

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

Annika Andreasson, Cybercom Secure
Fredrik Blix, DSV, Stockholm University

Annika Andreasson



- Information Security Consultant @ Cybercom Secure
- MSc Information Security from Stockholm University
- Previously Journal Manager @ The Review of Economic Studies
- Human side of Cybersecurity
- Co-author Fredrik Blix, DSV, Stockholm University



Presentation Outline



- Socio-Technical Model of Cybersecurity
- The 1177 Case
- Apply the Model to the Case
- Conclude

Cybersecurity in Organizations

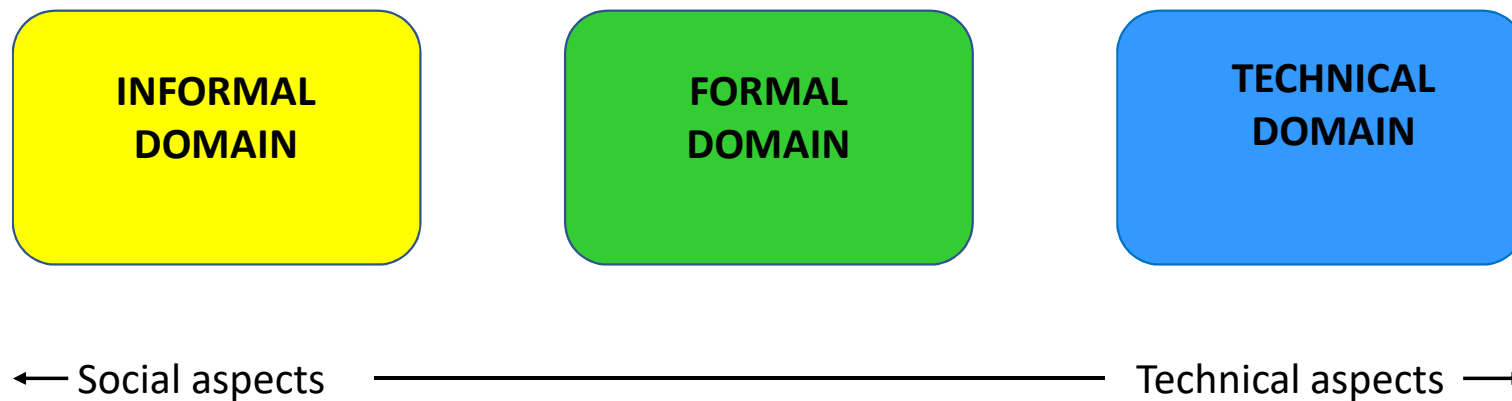


Fig. 1 A Socio-Technical Model of Cybersecurity

The 1177 Case – Background

- 18 February – Computer Sweden disclosure
- Vårdguiden 1177 – First line triage
- **2.7 million phone calls** – Three regions
- **170.000 hours** – wav-files

The 1177 Case – CEO comments

*This server is a so-called network-attached storage, NAS... We don't know when it happened, but ... **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...** 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 thought it too basic.***

Dagens Nyheter, February 19, 2019

The 1177 Case – Technical



Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 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	-	
 medical/	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

The 1177 Case - Technical



Index of /medical1

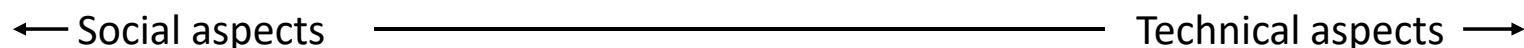
Name	Last modified	Size	Description
Parent Directory		-	
201b96d902adefa860e0fd4a191cf598@188.92.255.13:5060.wav	2017-03-13 09:10	44	
2011edd147a99c4c355d3c9c4441eeee.wav	2016-06-21 23:49	44	
2013/	2013-12-05 14:46	-	
2014/	2014-12-01 01:00	-	
2015/	2015-12-01 01:00	-	
2016/	2016-12-01 01:00	-	
2017/	2017-12-01 01:00	-	
2018/	2018-12-01 00:00	-	
2019/	2019-02-01 00:02	-	
Makefile	2015-10-26 16:30	503	
callparam/	2015-10-26 15:54	-	
do.sh	2019-02-13 15:11	0	
mh-20160524-002803-1464049543.37224.wav	2016-05-24 02:28	97K	
mh-20160524-003216-1464049890.37442.wav	2016-05-24 02:32	102K	
mh-20160524-003314-1464049972.37474.wav	2016-05-24 02:33	109K	
mh-20160524-003331-1464049967.37465.wav	2016-05-24 02:33	109K	
mh-20160524-003425-1464050044.37509.wav	2016-05-24 02:34	108K	
mh-20160524-003546-1464050118.37563.wav	2016-05-24 02:35	113K	
mh-20160524-003630-1464050161.37577.wav	2016-05-24 02:36	94K	
mh-20160608-230946-465427366.69769.wav	2016-06-09 01:09	117K	
mh-20160608-231315-1465427566.69853.wav	2016-06-09 01:13	98K	
mh-20160608-231326-1465427586.69862.wav	2016-06-09 01:13	109K	
mh-20160608-231607-1465427703.69919.wav	2016-06-09 01:16	110K	
mh-20160609-000150-1465430002.72342.wav	2016-06-09 02:01	98K	
mh-20160609-000202-1465430104.72474.wav	2016-06-09 02:02	98K	
mh-20160609-000203-1465430155.72484.wav	2016-06-09 02:02	98K	

```
FredrikBlix — nslookup — 67x26
Administrators-MacBook-Pro:~ FredrikBlix$ nslookup
> server ns1.gnits.net
Default server: ns1.gnits.net
Address: 188.92.248.10#53
> 188.92.248.19
Server: ns1.gnits.net
Address: 188.92.248.10#53

19.248.92.188.in-addr.arpa name = nas.voiceintegrate.com.
> nas.applion.se
Server: ns1.gnits.net
Address: 188.92.248.10#53

Name: nas.applion.se
Address: 188.92.248.19
>
```


What can the model tell us about 1177?



Failures in...

Informal Domain: Awareness, Culture, Arrogance

Formal Domain: Governance, Procurement, Legal Compliance

Technical Domain: Security Set-up, Patching, Configuration

Concluding remarks



- **All domains of the socio-technical model need to be considered!**
- **The model is useful before, during and after incidents**
 - **Before:** Consider all domains equally when designing cybersecurity controls
 - **During:** Identify domain(s) where incident occurred and tailor response
 - **After:** Lessons Learned to see how each domain facilitated incident and improve cybersecurity

Thanks for listening!



annika.andreasson@cybercom.com

blix@dsv.su.se