Embedding Cyber Security to Digital Transformation

21.5.2019 Kimmo Rousku
Tallinn, Estonia
@kimmorousku

• General Secretary for Finnish Public Sector Digital Security Management Board (VAHTI)
• Population Register Centre, from 1.1.2020 Digital and Population Data Services Agency
• Author, keynote speaker, nerd, gadget freak, novice biohacker, CISM, CISSP

Join to my networks:

Twitter: kimmorousku
LinkedIn: kimmorousku
Roles

• Ministry of Finance
  – The Ministry of Finance is responsible for developing information security in public administration in general and for steering information security in central government.
  – Public Sector Digital Security Management Board (VAHTI)
    ▪ All 12 ministries, municipalities, major security authorities
    ▪ As a whole >100 leaders, managers and experts #cooperation #together

• Population Registration Center
  – VAHTI operational support and Public Sector digital security services
  – Project / joint venture for Digital Security in Public Administration in 2019–2021
    ▪ Participants <150 organisations, target >250 this year
  – Digital security expert services using private (cyber) security companies
Same goals, different roadmaps

- Ministry of Finance
  - Public Sector Digital Security Management Board (VAHTI)
  - Population Registration Center – Public Sector digital services an VAHTI operational support

- Ministry of Transport and Communications
  - Finnish Transport and Communications Agency Traficom | National Cyber Security Centre
    - Cybersecurity situational awareness, GovCERT, CERT-FI
    - Assessment of authorities' information systems and telecommunications arrangements
    - [https://www.kyberturvallisuuskeskus.fi/en](https://www.kyberturvallisuuskeskus.fi/en)

- Ministry of Defence | Security Committee
  - Comprehensive Security in society – Finnish Cyber security Strategy

- Ministry of the Interior
  - National Bureau of Investigation, Cybercrime centre

- Ministry for Foreign Affairs of Finland
  - NSA - National Security Authority
  - Unit for Security Policy and Crisis Management, Ambassadors for Cyber & Hybrid Affairs

Finnish Defence Forces

Office of the Data Protection Ombudsman

**Strenghts: Co-operation Community**
SECURITY STRATEGY FOR SOCIETY

Government Resolution

FORESIGHT, PREPAREDNESS, OPERATIONAL CAPABILITY AND RECOVERY

AUTHORITIES
BUSINESS OPERATORS
ORGANISATIONS AND OTHER BODIES
CITIZENS

PREPAREDNESS COOPERATION FORUM

Coordination at local, regional and national level: joint assessment and situation picture
www.turvallisuuskomitea.fi
TOGETHER FOR A SAFE FINLAND
Finland and Cyber security – where are we now?
## ITU - Global Cybersecurity Index

### Europe region

<table>
<thead>
<tr>
<th>Member State</th>
<th>Score</th>
<th>Regional Rank</th>
<th>Global Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>United Kingdom</td>
<td>0.931</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>France</td>
<td>0.918</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Lithuania</td>
<td>0.908</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Estonia</td>
<td>0.905</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Spain</td>
<td>0.896</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>Norway</td>
<td>0.892</td>
<td>6</td>
<td>9</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>0.886</td>
<td>7</td>
<td>11</td>
</tr>
<tr>
<td>Netherlands</td>
<td>0.885</td>
<td>8</td>
<td>12</td>
</tr>
<tr>
<td>Georgia</td>
<td>0.857</td>
<td>9</td>
<td>18</td>
</tr>
<tr>
<td>Finland</td>
<td>0.856</td>
<td>10</td>
<td>19</td>
</tr>
<tr>
<td>Turkey</td>
<td>0.853</td>
<td>11</td>
<td>20</td>
</tr>
<tr>
<td>Denmark</td>
<td>0.852</td>
<td>12</td>
<td>21</td>
</tr>
</tbody>
</table>

- **Draft 15.5.2019** – [download](#)
UN E-Government index

Table 5.2.1: showing the top ten 2018 e-government index

<table>
<thead>
<tr>
<th>Country</th>
<th>Score</th>
<th>Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denmark</td>
<td>0.9150</td>
<td>1</td>
</tr>
<tr>
<td>Australia</td>
<td>0.9053</td>
<td>2</td>
</tr>
<tr>
<td>Republic of Korea</td>
<td>0.9010</td>
<td>3</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>0.8999</td>
<td>4</td>
</tr>
<tr>
<td>Sweden</td>
<td>0.8882</td>
<td>5</td>
</tr>
<tr>
<td>Finland</td>
<td>0.8815</td>
<td>6</td>
</tr>
<tr>
<td>Singapore</td>
<td>0.8812</td>
<td>7</td>
</tr>
<tr>
<td>New Zealand</td>
<td>0.8806</td>
<td>8</td>
</tr>
<tr>
<td>France</td>
<td>0.8790</td>
<td>9</td>
</tr>
<tr>
<td>Japan</td>
<td>0.8783</td>
<td>10</td>
</tr>
<tr>
<td>Rank</td>
<td>Country</td>
<td>National Cyber Security Index</td>
</tr>
<tr>
<td>------</td>
<td>--------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>15.</td>
<td>Switzerland</td>
<td>72.73</td>
</tr>
<tr>
<td>69.</td>
<td>Korea (Republic of)</td>
<td>38.96</td>
</tr>
<tr>
<td>55.</td>
<td>Iceland</td>
<td>46.75</td>
</tr>
<tr>
<td>13.</td>
<td>United Kingdom</td>
<td>75.32</td>
</tr>
<tr>
<td>20.</td>
<td>Netherlands</td>
<td>66.23</td>
</tr>
<tr>
<td>32.</td>
<td>Norway</td>
<td>62.34</td>
</tr>
<tr>
<td>6.</td>
<td>Denmark</td>
<td>81.82</td>
</tr>
<tr>
<td>38.</td>
<td>Sweden</td>
<td>57.14</td>
</tr>
<tr>
<td>8.</td>
<td>Singapore</td>
<td>80.52</td>
</tr>
<tr>
<td>31.</td>
<td>Luxembourg</td>
<td>62.34</td>
</tr>
<tr>
<td>29.</td>
<td>United States</td>
<td>63.64</td>
</tr>
<tr>
<td>10.</td>
<td>Finland</td>
<td>79.22</td>
</tr>
</tbody>
</table>
It’s not only high scores

• What’s your country’s capability on difference areas and aspects to Cyber security – from legal to some part of technical view
  – view to national state-level culture, attitude towards security
  – high rankings don’t stop Cyber attacks and other incidents
  – but probability and especially impact are lower in those countries than in the ones who are not so well prepared?

You need to measure not only on country level, but also
  – organisational level
  – the famous weakest link – according to many studies – it’s US – we humans | (un)intentional human error | hurry
One more challenge

- Attacks & incidents will be more common – because number of digital services (national level – globally) is increasing every year > the more we digitalize, the bigger the cyberattack surface > more cyber attacks
- More new technology > more ICT-related incidents + cyber attacks
  - IoT – AI – robotics – automation
Digital security and trust – road to even more digitalized 2020+ society
Manual – analog – digital transformation

#trust
Digital security as enabler #trust

1. Risk management
2. Business continuity
3. Information security (C-I-A-model)
4. Cyber security
5. Data protection & privacy (GDPR)
From global to local

- Finnish public sector national Digital security survey 2019 (150 organisation)

<table>
<thead>
<tr>
<th>Category</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. RISK MANAGEMENT</td>
<td>0.73</td>
</tr>
<tr>
<td>2. BUSINESS CONTINUITY</td>
<td>0.62</td>
</tr>
<tr>
<td>3. INFORMATION SECURITY</td>
<td>0.73</td>
</tr>
<tr>
<td>4. CYBERSECURITY</td>
<td>0.60</td>
</tr>
<tr>
<td>5. DATA PROTECTION</td>
<td>0.65</td>
</tr>
</tbody>
</table>

Average scale: 1.0 excellent – 0.0 nonexistent
It’s not cyber security we should be worried about

- ICT-incidents – minor problems 2.93
- ICT-incidents – major problems 3.87
- Information / cyber security incidents 4.09
- DoS attacks – minor 4.48
- DoS attacks – major 4.78
- Nothing has happened 5.00

- N=150 public sector organisations
Human centric digital security
Human centric digital security – securing your workday @workplace

Do we need
1. Risk management
2. Business continuity
3. Information security
4. Cyber security
5. Data protection
Human centric digital security – securing your workday @remote and home

Do we need
1. Risk management
2. Business continuity
3. Information security
4. Cyber security
5. Data protection
Human centric digital security – securing your workday @business trip

Do we need
1. Risk management
2. Business continuity
3. Information security
4. Cyber security
5. Data protection
Human centric digital security – securing your life @ leisure / free time

Do we need
1. Risk management
2. Business continuity
3. Information security
4. Cyber security
5. Data protection
Human centric digital security

Childhood/parents  Youth  Working life  Aging

Workplace  Remote work  Business trip  Leisure / free time

Risk management | Business continuity | Information security | Cyber security | Data protection
Finland’s Cyber security Strategy

FIGURE 1 Finland’s cyber threat scenario
According to the Vision:

- Finland can secure its vital functions against cyber threats in all situations.
- Citizens, the authorities and businesses can effectively utilise a safe cyber domain and the competence arising from cyber security measures, both nationally and internationally.
- Finland will be the global forerunner in cyber threat preparedness and in managing the disruptions caused by them.
How about our new strategy?
NCSI as valuable evaluation tool

GENERAL CYBER SECURITY INDICATORS

1. Cyber security policy development - 100%
2. Cyber threat analysis and information - 100%
3. Education and professional development - 100%
4. Contribution to global cyber security
   4.1. Convention on Cybercrime - 100%
   4.2. Representation in international cooperation formats - 100%
   4.3. International cyber security organisation hosted by the... - 0%
   4.4. Cyber security capacity building for other countries - 0%

BASELINE CYBER SECURITY INDICATORS

5. Protection of digital services - 80%
6. Protection of essential services - 0%
   6.1. Operators of essential services are identified - 0%
   6.2. Cyber security requirements for operators of essential... - 0%
   6.3. Competent supervisory authority - 0%
   6.4. Regular monitoring of security measures - 100%
7. E-identification and trust services - 100%
8. Protection of personal data - 100%
Kimmo Rousku
kimmo.rousku@vrk.fi
+358 50 566 2986

@kimmorousku

https://www.linkedin.com/in/kimmo-rousku-00539/