Task: Write case study

Topic: Student's choice

Type: Case study
Length: 2 pages
Formatting: MLA
Requirements: Provide case study

Student's choice

Student’s name

Name of institution

List of priorities

Based on SEC guidance to make appropriate disclosures (A17, Cynthia M. Krus), below is a list of prioritized information Sony needs to include in its communication response;

- Financial implications
- Compromise extent
- Fallback plan

- Legal implications
- Investigation
- Risk and impact

Although all the above are critical points of concern in the Sony communication response, the highest priority should be given to risk and impact, the extent of the compromise and the findings drawn from the investigation. Below is an expansion on the same.

On the realization of the hack, Sony is entitled to communicate to their clients of the financial expectations or the impact on the financial statements. It is most likely that the trading price of the Sony shares is also affected which also requires a response on how to compensate the shareholders or investors from the incident. Sony were prompt in responding to the extent of the network compromise though failed to offer the exact details on how this took place without being detected. The role of the IT team could probably need review or extra staff required to tasks such as intrusion detection. This is to ensure that such incidents will be easier to detect and act on in the event of a similar hack. This brings us to the issue that Sony is supposed to communicate on other means above this on a fallback plan from the present situation and ways to mitigate on similar

occurrences. As a shareholder, I would expect a communication highlighting that the company is looking forward to investing more on system security. An assessment should be scheduled, and the same communicated indicating the risk posed by the hacks and the potential impact lurking from malware that could probably have not yet been detected. Networks are weak, but it is even easier to penetrate from a social perspective. Employees must be enlightened on the power they have to derail the company from that issue. Investors want to hear whether any meeting or plans have been made to prepare staff on the matter and also check whether past or present disgruntled employee played a hand on the setback.

A communication would also be expected on the eventual investigation, findings and the legal implications if any. In Sony's case, several data protecting authorities expressed interest to delve into the breaches so as to ascertain how applicable their data protection law stood against any jurisdiction and the case that may crop up in their offices. For instance, the ICO, Information Commissioner's Office in the United Kingdom conducted their investigation into the network and subsequently gave Sony a monetary penalty at £250,000. Will such fines be shared among the stakeholders or will it eat into the company's profit?

The guidance for SEC staff identifies that SEC's existing disclosure rules do not reference to cybersecurity and public companies need to take into

consideration the uprising importance of cybersecurity. Subsequently, it is necessary to take appropriate actions ‘‘consistent with relevant disclosure considerations which conventionally arise in the connection with any kind of business risk.’’ In regard of this, guidance is similar to the guidance which has been issued by SEC in relation to both foreign political risks and the climate change

Therefore, communication response of the company should implicate the following steps:

1. imply online games service in which gamers could interact with other in the real-time battles quests and challenges.
2. Eliminate intrusion attacks hazards.
3. Develop consoles and release codes which could allow third-party software to be run on a system platform.
4. Release detailed public statement connected with the system blackout
5. Determine the full scope of the attack.
6. Determine whether the personal information or credit card numbers of account holders had been compromised.

7. Show the ways of obtaining a market presence and increasing revenues

8. Unveil the launch of the first Sony tablet computers

9. Communicate core points of information in regard with the network interruption

Work cited

FBI. FBI, 22 Sept. 2011. Web. 11 Nov. 2014. <http://www.fbi.gov/losangeles/press-releases/2011/member-of-hacking-group-lulzsec-arrested-for-june-2011-intrusion-of-sony-pictures-computer-systems>.

Krus, C. (n.d.). Who is listening? The SEC emphasizes importance of cybersecurity disclosure. *Journal of Investment Compliance,* 30-32.

Li, Shan. "Justice Department Probes Hacker Attack at Sony's PlayStation Network." *Los Angeles Times*. Los Angeles Times, 5 May 2011. Web. 11 Nov. 2014. <http://articles.latimes.com/2011/may/05/business/la-fi-sony-probe-20110505 >

Office of the Australian Information Commissioner, “Sony PlayStation Network: Statement from the Australian Privacy Commissioner, Timothy Pilgrim”, press release, Web. 11 Nov. 2014. <http://www.oaic.gov.au/news/statements/statement_130125-sony.html>.

"SOE - Customer Service Notification." *SOE - Customer Service Notification*. 2 May 2011. Web. 11 Nov. 2014.< https://www.soe.com/securityupdate/>

"Sony Succumbs to Another Hack Leaking 2,500 "old Records"" *Naked Security*. Web. 11 Nov. 2014. <http://nakedsecurity.sophos.com/2011/05/07/sony-succumbs-to-another-hack-leaking-2500-old-records/>.

"Sony Fined £250,000 after Millions of UK Gamers' Details Compromised." *ICO News Release:*. Web. 11 Nov. 2014. <http://www.ico.org.uk/news/latest_news/2013/ico-news- release-2013>.

Recommendations of the House Republican Cybersecurity Task Force (October 5, 2011). Web. < http://thornberry.house.gov/UploadedFiles/CSTF_Final_Recommendations.pdf>;

The White House, Fact Sheet: Cybersecurity Legislative Proposal (May 12, 2011). Web. <

whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal>

Overall Impression

Incorrect capitalization, inappropriate punctuation use, incorrect tense usage, typographic errors, a lack of organization, improper article usage, no in-text citations, and incorrect word usage. Pretty much everything went wrong. It hardly looks like a case study anyways. It resembles a hodgepodge of information that no one wants to read. If I was going to say anything to this writer, I would say, “Learn how to write a case study and actually check your paper for errors.” I can’t tell you how many times papers suck just because the writer did not check for errors. This is a prime example of this.