documents; a 2001 Supreme Court decision said a radio station couldn't be held responsible for broadcasting newsworthy audio recordings even if those recordings were originally made by someone in violation of wiretapping laws.

Sony Pictures is also trying to block distribution of the stolen data, hiring companies such as London-based anti-piracy firm Entura International to quickly remove links to download the information. The studio has been working with the FBI and cybersecurity firm FireEye to investigate the breach.

This is not the first time Sony has struggled with cybersecurity. In 2011, the company's PlayStation Network was compromised by hackers who stole the personal information of millions of gamers and knocked the network offline for weeks. The company is facing lawsuits from former employees alleging Sony was negligent in protecting the personal data workers entrusted it with -- such as medical data, social security numbers, e-mail correspondence and performance evaluations. (The company has offered a year of credit monitoring to current employees.)

How big a deal is this?

While the news has been dominated by big retail hacks over the past year, the Sony Pictures cyberattack was much more disruptive: It knocked out computer systems at the company, and the fallout from the wholesale distribution of internal documents is far different from having to respond to the theft of credit card numbers.

Many within the cybersecurity community hope this will act as a wake-up call to the companies about their vulnerability to digital adversaries -- both in terms of beefing up their current defenses and their back-up capabilities.

Some area also concerned about the precedent set by capitulating to the hacker's demands to stop the release of "The Interview," noting that the attackers have effectively managed to get their way by controlling the conversation. What happens if other groups adopt similar tactics to advance their agendas?

Many celebrities have tweeted their worries about what this means for the future of free speech and artistic expression, and they probably have point: In the wake of the cyberattack, another studio has reportedly pulled the plug on a film that was to be set in North Korea and to star Steve Carrell, according to Deadline.

Source : https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?noredirect=on&utm_term=.595b9b995a5e

Instructions

1. Please read case study A and B and answer the following questions

2. When submitting your assignment, the cover page of your assignment should contain the group name, initials, surnames and student numbers of all the group members who participated in the assignment. Students whose names do not appear on the cover page of the assignment will be awarded a zero mark.

3. **The closing date for assignment submission is the 4th May 2019 at 10h00 in class**.

4. No late or e-mailed assignment will be accepted.

Question 1 **[6]**

1.1 You have been appointed as an Information Technology (IT) Manager for Sony Corporation. As a manager, you understand that there are important decisions you will be making in order to improve the IT infrastructure of your organization. An important management decision, however is the Network Quality of Service (QoS) for bandwith-intensive apps and time-sensitive data. You need to devise means to apply QoS technology for effective network system within your organization. Discuss with the management how you will apply QoS technology to create two traffic tiers. Hlayisani **(6)**

Question 2 **[8]**

2.1 Sony has decided to invest massively in data networks, IP addresses, routers and switches to increase the productivty, security, user experience and customer service. Playing the role of an IT manager, Discuss the basic functions of your organization's network that you will focus on during the implementation. **(8)**

Matamela Tyindyi

Question 3 **[8]**

3.1 Discuss the difference between packet and circuit switching Shezi **(4)**

3.2 Which one would you recommend for Sony and why Kgatla **(4)**

Question 4 **[32]**

4.1 As an IT manager of Sony Corporation, the management team of your organization has approached you to assist in putting effective system in place for internal fraud prevention and detection. BRIEFLY explain to the management the three (3) fraud prevention tactics you will advise the management to use to make employees know that fraud will be detected by the IT monitoring system and punished. Maswanganye **(6)**

4.2 In order to prevent the cybercrime you experienced at Sony Pictures. You have been requested to come up with a cyber security strategy for Sony in order to prevent similar attacks. Discuss three ojectives of data and information systems security Pangwa **(6)**

4.3 What is a malware and what is that Sony Pictures can do to prevent malware attacking their computer networks Hlela **(4)**

4.4 As an IT manager of Sony Corporation, you have been requested to come up with a plan to prevent similar attacks like those that happened in October 2014. Discuss eight (8) objectives of a cybersecurity that Sony Pictures cybersecurity programme should aim to achieve **(16)** Dlamini Makhubele

TOTAL = 54