ELSEVIER

Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Economics and Finance 00 (2012) 000–000

Procedia
Economics and Finance

www.elsevier.com/locate/procedia

Case Study

Cyber Security Incident Report — Norsk Hydro

Suvi Leppänen, Shohel Ahmed, Robin Granqvist

"Aalto University, Otaniemi, Espoo and 02150, Espoo"

Abstract

Nineteenth of march an International aluminum industry suffered a cyberattack with worldwide consequences. The attack and the impact the attack had, will be discussed in this paper, as well as analyzing what could have been done better.

Keywords: Cyberattack; case study; Hydro Norsk; LockerGoga; aluminum industry

1. Introduction

In March, 2019 Norsk Hydro, a global leading Aluminum manufacturing company, faces a large scale ransomware attack. The ransomware, LockerGoga, infected 40 sites of the company globally and gained access to critical information and encrypted the data. This results in shutdown of the corporate network and disruption in the automated system of the manufacturing plant. Due to the lack of IT system, the business and manufacturing process of Hydro e.g., order processing and inventory management collapsed. This forces the company to resort to fully or partly manual operations. This cyber-attack has a significant impact on the Hydro's business. The cost is estimated to be between 400-450 million NOK, 41-46 million euros due to loss of production and associated cost.

The adversary uses the ransomware LockerGoga which exploits the weakness of the corporate Active directory system to propagate the attack payload to other machines in the network. The initial infection point for the attack is still unknown. The motivation is also unknown. However, the prominent speculation is disrupting the manufacturing rather than collecting ransom. In 2019, there were five known attacks from LockerGoga, all targeting manufacturing industries, provides us the same indication.

Hydro handled the cyber security incident, especially the communication part, in a procedural way. It provided clear instructions to the employees, to the shareholders, and to the outside world. The CIO and CFO regularly provided updates to the stakeholders. This contained the situation and even positively impacted their share price. On the other hand, there are considerable weaknesses in their Network regarding endpoint security, security monitoring, and securing the system by design perspective. This is a learning opportunity for others to follow the best practices of security principles to prevent further such attacks.

2. The Event

19.3.2019 Norsk Hydro experienced a ransomware attack by a third party. To understand this event this chapter will introduce the reader to the company, the ransomware used and the events right after the attack.

2.1. The Company

Hydro Norsk is a Norwegian global supplier of Aluminum. Hydro Norsk ASA was founded in 1905 and has today 35000 employees in 40 countries. In 2018 it had a revenue of 159,337 million Norwegian Kronas (NOK), which equals about 18,193 million US Dollars and a net income of 4,323 million NOK from ongoing operations. Hydro also has over 30 000 customers over the world and thrives on being a 360-degree global supplier of aluminum, but also produces the rolled and extruded products as well as extracts bauxite. [1]

The company has a long history of overcoming war and occupation as well as reinventing itself as a company and deciding on what to produce and how. All of it started in Norway, by using hydropower they had a process of capturing Nitrogen from the atmosphere. From there it became a bigger market with producing its own power and to making ammonium. While the company was based in Norway it has from the start been owned by global investors that have made the company more global. [2]

In Hydro's 2018 Annual report for investors they do mention a cybersecurity threat as a possible risk factor that must be taken into consideration. They state that Hydro's IT infrastructure is critical for their operations and that an attack could affect the process control systems, personal databases and external financial reporting. [2] While they mention this as a possible threat, they have no explanation or plans to protect against this possible threat, or what actions should be taken. It is although possible that the 2019 report will be different.

Hydro has an image of being environmentally friendly, they have many information pages on their homepage about their greener sustainable approach. However, there were some questions about their facility in Brazil that was accused of polluting the environment in February 2018. The Plant in Brazil is their main plant with the largest production rates. Hydro denied fault but did as they were asked and reduced production by 50 %. The event and suspicion got many investors to doubt their sustainable agenda and they were forced to react. [3-4]

Recent years have been challenging for Hydro, 2017 seemed to be a great year as they were on top of many lists as a great place to work, as well as making a lot of money that year. [5] The company's share price dropped by almost 40 % after the legal affairs in Brazil. The 18th of March Hydro announces that a new female CEO Hilde Merete Aasheim will be starting in May after the previous CEO goes for an early retirement. The speculation is that this happened partly to boost Hydro’s image. [6]

2.2. What happened?

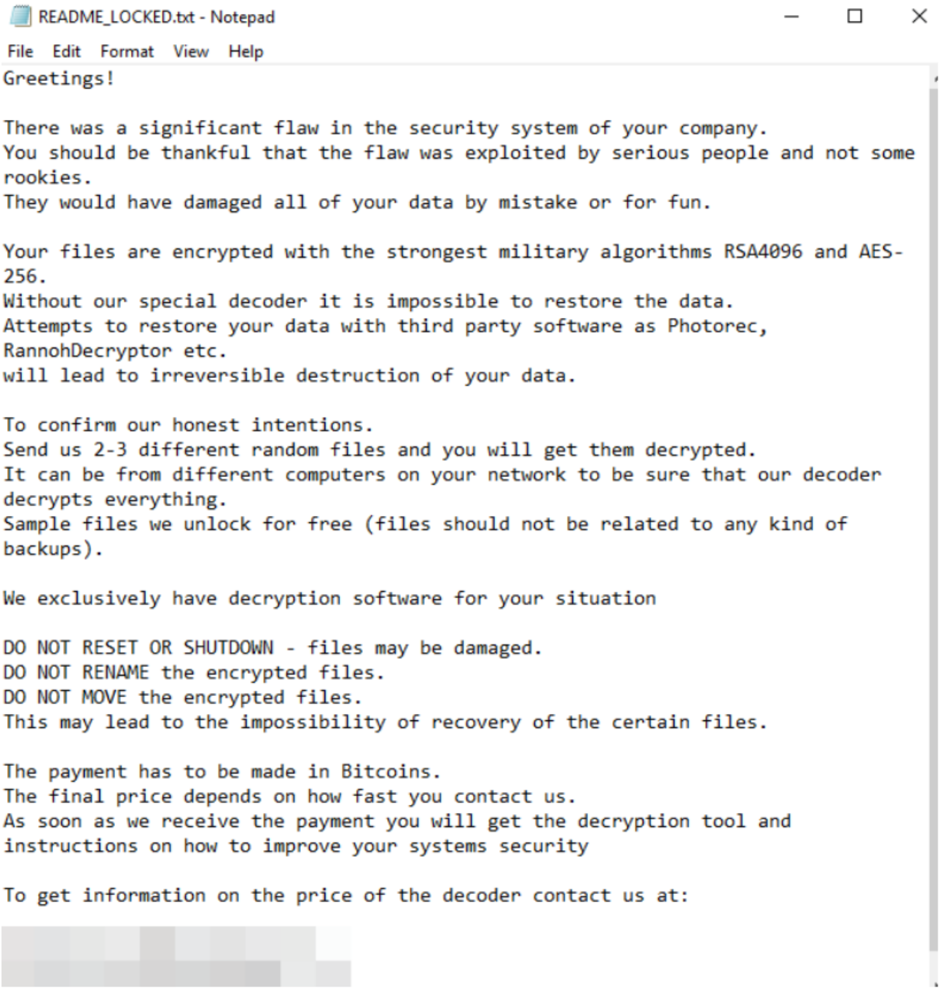
Late evening the 18th of March some of the Hydro Norsk’s staff noticed unusual behavior in their computer systems. Around midnight Norwegian time, all screens went black in offices and plants alike, in 40 different countries. As all systems were locked, and as someone gained access a ransom note was found. Something was wrong. At 5 am the next morning most of the company leaders were called, among them CIO Jo De Vliegher, shortly thereafter also the shareholders and media were informed. [7]

To avoid further damage, almost 22000 computers and thousands of servers were shut down and disconnected, by literally pulling out the cables on each one. Experts from IBM and Microsoft were flown in, and all personnel were forbidden to connect anything to the network. This meant that most of the plants were forced to manual operations, no orders could be managed, and the plants not designed for manual operations were shut down. [7]

Communication between employees continued using Office 365, which was unimpacted and most people used their phones or tablets to communicate with customers and the outside world. Facebook was also used as a communication platform to the outside world, and very quickly a temporary website was put up where the URL hydro.com was redirected. This website informed quickly that Hydro was under a cyberattack, and the main contact channels for further information. [8]

2.3. Ransomware LockerGoga

LockerGoga is the ransomware that infected Hydro Norsk. The ransom software became known in January when it infected Altran Technologies, in France. It forced Altran to shut down all its networks to be able to stop the virus progress. Which is essentially how the virus works. Once it has gained access to a system it will change users’ passwords as well as try to log them out, essentially denying access. It will also encrypt stored files of specific types, in all the accessible machines, meaning desktops, laptops and servers that are connected to the network. After this it leaved a README_LOCKED.txt file on the desktop with a ransom note. The ransom note can be seen in Fig. 1. After the encryption and password changes LockerGoga finishes its mission by disabling the network access. [9]



```
Greetings!

There was a significant flaw in the security system of your company.
You should be thankful that the flaw was exploited by serious people and not some
rookies.
They would have damaged all of your data by mistake or for fun.

Your files are encrypted with the strongest military algorithms RSA4096 and AES-
256.
Without our special decoder it is impossible to restore the data.
Attempts to restore your data with third party software as Photorec,
RannohDecryptor etc.
will lead to irreversible destruction of your data.

To confirm our honest intentions.
Send us 2-3 different random files and you will get them decrypted.
It can be from different computers on your network to be sure that our decoder
decrypts everything.
Sample files we unlock for free (files should not be related to any kind of
backups).

We exclusively have decryption software for your situation

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME the encrypted files.
DO NOT MOVE the encrypted files.
This may lead to the impossibility of recovery of the certain files.

The payment has to be made in Bitcoins.
The final price depends on how fast you contact us.
As soon as we receive the payment you will get the decryption tool and
instructions on how to improve your systems security

To get information on the price of the decoder contact us at:

[redacted]
```

Fig. 1. Ransom note left by LockerGoga virus [9].

For LockerGoga to gain access to a system it needs executive privileges. The main access point seems to be Windows Active Directory with admin rights. This means that the network was likely already compromised before the attack as the attackers had gained credentials to run these executive systems like PsExec and Boost library. [9-10] For a more detailed analysis of the virus code see [10].

LockerGoga virus seems to be targeted towards production industries as at least 5 attacks are known to happen during 2019. All the attacks seem to be aimed at manufacturing industries and as the virus makes it difficult for them to even pay the ransom, it would seem that the aim is more likely to disrupt service instead of gaining money. The encrypted files cannot be decrypted, and the ransomware is brutal in disrupting computer operations, all indicating that the purpose is more than ransoming for money. [11]

3. The effect

The attack had some serious consequences for the whole company, both operational and financial. Luckily, the attack did not lead to any safety related incidents [12]. To the best of our knowledge no persons have been injured, and no harm has been done to the environment.

3.1. Production

Hydro had to disconnect all plants and operations and had to switch to manual mode and other workarounds as far as possible. Out of the five largest departments Extruded Solutions were hit the hardest, followed by Rolled Products. Especially the Building Solutions business segment of Extruded Solutions had difficulties. Primary Metal could operate close to normal, but with a higher degree of manual operations. Energy and Bauxite & Alumina could continue normal production. [13]

In Extruded Solutions and Rolled Products there were in the beginning a lot of challenges with the production, and several plants had to temporary stop producing at all [13]. Two days after the attack, Rolled Products were running almost as normal, with a few exceptions. Extruded Solutions were running at about 50% of normal capacity [12].

One week after the attack, on March the 26th, Extruded Solutions had ramped up their production rate to 70-80% of normal, except in the Building Systems business, were production was still almost at a standstill [14].

On March the 28th, Extruded Solutions were running at 80-85% of normal, and the Building Solutions business segment had increased its production rate to 40-50% [15]. Two and a half weeks after the attack, on April the 5th the Extruded Solutions were running at an average of 90%, except Building Solutions were at 70% [16]. The last production update from Hydro was on April the 12th, three and a half weeks after the attack when the total average of Extruded Solutions were at 85-90%, but still local variations from plant to plant [17].

A good workforce spirit and moral inside the company helped Hydro recover from the attack. Workers were willing to spend a lot of extra hours and even work on weekends to help the company get back on its feet. Some personnel did work in tasks that were not in their duties. For example, some office workers helped out in the factory floor. [18], [19], [20].

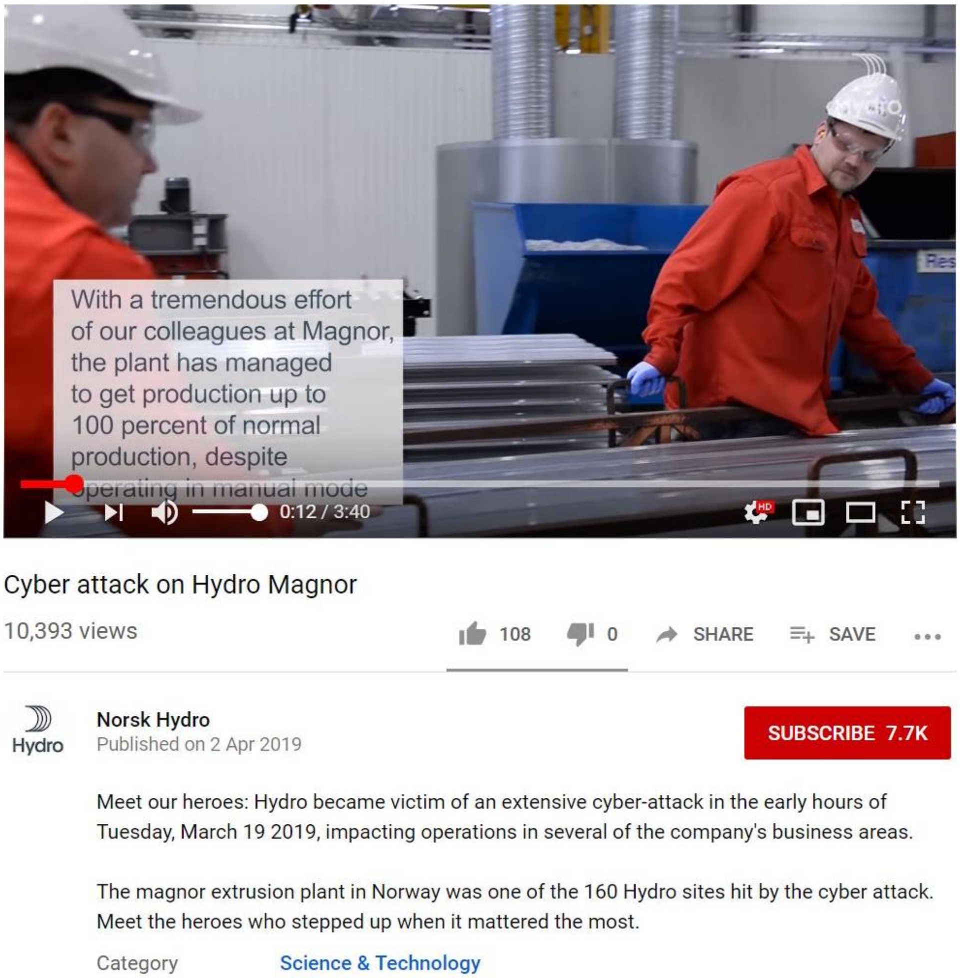
3.2. Financial

The total financial impact from the cyber-attack is estimated to be between 400-450 million NOK, 41-46 million euros. The department for Extruded Solutions was the most severely hit. Preliminary sales figures show that the quarterly sales dropped around 8% from 362 000 tonnes last Q1 to 333 000 tonnes this year. Although, Extruded Solutions have been focusing on value instead of volume and were estimating that the total sales tonnage would drop a little this year even under normal circumstances. Hydro has announced that they will postpone the complete first quarter report to June 5 due to the cyber-attack, so the final financial consequence is not known yet. Hopefully they will continue to give out open information on the financial impact of the attack. We would also like to know if the workers are compensated for their overtime in their efforts to get the company back running.[18]

3.3. Public relations

Hydro managed to keep a good image during the attack. They were fast to give out information that there has been an attack and were very open and transparent from the start. They regularly kept the public and their shareholders updated with information on their Facebook page, their temporary website and via webcasts. Hydro broadcasted their first webcast already on the same day as the attack, the 19th of March 2019 [13]. They continued to give out regular updates on the state of the company and the effects of the attack.

Two weeks after the attack Hydro published a YouTube video from one of its Norwegian plants. In the video the employees explained how the attack had affected their plant. They talked about how they had been able to keep up production through workarounds. They also mention their workers morale and how employees had been working overtime voluntarily. Figure 2 shows a screenshot from the video. [19]



With a tremendous effort of our colleagues at Magnor, the plant has managed to get production up to 100 percent of normal production, despite operating in manual mode

Cyber attack on Hydro Magnor

10,393 views

Norsk Hydro
Published on 2 Apr 2019

Meet our heroes: Hydro became victim of an extensive cyber-attack in the early hours of Tuesday, March 19 2019, impacting operations in several of the company's business areas.

The magnor extrusion plant in Norway was one of the 160 Hydro sites hit by the cyber attack. Meet the heroes who stepped up when it mattered the most.

Category Science & Technology

Fig 2. Screenshot from Youtube video [19]

Hydro used the publicity from a bad event in a good way. They managed to give out a reassuring and positive image of the company, and that they were doing a lot of effort to get their systems back running.

4. Lessons learned

The attack on Norsk Hydro and the response from the company presents a learning opportunity for others regarding how to handle a cyber incident especially the communication channel. Below we describe several lessons from technical, personal, and security environment perspectives.

The attacker infected the one of the endpoints of the IT network and from there propagated the attack to the whole corporate network. We do not know the actual reason and initial infection point behind the attack, but as far we know from public report, the attacker managed to install LockerGoga malware in one of the endpoints and the endpoint security system fails to detect abnormality of the system integrity. The endpoint security ensures attached devices to a computer network follows compliance to a security policy. The endpoint security software identifies and manages user’s access to a corporate network, performs regular security update, and do anti-virus scanning on the host. For example, in the Payment card industry (PCI-DSS) [21], all client requires compliance with the PCI security standard in addition to authentication to connect to a PCI-DSS processing server. In this case, there is a definite lack of endpoint security in the Hydro network to allow the malware in the first place and allowing the malware to infect the active directory.

4.1. Technical

4.1.1 Endpoint security

The attacker infected the one of the endpoints of the IT network and from there propagated the attack to the whole corporate network. We do not know the actual reason and initial infection point behind the attack, but as far we know from public report, the attacker managed to install LockerGoga malware in one of the endpoints and the endpoint security system fails to detect abnormality of the system integrity. The endpoint security ensures attached devices to a computer network follows compliance to a security policy. The endpoint security software identifies and manages user’s access to a corporate network, performs regular security update, and do anti-virus scanning on the host. For example, in the Payment card industry (PCI-DSS) [21], all client requires compliance with the PCI security standard in addition to authentication to connect to a PCI-DSS processing server. In this case, there is a definite lack of endpoint security in the Hydro network to allow the malware in the first place and allowing the malware to infect the active directory.

4.1.2 Security Monitoring:

In Norsk Hydro, the LockerGoga infected the Windows Active Directory (AD) server and used an elevated permission as a domain controller admin to compromise all active directory managed endpoints. Due to almost all internal security firewall allow traffic from the AD, the attacker was easily able to bypass the security controls placed inside the corporate network. However, this type of attack would require a significant amount of network activity from the AD server to the endpoints. This increase activity should have been identified by security monitoring tools. A security monitoring tool collects and analyses real time security events for both in the network and host. The tool aggregates data from the server logs, perform correlations on attributes and events, and alerts the user for possible attack scenario. In the Hydro case, the attack traffic from the AD controller to the endpoints, the commands to encrypt the data, unusual CPU behaviour for data encryption, and any external communication to the malware control central should have been identifiable by the security monitoring tool. Thus, there are definite lacking in the Hydro network for proper monitoring of security events.

4.1.3 Architecture

In Hydro, both the corporate and plant network are affected by the cyber attack. The most probable reason is both networks use the same AD server for managing user access and common elements management. This design provides the attacker an extended attack surface. A secure system should be designed using secure by default principle --- with proper risk analysis and control in place for each identified risk. For example, to secure network, it is recommended to have zones and even having air gaps among those zones. If air gapping is not possible, have a proper demilitarized zone (DMZ) with specialized monitoring of all traffic passing through the firewalls. Hydro could have created a completely two different active directory forest for corporate and plant network or could implement proper zoning and monitoring for all traffic.

4.2 People

Having the best architectural design, endpoint security, and intrusion detection systems cannot guarantee security unless people who administers and operates the system are security aware. The development a cyber security strategy should emphasis on educating people for safe usage behavior. Many of the recent attacks such as Bangladesh Bank Cyber heist [22] shows phishing attack [23] on person is used as an initial anchor to perform a larger attack such as an advanced persistent threat (APT) [24] event. The increase in number of phishing attacks and internal attacks on high value targets emphasizes the need for security awareness or training for each individual.

4.3 Environment

Cyber security should be managed from a holistic approach. Modern IT systems are complex in nature with dependency chain to multiple vendors each supplying a part of it. Take for example, corporate IT network in which network equipment, end points, service software e.g., email and antivirus software come from multiple vendors. The installation, upgrade and security patch update for each of this software will have different approaches. Thus, the network owner should carefully understand the strength and weakness of each vendor and their products. There should be clear terms and conditions regarding responsibilities for security management for each parity.

One of the areas where current system fails is information sharing during and after a cyber incident. The lack of information sharing and lack of learning from others resulted in spread of an attack vector to multiple targets. For example, Altran, a French engineering consulting company was infected by the same LockerGoga malware in January 2019. The attack on Norsk Hydro could have been prevented if Altran shared the information to security vendors and other companies to build preventive steps against such malware.

5. Evaluation against an Incident response plan

This section presents an incident response plan and evaluates Norsk Hydro cyber attack against the plan. An incident response plan consists of a set of instructions to identify, protect, detect, respond, and recover for cyber security incidents [25]. A security incident can have significant impact on company's business and operation which can last for months. The incident response plan guides (in Fig. 2) the organization to contain the incident and prepare for a range of events. Now we evaluate Norsk Hydro case against an ideal incident response plan.

- An incident response plan starts with a team which is responsible when a incident happens. It should clearly define roles and responsibilities for each members of the team. This will minimize confusion during a cyber incident. Norsk Hydro detected the security events on 19th march mid-night and by 5 AM Hydro disconnected their worldwide network. The Hydro sent posted notices to 40 of their offices and manufacturing facilities around the world and guides employees and manager what to do. Its informed stock markets and local law enforcement agencies regarding cyber attack. Their activities prove that they have prepared team to handle the incident.
- A proper communication procedure should be followed during an incident. A proper guidance should be provided to employees and all stakeholders and responsible for such action should be defined. In the Hydro case, we have seen proper communication channel from the CFO and CIO talking to media, providing daily update via webcast and video, and consolidating the stakeholders regarding their efforts to contain and recover from the situation.

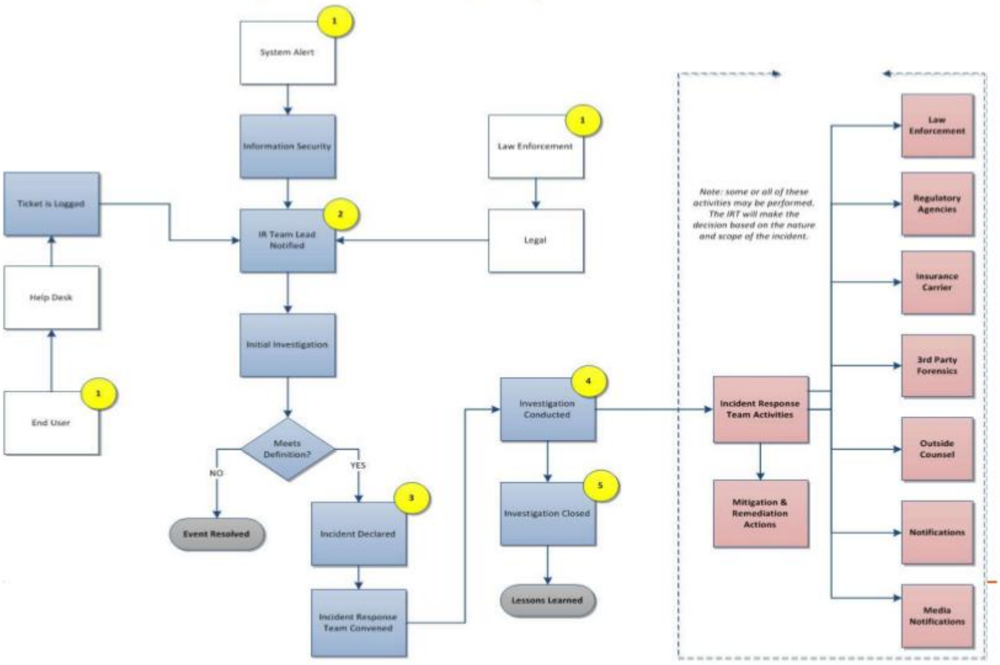


Fig. 3. Incident Response plan [26].

- Every incident should start with an investigation phase. Every incident should be dealt with top priority, only after an incident is investigated it should be assigned a priority. For Hydro, we have lack of information for other cases. For this particular case, Hydro bring expertise from Microsoft and third-party forensic company to investigate the event, thus fulfilling the requirement for early investigation phase.

- Have a plan for access to or location of critical information. This could be for example, backup data location, network diagrams, and emergency contacts for systems. This allows quick reach to necessary parties and information during an emergency. Additionally, each incident should follow a defined process, thus no one try to solve the problem of their own without following the process. An undefined process could lead to chaos and loss of vital data for further forensics analysis. In the Hydro case, from the outset it looks they followed the incident response procedure quite well. There are few areas they could improve such as, data restore and backup process. By taking regular read only backups, the system could be easily restored to a good known state within a short period of time.
- Every incident is an opportunity to learn for others. Every incident should be investigated, and the results provide feedback for future improvement of the incident response plan. The incident response plan is a living document requiring regular update due to change in persons, roles, and threat landscape. The learnings are important for others and improving overall cyber security posture. In the Hydro case, we can say their communications and initial handling of the incident worked well and is a learning opportunity for others. On the other hand, they could have done better job for critical information storage and retrieval by having proper backup mechanism.

6. Conclusions

As we have seen in this case, a ransomware attack can have broad consequences for a company if the virus is able to contaminate large portions of their network. Norsk Hydro handled the situation quite well in terms of incident response and communication, both internal and external. Hydro’s way of handling the incident openly and straightforward probably had a positive and reassuring effect to the public and the shareholders, thus limiting the financial impact of the attack. We do hope that Hydro will continue to be open with the results from their investigation and forensic reports. We would like to know how the perpetrators did get access to the network and how they did get admin rights. We would also be interested in knowing who the perpetrator is, and what was the purpose of the attack. Was it purely financial gain, to get the ransom? Or was it perhaps a rival that aimed to maim the production and reputation of Hydro?

There are also valuable learnings on improvements to others in this case. The most important is perhaps to have proper incident response plan. Hydro could have done things better with better backups of important data. A better network architecture and monitoring system could have limited the impact of the attack. It should also be desirable to have some sort of manual procedure or workaround in case of a serious cyber-attack. A good moral and spirit inside the company helped Hydro recover from the attack. Workers were willing to spend overtime at work in order to get the production rolling again.

The cybersecurity industry can also learn from this LockerGoga attack. The ransomware had already been used in a high-profile attack on Altran. It is important that information is shared more openly and rapidly between different security actors, both authorities, security vendors and the community. The vendors can then quickly implement the proper detections into endpoint security. This attack would then perhaps have been less effective or would not have happened at all. The battle between the good and the bad is of course a never-ending chase who is ahead, and the bad people will always come up with new innovative tricks.

References

[1] https://www.hydro.com/en-FI/about-hydro/facts/ 6.5.2019

[2] https://www.hydro.com/Document/Index?name=2018%20Annual%20report.pdf&id=8525 6.5.2019

[3] https://seekingalpha.com/article/4158560-norsk-hydro-downside-risk 6.5.2019

[4] https://www.theguardian.com/world/2018/mar/16/brazil-pollution-amazon-aluminium-plant-norwegian 6.5.2019

[5] https://www.forbes.com/companies/norsk-hydro/#17ce80fcb52d 6.5.2019

[6] https://af.reuters.com/article/metalsNews/idAFL8N21511A 7.5.2019

[7] https://www.nrk.no/norge/it-sjefen-i-hydro-om-dataangrepet_-_-man-tror-krisen-blir-stor_-sa-blir-den-enda-verre-1.14515043 7.5.2019

[8] https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880

[9] https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware 6.5.2019

[10] https://labsblog.f-secure.com/2019/03/27/analysis-of-lockergoga-ransomware/ 6.5.2019

[11] https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms/ 6.5.2019

[12] https://www.hydro.com/fi-FI/media/news/2019/update-on-cyber-attacks-march-21/ 12.5.2019

[13] https://www.hydro.com/fi-FI/media/news/2019/update-hydro-subject-to-cyber-attack/ 12.5.2019

[14] https://www.hydro.com/fi-FI/media/news/2019/update-on-cyber-attack-march-26/ 12.5.2019

[15] https://www.hydro.com/fi-FI/media/news/2019/update-on-cyber-attack-march-28/12.5.2019

[16] https://www.hydro.com/fi-FI/media/news/2019/update-on-cyber-attack-april-5/12.5.2019

[17] https://www.hydro.com/fi-FI/media/news/2019/update-on-cyber-attack-april-12/12.5.2019

[18] https://www.hydro.com/fi-FI/media/news/2019/operational-and-market-update-first-quarter-2019-alunorte-and-cyber-attack-lower-overall-production-levels/ 6.5.2019

[19] https://www.youtube.com/watch?v=S-ZlVuM0we0 12.5.2019

[20] https://www.youtube.com/watch?v=o6eEN0mUakM 12.5.2019

[21] PCI DSS Quick Reference Guide, Available at, https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf, Accessed 1 may, 2019.

[22] Bouveret, Antoine. Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. International Monetary Fund, 2018.

[23] Jagatic, Tom N., et al. "Social phishing." Communications of the ACM 50.10 (2007): 94-100.

[24] Virvilis, Nikos, and Dimitris Gritzalis. "The big four-what we did wrong in advanced persistent threat detection?." 2013 International Conference on Availability, Reliability and Security. IEEE, 2013.

[25] Framework for Improving Critical Infrastructure Cybersecurity, NIST, Available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[26] It's Not If But When: How to Build Your Cyber Incident Response Plan, Available at, https://www.kroll.com/-/media/kroll/pdfs/publications/kroll-us-cyber-response-plan-sep-2016-web.ashx?la=en