South Korean Winter Olympics, A Preventable Incident

Azer Hojlas

November 6, 2022

1 Introduction

According to the two attached articles in the assignment memo, sub-optimal security levels occur due to (1) organizations decentralizing the cyber-security decision making and (2) incentives being aligned in such a way that nobody really is accountable for preventing intrusions and theft, least of all those responsible for the protection of the organization. This report discusses mainly the first point, as the forthcoming example is a case where despite sufficiently allocated resources, an intrusion was made possible due to a decentralized decision making process.

South Korean Olympic Attack

An easily preventable incident that involves both aforementioned statements took place during the Winter Olympics in South Korea 2018. For a brief moment, all IT-related services went down, the most important being wifi and ticket authentication, rendering attendees (reporters, athletes and spectators) unable to access the events. What was initially believed to have been carried out by Chinese hackers or their North Korean neighbours, was later debunked by other in-depth investigations that pointed to other actors. The IT-department responsible for the games initially assumed that the disturbances were due to some technical failure. In fact, an attack was being carried out by a group who months before had gained access and laid in wait until the start of the games (Greenberg, 2019). Fortunately, the IT-department acted quickly and proceeded with cutting of services from the internet until all infected nodes were found. In no small part due to the quick-footed efforts of the IT-department, the services were back online in the span of 24 hours. The rest of the games carried on without any further sabotage.

Despite the early allegations of the suspected perpetrators, performing such an attack was not in the best interest of North Korea, as it occurred during the greatest thaw in relation since before the Korean war (Greenberg, 2019). Several months after the attack, numerous investigators (private contractors and security agencies) came to the independently separate conclusion that a Russian state-affiliated group of hackers had committed the attack. Furthermore, the group had planted false evidence and traces that upon a shallow inspection led the South Koreans to believe that their traditional regional enemies were beyond the attack. As there was no financial motive behind the attack (nobody issued a ransom request and no data appears to have been stolen), authorities on the matter arrived at the conclusion that it was simply a case of revenge, as Russia had been barred from the games on account of their state sponsored doping of athletes (Wallace & Giambalvo, 2022) several months before. This ban was cheered on by the majority of countries in the international community. Thus, this was seen as a Russian retaliation for what the Kremlin believed was unjust punishment, however childish that might sound.

The attack had several months earlier started out in typical fashion, by targeting the IT-department in an email phishing offensive (Murdock, 2018). Not sooner than the phishing attacks had been initiated were they detected by cyber security firm McAfee, which had been hired to safeguard the games from an incident just like the one that would occur some months later. Yet, for reasons unknown, the IT-department had decided to take no significant action against these attempts.

Discussion And Conclusions

As has been stated earlier, the South Korean Olympics committee knew about the phishing attempts months in advance, yet the IT-department decided that the matter was not worth pursuing. Looking at it from the point of view of the IT-department, pursuing the matter might have been very expensive. Phishing attempts are one of the most typical forms of attack. Thus, they are commonplace and happen regularly to organizations and even private citizens. Due to the sheer amount of emails that are produced in these targeted campaigns, analyzing the contents of and tracing the source of each individual email might prove to be a rather costly endeavour. Therefore, committing to an exhaustive analysis might not be viable from an economic point of view. Tolerating some level of insecurity is thus economically rational from both the perspective of the IT-deparment and most organizations in general (Bauer & van Eeten, 2009). However, the costs of the sabotage were not only borne by the IT-deparment, but also by external stakeholders, namely the athletes, reporters and spectators that for a while could not enter the stadiums. Additionally, both Korean states were negatively affected as accusations in the early stages of the attack had temporarily caused a hostile atmosphere between the two traditional belligerents. Ultimately, this was an attack on the Olympic games, and as such it is seen as a blemish on the record of the international olympic committe (IOC for short).

Thus we arrive at a classic case of misaligned incentives, where the organisation responsible for arranging the Olympics is incentivized to compromise on their cybersecurity efforts, where they take all the credit given the games have been conducted successfully, while other stakeholders share the costs if something bad were to happen. Given the information presented in the article by Bauer and van Eeten, it is suggested that decision making regarding the incident should not have been delegated solely to the IT-department. Instead, security should have been handled further up the organizational chain of command, namely the IOC. It can be assumed that the tolerable level of insecurity for the IOC is far lower than that of the IT-department in South Korea (the IOC having the ultimate responsibility of organizing the games leaves them with more to lose). As such, they might have recognized the potential consequences of the phishing attempts and decided that leaving the matter unattended would have been far too risky.

It would be wise to centralize the function of cybersecurity in the future in order to minimize the chances of such an attack happening again. The only thing standing in the way of implementing just that is the inevitable level of reluctance that some nations would harbour towards allowing a foreign NGO being in charge of such an event on their soil.

Another possible explanation for the occurrence of the incident is that of the misaligned incentives with regards to the partially outsourced cybersecurity function that Mcafee occupied. The cybersecurity firm fulfilled the job that they were meant to do, namely to do reconnaissance and report back the findings to the IT-department. As such, they really had no incentive to do more. They get paid regardless of if an attack occurs or not. If they perhaps had a stake in the outcome of the Olympic games, they would have been more alarmist in their reporting back to the IT-department. If they were partially held accountable for what had transpired during the games, maybe the outcome would have been different, as no accountability in the domain of cybersecurity inevitably leads to a higher degree of insecurity (Moore, 2010). In other words, the situation might have been stopped altogether if the firm had an incentive to be more vigilant, i.e in the form of performance based financial bonuses if the events carried on without disturbances. The flip side would also mean that the firm faces financial and or legal repercussions if they fail to achieve what is stated in their contract.

A personal proposal of the author is that the realm of cybersecurity should be more regulated and bureaucratised like accounting. Both are similar in their auxiliary roles to corporations. Financial auditors however are accountable for their actions to some degree. They are not responsible for the performance of the companies that they audit, they can however be held responsible if they they are complacent when putting their stamp on numbers that are unsound at best and fraudulent at worst. One such instance of the latter is the collapse of the accounting firm Arthur Andersen, that remained complacent when their client, Enron, reported annual figures that were clearly fraudulent (Brown et al, 2002). This turning of a blind eye was paid for by lucrative fees that Enron paid out in exchange for Arthur Andersens silence and esteemed auditory reputation. The subsequent penalties in the af-

termath of the Enron scandal bankrupted the firm.

Cybersecurity firms could play a similar role as auditing firms, where they are not responsible for incidents that occur, but can be held accountable in cases where there was ostensible evidence that an attack could have been prevented beforehand. This introduces an incentive for cybersec firms to have a vested interest and incentive in the successful protection of their clients, lest they want to face any potential regulatory repercussions. These kinds of changes would require a significant regulatory and legal effort from lawmakers. Additionally, the backlash from cybersec firms would be significant as this would significantly increase their workload and therefore impact profits in a negative way. Mcafee would not gladly accept responsibility for the 2018 Winter Olympics Attack, and I imagine that the pushback would be significant.

References

Bauer, J., van Eeten, J.G. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. Science Direct.
https://www.sciencedirect.com/science/article/pii/S0308596109000986?via%3Dihub

Brown, K,. WSJ auxilliary staff. (2002). Arthur Andersen's Fall From Grace Is a Sad Tale of Greed and Miscues
https://www.wsj.com/articles/SB1023409436545200

Giambalvo, E. Wallace, A. (2022). A timeline of Russia's state-sponsored Olympic doping scandal. Washington Post
https://www.washingtonpost.com/sports/olympics/2022/02/11/russia-olympics-doping-scandal/

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

Moore, T. (2010). The economics of cybersecurity: Principles and policy options.
https://www.sciencedirect.com/science/article/pii/S1874548210000429?via%3Dihub

Murdcoch, J. (2018). Winter Olympics 2018 under siege from hackers, McAfee warns. IBT
https://www.ibtimes.co.uk/winter-olympics-2018-under-siege-hackers-mcafee-warns-1654237