Global Forum
Shaping the future 2016

**DIGITALIZATION:** THE GLOBAL TRANSFORMATION

**Monday 19th & Tuesday 20th September 2016**

**Evoluon Center,** Eindhoven, Netherlands

SystemX
INSTITUT DE RECHERCHE TECHNOLOGIQUE

# Cybersecurity Best Practices

Philippe WOLF

## S7: Workshop Cyber and Supply Chain

# Theory of marginal gains

- Olympics cycling: Marginal gains underpin Team GB dominance

- Does it work in cybersecurity?

# Successive small corrections

- Marginal gains
  - More training programs
  - New security filters rules
  - Better definition of passwords
  - One more antimalware
- It is not sufficient in cyberdefence against a determined and prepared opponent
  - 50% better protection does not reduce the risk by half (weakest links, domino and butterfly effects)

# Radical changes are needed

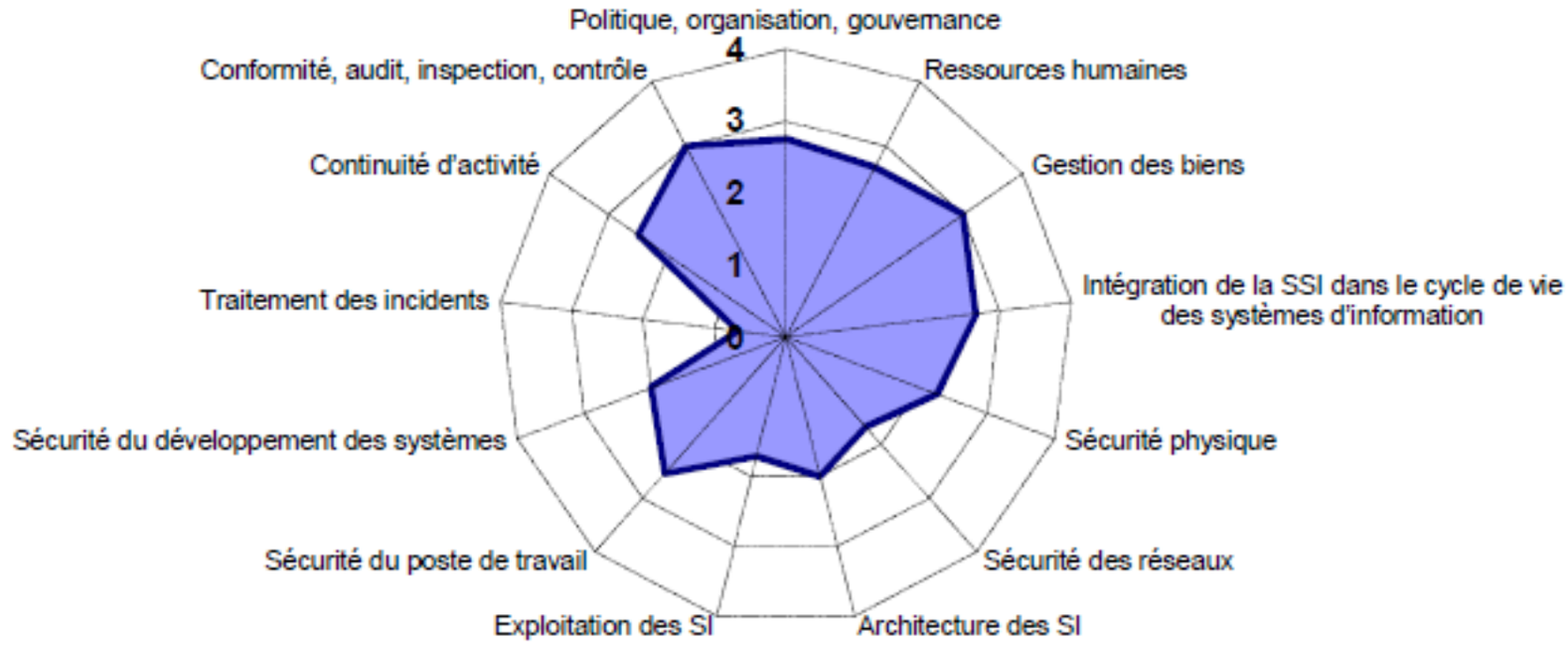
- Optimization of
  - employee behaviour
  - business and technology processes
- Best practices in a global approach
  - Compliance levels must exceed a few percent of existing standards
  - Efficiency needs control
    - Must cover the entire supply chain
- What framework to Use?
  - 3 examples (1US, 2 FR)

# NIST Cybersecurity Framework

- Cybersecurity — Executive Order 13636 — 2013
  - Improving Critical Infrastructure Cybersecurity
    - (1) information sharing
    - (2) privacy
    - (3) the adoption of cybersecurity practices (NIST with private sector)
      - 22 categories, 98 subcategories

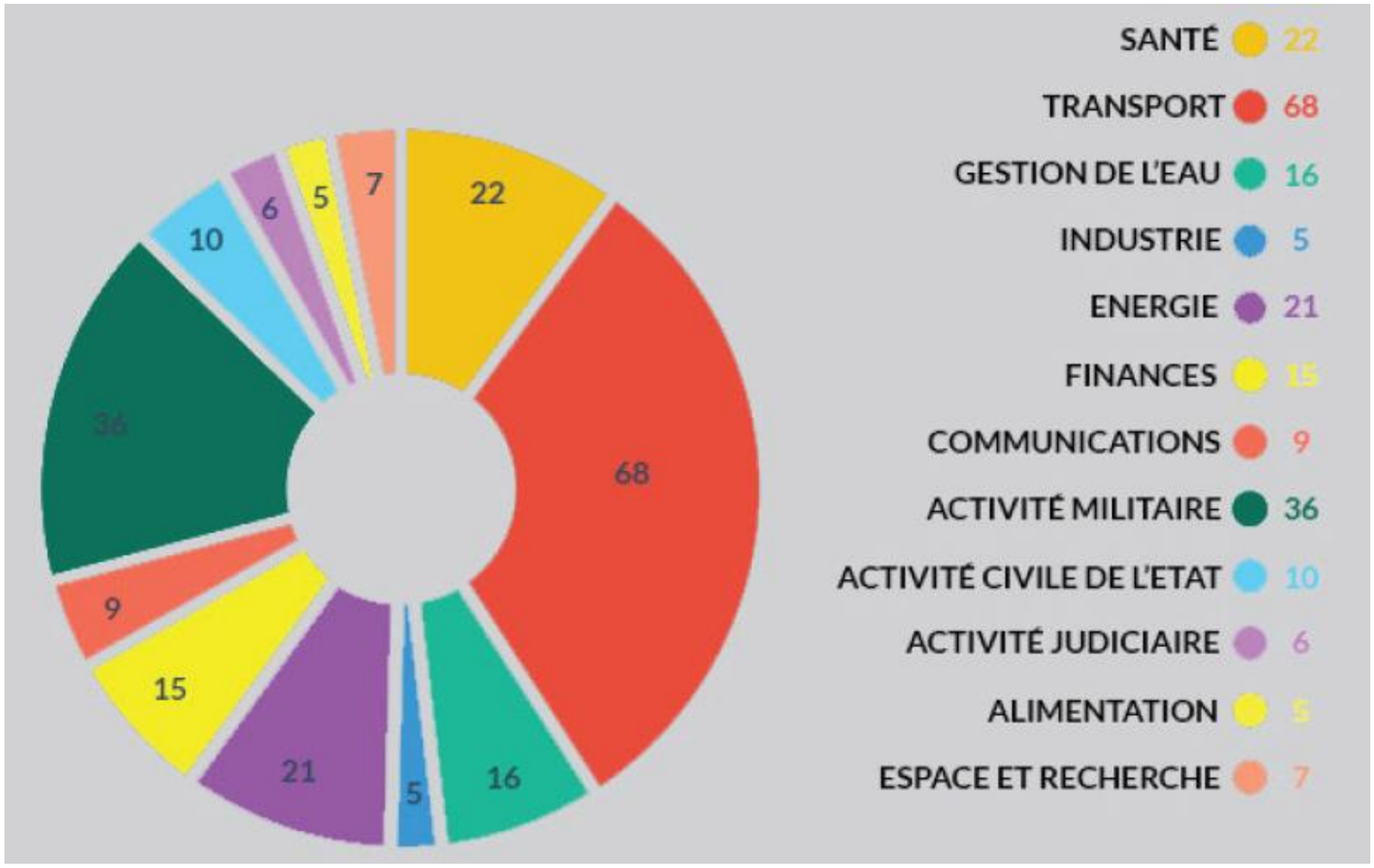

# French Public Cybersecurity Framework

- Circulaire Prime Minister — August 2014
  - Applicable to all public entities
    - 10 Principles
    - 13 ISO 27xxx Domains
    - 34 Objectives and183 Rules




# French Framework for Critical Infrastructures

- Written in Law
  - Applicable to all designated Vital Operators of Critical Infrastructures
    - 20 Domains
    - 71 Rules




# Matching of Frameworks

- They are compatible!
- They cover the necessary changes in a global approach
- The completeness seems fulfilled

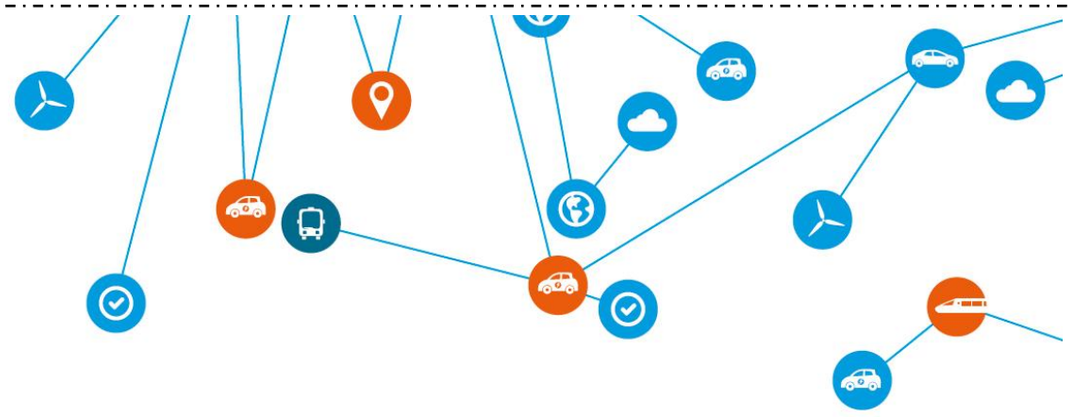
| | | | | | |
|---|---|---|---|---|---|
| | **Protective Technology (PR.PT):** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. | **PR.PT-3:** Access to systems and assets is controlled, incorporating the principle of least functionality | · **COBIT 5** DSS05.02<br>· **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2,<br>· **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7<br>· **ISO/IEC 27001:2013** A.9.1.2<br>· **NIST SP 800-53 Rev. 4** AC-3, CM-7 | **INT-REX-HS<br>PHY-TELECOM<br>PHY-CI-CTRLACC<br>PHY-CI-TRACES** | **13.1.** |
| | | **PR.PT-4:** Communications and control networks are protected | · **CCS CSC** 7<br>· **COBIT 5** DSS05.02, APO13.01<br>· **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6<br>· **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1<br>· **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7 | **PHY-TELECOM** | **16.3.** |
| | **Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood. | **DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed | · **COBIT 5** DSS03.01<br>· **ISA 62443-2-1:2009** 4.4.3.3<br>· **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4 | **PHY-SI-SUR<br>RES-ENTSOR** | **8.1.** |
| | | **DE.AE-2:** Detected events are analyzed to understand attack targets and methods | · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8<br>· **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2<br>· **ISO/IEC 27001:2013** A.16.1.1, A.16.1.4<br>· **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4 | **EXP-GES-ANTIVIR<br>EXP-JOUR-SUR** | **7.2.** |
| | | **DE.AE-3:** Event data are aggregated and correlated from multiple sources and sensors | · **ISA 62443-3-3:2013** SR 6.1<br>· **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 | **EXP-POL-JOUR** | **6.1.** |
| | | **DE.AE-4:** Impact of events is determined | · **COBIT 5** APO12.06<br>· **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI -4 | **EXP-OBSOLET<br>DEV-LOG-ADHER<br>TI-INC-REM** | **4.4.** |
| | | **DE.AE-5:** Incident alert thresholds are established | · **COBIT 5** APO12.06<br>· **ISA 62443-2-1:2009** 4.2.3.10<br>· **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8 | **TI-QUAL-TRAIT** | **9.1.** |
| | | | · **CCS CSC** 14, 16 | | |

# And now concerning the supply chain…

A lot has to be done to make these frameworks applicable through the entire supply chain

- Contracts
- Efficiency (audits, control)
- Liability
- Sanctions
- Education

SystemX
INSTITUT DE RECHERCHE TECHNOLOGIQUE



# Questions?

philippe.wolf@irt-systemx.fr