"Special Commando Move" - When Informal, Formal and Technical Cybersecurity Components Fail

Annika Andreasson[1][0000-0003-1748-] and Fredrik Blix[2][0000-0002-9925-1592]

[1] Cybercom Secure, P.O. Box 7574, 103 93 Stockholm, Sweden
[2] Department of Computer and Systems Sciences, Stockholm University, 106 91 Stockholm, Sweden

annika.andreasson@cybercom.com, blix@dsv.su.se

Abstract. In February 2019, 2.7 million phone calls to Swedish healthcare provider 1177 Vårdguiden were discovered to have been exposed online. In this paper, we posit that incidents like the 1177 case can be explained through a socio-technical model of informal, formal and technical domains where cybersecurity has failed. In the paper, we outline the events of the 1177 leak, we show how informal, formal and technical components of cybersecurity failed, and how the model could be used before, during and after incidents.

Keywords: socio-technical cybersecurity, healthcare, data breach

1 Introduction

With the increasing digitization and shift to e-government services, instances where personal data are processed are multiplying. Such processing needs to be lawful and secure, maintaining the confidentiality, integrity and availability of the information, for citizens to trust the services provided. The cybersecurity of the providers of such services is at the center of maintaining that trust.

One socio-technical model, based on the work of Stamper et al. (1991) and explained in Björck and Yngström (2001), classifies the domains of cybersecurity as formal, informal and technical. The informal domain includes organizational culture, organizational politics, interpersonal relations, etc. This domain contains the human ideas and human behavior and ideas relating to these. The formal domain of cybersecurity includes legal frameworks, organizational policies, standards, etc. These are usually written rules to align the behavior of humans in information systems. The technical domain includes the technical objects, or ideas, theories and models relating to these. In this position paper, we discuss how informal, formal and technical domain components all play essential parts in having a high level of cybersecurity. We believe that when IT incidents occur, we can identify failures in the model domains. As exemplified in the case we outline below, we believe that the reasons why a given incident occurs are usually to be found in *more* than one of the domains.

The paper is structured as follows: Section 2 provides a short healthcare background and outlines the 1177 case. Section 3 applies the model to the case. Section 4 concludes and presents future research.

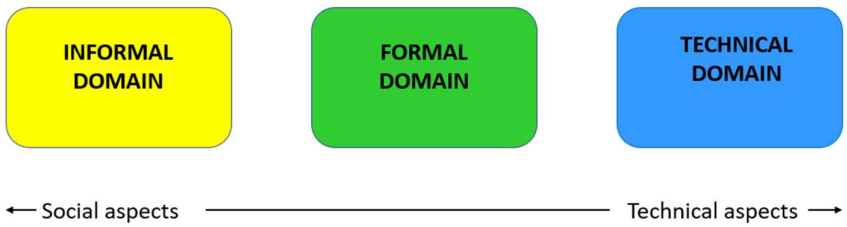

Fig. 1. A socio-technical model of cybersecurity

2 The case

2.1 Healthcare

The case we look at in this paper comes from the healthcare industry in Sweden. Healthcare is one of seven essential services identified in the NIS Directive as an area where the European Union member states shall work together towards increasing the security of network and information systems.

Healthcare in Sweden is free, and the 10 million citizens have a healthcare hotline as first line triage. They call 1177 if they need to discuss their health problems with a nurse and to get advice on whether they need to see a doctor or not. These phone calls are recorded and stored, forming part of the electronic medical records.

The 1177 case is an incident where 2.7 million recorded healthcare related phone calls leaked online while being stored on a network attached storage device at a sub-contractor.

When van Deursen, Buchanan & Duff (2013) asked a panel of information security professionals in the healthcare industry to rate different socio-technical risk scenarios to assess risks in healthcare, the outsourcing scenario with subcontractors and third parties did not rank among the top risks.

2.2 Exposure revealed

On February 18, 2019, the Swedish IT newspaper "Computer Sweden" published a story where they showed that 2.7 million recorded healthcare phone calls were leaked online (Dobos, 2019). Anyone could enter the URL and – without providing any password – directly listen to the recorded phone calls. Some of the wave-files were named by the telephone number of the caller, many of the recordings included unique personal ID numbers and names identifying the callers, and all calls contained sensitive personal data about the caller's health issues.

The server was taken offline before the story was published so there would be no risk that readers would start to download the available phone calls.

2.3 Reactions

The data breach mainly involved three regions using "Healthhelp"[1], which in turn used "Healthcall", that used a cloud-based call center solution provided by "Noise Integrate". In the first few days, the CEO of "Noise Integrate" was interviewed in Dagens Nyheter (Söderberg, 2019)and commented:

> *"This server is a so-called network-attached storage, NAS... You could say it is an internal hard drive which is not password protected since you can only reach it through the computer to which it is connected... We don't know when it happened, but probably during patching ... someone simply connected an internet cable to the hard drive. Then it got an ip-address... Regular people can't do it, but those with skills could perform a special commando move and sneak in through the back door... We do monitor our equipment for intrusions and so on... But this was like a personal home hard drive, you don't monitor that for intrusions, since you cannot access it... For some reason it got its own little cable to the internet. It would not have mattered if you did not know the server had this problem, but Computer Sweden found out.... These kinds of incidents happen because you have a lot of people around, not because someone deliberately is messing with you… We need to review our routines …We have checklists for all other systems, but not for this hard drive. Someone probably though it too basic. "*[2]

2.4 Legal consequences

In the first two days after the initial publication, "Healthhelp", "Healthcall" and "Noise Integrate" were acknowledging the leak and said that it was a mistake due to human factors. On the third day they changed the language on their web pages and instead of "leak" they started to talk about *dataintrång* (English: unauthorized data access). In line with this, they filed a police report against the journalist and the editor-in-chief at the newspaper that broke the story, claiming they had committed the crime *dataintrång.*

A week after the incident, on February 27, the Swedish Police and the Swedish Prosecution Authority started to investigate if "Healthhelp" may have committed a crime against healthcare "professional secrecy", by putting the records online. In parallel, there is an investigation by the Swedish Data Protection Authority if there has been a GDPR breach, and an investigation by Region Stockholm, on whether their agreements with "Healthhelp" were specific enough, with regards to security requirements. These four investigations are still ongoing at the time of writing.

---

[1] For the purposes of this paper, the names of the companies involved have been changed in the main body of the paper.

[2] Translations from Swedish to English by the authors, all errors are our own.

2.5 Cybersecurity

There were several technical components involved in this case.

First, we look at the server containing 170.000 hours of recorded sensitive calls, which was put online without any protection. Search engines like Shodan, ZoomEye and others have indexed the server, which is a Ubuntu Linux server that has been running since 2013. “Noise Integrate” have said that the hardware is a small network attached storage, NAS. In 2013, “Noise Integrate” install OwnCloud, a file sharing application, and add a Favicon icon, indicating a possible web server experiment. In 2015, a web interface for administration of the NAS is downloaded and unzipped. In 2016, the folder HTML was last changed, indicating a possible web server. Folders containing the phone calls synced here from the call center software are added in 2017. On the day the leak was published, they were running Apache 2.4.7, with 23 known vulnerabilities, not updated in the past five years.

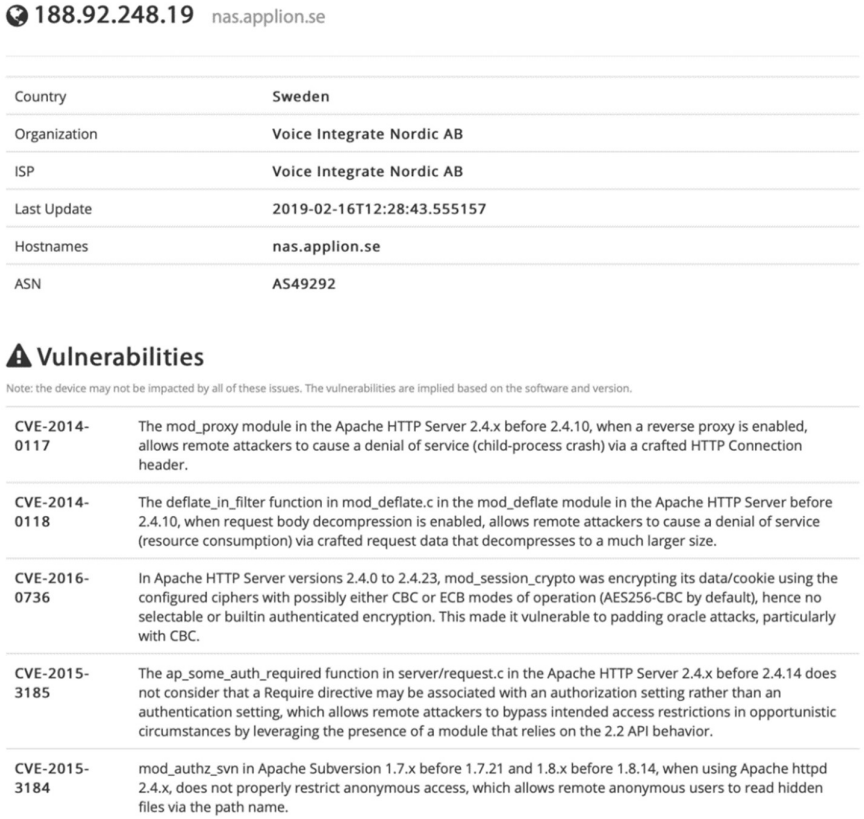

Fig. 2. Screenshot Shodan entry

Index of /

Name	Last modified	Size	Description
clip-two_v2.1/	2015-11-11 13:09	-	
favicon.ico	2013-08-22 11:40	1.6K	
html/	2016-06-24 07:49	-	
itell/	2017-01-02 08:04	-	
medicall/	2017-01-01 01:00	-	
owncloud-enterprise/	2013-08-06 12:12	-	
owncloud/	2013-08-06 12:12	-	
prebus/	2017-01-01 01:00	-	
snow/	2017-03-29 14:20	-	
themeforest-10290688-cliptwo-bootstrap-admin-template-with-angularjs.zip	2015-11-13 18:51	160M	

Apache/2.4.7 (Ubuntu) Server at 188.92.248.19 Port 80

Fig. 3 Screenshot Apache Server

Next, we look at the network situation.

The server has a static IP address on 188.92.248.19 and the firewall is open for the traffic to the IP on port 443 (the port that was used to access the recorded phone calls). There are DNS entries from nas.applion.se and nas.voiceintegrate.se.

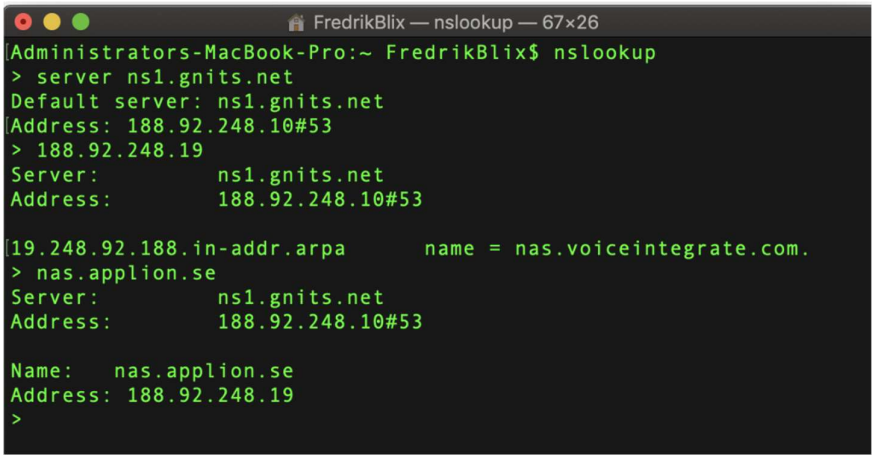

Fig. 4. Screenshot nslookup

2.6 Data breach

After the breach was revealed, “Noise Integrate” looked at the web server access log. They claim logs are missing for the years 2016 to 2018, and that all accesses logged were made between February 15 and 18, 2019.

The media reported that, since only 55 phone calls were downloaded, the risk is basically over. However, there has been no mention of other logs, and ways of getting the phone calls out of the server, such as rsync, scp, ftp, webdav.

The server had multiple severe vulnerabilities and quite possibly breached several times during the years has also not been discussed.

The fact that search engines, like Shodan and Chinese ZoomEye, have indexed the server and therefore have had access to the data has not been mentioned in the media.

2.7 Swedish government reaction

On March 1, the minister for Health and Social Affairs, Lena Hallengren, reported that the risk is over, and everyone can now safely call 1177 again! (Regeringskansliet, 2019) Meanwhile, the cloud-based call center system of "Noise Integrate" (Linux/Asterisk-based VoIP solution) has not been reported to have been verified for security, and at the time of writing "Healthcall" still take calls in Thailand.

3 Application of model

From what is publicly known about the 1177 case, we can identify failures in *all three* of the cybersecurity domains outlined in Section 1: *Informal*, *Formal* and *Technical*. The domains are enumerated and exemplified below

3.1 Informal

Examples of failures linked to the informal domain of human behavior:

i. *Awareness:* Someone at "Noise Integrate" connected the Network Attached Storage device to the Internet
ii. *Culture*: Someone at "Noise Integrate" excluded the NAS from intrusion monitoring and checklists as it was deemed too basic
iii. *Arrogance:* The CEO of "Noise Integrate" believed only highly skilled hackers could find the server's open port

3.2 Formal

Examples of failures linked to the formal domain of regulating human behavior:

i. *Governance:* "Noise Integrate" did not have management systems that prevented the storage unit to be attached to the internet
ii. *Procurement*: The Regions did not perform security audits at the subcontractors as part of the procurement procedure
iii. *Legal Compliance:* "Noise Integrate" did not comply with the GDPR, for example the Privacy by Design requirement

3.3 Technical

Examples of failures linked to the technical domain of technical artefacts:

i. *Security set-up:* The entire architecture at "Noise Integrate"
ii. *Patching:* The server had several known vulnerabilities and not updated in 5 years
iii. *Configuration*: The server had DNS entries

4 Concluding remarks and future work

It is our position that this socio-technical cybersecurity model is valuable before, during and after an incident.

Before By considering informal, formal and technical domains equally when designing controls for cybersecurity.

During By identifying in what domain(s) the incident is occurring to provide the most appropriate incident response.

After By performing post mortems where the informal, formal and technical domains are analyzed to provide thorough lessons learned on how the different domains facilitated the incident and improve cybersecurity.

There are different roads ahead for future research. One natural extension of this position paper would be to contextualize previous research in the area of socio-technical cybersecurity and to look at several cases where cybersecurity failed and see if repetitive patterns could be identified. Another part could be to look at to what extent organizations consider all three domains for a balanced socio-technical cybersecurity approach in their control design.

The *Technical* and *Formal* domains are well researched compared to the *Informal* domain. In a wider perspective, it would be beneficial to take an interdisciplinary view on *Informal* cybersecurity to identify models to understand, predict and change human cybersecurity behavior.

Acknowledgements. The authors would like to thank participants at STPIS 2019 and two anonymous referees for excellent comments that helped improve this paper.

References

Björck, F., & Yngström, L. (2001). IFIP World Computer Congress/SEC 2000 Revisited. *IFIP TC11 WG 11.8 Second World Conference onf Information Security Education* (pp. 209-222). Perth: School of Information Science, Edith Cown University.

Dobos, L. (2019, February 18). *2,7 miljoner inspelade samtal till 1177 Vårdguiden helt oskyddade på internet*. Retrieved March 15, 2019, from Computer Sweden: https://computersweden.idg.se/2.2683/1.714787/inspelade-samtal-1177-vardguiden-oskyddade-internet

Regeringskansliet. (2019, March 1). *Socialministern i möte med anledning av händelserna rörande 1177 Vårdguiden*. Retrieved from Regeringskansliet: https://www.regeringen.se/pressmeddelanden/2019/03/socialministern-i-mote-med-anledning-av-handelserna-rorande-1177-vardguiden/

Söderberg, N. (2019, February 19). *Ansvarig för Vårdguiden-haveriet: "Mänskliga faktorn"*. Retrieved March 15, 2019, from Dagens Nyheter: https://www.dn.se/ekonomi/ansvarig-for-vardguiden-haveriet-manskliga-faktorn/

Stamper, K., Liu, K., Kolkman, M., Klarenberg, P., Van Slooten, F., Ades, Y., & Van Slooten, C. (1991). From Database to Normbase. *International Journal of Information Management, 11*, 67-84.

van Deursen, N., Buchanan, W. J., & Duff, A. (2013). Monitoring information security risks within healthcare. *Computers & Security, 37*, 31-45. doi:10.1016/j.cose.2013.04.005