



Cybersecurity - a few thoughts

Fedil-ICT & EY

07/04/2017



THE GOVERNMENT
OF THE GRAND DUCHY OF LUXEMBOURG
Ministry of the Economy



- Major challenges in cybersecurity
- Focus of the Ministry of the Economy
- Examples; next steps
- “Best practice” approach



Cybersecurity needs a **transversal** and **cross-sectorial** approach

Behaviour

- Awareness

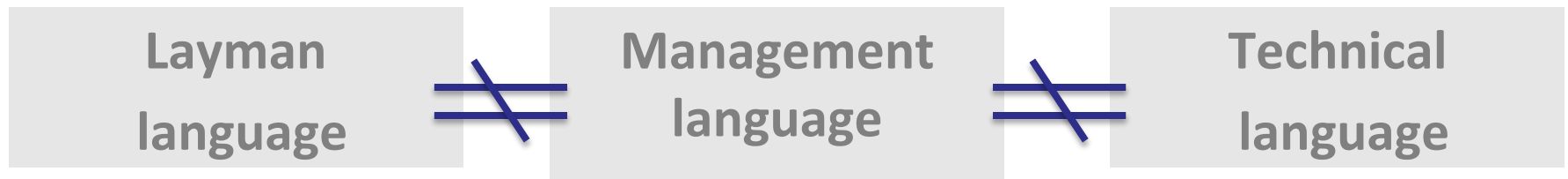
Organisation

- Policies
- Compliance

Technology

- Protection
- Detection

Challenge: implement effective and efficient **internal collaboration**



Major challenges



Challenge: to implement **all** proportionate and necessary measures

Behaviour

- Security charter
- Desk Instructions

Organisation

- Risk management

Technology

- Incident Response
- Human Resources

Challenge: to reach a **high level of maturity**



Challenge: to implement a **multi-stakeholder governance**:

Risk management
in the perspective
of citizens

Risk management
in the perspective
of customers

Risk management
in the perspective
of yourself

Challenge: to be **objective** and create **comparable results**

- Scope
- Impacts
- Scenarios and granularity
- Probabilities of threats
- Exploitability of vulnerabilities
- Choice of measures
- Effectiveness of measures
- Risk acceptance matrix



Cybersecurity is **not an individual, but a collective challenge**

- Cybersecurity is a fast moving target, increasing in complexity
- The regulatory framework becomes more and more demanding
- Lack of skilled people

Cybersecurity has become a differentiating factor for

- **companies**
- **whole sectors**
- **and even countries!**



Cybersecurity has become a factor of attractiveness and can provide a competitive advantage.

Cybersecurity is an economic opportunity for Luxembourg.



To **democratise** cybersecurity by

Reducing costs and complexity for everybody & fostering **collaboration**

- Provide **taxonomies, methods and tools** for everyone
- **Collaborate, Cooperate, Coordinate**
- Capitalise on **synergies** and **mutualise**



SAVOIR-FAIRE

- SOS**
Comment réagir en cas d'accident.
- LES BONS REFLEXES**
Apprenez les gestes qui sauvent.
- L'APPROCHE RSSI**
Renforcez vos défenses. Organisez votre protection.

Incident Coordination and Incident Handling



Publications and Presentations



STARTUP
SECURITY KIT



DIAGNOSTIC



**CIRCL
AIL**
Analysis of Information Leaks



**CIRCL
MISP**
Threat Sharing



**CIRCL
BGP Ranking**



**CIRCL
Passive DNS**



**CIRCL
Clean
USB Sanitizer**



**CIRCL
DMA**
Dynamic Malware Analysis



MONARC

Analyse de risques - My Risk analysis

Informations générales | Table des risques

Impact	M x V											
	0	1	2	3	4	6	8	9	12			
0	0	0	0	0	0	0	0	0	0			
1	0	1	2	3	4	6	8	9	12			
2	0	2	4	6	8	12	16	18	24			
3	0	3	6	9	12	18	24	27	36			
4	0	4	8	12	16	24	32	36	48			

$\Sigma R = I \times (M \times V)$

R : Risque - I : Impact - M : Menace - V : Vulnérabilité



Link cybersecurity to business in a PPP approach

Threat Intel

- Open TI
- Contextual TI
- Metrics for RA and governance

Training

- Technical
- Multi-disciplinary
- Teams
- Simulators
- Exercises

Testing

- Due Diligence
- ISMS
- Start-Ups
- Label
- Certificates



- **Separate** business and cybersecurity requirements – link them by providing the right impacts and scope
- **Harmonize** cybersecurity requirements; define scopes, define the right granularity for risk scenarios; follow threats and vulns.

This « **best practice** » approach:

- is **scalable** and **agile** and respects the principles of **necessity** and **proportionality**
- fosters a **structured and comparable** reporting in cybersecurity
- fosters **collaboration** and **exchange**
- Object oriented risk management allows **the implementation of multiples views**
- **Reduces the effort of multi-compliance**



Thank you for your attention

François Thill



LE GOUVERNEMENT

CESSEZ D'ÊTRE UNE PROIE SUR INTERNET. PROTÉGEZ VOS DONNÉES.

www.securitymadein.lu



Véronique M.
— VICTIME E-FRAUDE —
INDÉPENDANTE



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

SECURITY
MADEIN.LU

