National Cybersecurity Capacity Building

Lino Santos
@ Jornadas Computação Científica
I do not rely on technology to run my business
I am safe… I have five layers of firewalling
Cybersecurity is a tech issue…You should talk to my IT
A Cybersecurity company offered me a solution to comply with RGPD in an fortnight, should I buy it?
Table of contents:

1. Cyberspace and Cybersecurity
2. Portuguese National Cybersecurity Center (CNCS);
3. The importance of the human factor;
4. Developing Cybersecurity Capabilities;
1. Cyberspace and Cybersecurity
Cyberspace

• Refers to the usage of technology

• Powerful media that magnifies communication

• Compresses space and time

• Decentralized and aterritorial

• Utopian Liberty

• Sense of anonymization
Cybersecurity social construction

• 1988 - Morris worm
• 1990/1998 - Polymorphic viruses and worms
• 2007/2008 - Estonia and Georgia cyber attacks
• 2013 - Snowden revelations
• 2018 - Cambridge Analytica scandal
**Defence**
- Sovereignty
- Mission assurance
- Exploitation

**Market**
- Digital market
- Economy growth
- Consumers confidence

**Homeland security**
- Fight Cybercrime
- Critical Infrastructure Protection

**Civil Liberties**
- Privacy
- Freedom of speech
- Human rights on cyberspace
2. Portuguese National Cybersecurity Center (CNCS)
Portuguese National Cybersecurity Centre

Established in 2014, is the Portuguese Cybersecurity Authority

“Promotes the cyberspace usage in a free, trustable and secure fashion”

- Training and awareness
- Cybernorms
- National and International cooperation
- CERT.PT
3. The importance of the human factor
The technological network we live in is also made of humans.

The human factor is not the weakest one, it's the only one that really matters.

Liam Burnett-Blue
It is necessary to **strengthen** the **human factor** at different levels:

- User
- Developer
- Decision maker
1st keyword:

RESPONSIBILITY
of the user
DANGER:

NAIVETY

Confusion between the usefulness of technology and its benevolence.

Unawareness of malicious technical possibilities
2nd keyword: RESPONSIBILITY of developers/technicians
Security by design and security by default

• Security features integrated in the development, avoiding extra efforts by the user;
• Solve the cause, not the symptom;
• User-friendly security features.
3rd keyword:

AWARENESS of decision makers
The decision makers must have a **cybersecurity strategic** vision in order to value cybersecurity efforts in their organizations.
4. Developing Cybersecurity Capabilities
One of the main problems

“Growing asymmetry between the know-how needed to commit a cybercrime or launch a cyberattack, and the skills needed to defend against it. The crime-as-a-service model has lowered the barriers of entry to the cybercriminal market: individuals without the technical knowledge to build them can now rent botnets, exploit kits or ransomware packages.”

(ECA, 2019)
More problems

“Traditional recruitment channels are not meeting demand (…)

Nearly 90% of the global cybersecurity workforce is male (…)

At universities, cyber-related subjects are underrepresented on non-technical courses.”

(ECA, 2019)
Training and education is especially needed among:

- civil servants
- law enforcement officers
- judicial authorities
- armed forces
- educators

(ECA, 2019)
Cybersecurity has the largest demand as well as the largest gap between demand and supply.

Organizations that acknowledge that demand for a hard digital skill is high today and employees who are proficient in that hard digital skill.

<table>
<thead>
<tr>
<th>Digital Skill</th>
<th>Employer: Demand for this digital skill is high in my organization today</th>
<th>Employee: Proficiency level of skill</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity</td>
<td>68%</td>
<td>43%</td>
</tr>
<tr>
<td>Cloud computing</td>
<td>65%</td>
<td>42%</td>
</tr>
<tr>
<td>Analytics</td>
<td>64%</td>
<td>51%</td>
</tr>
<tr>
<td>Web development</td>
<td>64%</td>
<td>39%</td>
</tr>
<tr>
<td>Mobile application design and development</td>
<td>62%</td>
<td>38%</td>
</tr>
<tr>
<td>Data science</td>
<td>62%</td>
<td>45%</td>
</tr>
<tr>
<td>Big data</td>
<td>61%</td>
<td>41%</td>
</tr>
<tr>
<td>Master data management</td>
<td>61%</td>
<td>42%</td>
</tr>
<tr>
<td>User interface design</td>
<td>60%</td>
<td>39%</td>
</tr>
</tbody>
</table>

The demand for cybersecurity is not likely to diminish in the next few years

Percentage of organizations that acknowledge demand for cybersecurity is high in their organization

Today: 68%
In the next 2–3 years: 72%
In the next 4–5 years: 69%

PORTUGUESE STRATEGY 1.0

1 - Cyberspace security structure;
2 - Fighting cybercrime;
3 - Cyberspace and infrastructures protection;
4 - Education, awareness and prevention
5 - Research and development;
6 - Cooperation.
2018

Law 46/2018

- NIS directive implementation;
- Whole-of-Government and whole-of-Society perspective;
- Cyberspace Security Council;
- Cooperation;
- Incident notification.
2018...

PORTUGUESE STRATEGY 2.0 *to be*

- New technologies and new threats update;
- One of the main axes (2):
  - *prevention, education and awareness* - campaigns, literacy, training/school/universities, young talents, CS careers, talent retention, decision-makers training, articulation with EU and NATO.
ONE OF CNCS OBJECTIVES IS to promote cybersecurity training and human resources qualification.
CNCS
TRAINING PROGRAM

Cyber secure Citizen

Awareness

Train the Trainers
Cyber secure Citizen is a short and simple e-learning course, accessible to all citizens, providing the necessary knowledge for cyber-protection and cyber-hygiene good practices adoption.
Awareness in cybersecurity carries out actions throughout the country, addressing citizens/employees; technical workers; and decision makers.
Train the trainers consists of training trainers, nominated by partners, who will belong to a CNCS Trainers Stock, and will be able to give training at their own organizations and at organizations defined by CNCS.
ANOTHER OBJECTIVE IS

Strengthen national **Cybersecurity**.
Cyber Assessment Framework

OESs and DSPs (Mandatory Security Requirements)

- Energy
- Transport
- Health
- Banking
- Water supply
- Financial Mark
- Digital
- Infrastruct

Maturity Models

- Capabilities
- Actions

Cybersecurity Framework

- Identify
- Protect
- Detect
- Response
- Recover
Maturity Models

- No just controls and measures;
- Defines priorities and a way to progress;
- Provide technical guidance, training, tools and solutions;
- It is possible to compare with other organizations.
Cybersecurity Observatory

A knowledge **analysis and systematization platform**, identifying trends and articulating **several stakeholders** for information collection.
ENISA supports Portuguese National Cybersecurity Exercise on electoral process

In the context of the upcoming double elections in Portugal, the Portuguese National Cybersecurity Centre CNCS have requested the EU Agency for Cybersecurity ENISA to support a cybersecurity exercise on the electoral process.

Published on February 20, 2019

References

- [https://www.cmcs.gov.pt/recursos/noticias/a-processa-electoral-para-a-campanha-que-vai-a-]o-guia-de-segunda-ediscaco-do-exercicio-nacional-de-ciberseguranca
- [http://www.enisa.europa.eu/media/news-]items/news-items/2019/02
Thank You.

lino.santos@cnks.gov.pt