Analyse and Discuss (50% - 1875 words – 600 each after intro)

An Analysis and Discussion on Cyber-Attacks

Introduction: As more of the world moves online and companies collect more data about us, the threat of this data being stolen and / or the companies involved having their services disrupted becomes a more credible risk. In this essay, I will be analysing the attacks on Yahoo! in 2013 and 2014, the threat posed by Stuxnet and the recent breach of Norsk Hydro in 2019, as well as exploring what process I would choose in order to mitigate [XX].

Yahoo!: Balancing between Security and Retention

Outline

What is the incident?	• Two incidents, 2013 + 2014. • Both data breaches.
When did it happen?	• The first announced breach, **reported 22 September 2016**, had occurred sometime in **late 2014**, and affected over 500 million Yahoo! User accounts. Yahoo were aware of the intrusion in 2014 but didn't understand the extent until they were investigating an earlier breach, despite them claiming on 9 September that they were not aware of any earlier security breaches or "loss, theft, unauthorized access of acquisition" of user data. • A separate data breach, occurring earlier around **August 2013**, was **reported in December 2016**. Initially believed to have affected over 1 billion user accounts, Yahoo! Later affirmed in October 2017 that all 3 billion of its user accounts were impacted. wikipedia . • PRC (Privacy Rights Clearinghouse). (2017). Data breaches. Retrieved from https://www.privacyrights.org/databreaches • The public was made aware of Yahoo account names and passwords being sold from the 2013 breach in **July 2016**. wikipedia.
Who was the target?	• Yahoo
What was Taken / Damaged / Accessed / Stopped etc?	• 2013: One billion, email addresses, telephone numbers, dob, hashed passwords (some minority poorly, with MD5). Some encrypted and unencrypted security questions and answers. Data from this hack was found by InfoArmor to be sold on the dark web for $300K in August 2015, it was sold twice to spammers and once to a buyer asking if details of 10 specific US and foreign government officials were on the list. • 2014: 500 Million accounts targeted for the same information as in 2013. 32 Million accounts accessed. • Breach led to 80 non-Yahoo! accounts of specific targets being breached too.
Vulnerability	• System appeared to authenticate user based on cookie, exploited by modifying cookie to pose as another user without supplying a password.
Threats (Disclosure, Deception, Disruption, Usurpation)	• Disclosure (unauthorised access to data): Attackers got access to any account they wished, as well as the internal administration system at Yahoo • Deception (Acceptance of false information): Attackers tricked authentication servers into thinking they are authorised to view account information via forged cookies. • Disruption (Interruption of the service): None • Usurpation (Loss of control of the service): Although not evident to users, the attackers had enough control over the system that they were able to make changes to the English version of Yahoo search results to ensure that searches for erectile dysfunction medication produced a link to a fraudulent site the attackers controlled, then on to a legitimate website which paid commission to sites that drove traffic to itself, generating revenue for the attackers.

Threat actors	• Unknown in both instances but Yahoo believes it was the same attacker on both events. • Yahoo! claimed the 2014 breach was state-sponsored but did not name a country. Actor no longer in system by Sep 16 (lol). FBI investigated. Government agreed that it was a foreign state, likely Russia. • Some guess at China or Russia, others doubt it was a state actor at all. • Attack was similar to other Russian breaches. • F-Secure declared China to be their top suspect. • Doubters say it would be less embarrassing to Yahoo! to attribute the attack to a Nation State since they were in the middle to an acquisition. • However they are a large target. • InfoArmor – Reported they believed it was an Eastern European criminal gang that sold the info on to others. Likely related to 'Group E' who broker stolen data on the dark web, as they were the ones initially selling the data from what we understand. This was then picked up by 'Peace' who sold it on further. They commented that the breaches "opens the door to significant opportunities for cyber-espionage and targeted attacks" • FBI later charged 4 men, two that work for Russia's Federal Security Service. FBI also stated they were likely facilitated by the FSB. One of the 4 (Karim Baratov) was arrested and later admitted to hacking into at least 80 email accounts on behalf of Russian contacts.
Attack Pattern / Domain (Human Error, Privilege Misuse / abuse, cyber espionage, lack of training) CAPEC	• CAPEC-163 – Spear Phishing. Human error in getting phished. • CAPEC-633: Token Impersonation. Minted authentication Cookies. • State and corporate espionage. • https://capec.mitre.org/

Motivations	• Targeted to find information on specific people, such as government employees and employees of companies of interest to the attackers:
	  • users affiliated with U.S. online service providers, including but not limited to webmail providers and cloud computing companies
	  • Russian journalists and politicians critical of the Russian government
	  • Russian citizens and government officials
	  • former officials from countries bordering Russia
	  • U.S. government officials, including cyber security, diplomatic, military, and White House personnel
	  • https://www.justice.gov/opa/press-release/file/948201/download page 10.

Malicious / Accidental	• Malicious, targeting specific users.
Attacker skills	• Reasonably skilled, likely state funded.
Attack Vectors	• 2013: Possibly forged cookies, not sure at first. • 2014: cookie-based attack allowing attacker to authenticate as any other user without supplying a password. • Spear-Phishing attack on Yahoo employee where malware was installed to allow attackers backdoor access to the internal account management systems. • Nov-Dec 2014, User Database backup was stolen.

	• Oct 2014 – Nov 2016, user account information obtained by minting cookies both within and outside yahoo's network • Externally-minted cookies required a key unique to the account they were targeting (called a nonce), which was found in the User Database. 6.5K+ accounts were directly accessed in this way. • https://www.justice.gov/opa/press-release/file/948201/download
How much trust was there in the company before the attack?	• Yahoo had one of the largest userbases of any site in the world due to its age and the companies it had merged with over the years. Most people probably felt their data was safe with them. • Company had accounts for many older people or those that are not tech-savvy that might not necessarily think that there's a problem keeping their details on their yahoo account and would assume it was safe by default, as if they filed the information away themselves.
Impact on Company / Customers / Other	• Company: • Principle Lawyer Ronald S. Bell, quit by March 2017. • CEO Marissa Mayer bonus for 2016 and 2017 was pulled. She later quit in June 2017 after the sale of the majority of Yahoo to Verizon. • Customers: • Could be unaware that beaching Yahoo account also puts Flickr, Sky and BT accounts at risk due to merged accounts with these services. • Other:
Financial Impact	• Verizon's buyout of the majority of Yahoo! started in July 2016, shortly before the first announcement of a breach. They were not aware of the breach until two days before the public announcement. Initial price was $4.83B. Verizon looked to change the terms. After the second breach announcement, in Feb 2017, the deal was announced to go forward but the price dropped to $4.48B, a drop of $350M or 7.25%. • Company was not in a great financial situation before the attacks, their value had been in decline for years. Peaked at around $110B in the dotcom boom, recovered to between $60-90B after, was worth $30B in 2013 when cyber changes were proposed. https://qz.com/741056/the-stunning-collapse-of-yahoos-valuation/ • Eventually fined $35M for failure to disclose breach in a timely manner by US Securities and Exchange Commission (SEC). https://www.sec.gov/news/press-release/2018-71 • 23 Lawsuits, one mentions "intrusion into personal financial matters", another claims yahoo acted with gross negligence in dealing with the breach. • 5 lawsuits were combined into a Class Action Lawsuit in December 2016. Verizon and Altaba split the cost of an eventual $117.5 Million settlement in April 2019. • Wikipedia claims a second lawsuit was filed but no evidence of this case exists. • UK Information Commissioner's Office (ICO) fined £250K https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/06/yahoo-fined-250-000-after-systemic-failures-put-customer-data-at-risk/
Reputational Impact	• 90% of the twitter comments about yahoo were negative in October 2016, up from 68% in August. https://www.nytimes.com/2016/10/14/business/dealbook/verizon-says-yahoo-hack-could-reopen-4-8-billion-deal-talks.html

Ethical Impact	•
Relation to CIA	• Confidentiality - Prevent unauthorised access to sensitive information: Broken due to unauthorised users gaining access to user profiles. • Integrity- Prevent data being modified: Minimal effect. Although attackers would have had access to user profiles, Data integrity was breached through modification of search results on Yahoo for erectile dysfunction searches, forwarding users who click the top result through a server owned by the attackers in order to receive clickthrough commission. https://www.justice.gov/opa/press-release/file/948201/download • Availability - Accessibility of system to authorised users: No effect.
How long did it take to be identified? Incidence response team?	• Forever, lol. Almost 2 years before the later one was announced, and over 3 years had passed between the first hack happening and being announced. • US Senators demanded to know why it took so long to disclose the breach to the public. • SEC asked to investigate if Yahoo fulfilled their obligations under federal securities laws to properly disclose the attack and if the disclosure regime was adequate.
What was their response?	• Invalidated all previous cookies • Eventually implemented improved security features • Company was criticized for its delay • Did not force affected users to change their passwords as they thought it would drive users away from the service. • Counter argument: Yahoo spokeswoman, Suzanne Philion, said the company spent $10 million on encryption technology in early 2014, and that its investment in security initiatives will have increased by 60 percent from 2015 to 2016. https://www.nytimes.com/2016/09/29/technology/yahoo-data-breach-hacking.html
How could the response be managed better? Mitigation notes.	• Be faster in responding • Faster in deploying security updates
Misc References / Info	• https://en.wikipedia.org/wiki/List_of_data_breaches • "Yahoo Discloses New Breach of 1 Billion User Accounts". The New York Times. • McMillan, R., & Knutson, R. (3 October 2017). "Yahoo Triples Estimate of Breached Accounts to 3 Billion". The New York Times. • Class action lawsuit settlement • Wang, P., & Park, S. A. (2017). COMMUNICATION IN CYBERSECURITY: A PUBLIC COMMUNICATION MODEL FOR BUSINESS DATA BREACH INCIDENT HANDLING. Issues in Information Systems, 18(2). • Roumeliotis, G. & Toonkel, J. (2016) Yahoo under scrutiny after latest hack, Verizon seeks new deal Terms. • Yahoo has confirmed a data breach with 500 million accounts stolen, as questions about disclosure to Verizon and users grow (vox) • Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach • https://gdpr-info.eu/art-33-gdpr/ 72 hour limit for disclosure

Risk

Strategic Risk "Risks that threaten to disrupt the assumptions at the core of an organization's strategy" Set by the board.	• Prior to the attacks in 2013, Yahoo was warned that they were a target for state-sponsored hackers but they took a year before hiring a Chief Information Security Officer. https://www.vox.com/2014/2/28/11624050/yahoo-to-name-trustycon-founder-alex-stamos-as-next-chief-information • They then didn't fund security upgrades, so the CISO quit by 2015, possibly around the same time the company was being attacked (because they didn't pay for the security improvements). • Internal review found CEO and other executives knew of the intrusions but failed to inform the company or attempt to prevent further breaches. • 2014 Annual report mentioned cyber attack is a possibility but labelled it as "something we have little to no control over" alongside natural disasters and political unrest. IMO it doesn't look good to simply accept the risk of any and all cyber attack like that. • They accept their systems are vulnerable to viruses and other disruptions despite their "implementation of security measures" and wouldn't be able to promptly address attacks if they weren't detected. At least they're honest here, they didn't even mention that their security measures were adequate. Almost as if they knew an attack like this would happen sooner rather than later. • There is no mention of how the threat of such attacks is being avoided, mitigated or transferred beyond the mention of implemented security measures. • https://www.annualreportowl.com/Yahoo/2014/Annual%20Report?p=27 • Vulnerability Level: Vulnerable /~~ Reactive / Compliant / Proactive / Optimized~~
Tactical Risk "Chance of loss due to changes in business conditions on a real time basis"	• Yahoo's failure to respond to the initial attack despite knowing about it constituted to taking a tactical risk.
Operational Risk "Potential for losses due to uncertainty" User awareness	• There was no threat monitoring in place to instantly pick up on the attack, constituting to an operational risk.
Managing Risk Was the company risk adverse or did they welcome risk	• Appeared to welcome risk, as they had a seemingly lax attitude to security, was slow to implement new security features. • Did not give funding to the security team to implement their recommended security measures. • As an established company, they should have been more risk adverse. However, their financial situation likely made them more welcome to risk in order to get the company back to the market cap it was at 15 years previously.
How could the risk be handled better? Traceable, Auditable, Relevant, Rigorous. Support structure?	• Avoidance (High Freq, High Impact): Ensure systems are fully secure and data is encrypted. • Mitigation / Reduction: (High Freq, Low Impact) Employ countermeasures to look for unusual network activity and catch attackers before they can get a large amount of data or cause widespread damage.

Support from the top? Risk Assessments? Mitigation section notes.	• Transfer: (Low Freq, High impact) Employ a separate company to monitor the system and look for irregularities. Get insurance that covers data breaches and service interruption. • Acceptance: (Low Freq, low impact) Accept that a company that large will be targeted and nothing can stop that from happening.
References / Info	ACCA - Strategic and Operational Risks Tactical Risks

Privacy

How was privacy broken?	• Yahoo failed to secure their customer's data on numerous occasions.
Was there specific information leaked due to this attack (deanonymisation)?	• It is suspected that the attackers were going after information on specific users but found an exploit that allowed them to gather data from every account. Somebody that was looking to buy the data specifically asked for certain names.
Was the company found to be in breach of privacy legislation? ECHR?	• Yes, UK branch was fined £250,000 by the ICO due to breaking the Data Protection Act (1998), which was the legislation in place at the time of the attack. The fine covered the 515,121 UK-based accounts that were within the breach. Yahoo! fined £250,000 after systemic failures put customer data at risk. (2018, June 12). Retrieved November 25, 2020, from. Yahoo! were fortunate that GDPR was not in place at the time, as they would then need to pay $90M+ to the EU, or $268M post Verizon acquisition. Green, A. (2020, June 20). If the GDPR Were in Effect, Yahoo Would Have to Write a Large Check. Retrieved November 25, 2020, from
What data was being collected that didn't need to be (and was subsequently leaked)?	• It could be argued that the company did not need to collect telephone numbers and dates of birth but did so anyway. The act of taking this data isn't wrong per-se, and certainly isn't illegal to do, but by taking it and not storing it encrypted, they leave themselves open to losses from attacks such as these. Indeed, the Chief Information Security Officer at the time, Alex Stamos, pressed Yahoo! to adopt end-to-end encryption (NYT, 2016). It could be argued, however, that encryption on the servers or the data in-transit would not protect the end-user if the attackers could directly access the account via the cookie exploit.
What could've been done to stop privacy being violated? Mitigation notes.	• Store less data. • MD5 hash shouldn't be used. "Jonathan Care, research director at analysts Gartner, said: "MD5 hashing is vulnerable to an attack type called 'collision attacks' which means that an attacker can find a string of characters that will resolve to the same hash as a hashed password. MD5 is strongly deprecated and this points to troubling software development security practices in Yahoo or its suppliers."" https://www.theguardian.com/technology/2016/dec/15/security-experts-yahoo-hack
References / Info / Further notes	

Security Policies

What security policies were in place? Why did they fail? Master policy, change management, physical security, email, encryption, vulnerability management, media disposal, data retention, acceptable use, access control, information security, incident response, remote access, disaster recovery, business continuity plan	Only able to find one policy (Privacy) and the Software License Agreement, which is undated. We're able to use the Wayback Machine to see what privacy policy was in place at the time of the attack and how it was updated since. • **Policy:** Privacy • **Living Document:** No, the policy in place at the time of the attack was last updated 13 May 2011. It was next updated after the attack was disclosed, on 8 May 2017, but this only changed the contract address at the bottom. There was another update that occurred on 13 June 2011, but this only changed the update date, bizarrely. Many security analysts, including IT consultancy firm Pensar recommend reviewing policies at least annually (Williams, M. 2018). • **Unambiguous:** Not really, uses technical language (IP Address, Cookies) and is written in a more "legalese" way which makes it harder to understand. Does not specifically state the companies they work with, only 'trusted partners'. Only mentions they have safeguards that comply with the law to protect personal information (but clearly that wasn't enough). • **Realistic**: Yes, rules don't make it difficult to use the service. • **Enforceable**: Does not list how they enforce the policy. • **Inclusive**: Does include separate parts for children. • **Endorsed**: No, the CEO was found to actively work against the security team. • **Attainable**: Yes, but the policy doesn't really state much anyway. • **Why failed? Issues with Policy or people following policy?** 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.
Integrity Policy violated?	• Users wrote their own programs? Not that we're aware • Programmers testing on production? Not tested correctly? N/A • Dev program incorrectly installed on Production? Yes, malware installed via compromised employee account. • Installing to production was not controlled and / or audited? N/A • No access to logs for managers and auditors? N/A
Was a security policy audit carried out after?	• No evidence of an audit found. This could be due to finances.
Was there a User Agreement / EULA? Was it violated?	• Only Software license agreement. Wayback Machine only has page from December 2015 which could not be retrieved. Software License Agreement does not have a date for when it was last modified or reviewed. Nothing specifically mentioned about cookies. • Section 1.2 (iii) mentions not to use the software in an unlawful manner, which was violated when the attackers gained access to the system, stole the user database and minted cookies using yahoo's internal tools. • Section 1.2 (vi) mentions not to derive income from the software. This was violated as the attacker used access to the system to sell account details to the FSB agents for $100 per account. • https://policies.yahoo.com/ie/en/yahoo/terms/product-atos/toolbar/index.htm
Conformed to Biba Model for data integrity? Bell-LaPadula Model?	• Biba – No read down, no write up, no lower process requesting access: N/A • Bell-LaPadula – No read up, No write down, DAC specified with access matrix: N/A

What should be included in the security policy to stop it happening again? Mitigation notes.	• Models: Bell-LaPadula / Biba / MAC / DAC Elements of a security policy: • Overview + Purpose – what constitutes success: • Scope – what was covered (people/infrastructure): • Policy – Rules and consequences: • Compliance – Who's monitored, what privacy is provided: Why is policy referring to office in India? Should also have a Last reviewed date if no changes were made. A log of changes or reasons for review would be good, too.
References / Info / Further notes	https://blog.eduonix.com/networking-and-security/learn-different-types-policies-procedures-cissp/ Yahoo! Privacy Policy, Updated 13 May 2011, retrieved 9 Jan 2016 Williams, M. (2018) Ask an expert: how often should our IT policies be reviewed and updated?

Threat Monitoring

Was threat monitoring in place? Real time?	• No evidence of a large-scale threat monitoring system in place which is backed up by the fact that Yahoo did not know customer details had been taken until long after the attackers were gone.
What detection methods? SIEM (QRadar, Splunk) / Threat Intelligence Provider / Traffic analysis Framework / Dissassmbler / Proxy / Cyber Platform / IDS (Cisco AMP) / SOAR / SIRP / Logging	• None
Cyber Killchain (Lockheed Martin)	• Reconanisance: • Weaponisation: • Delivery: • Exploitation: • Installation: • C+C: • Actions on Objectives:

Defence Framework? Identify, Protect, Detect, Respond, Recover.	• NIST framework likely not followed as there was no real-time monitoring in place. Their implementation barely even corresponds to Tier 1 on the NIST framework implementations, as their response appeared ad-hoc and the organization did not collaborate with or receive information from other entities. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
Thread Modelling Framework? Define – Diagram – Identify – Mitigate – Validate – Define. P.A.S.T.A, STRIDE, TRIKE?	• Doesn't appear to have been in place.
Efficiency Statistics? MTT detect, respond, contain, eradicate	• N/A
Was threat modelling used? What type, how? If not, would one have helped? How?	• No. Yes it would have helped in catching the exploit as it started, meaning either the attackers would have been stopped before they took any information at all, or they would've taken the bare minimum.
Was a system implemented or changed after the attack? What lessons were learned? Bespoke threat monitoring approach? Mitigation notes.	• Requires real-time monitoring • Detection methods that could be used etc • Follow NIST framework to at least tier 2. • Threat modelling https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html • Automated systems? • Should have detected multiple users logging in from one place. (IP/Machine) Likely was recommended but would never have been implemented due to C-suite objections. (resulted in cyber guy leaving • Threat modelling would have helped in catching the exploit as it started, meaning either the attackers would have been stopped before they took any information at all, or they would've taken the bare minimum.
References / Info / Further notes	

Human Aspects

Usability? Learnability, Efficiency, Memorability, Errors, Satisfaction.	• Cookies were used to make the user experience a little easier meaning they wouldn't need to log in every session but opened the door to this exploit.
Employees bypassed security systems?	• No

Too confusing, clumsy, hard to remember passwords, security too complex, too much technical terminology, forcing uninformed decisions on users, user using easy-to-hack password.	
Insider? If so, detail why they did it. Role-based detection in place?	• A malicious insider was never identified, but an accidental insider allowed attackers access to the system.
What could be done to mitigate the human aspects? Reduce cognitive load, make state visible, give informed feedback, design to not reduce performance. Mitigation notes.	• An argument could be made for restricting the use of cookies but in reality this isn't feasible since users would quickly abandon the service if they had to log in every time they opened the page. The only real way to get around this would've been to ensure the exploit was never useable in the first place by disallowing multiple logins from the same address, or monitoring for such.
References / Info / Further notes	

Social Engineering

What techniques were used? Office visitors, Evesdropping, shoulder surfing, dumpster diving? Phishing (all types) catfishing? Social media?	• Initially thought to be remote, but FBI indictment mentioned that Spear Phishing was used to get an administrator in the company to install malware to give the attackers a backdoor into the system. This later allowed the attackers to use yahoo's Account Management Toolwell as minting cookies. • These attacks seemed to be specifically targeted towards a number of • UNITED STATES OF AMERICA V. DMITRY DOKUCHAEV, IGOR SUSHCHIN, ALEXSEY BELAN, and KARIM BARATOV
Was a framework used? Information gathering, elicitation, pretexting, mind tricks, influence	• It's not understood what framework was used exactly, but it's clear from the thousands of accounts that were specifically targeted that information gathering was at the core of the operation.
What could have been done to mitigate the	• Get employees to understand not to install programs on company machines • Use real-time monitoring to ensure only programs that have an identified hash run on the system.

threat of social engineering? Mitigation notes	
References / Info / Further notes	

Stuxnet – The Dawn of Cyberwarfare

Outline

What is the incident?	• Worm designed to infect Windows machines and target Siemens Step7 software control software to look for specific Programmable Logic Controllers (PLCs) connected to the system, specifically targeting PLCs that run motors spinning a specific speed, which is the same motor speed used to turn centrifuges which enrich uranium. The malware included in the worm then modifies the rotation speed of the motor to cause damage to the centrifuge components and hides these speed changes from monitoring software. Stuxnet: A Breakthrough • Specifically targeted to a certain program running certain controllers running certain motors.] • Later considered the first significant
When did it happen?	• Found in June 2010, likely worked on since 2005 and activated March-April 2010, though a variant appeared in June 2009.
Who was the target?	• Five domains in Iran across three waves from 22 June 2009 to 14 April 2010. Domains unknown. 12,000 infections. W32 Stuxnet dossier. P7-11 • Likely endpoint target was the uranium enrichment centrifuges at the Natanz nuclear facility in Iran. • Part of operation Olympic Games
What was taken / Damaged?	• Worm infected 200,000 computers, damaged 1000 machines Sheep dip your removable storage devices to reduce the threat of cyber attacks and ruined almost 1/5 of Iran's nuclear centrifuges. The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought. Was only spread via USB sticks and local networks.
Vulnerability	• Exploited four zero-day flaws to spread through Windows machines Stuxnet attackers used 4 Windows zero-day exploits. • Server Service (patched in MS08-067), • LNK flaw (MS10-046), • print spooler (MS10-061). Two Elevation of privilege holes not previously disclosed, • later found to be via keyboard layout file (CVE-2010-2743, fixed with MS10-073) https://www.welivesecurity.com/2010/10/15/win32k-sys-about-the-patched-stuxnet-exploit/ • and via Task Scheduler (CVE-2010-3338, fixed with MS10-092) • https://www.zdnet.com/article/attack-code-published-for-unpatched-stuxnet-vulnerability/ https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-044.pdf stuxnet dossier
Threats (Disclosure, Deception, Disruption, Usurpation)	• **Disclosure** (unauthorised access to data): Yes, in this attack the worm gets access to data coming from PLCs connected to the system. In addition, the attackers also had access to the private keys for digitally signing drivers from JMicron and Realtek Symantec w32 Stuxnet Dossier (which were later revoked. Source). • **Deception** (Acceptance of false information): Yes, the payload tricks the computer into thinking it's harmless, and the payload itself masked what it was doing to the motors by sending back false readings to the monitoring software. • **Disruption** (Interruption of the service): Yes, Stuxnet was designed to cause damage to centrifuges and interrupt the enrichment of uranium, causing downtime while engineers replaced them. • **Usurpation** (Loss of control of the service): Yes, by taking control of the system and remaining even after equipment was replaced, Stuxnet was well designed to take control of the system it was designed to attack. • https://ieeexplore.ieee.org/abstract/document/5772960

Threat actors	• Linked to Equation Group, as they used two of the same zero-day exploits. • Ilias Chantzos, director of government relations at Symantec, estimated the manpower required to develop Stuxnet to have been 5 to 10 people working for six months with access to SCADA systems (step7). - Lessons from Stuxnet
Attack Pattern / Domain (Human Error, Privilege Misuse / abuse, cyber espionage, lack of training) CAPEC.	• CAPEC-233: Privilege Escalation – both disclosed and undisclosed. - W32 Stuxnet Dossier pg2. • CAPEC-442: Infected Software – Malware + worm • CAPEC-74: Manipulating State – Hardware • CAPEC-167: White Box Reverse Engineering – Likely had access to step7 system for probing (see above). • CAPEC-457: USB Memory Attacks – Possibly intentional if insider (Symantic w32 Stuxnet Dossier). • CAPEC-641: DLL Side-Loading – dossier pg17 • CAPEC-203: Manipulate Registry Information – dossier p17 • CAPEC-242: Code Injection – into services.exe to infect removable drives and Step7 software to infect Step7 projects. • CAPEC-206: Signing Malicious Code - MrxNet.sys load driver, signed by Realtek dossier p13
Motivations	• Symantec say Stuxnet is a threat targeting a specific industrial control system likely in Iran, such as a gas pipeline or power plant. The ultimate goal of Stuxnet is to sabotage that facility by reprogramming programmable logic controllers (PLCs) to operate as the attackers intend them to, most likely out of their specified boundaries. W32 Stuxnet Dossier pg2. • In Stuxnet: the emergence of a new cyber weapon and its implications, the authors plainly lay out that the worm was specifically designed to sabotage the Iranian nuclear program by targeting industrial control systems
Malicious / Accidental	• Malicious and targeted, all features of Stuxnet were intentionally designed to affect specific software and hardware.
Attacker skills	•
Attack Vectors	• The creators knew that its target wouldn't be reachable through the Internet. Thus, the initial infection vector was via a removable flash drive. • If Vista/7/Server 2008 R2, Task Scheduler vulnerability. • If XP/2000, local privilege escalation MS10—073.
How much trust was there in the company before the attack?	• You would expect a nuclear facility to be safe.
Impact on Company / Customers / Other	• Company: Natanz nuclear facility was said to have lost over a thousand centrifuges, 20% of the total on site. • Customers: N/A • Other: This was the first suspected case of cyberwarfare. Fears were raised as to whether this could count as an act of war and whether Iran would choose to respond with an attack of their own against US installations and troops in Iraq and Afghanistan. Fortunately, I could not find evidence of any physical counterattack in response to Stuxnet, but a DDoS attack on US Banks in 2012 was linked to Iran and assumed to be a retaliatory move by the nation state. https://www.justice.gov/opa/file/834996/download
Financial Impact	• Cost to replace the IR-1 centrifuges estimated at $20,000 each, so over $20,000,000 in total, though this is only a very rough estimation due to the fact that the centrifuges are manufactured within Iran, with no information being given to the outside world. https://www.armscontrolwonk.com/archive/302363/what-does-natanz-cost

Reputational Impact	• Showed that the Iranian nuclear program could be slowed by means other than diplomacy or direct military intervention.
Ethical Impact	• Opened the gates to cyberwarfare across the world. With no rules to govern cyberwarfare, it's only time before equipment more critical to human life is targeted. Effective cyber attacks by such nations [as Iran and North Korea] on critical infrastructure could create significant problems – Stuxnet and the future of cyber war. P35-36
Relation to CIA	• Confidentiality - Prevent unauthorised access to sensitive information: Realtek failed here, they lost access to their driver signing key. Information on the system seems to not have been the target, and no significant information seems to have been collected by the C+C server in the main attack, though it was theorised that earlier breaches allowed hackers to see what software and hardware was in use at the plant. Duqu worm? • Integrity- Prevent data being modified: Malware modified a large amount of systems. • Availability - Accessibility of system to authorised users: Access to the system as a whole was not interrupted for authorised users but availability of the enrichment system to do the job it was required to do was impacted.
How long did it take to be identified? Incidence response team?	• Approximately one year, June 2009 to June 2010 - W32.Stuxnet Dossier • Detected by a malware detection firm in Belarus. https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet
What was their response?	• See above
How could the response be managed better? Mitigation notes.	• Hard to say.
Misc References / Info	Stuxnet and the Future of Cyber War Stuxnet: Dissecting a Cyberwarfare Weapon

Risk

Strategic Risk "Risks that threaten to disrupt the assumptions at the core of an organization's strategy"	• Due to this being a very sophisticated attack, it is hard to find blame at the strategic level. • The sophistication in this attack shows that there were no easy attack vectors, so defence was likely quite high. • Officials at the Natanz plant would know that the risk of being attacked somehow was high, and so security was baked into the site from the beginning. For instance, although the site isn't as physically secure as the nuclear plant at Fordow, Iran, the main chamber is still 20m underground and reasonably well hidden. It is also protected by anti-aircraft guns. https://uk.reuters.com/article/us-iran-nuclear-strike/iran-nuclear-sites-may-be-beyond-reach-of-bunker-busters-idUSTRE80B0WM20120112 • There was no hint beforehand that an attack like this could or would be carried out, therefore there was no way for officials to estimate how to counter it.

	• The only weak link was that it's possible there was an insider that leaked information about the system and allowed the plant to be infected via USB stick, though the related attacks on other sites show this might not be the case. If this was true, however, officials could be found to be liable for not compensating engineers enough. • Vulnerability Level: ~~Vulnerable / Reactive~~ / Compliant /~~ Proactive / Optimized~~
Tactical Risk "Chance of loss due to changes in business conditions on a real time basis"	• The systems that were attacked were appropriately air-gapped to ensure attacks would not come from online, and that information about the plant's systems could not get out. • 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 wasn't right when the centrifuges started breaking en-masse and their computers were saying the centrifuge was running normally when it was actually going slow.
Operational Risk "Potential for losses due to uncertainty" User awareness	• The attack didn't target known exploits that could be countered by keeping software up-to-date. • However, since somebody eventually plugged in an infected USB memory stick into a critical computer, this could be a failure of user awareness. • We have to understand, however, that with an air-gap, the only way to get information off of the internal machine or deliver updates to software on the machines is via USB key, and if the machine in the plant on the other side of the air gap was infected, there would be no way for our user to do these tasks safely.
Managing Risk Was the company risk adverse or did they welcome risk	• All of the above showed there was a lot of risk adversity at the plant, which is to be expected of such a critical site.
How could the risk be handled better? Traceable, Auditable, Relevant, Rigorous. Support structure? Support from the top? Risk Assessments? Mitigation section notes.	• Avoidance: • Mitigation: • Transfer: • Acceptance:
References / Info	ACCA - Strategic and Operational Risks

Privacy

How was privacy broken?	• N/A
Was there specific information leaked due to this attack (deanonymisation)?	• Not of people, no.

Was the company found to be in breach of privacy legislation? ECHR?	• No.
What data was being collected that didn't need to be (and was subsequently leaked)?	• No.
What could've been done to stop privacy being violated? Mitigation notes.	• N/A
References / Info / Further notes	

Security Policies

What security policies were in place? Why did they fail? Master policy, change management, physical security, email, encryption, vulnerability management, media disposal, data retention, acceptable use, access control, information security, incident response, remote access, disaster recovery, business continuity plan	• Although we have no access to the policies at Natanz, we can say that since a security policy involving use of systems at the plant, and/or regarding physical media use was broken when a USB stick clearly from outside of the plant, was inserted into a machine on the secure side of the air gap. This would be assuming this was in a policy to begin with, which I shall considering how complex the exploit had to be in the first place. • This policy could likely have been broken due to it being easier for the user to extract information from the system or put information into the system via usb stick than using any other method. The security policies in place should have stated that outside memory sticks were not allowed and staff and visitors should be supplied with what they need.
Integrity Policy violated?	• N/A
Was a security policy audit carried out after?	• No idea.
Was there a User Agreement / EULA? Was it violated?	• None known of.

Conformed to Biba Model for data integrity? Bell-LaPadula Model?	•
What should be included in the security policy to stop it happening again? Mitigation notes.	• Models: Bell-LaPadula / Biba / MAC / DAC Elements of a security policy: • Overview + Purpose – what constitutes success: • Scope – what was covered (people/infrastructure): • Policy – Rules and consequences: • Compliance – Who's monitored, what privacy is provided: •
References / Info / Further notes	https://blog.eduonix.com/networking-and-security/learn-different-types-policies-procedures-cissp/

Threat Monitoring

Was threat monitoring in place? Real time?	• This would be expected. It's possible previous attacks were caught by a threat monitoring system, which would account for why zero-day exploits were required in Stuxnet.
What detection methods? SIEM (QRadar, Splunk) / Threat Intelligence Provider / Traffic analysis Framework / Dissassmbler / Proxy / Cyber Platform / IDS (Cisco AMP) / SOAR / SIRP / Logging	• N/A
Cyber Killchain (Lockheed Martin)	• Reconanisance: Extensive, the attackers clearly knew the system inside-out, down to the software and hardware controllers used. • Weaponisation: Multiple zero-day exploits. • Delivery: Via USB due to air gapped systems. • Exploitation: Possible insider, but multiple previously-unknown vulnerabilities. • Installation: Automatic. • C+C: Existed only to update the malware and retrieve basic information from outside the air gap. Dossier p5. • Actions on Objectives: All automated, executed when the worm discovered it's on a computer running Step7.
Defence Framework?	• N/A

Identify, Protect, Detect, Respond, Recover.	
Thread Modelling Framework? Define – Diagram – Identify – Mitigate – Validate – Define. P.A.S.T.A, STRIDE, TRIKE?	• Unknown.
Efficiency Statistics? MTT detect, respond, contain, eradicate	• Unknown
Was threat modelling used? What type, how? If not, would one have helped? How?	• Probably, for same reasons as above.
Was a system implemented or changed after the attack? What lessons were learned? Bespoke threat monitoring approach? Mitigation notes.	• • Blockchain? • Automated systems? • Robust algorithm for attack detection based on time-varying hidden Markov model subject to outliers
References / Info / Further notes	

Human Aspects

Usability? Learnability, Efficiency, Memorability, Errors, Satisfaction.	•
Employees bypassed security systems? Too confusing, clumsy, hard to remember passwords, security too complex, too much technical terminology, forcing uninformed	• Possibly. An infected USB stick was used on the air-gapped systems somehow, though the employees could have been following standard procedure and Stuxnet could have passed onto that memory stick from elsewhere on the open side of the air gap.

decisions on users, user using easy-to-hack password.	
Insider? If so, detail why they did it. Role-based detection in place?	• The possibility remains, see above.
What could be done to mitigate the human aspects? Reduce cognitive load, make state visible, give informed feedback, design to not reduce performance. Mitigation notes.	• ..
References / Info / Further notes	

Social Engineering

What techniques were used? Office visitors, Evesdropping, shoulder surfing, dumpster diving? Phishing (all types) catfishing? Social media?	• Office visitors - 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. http://www.payvand.com/news/10/oct/1169.html . If this is taken as referring to IAEA nuclear inspectors than this would explain how Stuxnet moved around systems over Iran and elsewhere in relatively short time when the worm itself only uses USB and local networks as a transmission medium.
Was a framework used? Information gathering, elicitation, pretexting, mind tricks, influence	• unknown
What could have been done to mitigate the threat of social engineering? Mitigation notes	• n/a
References / Info / Further notes	

Norsk Hydro Ransomware Attack – Assurance and Insurance

Outline

What is the incident?	• LockerGoga Ransomware attack.
When did it happen?	• 19 March 2019, around midnight AM CEST screens went black.
Who was the target?	• Norsk Hydro (aka Hydro). As of 2016 Hydro was understood to be the seventh largest aluminium company in the world with a global production of 6.5M mt of products in 2015. https://www.alcircle.com/news/top-ten-alumina-companies-in-the-world-26529
What was taken / Damaged?	• Whole global operation hit, with Extruded Solutions having suffered the most significant operational challenges and financial losses. • Other areas able to keep up production manually rather than using automated systems. • https://www.hydro.com/en-GB/media/on-the-agenda/cyber-attack/ •
Vulnerability	• Attackers spent up to three weeks infiltrating Active Directory, a system for managing Windows computers, and installing LockerGoga. • https://www.nrk.no/norge/it-sjefen-i-hydro-om-dataangrepet_-_-man-tror-krisen-blir-stor_-sa-blir-den-enda-verre-1.14515043 • They have found 4 variants of the virus, numbered 1200, 1510, 1440 and 1320 •
Threats	• **Disclosure** (unauthorised access to data): Data doesn't appear to have been taken, only encrypted by LockerGoga. Attackers did have some form of remote access to the system, however. • **Deception** (Acceptance of false information): Once the attackers had access, the system allowed them to freely modify files on the system through the LockerGoga virus. • **Disruption** (Interruption of the service): Major threat, aluminium production was heavily affected while the automated systems were down. • **Usurpation** (Loss of control of the service): Yes, no control over parts of the system being encrypted in the attack. The original service that was attacked was permanently lost, and a new system was built in its place.
Threat actors	• Unknown, only that different versions of the same malware was used in other attacks just two weeks before this, against the companies Hexion and Momentive. https://www.scadafence.com/norsk-hydros-lockergoga-ransomware-propagation-detection-mitigation/ • One source reports that the French police are in contact with the National Police of the Ukraine to look for four suspects in connection with the development of LockerGoga, however the source of this article could not be retrieved either live or on the Wayback Machine, and direct quotes given in the article do not show up on any other search result on Google, Yahoo or Bing. Therefore, I feel I cannot accept this source as valid evidence in this report. https://blog.gridinsoft.com/france-are-looking-for-lockergoga-ransomware-developers-in-ukraine/
Attack Pattern / Domain (Human Error, Privilege Misuse / abuse, cyber espionage, lack of training) CAPEC.	• CAPEC-206: Signing Malicious Code – Code avoided detection by being signed by the fake 'ALISA LTD' entity by Sectigo RSA Code Signing CA https://ieeexplore.ieee.org/abstract/document/8884472 • CAPEC-644: Use of Captured Hashes (Pass The Hash) – only a possibility, but this is a way an attacker can gain access to Windows Active Directory https://www.scadafence.com/norsk-hydros-lockergoga-ransomware-propagation-detection-mitigation/ • Encrypted files.

Motivations	• Not fully known. Appears to be for ransom money but it's possible it was to simply disrupt the company's systems. file:///C:/Users/msidd/OneDrive%20-%20University%20of%20East%20Anglia/Modules/2%20Introduction%20to%20Cyber%20Security/Coursework%202%20-%20Report/hydro%20research/Group%20CSS%20Norsk%20Hydro%202019.pdf https://mycourses.aalto.fi/pluginfile.php/923542/mod_folder/content/0/Group%20CSS%20Norsk%20Hydro%202019.pdf?forcedownload=1
Malicious / Accidental	• Malicious attack, possibly accidental infection vector
Attacker skills	• Low. The attack and ransomware wasn't particularly sophisticated in itself, the biggest challenge for the attackers was getting a valid certificate to hide the intentions of the ransomware, and getting it into the system.
Attack Vectors	• The attack may have started with an e-mail, but it is not yet publicly known how the attackers got in. • https://www.nrk.no/norge/it-sjefen-i-hydro-om-dataangrepet_-_-man-tror-krisen-blir-stor_-sa-blir-den-enda-verre-1.14515043
How much trust was there in the company before the attack?	• Company had been established for over 100 years, had never had a large-scale attack against them before.
Impact on Company / Customers / Other	• **Company**: Hydro lost some production of primary metal within Norway early on the day of the attack but noted later in the day that they were working manually at normal levels. • Extruded Solutions and Rolled Products had temporary stoppages at several plants on the day of the attack. • https://www.hydro.com/fi-FI/media/news/2019/update-hydro-subject-to-cyber-attack/ • By the 21 March, Rolled products was mostly up and running again, Extruded Solutions was only at only 50% at this point. https://www.hydro.com/fi-FI/media/news/2019/update-on-cyber-attacks-march-21/ • Product output from Extruded Solutions was expected to increase to 60% on 25 March https://www.hydro.com/fi-FI/media/news/2019/update-on-cyber-attack-march-25/ • And didn't report an increase to normal rates until the 1 April, almost two weeks after the attack. Even then, they reported needing to use extensive manual workarounds to achieve their desired output. https://www.hydro.com/fi-FI/media/news/2019/update-on-cyber-attack-april-1/ • **Customers**: • **Other**:
Financial Impact	• Between 550-650 million NKr (£47 million to £55.5 million) in damages estimated in brief given by the company https://www.hydro.com/en-GB/media/on-the-agenda/cyber-attack/ • Listed as 650-750 million NKr (£55.5 million to £64 million) • Cyber insurance covered some of the losses. Hydro claimed 33 million NKr (£2.82 million) back in Q3 2019 https://www.reinsurancene.ws/norsk-hydro-claims-first-3-6mn-from-its-cyber-insurance/ • With a further 187 million NKr (£16 million) claimed in Q4 2019 https://www.reinsurancene.ws/norsk-hydro-claims-a-further-20-2mn-from-its-cyber-insurance-in-q4/

	• There seems to have been another 192 million NKr (£16.4 million) in insurance paid out between Q1 and Q3 2020, too https://uk.reuters.com/article/norsk-hydro-results/norsk-hydro-3q-earnings-rises-unexpectedly-on-market-recovery-insurance-idINL8N2HD5ZV bringing the total recovered so far to 412 million NKr (£35.18 million), which equates to 75% of the estimated lower-bound of the damages dealt to the company. Very strong. • Likely thanks to the open nature 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. **/pic stock price/** • 11.71 NKr = £1.
Reputational Impact	• The fact that Hydro did not attempt to hide the issue and were open to their customers and stakeholders all along and remained outwardly positive despite the issues they were facing, which would have both reassured customers and kept their reputation looking good. • Hydro refused to bow down to the attackers and pay the ransom, reported the attack to the police straight away as well as being open about what happened (as above). This lead to one source to claim that this lead to a boost in the company's reputation https://www.cpomagazine.com/cyber-security/reputation-intact-despite-projected-cost-of-75-million-for-norsk-hydro-cyber-attack/
Ethical Impact	• Not paying the ransom was the best move ethically, 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 for no payoff.
Relation to CIA	• **Confidentiality** - Prevent unauthorised access to sensitive information: It doesn't appear that sensitive information was taken in this attack. • **Integrity**- Prevent data being modified: Ransomware was remotely installed and many files were encrypted leading to a loss of data integrity. • **Availability** - Accessibility of system to authorised users: Major threat, aluminium production was heavily affected while the automated systems were down. Hydro lost control over parts of the system being encrypted in the attack.
How long did it take to be identified? Incidence response team?	• 2-3 Weeks https://www.nrk.no/norge/it-sjefen-i-hydro-om-dataangrepet_-_-man-tror-krisen-blir-stor_-sa-blir-den-enda-verre-1.14515043
What was their response?	• All PCs and servers across the company was reviewed, cleaned for any malware and safely restored, according to strict guidelines to ensure security and safety. • Encrypted PCs and servers were rebuilt based on back-ups. • We have reorganized our security team to better detect and respond to cyber incidents. • Hydro is in dialog with relevant Norwegian and international authorities, including Norway's National Investigation Service (Kripos) and the Norwegian National Security Authority (NSM). • https://www.hydro.com/en-GB/media/on-the-agenda/cyber-attack/ • Hydro's crisis management center houses IT experts, who have flown in from the USA and Asia, and work around the clock with Hydro employees to rebuild and secure the company's computer systems. • Already at 05:00, 19 March, crisis staff will be deployed on Vækerø. Shortly afterwards, shareholders and the media are notified.

	• When we discovered that we were attacked, we pulled out cables everywhere and shut down all the systems to avoid further damage. It involved 22,000 PCs and thousands of servers. Everything was disconnected from the network and apart. Nobody was allowed to reconnect. • It will take several months before everything is as normal. • Did not pay ransom. "We have built up a completely new infrastructure. We create a new core, then we connect more and more. We put everyone in a new and safe zone where we have even better control" • In several media, Hydro has been praised for its openness about the attack. • https://www.nrk.no/norge/it-sjefen-i-hydro-om-dataangrepet_-_-man-tror-krisen-blir-stor_-sa-blir-den-enda-verre-1.14515043 • Microsoft Detection and Response team (DART) travelled to Oslo to assist with recovery https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/ • Gave regular updates through the news section of their website, beginning on the day of the attack and continuing for the next two weeks. https://www.hydro.com/fi-FI/media/news/?year=&category=&p=21 • Clearly a good response plan in place. file:///C:/Users/msidd/OneDrive%20-%20University%20of%20East%20Anglia/Modules/2%20Introduction%20to%20Cyber%20Security/Coursework%202%20-%20Report/hydro%20research/Group%20CSS%20Norsk%20Hydro%202019.pdf p9 • All PCs and servers across the company were reviewed, cleaned and safely restored, according to strict guidelines to ensure security and safety. Encrypted PCs and servers were rebuilt based on back-ups. https://www.hydro.com/Document/Index?name=Annual%20report%202019%20web.pdf&id=506433 p111
How could the response be managed better? Mitigation notes.	•
Misc References / Info	• Only thing changed in the report from Hydro after 14 November 2019 is the date. • Ransom note image shows use of Windows Server 2008. No Risk. https://miro.medium.com/max/700/1*SOHRtJVPbpRSX-9mO7Vrlw.png

Risk

Strategic Risk "Risks that threaten to disrupt the assumptions at the core of an organization's strategy"	• The company has a robust cyber insurance in place with recognized insurers. https://www.hydro.com/en-GB/media/on-the-agenda/cyber-attack/ • Excellent use of risk transfer. • The company admitted they are exposed to the threat of cyber-attacks including viruses, and that cyber crime is increasing globally. • They mention, however "Hydro has launched several initiatives to increase the robustness of its IS/IT infrastructure against malicious attacks by improving system infrastructure and educating employees to develop and improve secure work processes and routines. However, these initiatives may fail to deliver the expected results or prove to be inadequate to prevent cyber attacks or security breaches that manipulate or improperly use our systems or networks.

	• "Awareness building in cyber security has been the priority for 2018. The activities conducted are related to data protection, including GDPR, and cyber exercise related to email phishing. We continue to harmonize and integrate security services between Extruded Solutions and the other business areas in Hydro. In addition, all new employees have to complete a course in cyber security in Hydro Academy." • Despite this focus, there is no mention of how they monitor for threats, and an attack against them was still successful. • https://www.hydro.com/Document/Index?name=2018%20Annual%20report.pdf&id=8525 • Vulnerability Level: ~~Vulnerable / Reactive~~ / Compliant / ~~Proactive / Optimized~~
Tactical Risk "Chance of loss due to changes in business conditions on a real time basis"	• Allowing outside access to the company (DART) allowed them to respond quickly and effectively.
Operational Risk "Potential for losses due to uncertainty" User awareness	• Perhaps threat monitoring could have been better • Someone opened a dodgy email.
Managing Risk Was the company risk adverse or did they welcome risk	• Quite risk adverse on the cyber side. They had defences in place, training offered and insurance to cover losses. • Infront rated the company as a whole a risk score of 7.00, meaning it is relatively low risk, especially compared to other aluminium companies https://www.infrontanalytics.com/fe-EN/01264SN/Norsk-Hydro-ASA/gprv-risk
How could the risk be handled better? Traceable, Auditable, Relevant, Rigorous. Support structure? Support from the top? Risk Assessments? Mitigation section notes.	• Avoidance: • Mitigation: • Transfer: • Acceptance:
References / Info	ACCA - Strategic and Operational Risks

Privacy

How was privacy broken?	• N/A
Privacy policy	• Section 3.9 of the Code of Conduct covers Data Protection and Privacy and only really mentions that the company must protect personal data that it holds, and they must only hold relevant data, which is in line with GDPR. Since there is no evidence of the company losing personal information, this policy was not violated.

Was there specific information leaked due to this attack (deanonymisation)?	• No
Was the company found to be in breach of privacy legislation? ECHR?	• No.
What data was being collected that didn't need to be (and was subsequently leaked)?	• None.
What could've been done to stop privacy being violated? Mitigation notes.	•
References / Info / Further notes	

Security Policies

What security policies were in place? Why did they fail? Master policy, change management, physical security, email, encryption, vulnerability management, media disposal, data retention, acceptable use, access control, information security, incident response, remote access, disaster recovery, business continuity plan	• Policy: Health, Safety, Security, Environment (HSE) https://www.hydro.com/Document/Index?name=Health%2C%20security%2C%20safety%20and%20environment%20policy&id=3010 • **Living Document**: No, as of December 2020, last revision was 01 December 2016. • **Unambiguous**: Lays things out simply but makes many references to internal procedures for further information, which don't appear to be externally accessible, at least without contacting the company. • **Realistic**: Appears to be realistic, with nothing out-of-the-ordinary. However, this means that there is not enough detail to form a good conclusion. • **Enforceable**: There is no mention of how this policy is to be enforced. • **Inclusive**: There is no specific mention in the document for computing, IT, or cybersecurity, therefore the parts of the company that we are most interested in were not specifically included. Section three, scope, mentions intellectual assets as an element of security, but not how the company goes about protecting it. • **Endorsed**: 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. • **Attainable**: Section nine, concerning Documents and Records mentions "Official procedures shall be approved, documented, maintained and updated, accurate, legible and identifiable." However, the fact that this document alone has not been updated for over four years tells me that this procedure has not been maintained or updated, and therefore may no longer be accurate.

	• **Why failed? Issues with Policy or people following policy?** I would say that this policy failed in that it didn't cover enough information, especially in regards to information security to ensure employees knew their responsibilities regarding cybersecurity. There is the possibility that further information exists in a procedure, but these are not accessible online to the public.
Integrity Policy violated?	• Users wrote their own programs? • Programmers testing on production? Not tested correctly? • Dev program incorrectly installed on Production? • Installing to production was not controlled and / or audited? • No access to logs for managers and auditors? None of these. Unable to find integrity policy.
Was a security policy audit carried out after?	• Audit committee in place and met 10 times during FY2019 https://www.hydro.com/Document/Index?name=Annual%20report%202019%20web.pdf&id=506433 but meeting agendas and minutes were not made public.
Was there a User Agreement / EULA? Was it violated?	• Not found.
Conformed to Biba Model for data integrity? Bell-LaPadula Model?	• Biba – No read down, no write up, no lower process requesting access: • Bell-LaPadula – No read up, No write down, DAC specified with access matrix:
What should be included in the security policy to stop it happening again? Mitigation notes.	•
References / Info / Further notes	https://blog.eduonix.com/networking-and-security/learn-different-types-policies-procedures-cissp/

Threat Monitoring

Was threat monitoring in place? Real time?	• Hydro had not seen any signs of an attack before the screens went black. https://www.nrk.no/norge/it-sjefen-i-hydro-om-dataangrepet_-_-man-tror-krisen-blir-stor_-sa-blir-den-enda-verre-1.14515043 • Antivirus' missed the Malware, all 67 security products on virustotal came up negative • The ransomware version 1320, which is under analysis, has the following digital certificate issued to the fake 'ALISA LTD' entity by Sectigo RSA Code Signing CA, well known for signing abuse according to the Chronicle research • https://ieeexplore.ieee.org/abstract/document/8884472 • No airgap between manufacturing systems and corporate network allowed the virus to spread across the entire network.

	• Automated incident response was seemingly not used, meaning it may have spread further than necessary. https://www.scadafence.com/norsk-hydros-lockergoga-ransomware-propagation-detection-mitigation/ p6
What detection methods? SIEM (QRadar, Splunk) / Threat Intelligence Provider / Traffic analysis Framework / Dissassmbler / Proxy / Cyber Platform / IDS (Cisco AMP) / SOAR / SIRP / Logging	• Despite what some security professionals may say, endpoint security would likely not detect the ransomware, due to the fact that the ransomware was signed. https://www.scadafence.com/norsk-hydros-lockergoga-ransomware-propagation-detection-mitigation/ • For the same reason, the encryption process would likely not have been picked up via file entropy detection or usage of crypto APIs – SCADAfence.
Cyber Killchain (Lockheed Martin)	• Reconnaissance: • Weaponization: • Delivery: • Exploitation: • Installation: • C+C: • Actions on Objectives:
Defence Framework? Identify, Protect, Detect, Respond, Recover.	• No evidence it existed, but the quick response showed there was likely a framework in place.
Thread Modelling Framework? Define – Diagram – Identify – Mitigate – Validate – Define. P.A.S.T.A, STRIDE, TRIKE?	• No idea.
Efficiency Statistics? MTT detect, respond, contain, eradicate	• N/A
Was threat modelling used? What type, how? If not, would one have helped? How?	•

Was a system implemented or changed after the attack? What lessons were learned? Bespoke threat monitoring approach? Mitigation notes.	• New system built https://www.hydro.com/Document/Index?name=Annual%20report%202019%20web.pdf&id=506433 p111 • Hydro has launched several initiatives to increase the robustness of its IS/IT infrastructure against malicious attacks by improving system infrastructure and educating employees to develop and improve secure work processes and routines. We have reorganized our security team to better detect and respond to cyber incidents, and the company has a robust cyber insurance in place with recognized insurers. https://www.hydro.com/Document/Index?name=Annual%20report%202019%20web.pdf&id=506433 p111 •
References / Info / Further notes	https://www.hydro.com/Document/Index?name=Annual%20report%202019%20web.pdf&id=506433 early 2020

Human Aspects

Usability? Learnability, Efficiency, Memorability, Errors, Satisfaction.	•
Employees bypassed security systems? Too confusing, clumsy, hard to remember passwords, security too complex, too much technical terminology, forcing uninformed decisions on users, user using easy-to-hack password.	• Likely human error in clicking a malicious email link, despite training. • Impact may have been lessened or mitigated through the use of admin accounts only for specific tasks, and general accounts used by administrators at all other times. https://www.scadafence.com/norsk-hydros-lockergoga-ransomware-propagation-detection-mitigation/
Insider? If so, detail why they did it. Role-based detection in place?	• Doesn't appear to be the case.
What could be done to mitigate the human aspects? Reduce cognitive load, make state visible, give informed feedback, design to not reduce performance. Mitigation notes.	•

References / Info / Further notes	

Social Engineering

What techniques were used? Office visitors, Evesdropping, shoulder surfing, dumpster diving? Phishing (all types) catfishing? Social media?	• Likely spear phishing but unknown.
Was a framework used? Information gathering, elicitation, pretexting, mind tricks, influence	• No idea.
What could have been done to mitigate the threat of social engineering? Mitigation notes	•
References / Info / Further notes	

Mitigation for [chosen Hack] (30% - 1125 words)

How could the Response be handled better?	•
How could the RISK be handled better?	• Identify Assets, Vulnerability Assessment, Threat Assessment, Risk Assessment, Define Countermeasures. • Board: Define objectives and requirements, define risk tolerance identify and allocate resources, act and sponsor and champion for risk management, develop and communicate risk management policy, provide direction. • Risk Manager • Business Unit Managers • Staff REFERENCE: Jones, A., & Ashenden, D. (2005). *Risk management for computer security: Protecting your network and information assets.* Elsevier. P192-194,
What could've been done to stop privacy being violated?	•
What changes should be made to the security policies?	• Risk Management Policy in place. Introduction, Authority, Scope, Definitions, Strategy and Approach, organisations and responsibilities, process and procedures, planning, risk assessment, risk control/mitigation, risk monitoring. REFERENCE: Jones, A., & Ashenden, D. (2005). *Risk management for computer security: Protecting your network and information assets.* Elsevier. P227
Was a system implemented or changed after the attack? What lessons were learned?	•
What could be done to mitigate the human aspects?	• Hadnagy?
What could have been done to mitigate the threat of social engineering?	Hadnagy Chapter 9. • 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 • Developing scripts • Learn from audits • Create a security culture

References / Info / Further notes	https://owasp.org/www-project-top-ten/ - What attacks to look out for.

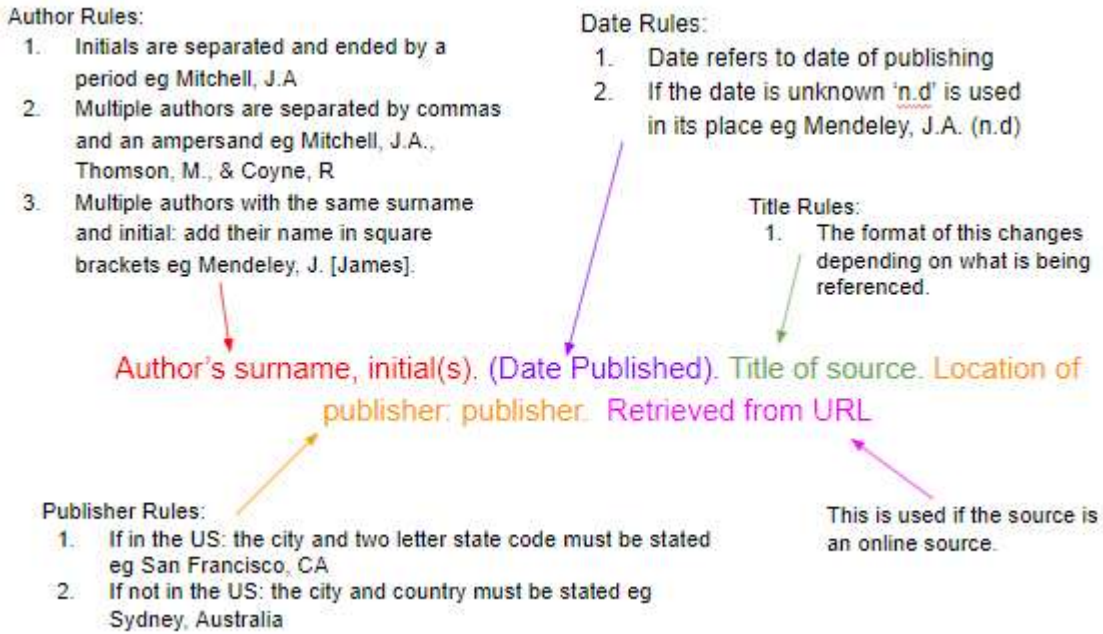
Reflexive Writing (10%, one page)

Stuff here

Conclusion:

General Notes

https://www.mendeley.com/guides/apa-citation-guide



This was explained in a paper credited to \citet{surname_year}.
The first paper \citep{surname_year} explains […]