CyberSecurity_Study

Security practices for providers of essential services in Luxembourg

While the world is becoming more resource-constrained, globalized and urbanized, governments and organizations seek more efficient and smart solutions in responding to shifts in preferences and expectations. The new waves of technology – the Internet of Things (IoT), Artificial Intelligence (AI), robotics, virtual reality and sharing economy platforms – are taking existing products and services to a new level. Just in recent years, investor funding in AI has risen nearly sevenfold, from 45 million USD in 2010 to 310 million USD in 2015[1]. Across industries, the widespread rollout of robotics is already under way, with spending expected to reach 67 billion USD annually by 2025[2].

The intense advance of technologies has been an ongoing research topic. Three themes – intelligent, digital, and mesh – form the basis for the Top 10 strategic technology trends for 2017[3] according to Gartner Top 10 Strategic Technology Trends. Pointing out these trends such as advanced machine learning, intelligent apps, blockchains, conversational systems, digital technology platforms, and adaptive security architecture, the report implies digitization of the World to be experienced by individuals, organizations and governments.

EY, in its recent research[4], has outlined three root causes of the global transformative trends which are technology, globalization, and demographic change. These main forces define the present and shape the future by their impact on businesses, economies, industries, societies and individual lives. Different types of innovations based on technologies and new business models, are altering consumption patterns and are ubiquitous in day-to-day activities from health care to education and banking.

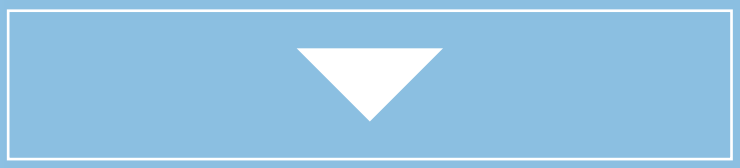
1 "Deep Interest in AI: New High in Deals to Artificial Intelligence Startups in Q4'15," CB Insights, February 2016.
2 International Federation of Robotics; Japan Robot Association; Japan Ministry of Economy, Trade & Industry; euRobotics; Company Fillings, Boston Consulting Group; EY Analysis.
3 "Gartner's Top 10 Strategic Technology Trends for 2017"
4 The upside of disruption Megatrends shaping 2016 and beyond, EYQ, 2016

READ MORE

In the light of the accelerated pace of progressive technologies, the number and cost of security incidents and data breaches continuously increase. The most recent researches internationally demonstrate steady growth of data breaches cost and the severity of impact caused by them with malicious or criminal attacks being the prevailing root of these breaches. According to the research conducted by Ponemon Institute[5] involving 383 companies from 12 countries, the average total cost of data breach increased by 29% since 2013 and reached 4 million USD in 2016 while the average cost per lost or stolen record increased by 15% since 2013 and amounted to 158 USD.

The component of the 4 million USD cost of data breach

The cost of data breach per record varies by industry and is higher for heavily regulated sectors such as healthcare, education and finance because of fines and the higher than average rate of lost business and customers.



5 "2016 Cost of Data Breach Study: Global Analysis", June 2016, Benchmark research conducted by Ponemon Institute LLC and sponsored by IBM

Lost business cost
1,63 million USD

Abnormal turnover of customers, increased customer aquisition cost, reputation losses, diminished goodwill

Post response
1,10 million USD

Helpdesk, inbound communications, special investigations, remediation, legal expenditures, product discounts, identity protection service, regulatory interventions

Detection and escalation
1,09 million USD

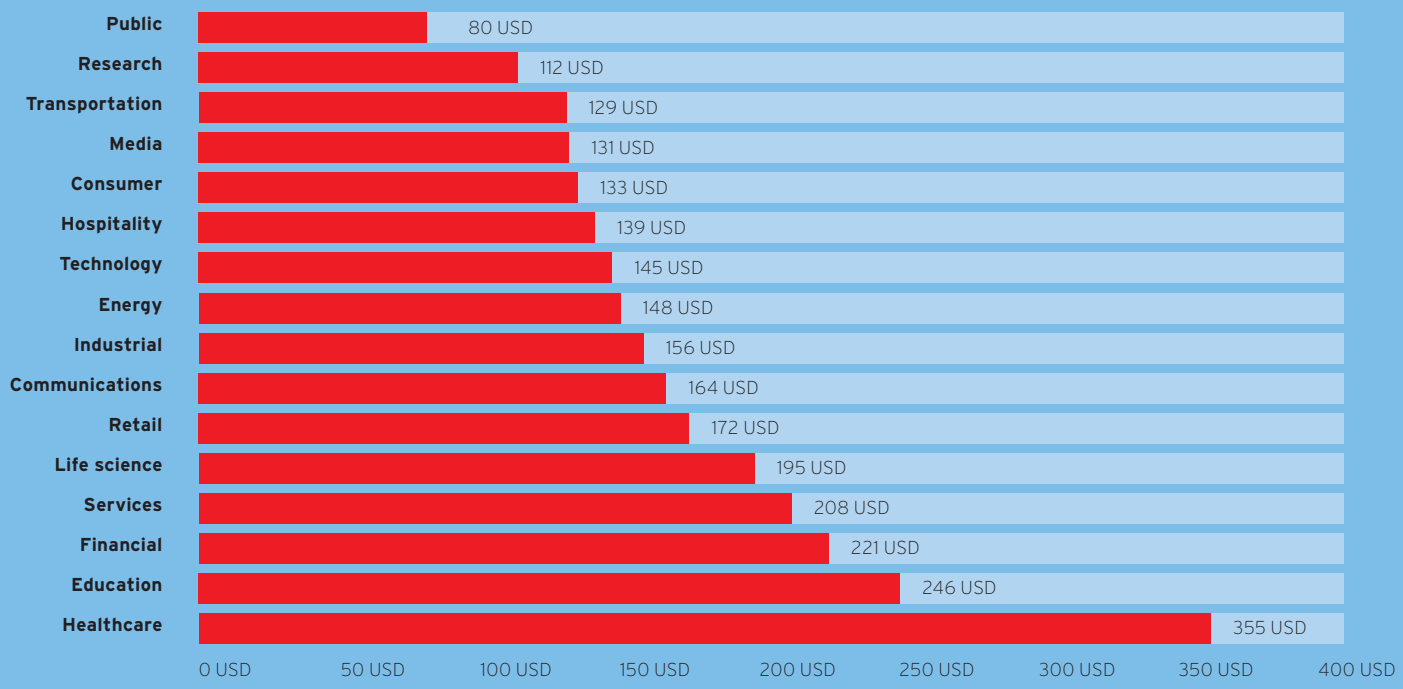
Forensic and investigative activities, assessment and audit services, crisis team management and communications to executive management and BoD

Notification
0,18 million USD

Diclosure of data breach

Cost per record by industry classification, measured in USD

Over recent years and under the pressure of more regulation, organizations have invested in their corporate shield. Significant progress has been made in taking measures to strengthen this shield and in the last two to three years, organizations focus more on their capabilities of detection and escalation. Most organizations however are lagging behind in preparing their reaction to a breach, still ignoring the all-too-familiar statement, "it's not a matter of 'if' you are going to suffer a cyber-attack, it's a matter of 'when' (and most likely you already have...)." The statement is constantly justified as even the most notorious incidents have led to a sensational data leakage involving world famous companies all around the globe.



According to EY's most recent Global Information Security Survey[6] over the last two years, 87% of board members and C-level executives have said that they lack confidence in their companies' level of cybersecurity. Further results of the survey are presented below.

SEE BELOW

Indicative results of the
2016 EY Global Information Security Survey

44%
do not have a Security Operations Center (SOC)

64%
do not have, or only have an informal, threat intelligence program

62%
would not increase their budgets after experiencing a potentially harmless breach

49%
see identifying suspicious traffic over their networks as challenge

86%
do not think that their information security function is meeting the needs of the organisation

89%
do not evaluate the financial impact of every significant breach

56%
mention that lack of skilled resources is one of the key challenges

53%
say their budgets increased over the last 12 months

57%
have had a recent significant cyber incident

55%
say careless employees are their biggest vulnerability

52%
say malware is their biggest threat

51%
say phishing is their biggest threat

57%
rated BCM as their joint top priority, alongside data leakage/date loss prevention

5%
have recently made a significant change to their strategy and plans

42%
have no communications strategy or plan

39%
say they would issue public statement to the media within the first week while investigations continue

According to the latest European study on digital transformation by the European Commission[7], the Grand Duchy occupies an honourable 6th place based on the Digital Transformation Enablers' Index (DTEI). Luxembourg is considered to be one of top-10 most digitized countries[8] worldwide together with countries such as Japan, Norway, Sweden, Finland, the Netherlands, Switzerland and Singapore. The assessment is based on the Network Readiness Index (NRI) and has been conducted for 139 countries which "measures the capacity of countries to leverage Information and Communications Technologies (ICTs) for increased competitiveness and well-being with consideration to recent innovation trends through the lens of NRI".

Even for a country being so profound in ICTs, there are still areas to be attained to and cybersecurity is one of the highest priority among them. This is constantly justified through occurring security incidents and breaches, an example of which is the most recent successful attack on the state's internet infrastructure. Overall in 2016, there were over 120,000 events and 900 incidents registered which led to approximately 4,000 special investigations[9].

Public initiatives for Cyber resilience in Luxembourg

Considering the abovementioned, it is natural that cybersecurity initiatives in Luxembourg are continuing to grow. Currently, there are various organizations which work with each other at country level to address the different dimensions of cybersecurity. One of them is GOVCERT.LU – the Computer Emergency Response Team of the Luxembourg government, whose role is to manage incidents related to the governmental information systems and critical infrastructures, coordinates with the Cybersecurity Board (CSB) of Luxembourg. One of the purposes of this collaboration is to provide a national cybersecurity policy, strategy and roadmap which are up-to-date and address the security needs of the governmental organizations within the country.

Similarly, another service of the Ministry of Luxembourg, Computer Incident Response Centre Luxembourg (CIRCL), which is a comparable country initiative. It is also designed to ensure review, report and respond to computer security threats and incidents as well as provide a dependable and trustworthy point of contact for anyone wishing to report security incidents for communes, non-governmental organizations or the private sector. It offers classes to its members and shares field experience through a set of trainings and technical courses.

Establishments such as the Cyber World Awareness and Security Enhancement Services (CASES) play a significant part in promoting activities to create awareness and communicate best practices on the subject of security. In addition to this, and even if several pre-existing services have already been present in Luxembourg, as of February 2015, the country has further increased open communication and transparency among the different players.

With the advent of Security Made in Luxembourg (SMILE), Luxembourg is now equipped with a single and centralized online source of information, guidelines, best practices and news for those interested and involved in cybersecurity initiatives. The goal of SMILE is to also provide a toolbox with useful cybersecurity solutions for private users, organizations and the wider ICT community. One evident measure, which has been taken as a result of SMILE, is that of utilizing a common Malware Information sharing platform. The platform allows users to share threat indicators with each other among the private and public sector.

Finally, FEDIL, The Voice of Luxembourg's Industry, has been working for many years now on actively contributing to several initiatives in Luxembourg, mainly for organization of the industrial sector. It provides support to members in all kinds of areas notably in cybersecurity.

FEDIL-ICT and EY Cybersecurity annual studies

The cybersecurity study[10] conducted by FEDIL-ICT and EY in 2016 aimed at providing organizations and companies in Luxembourg, guidance on adopting a common approach in regards to security objectives, security requirements and security measures. At the core of the study, 10 security domain areas have been covered combining both a strategic and operational direction:

- **Cybersecurity Strategy:** Awareness, People competencies, Framework security, Risk and Assurance, Design and Architecture, and
- **Cybersecurity Operational:** Data Protection and Privacy, Identity and Access Management, Continuity and Resilience, Threat Management, and Technology Protection.

The study was directed at the providers of essential services in Aerospace industry, Aviation, Banking, Healthcare, Power and Utilities, Public sector, Telecommunication and Start-ups. For the purpose of the study, security and business stakeholders provided their opinions on the security areas out of suggested 10 key domains.

The analysis was performed through a series of interviews with different organizations. The first step was to identify the participants who could provide the most pertinent insight. This was done by contacting relevant panelists (such as CIO's, CISO's CTO's) of the biggest players of the strategic industries in Luxembourg. Afterwards series of interviews were conducted based on a set of 50 practice rules which

6 "Path to cyber resilience: Sense, resist, react", EY's 19th Global Information Security Survey 2016-17
7 Digital Transformation Scoreboard 2017: Evidence of positive outcomes and current opportunities for EU businesses, January 2017
8 "The Global Information Technology Report 2016" by the World Economic Forum.
9 According to statistics by CIRCL
10 "Security practices for providers of essential services in Luxembourg"

Deuxième génération de moteurs et chaîne cinématique
+ Predictive Powertrain Control
+ Analyse de mise en exploitation FleetBoard

Efficience sur toute la ligne.

Le système PPC et l'analyse de performance FleetBoard sont disponibles en option.
Pour plus d'informations, veuillez contacter votre distributeur Mercedes-Benz.

Mercedes-Benz
Trucks you can trust

Mercedes-Benz Luxembourg S.A.
Mercedes-Benz Leudelange – 3, rue Nicolas Brosius, L-3372 Leudelange, Tel.: 26 37 26-1 (Vente et Service)
Mercedes-Benz Roost – 2, route de Cruchten, L-7759 Roost, Tel.: 26 80 85-1 (Service)

were derived from common security standard frameworks (such as ISO270001, BSI C5, NIST and COBIT 5). Based on the inputs collected from these interviews and the available resources, an analysis was performed in order to identify which key players were leading in particular disciplines and the areas in which further development was required. Consequently, specific aim and requirements in the form of 50 security practices have been described for each of the areas to be reached by the organisations wanting to excel in bringing their cybersecurity to the highest level according to global best practices and specific industry standards. These were grouped in 10 areas and can be described as the following:

- **Awareness** about practice rules of security and regular trainings for staff, including specific trainings on technical aspects for IT and IS staff,
- **People Competencies** should be developed and maintained, relying on Chief Information Security Officer (CISO) and a qualified workforce of IT security professionals,
- **Security Framework** is essential for each organization moving towards IS enhancement. Thus, organizations with support of the top-management should retain a set of IS policies and procedures and perform regular assessments of IT and IS,
- **Risk and Assurance** implies a regular monitoring and reporting on IS functions as well as risk management activities,
- **Security Architecture** implies maintaining high-risk profile devices and critical information assets together while performing dedicated technical reviews and audits and enforcing relevant policies and procedures on the practice of bringing your own device (BYOD), remote access and software management,
- **Data Protection and Privacy** is about identification of a high-valued data and data classification as well as establishing relevant privacy procedures and controls,
- **Identity and Access Management** prescribes the rules and procedures for logical and physical access management involving passwords management, user and privileged accounts control and handling,

- **Continuity and Resilience** involves conducting Business Impact Analysis (BIA) along with adopting a strategy for business continuity and disaster recovery,
- **Threat Management** requires the establishment of a comprehensive incident management process and implementation of a proactive threat treatment approach,
- **Technology Protection** involves adopting a set of technical controls and measures in order to provide security for network, operation systems and applications.

5 SECURITY TOPICS FOCUSED IN AN OPERATIONAL INSIGHT

5 SECURITY TOPICS FOCUSED IN A STRATEGICAL INSIGHT

Another important part of the study was to perform a maturity assessment of the respondents in the 10 defined areas, conducted based on two key functional aspects which made up the questionnaire.

As key outcomes of more than 50 interviews performed with panelists, the majority of sectors have reached the minimum standard level. Nonetheless, while we expected some security fields, like "Awareness" or "Data Protection and Privacy", to be ones of the most covered topics, for most respondents, we observed that capabilities of majority of companies are slightly behind.

Also, in view of Luxembourg's ambitions to develop the ICT sector, cybersecurity is becoming a strategic pillar to enable digital transformation of the country. From that perspective, it is worthy to note the good positioning of startups and ICT companies in the cybersecurity landscape.

Data Protection and Privacy is a trend topic and benefits from a very disparate coverage level in Luxembourg. We noted that certain sectors, where data protection is a main component of the core business, were in the leading position on that matter. Technological evolution and increasing amount of manipulated data will lead to important challenges on Identity Access Management and Technology protection (e.g. encryption, digital signature, etc.) in the coming years. Indeed, we observed also a correlation between the capability to invest in R&D and the level of maturity in the field of technology protection.

Also, Threat Intelligence and vulnerability management are growing topics but still a new field in the Luxemburgish environment, as reflected in the results of our interviews. It is worthy to note a real effort among all panelists to reinforce their capabilities in Cyber threat management, in alignment with evolution in European regulations (e.g. Directive NIS, Regulation 910/2014/EU – Electronic identification and trust services for the electronic market, 8/2014).

The results on the category "Functional capabilities" also reflect a satisfying commitment and sponsorship at the top-management level given that cybersecurity is now on the top of the agenda of boards and C-level meetings.

Nevertheless, all of the companies interviewed agree on the fact that it is currently really complicated to find out new talents in cybersecurity (private, public, advisory, companies) and that it is now crucial to set specific talent and training programs in order to meet the decision-makers expectations and sustain cybersecurity challenges over the years.

Our collaborative study has shown that while Luxembourg is on a steep progression towards improvement of security measures, and even if it has led to continuous positive outcomes, more collaboration among the different stakeholders and an augmented level of standardization in the security measures is welcomed bearing in mind the need to address each businesses specific needs.

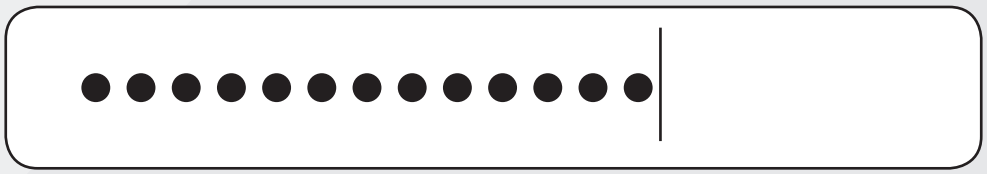
Following these observations, and thanks to intended sectorial initiatives led by key public representatives such as SMILE and the Ministry of the Economy with its new Cybersecurity Competence Center (C3) which will pave the way of providers of essential services in their cybersecurity journey, we can conclude that Luxembourg is now organized to strengthen its security footprint and to become a key player on that field. In order to succeed in standing up from the crowd, all actors need, starting from now, to keep Luxembourg Cybercommunity living and continue to share and enrich the catalog of best practices.

Still, with respect to this, another FEDIL initiative supported by EY has been launched. This will be exposed in the form of a collaborative tool designed to share security practice rules via an online assessment which would produce dynamic feedbacks and recommendations for the online participants.

FEDIL-ICT Cybersecurity Awareness Increase Initiative

The uniqueness and importance of the initiative impose specific demands to the capability, usability and support of the tool thus bringing up the following requirements:

- Accessible for any company in the Grand Duchy
- Dynamic assessment of the maturity against practice rules and/or companies of the same sector/same size
- Profound file/data maintenance options in terms of usability and data processing
- Integration with other data processing packages for alternative display and reporting facilities
- Flexible reporting tools with standard layouts and options for their customization
- Appropriate user support and explicit FAQs
- Multi-year follow up of data
- State-of-the-art in terms of security and data protection
- Flexible anticipated workplace environment while easily accessible and user friendly



The assessment will be carried out for the willing organizations in several steps, which may be described as following:

1. Determining the business profile and completing some basic information about the company (e.g. approximated revenue, number of employees, main industry). This is necessary in order to perform benchmarking only with comparable organizations.
2. Choosing a focus point out of proposed security areas depending on the nature of company's industry and core of business as well as maturity level.
3. Answering the questionnaire. On each of the selected security areas, a set of questions will be proposed allowing to evaluate the maturity level of the organization. This estimated maturity will be then compared with companies having the same characteristics.
4. Setting the objectives and desired future state. Based on the position among company's peers a maturity objective would be set. The tool will provide a description of best practices, an action plan and some relevant material to achieve the desired objective.

With all that, FEDIL intends to build a strong and solid solution enabling comprehensive and easily accessible aid for the organizations and companies in Luxembourg in raising their cybersecurity awareness. This is going to be the 1st Cyber tool for Luxembourg built in a collaborative way with the main providers of essential services of the country, also aligned with a National Cybersecurity Strategy and Digital Luxembourg initiative. It's a new opportunity for adopting a nationwide benchmarking against peers and sharing experience and lessons learnt in terms of reinforcement of a digitized and secure country brand through promotion of security practice rules.

Concluding remarks

Threats of all kinds continue to evolve, and today's organizations find that the threat landscape changes and presents new challenges every day. In response, organizations have learned to defend themselves and respond better, moving from basic-level measures and ad hoc responses to sophisticated, robust and formal processes. Key events such as the increase in digital innovation, expansion of connected products, changing regulatory landscape and the explosion in cybercrime are just a few examples of why organizations needed to evolve their defensive and protective measures.

The Government of the Grand Duchy of Luxembourg and companies operating on its territory are doing their best in order to maintain the status of the highly-developed and mature country reflecting their attitude towards ICTs and cybersecurity. Those initiatives aimed at increasing cybersecurity awareness amongst the citizens, organizations and companies are demonstrating great results in terms of progress and efficiency of efforts applied. To develop a secure IT environment means to respond proactively to a constantly changing IT environment and have in place fundamental activities to strengthen IT security within organizations. Cybersecurity is no longer an issue reserved to IT specialists only and culture of risk management, involving risk assessment and the implementation of security measures appropriate to the risks faced, should be promoted and developed through appropriate regulatory requirements and voluntary industry practices.

About the authors:

EY Luxembourg Project Managers

Brice Lecoustey
Partner, Advisory Leader for the Commercial and Public sector at EY Luxembourg

Kevin d'Antonio
Manager, Advisory Services, EY Luxembourg

FEDIL-ICT Project Managers

Gérard Hoffmann
Chairman, FEDIL-ICT

Edith Magyarics
Board Member, FEDIL-ICT

Daniel Biedermann
Board Member, FEDIL-ICT

Céline Tarraube
Secretary General, FEDIL-ICT