“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
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 /

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

Apache/2.4.7 (Ubuntu) Server at 188.92.248.19 Port 80
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