Cybersecurity Incident Analysis

Martin Siddons

1 Introduction

In this report I will explore the attacks on Yahoo and Norsk Hydro, as well as the Stuxnet worm, what made the companies involved vulnerable and how they dealt with these threats.

2 Yahoo! - Balancing Security with Retention

In September 2016, Yahoo announced that 500 million user accounts had been affected by a data breach from late 2014. Three months later they announced that another breach occurred in August 2013 affecting over three billion user accounts, the largest ever data breach announced to the public (Trautman and Ormerod, 2016). Investigations by the FBI found the attack was state funded and lead to the indictment of two men working for Russia's Federal Security Service and two other Russian citizens (of Justice, 2017). This lead to the arrest of Karim Baratov, who admitted to directly accessing at least 80 email accounts using stolen credentials and was sentenced to five years in prison and a fine of $2.25 million (£1.69 million)[1] with additional restitution (of Justice, 2018).

According to of Justice (2017), the attack itself consisted of spear phishing a Yahoo employee and having them install malware allowing the attackers backdoor access to the internal account management systems. Attackers then copied the Yahoo user database and used tools to mint cookies using a unique key in that database, allowing access to any account without knowing its password.

Laws such as GDPR state that data breaches must be reported no later than 72 hours after becoming aware (GDPR, 2018), but Yahoo were lucky that the law had yet to come into effect at the time of the breach otherwise they stood to be fined at least $90 million (£67.67 million) (Green, 2020). The company was criticized for its delay, with the SEC opening investigations due to evidence that employees were aware of "prior access" in late 2014 (SECURITIES and COMMISSION, 2016).

In response to the attack, Yahoo invalidated cookies, but according to Perlroth and Goel (2016), CEO Marissa Mayer decided not to force affected users to change passwords as she was concerned it would drive users away from the service. This choice possibly ensured that some accounts affected but not identified in the attack were left vulnerable. Yahoo had been having issues with user retention and finances for years prior (Griswold, 2016), which had a clear effect on how security was handled.

Financially, the company was in the process of being bought by Verizon, which lead to the buyout price decreasing by $350 million (£263.2 million), or 7.25%. From an initial 23 lawsuits (Goel, 2016), five were combined into a Class action lawsuit in December 2016, which settled in April 2019 for $117.5 million (£88.35 million). The US Securities and Exchange Commission (SEC) fined Yahoo $35 million (£26.32 million) for failure to disclose the breach in a timely manner (CALIFORNIA, 2019) and the UK Information Commissioner's Office (ICO) fined Yahoo £250 thousand (ICO, 2018). Reputationally, it was reported by Goel and Perlroth (2016) that analysis by Spredfast found 90% of twitter comments about Yahoo were negative in October 2016, compared to 68% in August.

In regards to the CIA triangle, confidentiality was broken as unauthorised users gained access to user profiles and integrity of data was broken due to the modification of search results for

[1] 1 GBP = 1.33 USD

erectile dysfunction being modified to forward users that clicked on the top result through a server owned by the attackers in order to receive clickthrough commission (of Justice, 2017).

In terms of risk, despite Yahoo being a frequent target for nation-state spies (Perlroth and Goel, 2016), they took over a year to hire a new Chief Information Security Officer (CISO) following the departure of Justin Somaini. (Hesseldahl, 2014). According to Perlroth and Goel (2016), the new CISO repeatedly had difficulties obtaining funding for security improvements including intrusion detection, likely due to the relatively poor financial situation the company was in. The 2014 Yahoo Annual Report mentioned cyber attack as a possibility but labelled it as "something we have little to no control over" alongside natural disasters and political unrest (Yahoo, 2015). The report also fails to mention how such attacks are being avoided, mitigated or transferred beyond the mention of implemented security measures, which aren't discussed. Yahoo's failure to respond constituted to taking a tactical risk. There was also no threat monitoring in place to instantly pick up on the attack, constituting to an operational risk. They appeared to welcome risk, had a lax attitude to security and were slow to implement new security features (Menn et al., 2016).

Regarding privacy, we know from court documents that at least 30 million Yahoo accounts were breached by the attackers, and that this exploit allowed specific users to be targeted (of Justice, 2017).

I have analysed the privacy policy as it stood at the time of the attack (Machine, 2016). From May 2011 to the point Yahoo was acquired by Verizon, there were no functional changes to the privacy policy, and no sign it had been reviewed, showing that it wasn't a living document. Many security analysts, including IT consultancy firm Pensar recommend reviewing policies at least annually (Williams, 2018). The privacy policy feels ambiguous in its use of legal writing style, making it hard to understand; it doesn't name the companies Yahoo works with, simply using 'Trusted Partners'. The rules at least appeared realistic as they don't make it harder to use the service, but don't list how the policy will be enforced. It feels inclusive at least, having separate sections regarding accounts for children. I can say for certain that it wasn't endorsed though, considering how the CEO was actively working against the security team regarding funding. In conclusion, I feel the privacy policy failed its job as it was long overdue for review, didn't give enough information and was actively worked against by the CEO.

It was likely the NIST framework was not followed as there was no real-time monitoring in place. Yahoo's security implementation barely even corresponds to tier one on the NIST framework implementations (NIST, 2018), as their response appeared ad-hoc and the organization didn't collaborate with or receive information from other entities.

Regarding the human and social engineering aspects of the attack, it's possible that training wasn't sufficient enough for the admin team which allowed the initial spear phishing attack to occur. It isn't understood what social engineering framework was used, but it's clear from the specific targeting of some accounts that information gathering was at the core of the operation.

3 Stuxnet – The Dawn of Cyberwarfare

Stuxnet was a worm found in June 2010, designed to infect Windows PCs and target Siemens Step7 control software, looking for certain connected Programmable Logic Controllers controlling motors running at a certain speed. The malware contained within then modifies the rotation speed of the motor to attempt to cause damage to whatever it's connected to. It then attempts to infect other machines on the local network and connected USB flash drives (Chien, 2010). Due to how specific it was and how infections occurred in multiple Iranian government facilities (Falliere et al., 2011), it was understood the endpoint was uranium enrichment centrifuges at the Natanz nuclear facility, where over a thousand centrifuges were damaged (Lindsay, 2013). Stuxnet was operating for approximately one year before being detected (Falliere et al., 2011).

The worm and its payload cover all four threat types (Disclosure, Deception, Disruption, Usurpation), as explained by Falliere et al. (2011). Stuxnet gets access to data coming from the PLCs connected to the system. The attackers also had unauthorised access to private keys from JMicron and Realtek for signing embedded driver files (Falliere et al., 2011). The payload causes the target system to accept false information, and the payload itself deceives the motor monitoring software by sending back false readings. Stuxnet was designed to cause interruption to uranium enrichment systems, causing downtime while they were replaced. Finally, the payload took control of the system and could retake control after equipment was replaced.

As analysed by Kamiński (2020), Stuxnet is understood to be a part of a larger operation codenamed "Olympic Games", where the USA and Israel worked to prevent the development of Iran's nuclear program.

Financially, the cost to Iran is unknown, but one analyst estimates that at the Natanz plant alone, over $20 million (£15 million) of equipment needed replacing (Forden, 2009). Reputationally, the attack showed that the Iranian nuclear program could be quietly slowed by means other than diplomacy or direct military intervention. Ethically, it could be said that this opened the gates to cyberwarfare across the world. Falliere et al. (2011) echoes this thought, saying "Effective cyber attacks by such nations [as Iran and North Korea] on critical infrastructure could create significant problems".

In terms of risk, the sophistic nature of the attack shows there were no easy attack vectors, so defence was likely high. There was no hint beforehand that an attack like this could or would be carried out, so there was no way for Iranian officials to estimate how to counter it. Tactically, the systems were appropriately air-gapped to ensure online attacks were impossible (Lindsay, 2013). Due to the secrecy of the target, we don't know if the attack was detected before June 2010. I would imagine, however, that engineers at the Natanz plant would quickly realise something was amiss as centrifuges began breaking. Operationally, keeping software up-to-date wouldn't have countered the zero-day exploits. These show that there was a culture of risk adversity at the plant, which is to be expected of such a critical site.

Threat monitoring would be expected, but given the secrecy around the site, we will likely never know. It's possible that previous attacks were caught by a threat monitoring system, which would necessitate the zero-day exploits used in Stuxnet. Regarding the cyber killchain, Reconnaissance was extensive, as the attackers clearly knew the system inside-out. Weaponization was via four zero-day flaws (Naraine, 2010) and delivery was via USB memory which exploited previously unknown vulnerabilities. Installation happened automatically, C+C existed only to update the malware and retrieve basic information outside the air gap (Falliere et al., 2011). Actions on objectives were all automated, executed when the worm discovered it was on a computer running Step7.

Finally, regarding social engineering, Iran's Ministry of Communications was quoted as saying the source of the outbreak was "foreign experts" that inadvertently introduced the virus via memory sticks (Payvand, 2010). If this refers to IAEA nuclear inspectors than this would explain how Stuxnet moved around systems over Iran and elsewhere in relatively short time without aid of the internet for propagation.

4 Norsk Hydro – Assurance and Insurance

On 19 March 2019, Norsk Hydro (aka Hydro), one of the largest aluminium companies in the world (Gupta, 2016) was hit by a LockerGoga ransomware attack, causing their global operation to go down, with many returning to manual operation the following day, but full production not returning until almost two weeks later (Haugetraa and Molland, 2019b). It was found that attackers spent up to three weeks infiltrating Active Directory, a system for managing Windows computers, and installing LockerGoga (Tomter and Gundersen, 2019). It remains unknown who

was behind the attack. One source indicates French and Ukrainian police are looking for four Ukrainian suspects (Krasnogolovy, 2019), however the quote source couldn't be verified so I feel I cannot accept it as valid evidence in this report. It's not known how the attackers first got into the system, with Hydro assuming it started with an email (Tomter and Gundersen, 2019). The motivation behind the attack is also unknown, on the surface it appears to be for ransom money, but it's possible it was to just disrupt the company's systems (Leppänen et al., 2019).

Threats involved the system accepting false information allowing the attackers to modify files using the malware, Disruption as aluminium production and sales was halted while the automated systems were down, and usurpation as users had no control over files becoming encrypted. The malware managed to avoid detection due to being signed by the fake 'ALISA LTD' entity by Sectigo RSA Code Signing CA (Adamov et al., 2019). Financially, the attack is estimated to have cost Hydro between 550-650 million NKr (£47 million to £55.5 million[2]) in damages (Haugetraa and Molland, 2019a) with 412 million NKr (£35.18 million) in cyber insurance paid out as of December 2020 in three separate batches, or 75% of the lower-bound cost estimate of the attack (Gallin, 2019), (Gallin, 2020), (Staff, 2020). Thanks to the open response of Hydro to the attack, their stock price was barely affected, seeming to vary more due to the industry they deal in than the news around the company itself, as shown in 1.

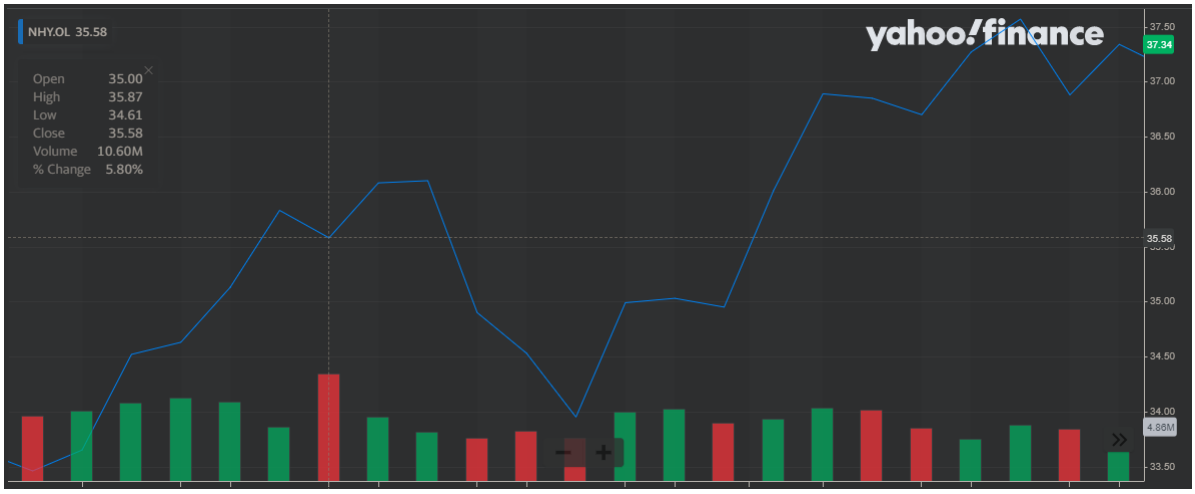

Figure 1: Stock price for Hydro before and after the attack

Reputationally, not bowing down to the attackers ransom, reporting the attack immediately, being open and keeping customers up-to-date led Lindsey (2019) to claim this resulted in a boost in the company's reputation. Not paying the ransom was also the best move ethically in my opinion, and if more companies did so, it's possible attackers wouldn't try to use ransomware in the future as it wouldn't be worth the investment. Regarding CIA, ransomware modified files, affecting integrity, and automated systems were heavily affected, impacting availability.

Regarding risk, the strategic choice of having robust cyber insurance (Haugetraa and Molland, 2019a) is excellent use of risk transfer and shows Hydro is risk adverse. Their 2018 annual report mentions that awareness of cyber security as a priority in 2018 and that employees had to complete a course in cyber security (Hydro, 2019). It's likely this led to less damage being done, though considering they were still attacked, this training likely needed reviewing. Tactically, allowing outside access to the company via Microsoft DART (briggs, 2019) allowed a quick and effective response.

I reviewed the Health, Safety, Security, Environment (HSE) (Brandtzæg, 2016) policy to find if it failed its purpose. Since it was last revised on 01 December 2016, I wouldn't consider it a living

[2]1 GBP = 11.71 NKr

document. Section four talks about accountability and how HSE culture is established through viable leadership, showing that they understand such policies must be endorsed from the top down to be effective, but there is no mention of how this policy is to be enforced. I would say that this policy failed in that it didn't cover enough information, especially regarding information security to ensure employees knew their responsibilities regarding cybersecurity. There is the possibility that further information exists in a procedure, but these aren't accessible online to the public. According toHydro (2020), an audit committee met 10 times during FY2019 however meeting agendas and minutes weren't made available to the public.

In regards to threat monitoring, Hydro admitted that there were no signs of an intrusion before their screens went black (Tomter and Gundersen, 2019). However, this could be down to the fact that the ransomware was signed, which may also explain why file entropy detection wouldn't catch the encryption of files (Shaked, 2019). According to Beaumont (2019), out of 67 security products configured on Virustotal, every result came up negative. We can find fault in Hydro's implementation of security, however. If there was an airgap between manufacturing systems and the corporate network, it is likely the impact on day-to-day manufacturing would have been severely limited, possibly only affecting sales. There is no direct evidence of a defence framework, but the quick response by Hydro showed that there likely was one in place.

5 Mitigation Processes for Yahoo!

Out of these three events, in my opinion Yahoo handled the situation the worst and would benefit the most from enhanced mitigation efforts. Their response was far too slow, even after they identified an incident it took three months for the earlier breach to be detected. I would agree with the findings of Wang and Park (2017) that Yahoo shouldn't try to use the attackers as a scapegoat but admit the truth that they didn't have the necessary security in place to prevent the attack. This could be turned into a slight positive when speaking to investors by framing the lack of security to be down to financial priorities lying elsewhere to return more revenue to them.

There are four forms of risk management that are relevant to Yahoo's situation. For avoidance, they can ensure systems are fully secure by encrypting it on the server and in transit. To mitigate, they can employ real-time countermeasures to catch attackers before they can get a large amount of data or cause widespread damage. To transfer risk, Yahoo could employ a separate company to monitor the system and look for irregularities as well as get insurance that covers data breaches and service interruption. Finally, they must accept that a company that large will be targeted and nothing can stop that from happening, only that they must rely on the other three forms to ensure an attack doesn't cause damage. According to Jones and Ashenden (2005), risk is handled by identifying assets, completing vulnerability, threat and risk assessments, and defining countermeasures. The role of the board is critical in providing this direction, but a dedicated risk manager or business unit managers can ensure that staff are well informed to deal with risk on a day-to-day basis.

Privacy violation could have been mitigated a little by simply storing less data about users. In addition, the MD5 hashes shouldn't be used to secure passwords as has been deprecated for a while. Indeed, Gibbs (2016) points to this being a tell-tale sign that Yahoo security practices were severely outdated.

The security policy in place was severely out-of-date and would need addressing – it should have a 'Last Reviewed' date if no changes were made as well as a log of changes or reasons for review. Jones and Ashenden (2005) describe how a Risk Management Policy can be used to identify risks to the business and how those risks are being controlled. The authors go on to discuss other policies that are required such as for information security, which I feel would be of great benefit for Yahoo in this case. I feel that a real-time monitoring system and threat modelling wasn't

in place during the time of the attacks, this would undoubtedly have saved Yahoo early on by alerting them that the user database was being downloaded, or that thousands of logins were being granted on one IP address. This system could also be tweaked to ensure only programs that have an identified hash can run on the system. I would recommend the NIST framework should be followed to at least tier two (NIST, 2018).

Regarding the human and social engineering aspects of the attack, training must be offered at least to all admin users of the system due to someone in that part of the company being responsible for opening the door to the attack. I would also recommend that users only log in to admin accounts when they must use admin features and be forced to log into standard user accounts when, for example, accessing emails. In Hadnagy (2011) chapter 7, the author recommends the use of a Social Engineering Toolkit (SET) to perform a test spear phishing attack to train users on what to look for, which I feel is a great method compared to an online training course many companies offer. The author goes on to lay out some mitigation steps in chapter 9 which I would also agree with, these are:

- Learn to identify what an attack looks like.
- Create personal security awareness program
- Create awareness of the value of the information being sought
- Keep software updated
- Develop scripts
- Learn from audits

6 Conclusion

In conclusion, the attacks show that signed code doesn't mean it's secure. They show that any company can be targeted and it's up to them to ensure they deal with potential threats before they happen and store their customer details securely. Also, that when things do go wrong, that the company has cyber insurance in place and are open with customers, stakeholders, and law enforcement to minimise damage.

References

Adamov, A., Carlsson, A., and Surmacz, T. (2019). An analysis of lockergoga ransomware. In *2019 IEEE East-West Design & Test Symposium (EWDTS)*, pages 1–5. IEEE.

Beaumont, K. (2019). How lockergoga took down hydro ransomware used in targeted attacks aimed at big business.

Brandtzæg, S. R. (2016). Health, safety, security, environment (hse) policy.

briggs, B. (2019). Hackers hit norsk hydro with ransomware. the company responded with transparency.

CALIFORNIA, U. S. D. C. (2019).

Chien, E. (2010). Stuxnet: A breakthrough. *Symantec.com*.

Falliere, N., Murchu, L. O., and Chien, E. (2011). W32. stuxnet dossier. *White paper, Symantec Corp., Security Response*, 5(6):29.

Forden, G. (2009). What does natanz cost?

Gallin, L. (2019). Norsk hydro claims first $3.6mn from its cyber insurance.

Gallin, L. (2020). Norsk hydro claims a further $20.2mn from its cyber insurance in q4.

GDPR (2018). Art. 33 gdpr – notification of a personal data breach to the supervisory authority.

Gibbs, S. (2016). Security experts: 'no one should have faith in yahoo at this point'.

Goel, V. (2016). Yahoo employees knew in 2014 about state-sponsored hacker attack.

Goel, V. and Perlroth, N. (2016). Verizon says yahoo hack could reopen $4.8 billion deal talks.

Green, A. (2020). If the gdpr were in effect, yahoo would have to write a large check.

Griswold, A. (2016). The stunning collapse of yahoo's valuation.

Gupta, D. (2016). Top ten alumina companies in the world.

Hadnagy, C. (2011). *Social engineering: the art of human hacking*. Wiley Publishing, Inc.

Haugetraa, L. and Molland, H. (2019a). Cyber-attack on hydro.

Haugetraa, L. and Molland, H. (2019b). Update on cyber attack april 1.

Hesseldahl, A. (2014). Yahoo to name trustycon founder alex stamos as next chief information security officer.

Hydro (2019). Hydro 2019 annual report.

Hydro (2020). Hydro 2020 annual report.

ICO (2018). Yahoo! fined £250,000 after systemic failures put customer data at risk.

Jones, A. and Ashenden, D. (2005). *Risk management for computer security: protecting your network and information assets*. Elsevier Butterworth-Heinemann.

Kamiński, M. (2020). Operation "olympic games." cyber-sabotage, as a tool of american intelligence aimed to counteract the development of irans nuclear program. *Security and Defence Quarterly*.

Krasnogolovy, V. (2019). France are looking for lockergoga ransomware developers in ukraine.

Leppänen, S., Ahmed, S., and Granqvist, R. (2019). Cyber security incident report—norsk hydro. *Procedia*.

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, 22(3):366, 380, 383.

Lindsey, N. (2019). Reputation intact despite projected cost of $75 million for norsk hydro cyber attack.

Machine, W. (2016). Yahoo privacy policy.

Menn, J., Finkle, J., and Volz, D. (2016). Yahoo security problems a story of too little, too late.

Naraine, R. (2010). Stuxnet attackers used 4 windows zero-day exploits.

NIST (2018). Framework for improving critical infrastructure cybersecurity, version 1.1. *National Institute of Standards and Technology*.

of Justice, T. U. S. D. (2018). International hacker-for-hire who conspired with and aided russian fsb officers sentenced to 60 months in prison.

of Justice, U. D. (2017).

Payvand (2010). Iran identifies sources of stuxnet virus in its computers.

Perlroth, N. and Goel, V. (2016). Defending against hackers took a back seat at yahoo, insiders say.

SECURITIES, U. S. and COMMISSION, E. (2016). Yahoo q2 2016 sec filing.

Shaked, O. (2019). Norsk hydro's lockergoga ransomware propagation detection & mitigation. *White paper, SCADAfence*.

Staff, R. (2020). Norsk hydro 3q earnings rises unexpectedly on market recovery, insurance.

Tomter, L. and Gundersen, M. (2019). It-sjefen i hydro om dataangrepet: – man tror krisen blir stor, så blir den enda verre [the it manager at hydro about the computer attack: - you think the crisis will be big, then it will be even worse](google, trans.).

Trautman, L. J. and Ormerod, P. C. (2016). Corporate directors' and officers' cybersecurity standard of care: The yahoo data breach. *Am. UL Rev.*, 66:1231.

Wang, P. and Park, S.-A. (2017). Communication in cybersecurity: A public communication model for business data breach incident handling. *Issues in Information Systems*, 18(2).

Williams, M. (2018). Ask an expert: how often should our it policies be reviewed and updated?

Yahoo (2015). Yahoo 2014 annual report.