FEDIL CYBERSECURITY ASSESSMENT ONLINE TOOL

17 October 2019

WELCOME WORDS

JEAN-LOUIS SCHILTZ
FEDIL Vice-Chairman
Chairman FEDIL-Digital & Innovation – Board Group

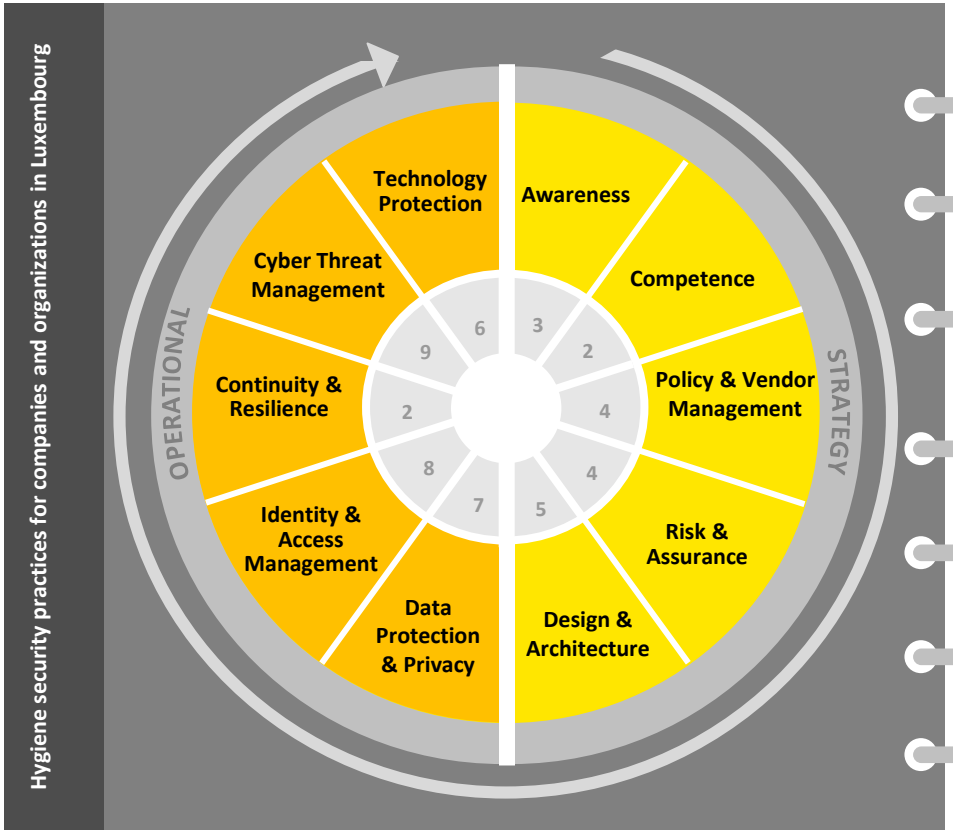
CYBERSECURITY CHALLENGES FOR THE INDUSTRY

PASCAL STEICHEN
CEO, SECURITYMAIDEIN.LU

PRESENTATION OF „FEDIL CYBERSECURITY ASSESSMENT ONLINE TOOL“

BRICE LECOUSTEY
Advisory Partner, EY Luxembourg
ALEJANDRO DEL RIO
Cybersecurity & Data Privacy Manager, EY Luxembourg

We built in collaboration with companies and organizations a set of security practices, which aimed to strengthen and facilitate the journey towards the protection against new threats



COMPLIANCE

› We have outlined a corpus of hygiene practices of cyber security, mapped on main security standards (ISO27001, NIST), new requirements from EU regulations (GDPR, NIS Directive) and best practices launched by national agencies in boarder countries (e.g. ANSSI, BSI).

› These rules are business oriented and not only aligned with Luxembourg requirements and specificities, but also with objectives of "The National Cyber Security Strategy III"

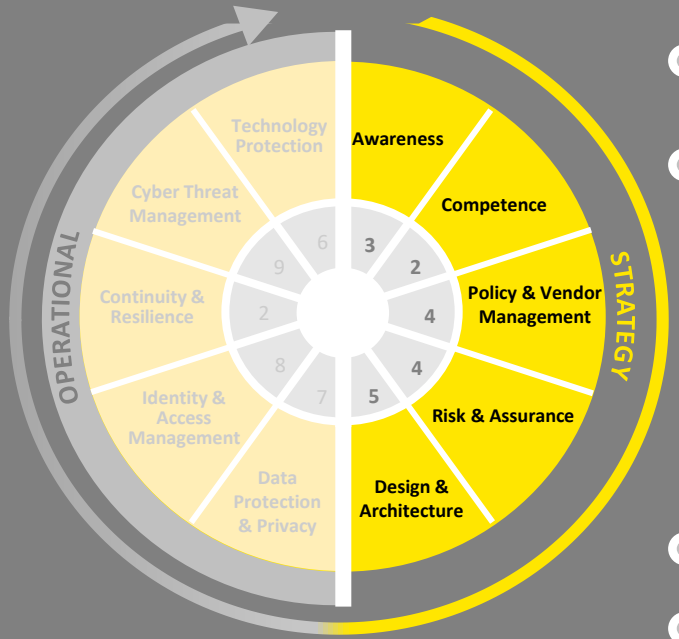
PROVIDERS OF ESSENTIEL SERVICES (*initial approach*)

› It was confirmed in 2016 the set of hygiene practices through round interviews with cyber security stakeholders, following providers of essential services (aligned with ANSSI/HCPN lists) :

- Professionals of Financial Sectors
- Big 4 firms
- National Telecoms and Internet Network providers
- Digital market players
- Headquarters of national and international firms
- Energy & Utilities providers
- Healthcare relevant actors
- Aerospace cluster
- Transports services providers

What is the minimum level of standards which should be applied ?
Cyber security strategy

Hygiene security practices for companies and organizations in Luxembourg



CYBER SECURITY STRATEGY - CONSENSUS OF BEST PRACTICES

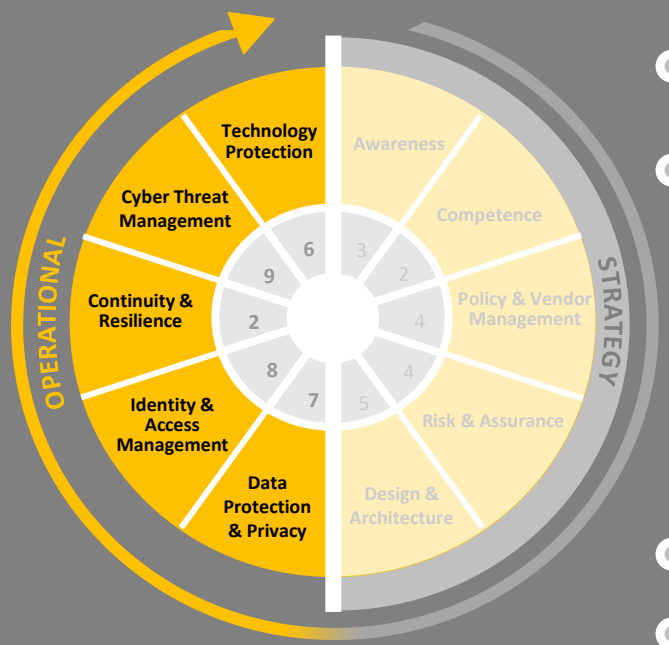
- All employees are annually informed about hygiene rules of security and trained on a real-time basis and based on user behaviors
- The organization has defined an enterprise-wide security awareness program
- The organization has developed a process to identify roles that require specialized security training based on roles and/or risks
- Information security is visible at the Board level. Information security updates are provided to the Board every time the Board meets
- The information security organization is fully staffed and all resources have sufficient knowledge and skills to execute their responsibilities
- Define an IT security policy. Assess whether the policy is in line with leading best practices (e.g. ISO27001)
- Key security projects are sponsored. Resources and budget for treatment of risks are considered
- Vendor risk is a key item on the enterprise risk agenda and vendor risk is monitored on a regular basis
- Information security risk management policies guide a consistent organizational approach for framing risk
- Remote access to the corporate network, including network administration, is only allowed to company-trusted equipment

⏩ Based on our first round of interviews, we have identified that some sectors, such as Transport services and Telecommunications, have already gone further than the consensus according to their strong level of digitalization and level of maturity in the field of cyber security.

⏩ For example, some actors in these areas have already crossed the not of industrialization for Password management and Asset inventory. Also, all actors interviewed in these sectors are a step further in terms of security policy and risk management.

What is the minimum level of standards which should be applied ?
Cyber security operational

Hygiene security practices for companies and organizations in Luxembourg



CYBER SECURITY OPERATIONAL - CONSENSUS OF BEST PRACTICES

- Data classification exists, along with a standard, and tools are used to ensure all critical data is classified and secured appropriately
- A policy covering cloud security has been formally defined, documented, published and communicated, which is mapped to industry standards
- A policy covering mobile security has been formally defined, documented, published and communicated, which is mapped to industry standards. Company's devices are centrally managed through a management system (MDM - mobile device management)
- Appropriate privacy policies and procedures describing normal use and retention period of information of personal information have been developed
- Multi-factor authentication is required for use of privileged access and access to any sensitive/confidential data
- Physical security controls are effectively logged and monitored
- Critical business process/application has been identified through consistent Business Impact Analysis
- Incident response plan is regularly tested and every time their incident response plan changes considerably; results are used to update and enhance the plan
- The company has published guidelines for security software development

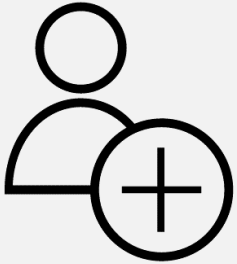
⏩Based on our first round of interviews, we have identified that some of sectors, such as Healthcare and Aerospatial, have already gone further than the consensus according to their risk appetite and level of threats.

⏩Some actors of Healthcare have adopted advanced data encryption solutions while certain telecommunication players are slightly further the best practices on Business continuity, as business is highly committed to prevent any operational disruption.

Next steps

Actions to be considered in next stages to go further

For all companies to start using the tool as a first step



Increase awareness towards this tool to have more participants

Strengthen collaboration between public bodies and private sector

Thank you !

PANEL DISCUSSION FEEDBACK FROM THE INDUSTRY

MODERATOR: PASCAL STEICHEN, CEO, SECURITYMADEIN.LU

DONIA EL KATEB, IT Security Lead, Luxtrust

YANNICK KIRCHHOFFER, CIO, Luxair

PATRICK NJIWOUA, CIO, Ketterhill

FARUK SARI, Assistant CISO, Goodyear

FEDIL

The Voice of Luxembourg's Industry

EY

Building a better working world

7, rue Alcide de Gasperi
Luxembourg-Kirchberg
Boîte postale 1304
L-1013 Luxembourg

fedil@fedil.lu
tel: +352 43 53 66-1
fax: +352 43 23 28
www.fedil.lu