Security – the Santhea Approach

Philippe Costard
HOPE

July 10th, 2019

Agenda

- GDPR Projet
- NIS Project
- Secure Healthcare Community

GDPR Project

- Q4-2017 – beginning of the project
- 4 people (1 lawyer, 1 doctor, 1 cybersecurity specialist, 1 coordinator) + 1 lawyer
- DPOaaS
- Q1-2018 – 30 members
- 20 hospitals (160 beds – 1500 beds)
- 10 smaller institutions (rest-houses, …)

GDPR – Main tasks

- Register of processing activities
- Data subjects rights
  - Employees
  - Patients
- Management of data leaks
- Review of subcontracting documents
- Policies
- DPIA (risk analysis)

GDPR project – Steering committee

- Members
  - General Manager
  - Medical Director
  - GDPR Project Manager
  - DPO (Santhea)
  - IT Manager
  - Other experts
- Monthly meetings to verify the status of the compliance

GDPR project – Santhea contribution

- Typical register of processing activities (hospitals, rest-houses, nurseries, …)
- Register of processing activities tool (cloud-based)
- Identification of processing activities needing a DPIA
- Identification of typical risks for each processing activity
- Documents
  - Data subject access rights (web site – admission)
  - Privacy statements
  - Addendum to the employment contracts
  - GDPR terms and conditions for controller's contracts
  - …
- DPOaaS – remote and local assistance – interface with the Data Protection Authority
- Multidisciplinary support team (lawyers, doctor, cybersecurity)
- Review of common subcontractor's contracts

NIS Directive - Timing

- Published in July 2016
- Entry into force August 2016
- Translation in national law before May 9th, 2018
- 19 countries on time
- 8 countries late
- Belgium has approved the draft legislation on March 21st, 2019
- Officially published on May 3rd, 2019

NIS Directive - Obligations

- Member states need to designate a national authority
- Member states need to cooperate
- Operators of Essential Services (OES) need to take appropriate technical and organizational measures to manage cybersecurity risks
- OES need to take appropriate measures to prevent and minimize the impact of incidents

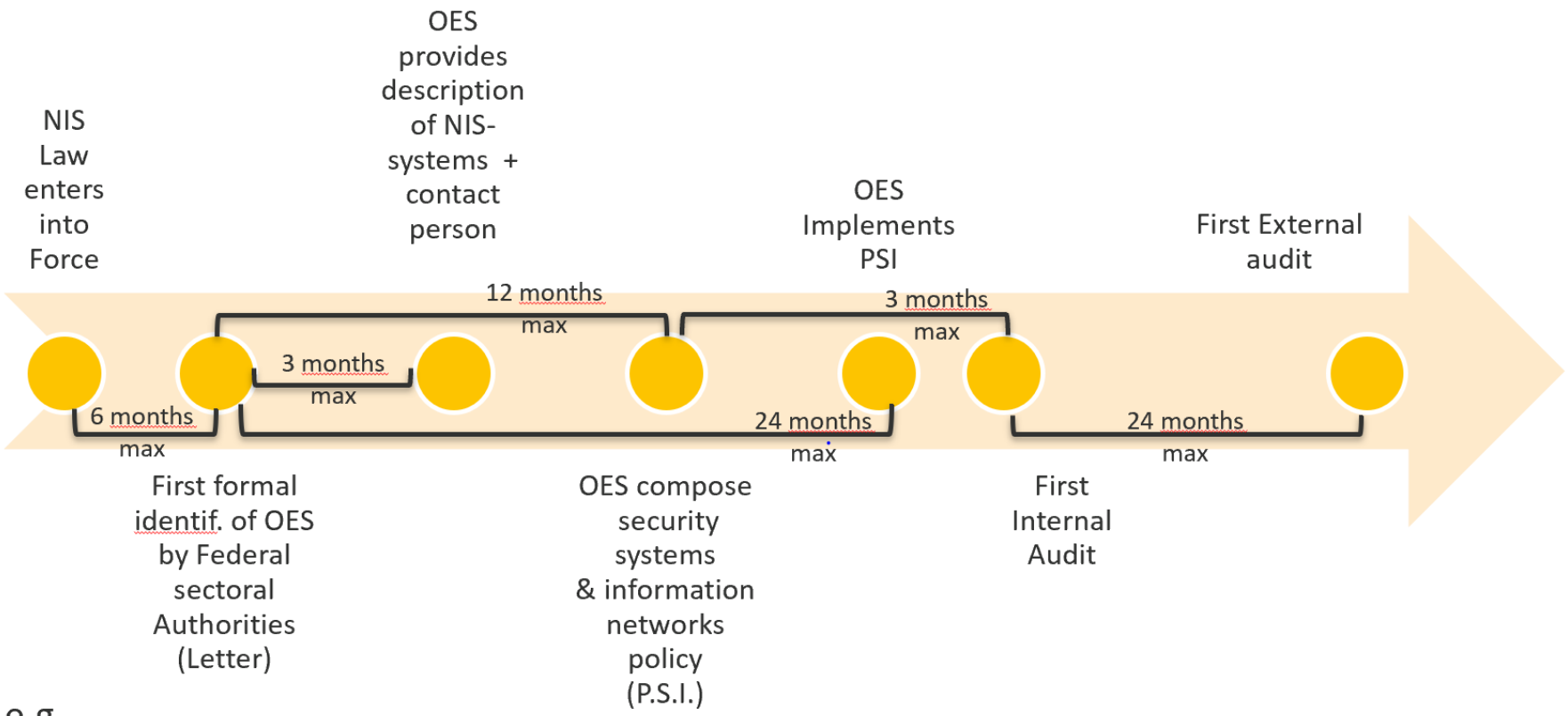
NIS Directive - Obligations

- OES need to prove its conformity with the security requirements general obligations based on a risk analysis
- An ISO 27001 certification (or recognized equivalent standard) will give a conformity presumption
- Internal security audit every year
- External – independent audit every 2-3 years

NIS Directive - Obligations

- OES need to communicate every significant security incident
- OES need to rectify every non-conformity discovered during the external audit within 3 months
- Penalties for hiding security incidents
- Penalties for not fixing identified non-conformities

NIS Directive - Timeline



e.g.

May 2019	Nov 2019	Feb 2020	Nov 2020	Nov <-> Feb 2021	2021	Feb 2023

NIS Directive - Actions

- Inform members about the local legislation status and obligations
- Alert members about cybersecurity risks
  - Availability vs. Confidentiality / Integrity
- Meet ministerial cabinets and sectoral authority to discuss budget and applicability

NIS Directive – Security Working Group

- Organize information security meetings
- Members share experience and best practices
  - ISO 27001 conformity
  - Data governance
  - Network isolation
  - Strong authentication
  - Cyberattack feedback
  - …

Secure Healthcare Community

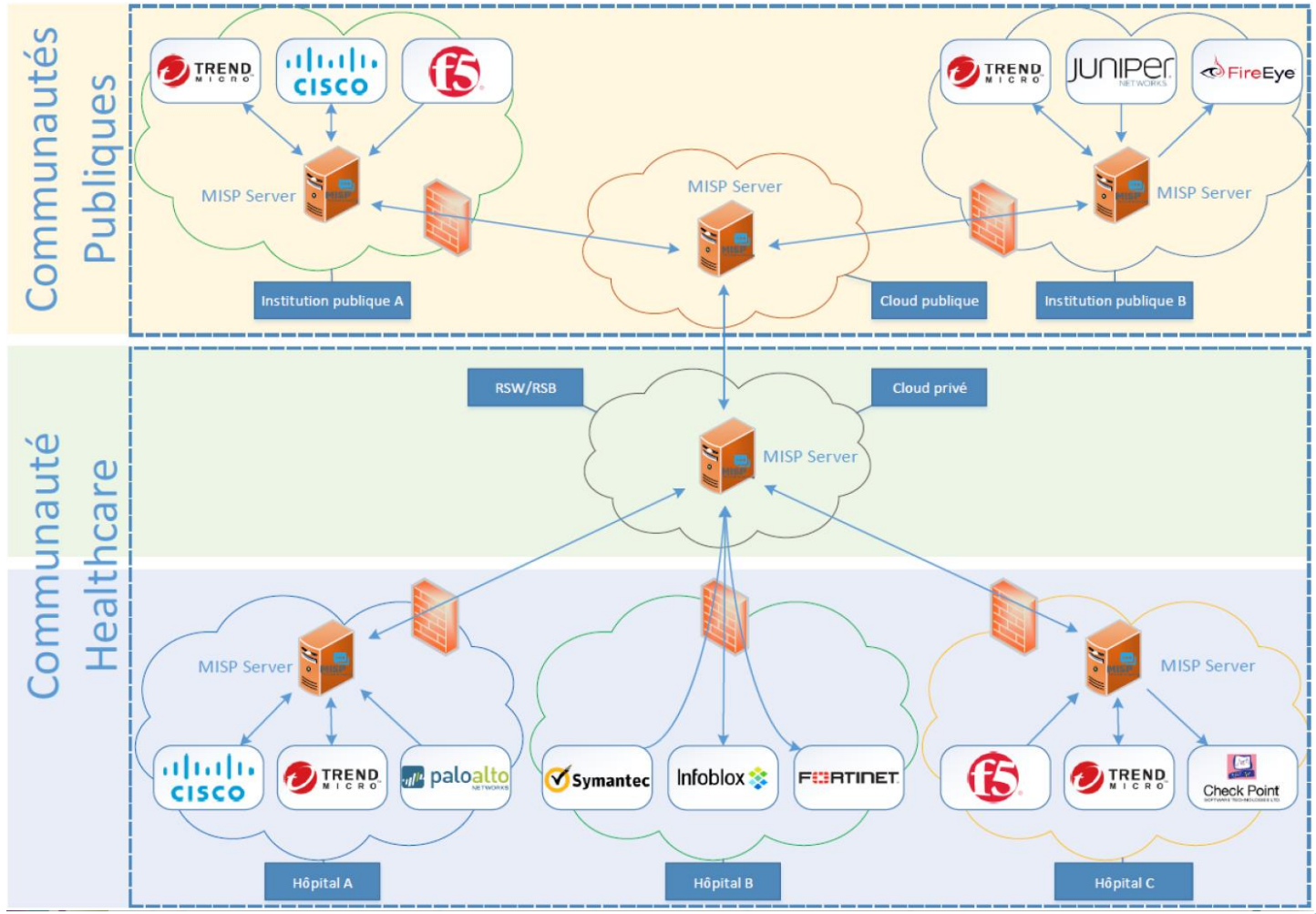
“Cyber threat information is any information that can help an organization identify, assess, monitor, and respond to cyber threats. Cyber threat information includes indicators of compromise; tactics, techniques, and procedures used by threat actors; suggested actions to detect, contain, or prevent attacks; and the findings from the analyses of incidents. Organizations that share cyber threat information can improve their own security postures as well as those of other organizations” - NIST

Malware Information Sharing Platform

Malware: *software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system*

- Open source platform
- Developed by Belgian Defense and NATO
- Used by 6000+ organizations worldwide
- Vendor independent
- Open API

Malware Information Sharing Platform



Conclusion

"There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked."

John Chambers, former CEO, Cisco