Cover Story

Cybersecurity

A perpetual duel between innovation and intrusion

TEXT Stéphane Etienne / Hypallages
TRANSLATION FROM FRENCH Martin Davies

In a world where the boundary between what is virtual and what is real is becoming increasingly blurred, IT security is evolving at an unprecedented rate. The Covid-19 pandemic acted as a catalyst for an accelerated digital transformation, disrupting our lifestyles and redefining the contours of digital security. Digitalisation has become imperative for business continuity, but this exposes companies to a broader and more complex range of threats than ever before. In this changing landscape, cybersecurity is no longer an option, but a vital necessity, requiring bespoke strategies to protect critical digital assets. But how to proceed? What should you pay attention to? How will cyber threats evolve in the years to come? This month's article attempts to answer these questions.

Contemporary technological advances, although holding out big promises for the future of our society, also raise challenges in terms of cybersecurity. Among these challenges, three areas particularly stand out: connected objects, quantum computing and artificial intelligence.

The Cyber Resilience Act and connected objects

Connected objects are increasingly present in our daily lives, whether at home or work. However, although they often collect personal data, few of them are properly protected. According to a study carried out in March 2020 by Palo Alto Networks, a world leader in the field of cybersecurity, nearly 60% present vulnerabilities that could be exploited by cybercriminals and 98% of data traffic from connected objects in the professional environment is not encrypted.

To remedy this, the European Commission proposed the Cyber Resilience Act in September 2022, which should soon come into force. This future regulation will improve the security of digital products in the European Union. It requires manufacturers to consider cybersecurity during product design and development and details essential cybersecurity requirements for affected products, such as the need for products to be delivered without known vulnerabilities and to support secure configurations by default. In addition, it establishes reporting obligations for manufacturers should vulnerabilities be exploited or if incidents have an impact on security.

However, concerns have been raised that these regulations could impact on small businesses and software developers as adapting existing products to new requirements could require significant resources beyond the reach of small organisations. In addition, it could have a dissuasive effect on the development of free software in Europe, which would go against the European Union's objectives of innovation and digital sovereignty.

Coming soon - the quantum threat?

Connected objects are not the only thing to pose a challenge to cybersecurity. Another, much more important, lies in quantum computing. Unlike classical computers which operate with classical bits – either 0 or 1 – quantum computers are based on qubits. These quantum information units are characterised by their ability to adopt states of superposition and entanglement, allowing a qubit to represent 0, 1 or both simultaneously and to link its state to that of another, independently of the distance that separates them.

These extraordinary properties allow quantum computers to process a multitude of calculations in parallel and give them the ability to solve complex mathematical problems – those on which current cryptographic systems are based – much more efficiently than the most efficient algorithms run on classical computers. Thus, quantum computers could in the future compromise the security of many cryptographic systems widely used today, making it imperative to develop new cryptographic methods resistant to quantum attacks. The urgency is all the more palpable as more and more cybercriminals accumulate encrypted data in the hope of decrypting it later when they have quantum computers at their disposal.

“Quantum computers could in the future compromise the security of many cryptographic systems widely used today."

A practical guide to understand and prepare

In February 2023, the Chamber of Commerce published a practical guide dedicated to cybersecurity to understand, prepare for, and know how to react to cyberattacks. This manual offers an overview of security risks, provides testimonials from companies that have been victims of an attack, highlights human errors to avoid, and details the different forms of cyberattacks. It also provides a three-key-step methodology to protect your business, explains the infection process, and includes a self-assessment questionnaire. A non-exhaustive list of tools and solutions and useful contacts complete this guide, available in French and English and downloadable free of charge from the Chamber of Commerce website in the Publications section.

More informations:

Find the practical guide by scanning the QR Code

And why not take out cyber insurance?

Until recently, cyber risk coverage was only offered to large companies and individuals. From now on, SMEs and self-employed people can also benefit from cyber insurance thanks to the professional cyber solution from the Le Foyer group. The offer, the only one currently on the Luxembourg market, covers various aspects such as gross margin losses following a cyber-attack, costs incurred to remedy the threat, continue the business, and rebuild the e-reputation as well as the claims from injured third parties. An assistance component is also planned and includes services such as analysis of the seriousness of the threat, advice on actions to take, notification of victims, and even negotiation with the cybercriminal.

> *"By analysing trends and learning from past incidents, AI will soon be able to predict and prevent future attacks before they happen."*

01

In this context, two cryptographic approaches are emerging to respond to the challenges posed by the advent of quantum computing: post-quantum cryptography and quantum cryptography. The first develops new mathematical algorithms which would remain inviolable even for a quantum computer. The second is based on the principles of quantum physics. One of the best-known examples is Quantum Key Distribution (QKD), which allows two parties to generate a shared and secure secret key. If a hacker tries to spy, he will inevitably disrupt the photons – the particles of light – used in the key and alert both parties to an attempted intrusion. This can be like having a conversation using a secret language that only you and your interlocutor know. If anyone else tried to learn it, you would know immediately.

Luxembourg aims to become a pioneer in the field of automatic key distribution with the INT-UQKD project, supported by the European Space Agency (ESA) and managed by RHEA System Luxembourg in collaboration with Post Luxembourg, the SnT (Interdisciplinary Centre for Security, Reliability and Trust) from the University of Luxembourg, HITEC Luxembourg, evolutionQ (Canada) and SpeQtral (Singapore). This project aims to demonstrate the applicability of QKD technology in operational IT environments through the deployment of networks between Luxembourg, Belgium, Singapore, Canada and the United Kingdom.

Artificial intelligence, a two-sided technological coin

Artificial intelligence also presents a paradox: it is both a shield and a sword in the cybersecurity arena. On the one hand, AI is a security enabler, capable of analysing massive volumes of data to detect atypical behaviour or attempted cyberattacks much more quickly than traditional methods.

When faced with a threat, AI-driven systems can take autonomous actions to contain or neutralise the attack without human intervention. By analysing trends and learning from past incidents, AI will soon be able to predict and prevent future attacks before they happen.

On the other hand, AI can be abused by cybercriminals to orchestrate ever more sophisticated attacks. In particular, they can use it to test and refine their malware in simulated environments until it becomes undetectable. Thanks to AI's ability to analyse and exploit enormous amounts of personal information available on social networks and the Internet, attacks are becoming increasingly personalised and targeted, targeting key people within companies like financiers, human resources staff and managers. Scam content is becoming more and more convincing and is more easily able to deceive users. Some hackers go even further by using AI to dissect user behaviour patterns and exploit vulnerabilities such as recurring use of similar passwords. Others focus on scrutinising company finances to demand appropriate ransoms when they manage to take their data or computer systems hostage.

01. Connected objects are increasingly present in our daily lives, whether at home or work. Although they often collect personal data, few of them are properly protected.

02. The European Commission proposed the Cyber Resilience Act in September 2022, which should soon come into force. This future regulation will improve the security of digital products.

Fabrice Aresu
General manager
LuxTrust

"Digital trust is a constantly evolving profession"

What digital solutions does LuxTrust offer and for which sectors of business?

Our company positions itself as an expert in electronic identity. It offers individuals, businesses, and administrations a range of services designed to strengthen the security of online transactions, authenticate users, and guarantee the completeness and confidentiality of data. Our solutions apply to all sectors of business and can adapt to the specific security requirements in each area.

Is your scope of action limited to Luxembourg?

Not at all. Even if most of our activities are concentrated in Luxembourg, we are also developing abroad. We have opened offices in Paris, Brussels and, more recently, in Monaco. Our company enjoys international recognition in part due to its compliance with European regulations such as the eiDAS (Electronic Identification, Authentication and Trust Services) regulation which establishes a legal framework for digital trust services throughout the European Union. This compliance ensures that LuxTrust services can be used beyond the borders of Luxembourg. Our COSI platform also plays a significant role in this international recognition. This innovative solution allows users to sign, manage, and store their electronic documents in a completely secure manner.

Won't recent technological advances such as artificial intelligence significantly change your activities?

The continuous improvement of our technologies is at the heart of our strategy. A clear example of this evolution is the gradual replacement of the authentication token, which had become more exposed to the risks of fraud, which have evolved considerably. Advances in artificial intelligence have allowed hackers to perfect their methods, particularly through increasingly convincing fraudulent emails and SMS messages, and to target their victims with increased precision. The financial impact of these frauds has changed in scale, regularly exceeding one hundred thousand euros per victim. Faced with this growing threat, our quest for more robust technological solutions to strengthen security is constant. We are engaged in a perpetual struggle, similar to that of cat and mouse, against hackers who lack neither the time nor the ingenuity to deceive the vigilance of users.

Jean-Guy Roche
CEO, Rcarré

"1% of turnover is enough to protect yourself effectively"

What are the circumstances that pushed you to create within your group Rsecure, a company specialising in cybersecurity for small and medium-sized businesses?
The creation of Rsecure results from a conjunction of two major events. In March 2021, our cloud infrastructure was the target of a major attack, immobilizing 2,000 of our users. This direct experience with cybercrime, combined with our active search for cybersecurity expertise, crystallized our decision. Having had the chance to start my career alongside Luc Cottin, who then excelled as CISO (Chief Information Security Officer) for large organisations, I saw in him the ideal pillar to lead our new entity. From the start, our motivation was clear: faced with a market that mainly focuses on large clients such as banks and insurance companies, leaving aside small structures, Rsecure was created to fill this void by offering VSEs and SMEs tailor-made cybersecurity solutions.

What does the HOP methodology implemented by Rsecure consist of?
The HOP methodology is a holistic approach to cybersecurity. It rests on three pillars. People: we raise awareness among employees and managers about cyber threats and establish a culture of security within the company. Tools: we implement security solutions adapted to the needs of the company and monitor and maintain IT systems. Processes: we define a clear and concise security policy and establish procedures with the client for the management of security incidents.

In your opinion, it is possible for a VSE or SME to invest in cybersecurity at an affordable cost. Can you give us an order of magnitude?
With a budget equivalent to 1% of its turnover, a company can train itself and have the adequate tools to protect itself. Rsecure ensures that all the solutions proposed are accessible to small structures. The Egide product, recently launched in collaboration with the Belgian company Esia, illustrates this approach perfectly. This small box connected to the company network allows security to be managed globally through a single platform. It offers a practical, easy-to-use solution with a transparent pricing structure adapted to the needs of SMEs.

03

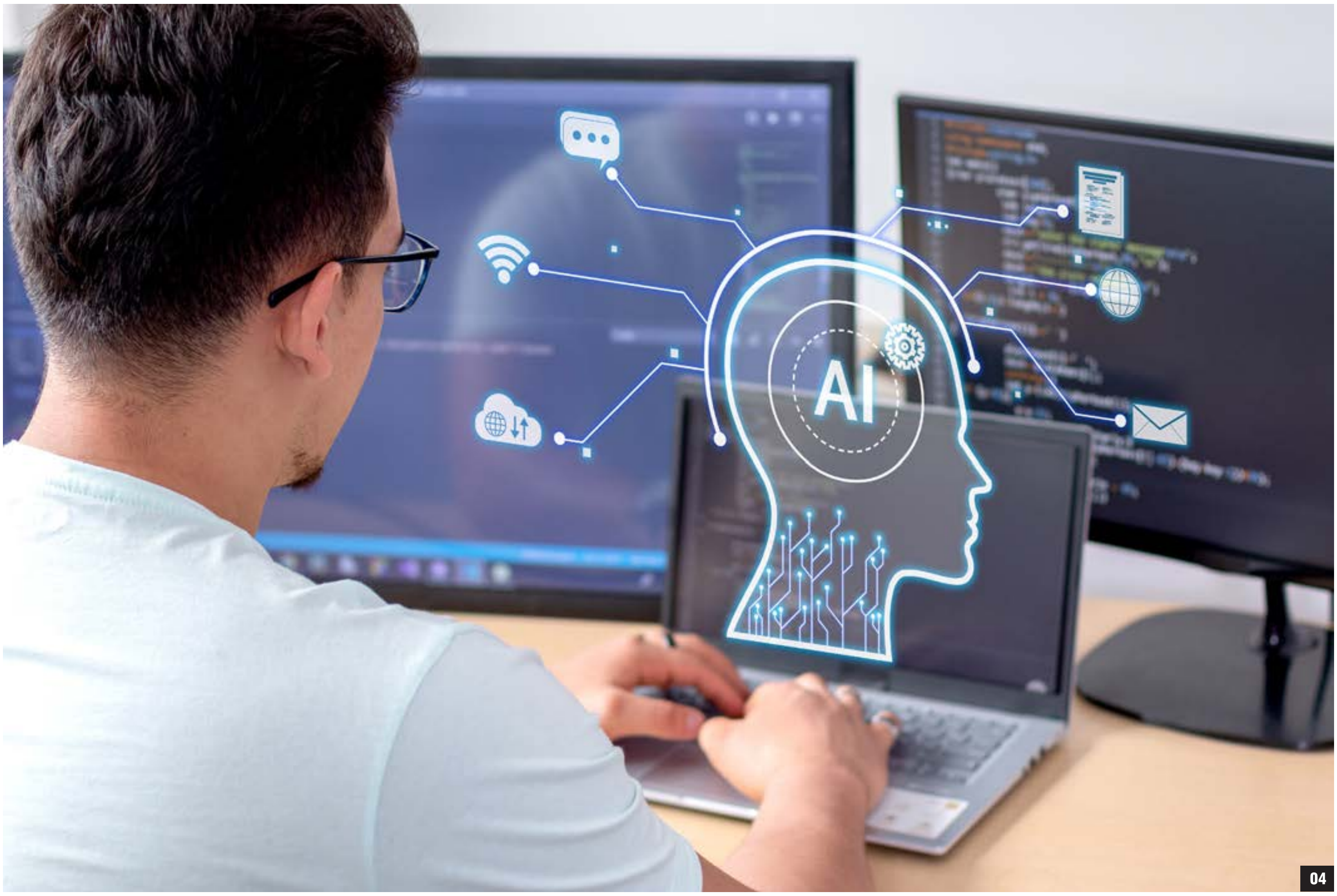
The political issue of cyber-resilience

Is Luxembourg ready to face these increasingly sophisticated attacks? A priori yes, if we judge by the different strategies and structures put in place which reflect the country's desire to make resilience in digital domains a major political and societal issue.

In 2021, Luxembourg launched its fourth national cybersecurity strategy covering the period until 2025. Developed by a working group bringing together the main public structures active in IT security, it is based on previous strategies and includes a series of measures which can be broken down into three main objectives. The first objective aims to establish a digital environment where trust is the cornerstone, emphasises the importance of guaranteeing the security of personal data and respect for online privacy and tries to promote a culture of cybersecurity through awareness campaigns and the implementation of targeted training. The second objective focuses on strengthening the security of digital infrastructures. The third pillar aims to promote a digital ecosystem where businesses and start-ups can thrive within a clear and secure regulatory framework. It includes specific initiatives such as supporting research and development, encouraging partnerships between academic institutions, the private sector and the Government as well as promoting entrepreneurship in the cybersecurity sector.

03. In the future quantum computers could compromise the security of many cryptographic systems widely used today.

04. Artificial intelligence also presents a paradox: it is both a shield and a sword in the cybersecurity arena.



04

To implement its strategy, Luxembourg can rely on its key players, starting with the High Commission for National Protection (HCNP). Placed under the responsibility of the Prime Minister, the HCNP's mission is to constantly, and in all circumstances, ensure the overall protection of Luxembourg against all forms of threats that could undermine the sovereignty and independence of the country. In this context, it coordinates national crisis response efforts, including those related to cybersecurity. Its action in this area is defined through the “Cyber” emergency plan to deal with large-scale attacks against information systems in the public or private sector which would be likely to cause serious consequences for the country and its population.

The HCNP interacts closely with other key entities in the Luxembourg cybersecurity ecosystem. It serves as the National Information Systems Security Agency (NISSA) whose main functions are to implement the general information security policy of the State; and to define and support, in consultation with State administrations and services, a risk management approach. The HCNP also oversees the Government Centre for Computer Emergency Treatment (Governmental CERT/GOVCERT) responsible for receiving, examining and responding to computer security incidents that compromise Luxembourg, its citizens or its economy.

The High Commission also chairs and serves as secretariat of the Interministerial Committee on cyber-prevention and cybersecurity. Established by the Luxembourg government on 13th December 2017, this committee's main missions are to harmonise and coordinate the actions of the different ministries and administrations in terms of IT security, to define strategic orientations, and to ensure the implementation of action plans and adopted measures and to discuss the positions to be adopted by national representatives in European and international forums.

The gateway to enhanced cyber resilience

In the private sector, inspired by the government's desire to create a national centre of excellence for security, an economic

> *“Luxembourg is increasingly positioning itself as one of the world leaders in the field of IT security.”*

05

06

05. 06. If today AI can be be used to orchestrate ever more increasingly sophisticated attacks by cybercriminals, it will soon soon be able to predict and prevent future attacks before they happen.

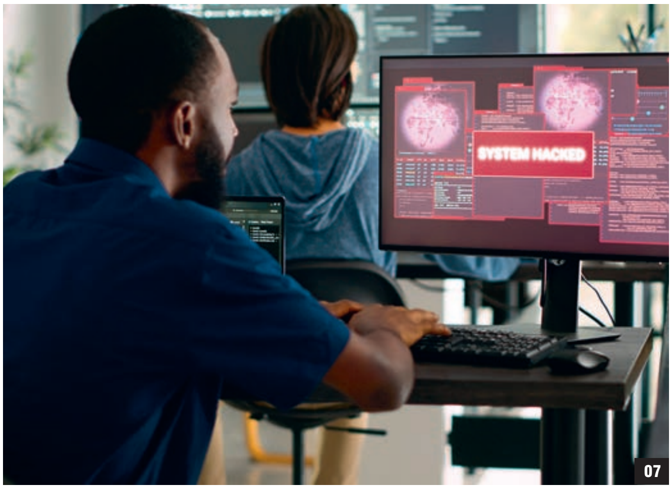
interest group (E.I.G) called Security Made in Lëtzebuerg was set up in May 2010. Restructured to become the Luxembourg House of Cybersecurity (LHC) in October 2022, the agency, supervised by the Ministry of the Economy, aims to be a key player in cyber-resilience by bringing together all the public information security stakeholders to facilitate collaboration, innovation and synergies and thus make Luxembourg a pioneer of an open and trusted cybersecurity data economy.

To achieve its ambitious objectives, the Luxembourg House of Cybersecurity collaborates with several partners. Among these are Bee Secure, a government initiative which raises awareness among the general public about the more secure and responsible use of digital technologies; Digital Learning Hub, which offers short and practical training in IT for professionals wishing to perfect or improve their skills or change careers; and Luxembourg Digital Innovation Hub, which focuses on the digital transformation of Luxembourg industry by integrating an important cybersecurity component.

The LHC also has two centres of expertise: CIRCL (Computer Incident Response Centre Luxembourg) and NC3 (National Cybersecurity Competence Centre). The first is a government initiative designed to collect, investigate, report and respond to computer security threats and incidents. Its team of experts acts like a fire brigade, capable of responding quickly and effectively as soon as threats are suspected or detected or when incidents occur. The CIRCL constitutes a reliable and trusted point of contact for the private sector, municipalities and non-governmental entities in Luxembourg. The National Cybersecurity Competence Centre (NC3) has developed its activities around three pillars: supporting the development of cybersecurity capabilities and skills, contributing to developing the industrial base of cybersecurity in the country and consolidating the strategic autonomy of the European Union.

The Luxembourg House of Cybersecurity thus proposes several activities in the three dimensions – behavioural, organisational and technical - of cybersecurity. Its spearhead undoubtedly remains Room #42. Intended for companies wishing to train in cybersecurity, the room offers a realistic experience by simulating a work environment plagued by computer security incidents. All scenarios are based on real events and participants must make high-impact decisions within a time limit – between 1 and 2 hours – and with minimal information. The goal is to exploit even the smallest vulnerabilities to enable businesses to detect and close gaps and implement best practices to prepare for real-world challenges.

Finally, always to encourage networking and promote Luxembourg's expertise in the field, the Luxembourg House of Cybersecurity manages the national security portal (www.cybersecurity.lu). Aimed at seasoned professionals and beginners alike, the portal offers a wide variety of features to help users stay informed and improve their cybersecurity skills: from tips and best practices to information on current standards, rules and laws through job offers and internships and the latest news from the Luxembourg ecosystem. The platform is collaborative: anyone is free to suggest content and, for



07. Scam content is becoming more and more convincing and can more easily deceive users.

> *“Many people, even those very high levels of education, have not fully integrated safe behaviours into their daily routine."*

certain sections, to contribute directly to the content as a member of the ecosystem. All Luxembourg IT security players can request to be listed free of charge, whether as a private operator, public operator or association.

Luxembourg, a digital fortress?

Given the considerable efforts made by the country, it is legitimate to ask if they are bearing fruit. Undeniably the answer is yes, although it is always difficult to obtain reliable and recent figures regarding Luxembourg's cybersecurity ranking on either a European or a global scale. What we can safely say is that the country has improved its ranking from year to year and is increasingly positioning itself as one of the world leaders in the field. According to the latest global cybersecurity index for the year 2020 published by the International Telecommunications Union (ITU), the United Nations' specialised agency for information and communication technologies, Luxembourg would rank 13th out of 182 countries evaluated and would be 7th out of 46 countries in Europe, i.e. level with Germany.

Pierre Van Wambeke
Founder and CEO
SeeZam

> *“Unlimited encryption is an undeniable asset for Luxembourg”*

Can you briefly explain the services offered by SeeZam?

SeeZam is a Luxembourg company created in 2009. It offers an online safe intended for the protection, collection, distribution, and sharing of sensitive data for companies, private and public organisations as well as individuals. Like a physical safe in a bank, it is a small, ultra-secure space that will require the user to sort everything they wish to deposit there. Our clients come from all sectors of business and are of all sizes, from small businesses to the largest companies in the country.

SeeZam has recently expanded its offering with a solution dedicated to whistleblowers. What is it about?

Following a European directive transposed into the Luxembourg law of 17th May 2023, companies with more than 50 employees are now required to set up a channel for reporting offenses or harassment. This system must ensure optimal security and preserve the complete confidentiality of the process, protecting both the identity of the whistleblower and the interests of the company. SeeZam meets this obligation with a solution that is both practical and efficient, directly integrated into its virtual safes. The form completed by the whistleblower is protected against any interception before it is sent to the report processing area.

How can you guarantee absolute confidentiality of the data stored in your virtual vaults?

Thanks to our very high-level encryption keys, the content of our users' accounts is accessible neither by us nor by the companies that make it available to their employees or their customers. In other countries, this would not be possible. Luxembourg is one of the only countries to offer a legal framework that allows unrestricted use of encryption techniques. To be clear, even if the legal authorities asked us to do so, we would be unable to decrypt our customers' data. In addition, our procedures are evaluated through annual audits according to SOC2 (Service Organization Control 2) standards and we regularly carry out, on average four times a year, penetration tests to strengthen our infrastructure against possible vulnerabilities. It is this operational philosophy focused on confidentiality and security that makes our business model unique.

```
void groups_free(struct group_info *group_info)
{
  if (group_info->blocks[0] != group_info->small_block) {
    int i;
    for (i = 0; i < group_info->nblocks; i++)
      free_page((unsigned long)group_info->blocks[i]);
  }
  kfree(group_info);
}
EXPORT_SYMBOL(groups_free);
```

The dynamic map of the Luxembourg cybersecurity ecosystem, available on the Luxinnovation website , seems to confirm the sector's robustness. It lists 310 companies active in the field, which offer solutions covering almost the entire cyber risk management value chain, with particular expertise in risk identification and system protection. Another positive element is that 50% of these companies were created in the last 5 years and 24% of them are start-ups, which demonstrates a strong innovation potential.

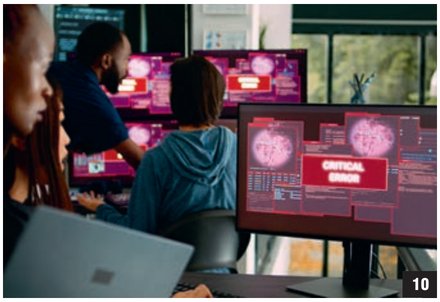
Luxembourg is also asserting itself internationally. Cybersecurity Luxembourg is a national label whose mission is to facilitate the international opening of Luxembourg's expertise in cybersecurity. All members of the Luxembourg ecosystem are encouraged to adopt it. The brand is also regularly highlighted during Luxembourg's participation in international forums on cybersecurity, such as the InCyber Forum (FIC) which is held in Lille. This major event, recognised for its rich programme of conferences, workshops and exhibition spaces, annually brings together the entire European cybersecurity and trusted digital ecosystem: from end customers to service providers including solution providers, consultants, law enforcement, state agencies, schools and universities. The next edition will take place from 26th to 28th March 2024 with a Luxembourg pavilion bringing together various players from the national ecosystem.

The country is also active within several European and international bodies. These include EU CyberNet, a European Union initiative that aims to strengthen cybersecurity globally by bringing together experts and policymakers from the European Union to share their knowledge, vision and experience. In 2022, Pascal Steichen, the CEO of the Luxembourg House of Cybersecurity, was elected to serve for three years as the first president of the board of directors of the European Centre of Competence in Cybersecurity (*see the interview with Pascal Steichen*).

Luxembourg recently stood out on the world stage with the launch of the Luxembourg Cyber Defence Cloud (LCDC). With a budget of 250 million euros spread over twelve years, from 2024 to 2035, this project aims to build and host a fully private cyber defence cloud to the highest international standards. This project will not only help build one of the most secure defences in

08

09



10

> *“Many managers still wrongly believe that their structure is too small to be attacked without realising how disastrous the consequences of a cyberattack can be.”*

Luxembourg but will also benefit its partners in the European Union and NATO. For this project, the Ministry of Defence benefited from the support of the NATO Support and Procurement Agency (NSPA), which will use it for its own needs.

The level of maturity is still weak

Although Luxembourg has undeniable strengths, not everything is rosy. One of the major challenges for Luxembourg lies in the difficulty of attracting and retaining specialised talent. Cybersecurity is a rapidly evolving field, requiring specialised and constantly updated skills. Even though most large companies, especially financial ones, offer generous salaries, this is not enough. A study carried out by the specialist site The Techshielder revealed in 2021 that

08. Cybersecurity is a rapidly evolving field, requiring specialised and constantly updated skills.

09. 10. Every business benefits from implementing a robust approach to security early in the digital transformation process.

Pascal Steichen
CEO, Luxembourg House of Cybersecurity

“We need more innovative start-ups”

In your opinion, what are the weak points in Luxembourg's cybersecurity ecosystem?
Currently, we observe that there are a limited number of actors in Luxembourg capable of detecting and responding to attacks. Many companies experience enormous difficulties in finding suitable partners and are increasingly turning to CIRCL (Computer Incident Response Centre Luxembourg) to support them. However, our role is limited, and we do not wish to compete with the market. To address this crying need, we must encourage innovation, identify promising start-ups, and bringing them together to strengthen the ecosystem in these critical areas.

What initiatives can be taken so that start-ups become more active in cybersecurity?
Cybersecurity has been added as an area of innovation in the Fit 4 Start program, an initiative managed by Luxinnovation and aimed at supporting innovative start-ups in the information and communication technology (ICT), health, and space sectors. In collaboration with Technoport, the Luxembourg House of Cybersecurity is currently developing a programme to support and boost innovative companies.

We also plan to establish a common European data space dedicated to cybersecurity, including threats, best practices, and solutions existing on the market. It will be a sort of marketplace that will encourage innovative projects. Start-ups will be able to test their products there and gather relevant information on business needs. As for businesses, they will be able to find solutions to meet their most urgent cybersecurity needs.

You have been appointed Chairman of the Board of Directors of the European Cybersecurity Competence Centre (ECCC). What are its missions?
The ECCC aims to strengthen Europe's capabilities and competitiveness in cybersecurity, in collaboration with the coordination centres, to build a strong community in this area. Based in Bucharest, its mission will be to make strategic investment decisions, support the deployment of innovative solutions, and facilitate the sharing of skills and capacities of all relevant stakeholders, in particular research and communities, industrial companies, and public authorities.

PwC Cybersecurity & Privacy Day 2024

The PwC Cybersecurity & Privacy Day is an annual event organised by PwC Luxembourg. The 2024 edition will take place on June 5th at PwC's premises and will revolve around the theme "The AI paradox: a blessing or a curse?". The event features presentations by cybersecurity and data protection experts, interactive workshops, case studies, and discussion panels. A competition will feature five finalists presenting their cybersecurity projects. The day before, a session dedicated to CEOs will address the strategic issues of cybersecurity and confidentiality, in an approach specifically designed for business leaders.

The 5 biggest security incidents in 2023

The cybersecurity company ESET compiled a list of the 5 biggest security incidents of 2023[1]:

1. MOVEit, a secure file transfer solution, fell victim to Clop ransomware. More than 2,600 organisations were affected.
2. More than 40 million registered voters in the United Kingdom had their personal information stolen.
3. Following human error, the details of 10,000 officers and employees of the Northern Ireland Police Service were leaked online.
4. More than 3.8 billion files stored on the DarkBeam platform, a digital risk management solution, were made public due to mishandling.
5. According to the Indian Council of Medical Research (ICMR), 815 million people had their personal information put up for sale following a mega-breach.

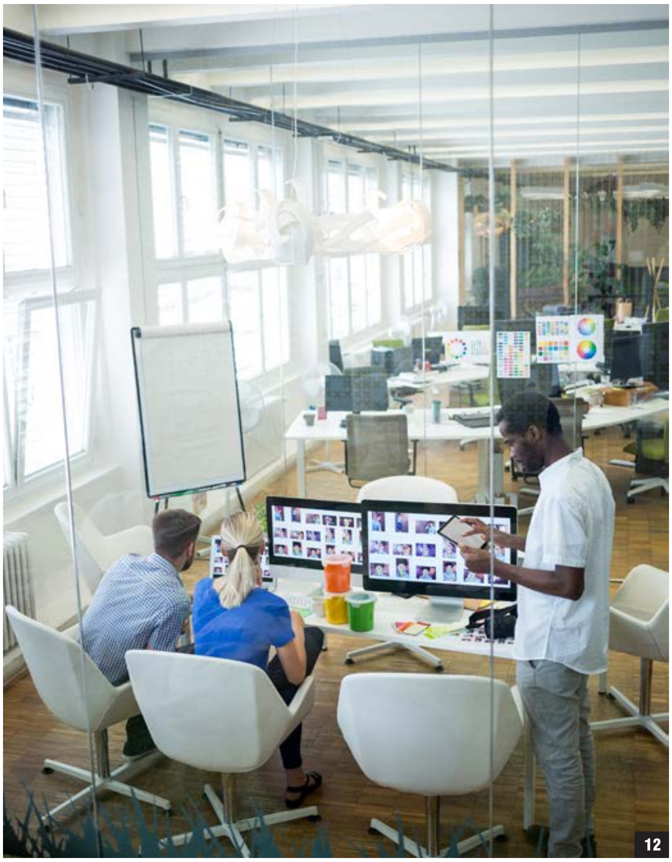
11

although Luxembourg is the city which pays the highest salaries in the field of cybersecurity – around 130,000 euros p.a. on average – it is penalised by the cost of living much higher than elsewhere and the number of places it offers is significantly lower than that of its competitors.

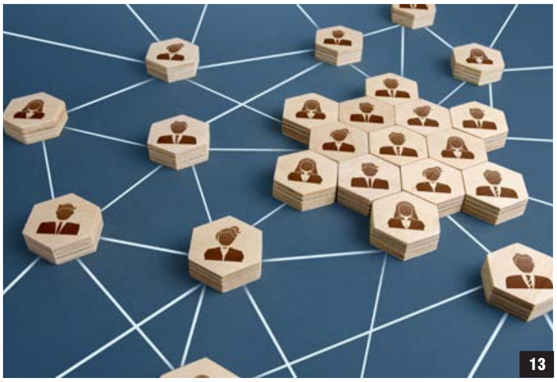
There are certainly some very concrete training courses adapted to the needs of the market such as the BTS in cybersecurity from the Lycée Guillaume Kroll in Esch-sur-Alzette, the European Master's in Cybersecurity from the European Institute of Excellence School in Luxembourg, the Master's in Information Systems Security Management from the University of Luxembourg or the training provided at the House of Training or the Luxembourg Lifelong Learning Centre (LLLC) of the Chamber of Employees. The problem is that these training courses do not always meet the wishes of companies, most of whom continue to favour graduates, require proven experience in the field and very rarely offer internships.

Another weakness lies in the level of cybersecurity maturity in the population which is not as high as one might hope. Many people, even those with a very high level of education, have not completely integrated safe behaviours into their daily routine, whether in the private or professional sphere. They continue to use the same passwords for years, do not regularly update their software and are not vigilant enough against cyberattacks. The recent phishing attacks imitating CNS and LuxTrust which produced numerous victims are unfortunate proof of this.

[1] https://www.welivesecurity.com/en/cybersecurity/year-review-10-biggest-security-incidents-2023/



12



13

11. Many leaders still wrongly believe that their structure is too small to be subject to attack.

12. There are certainly very concrete training courses adapted to the needs of the market.

13. In today's interconnected digital world, experiencing a cyberattack has almost become inevitable.

> *"More and more cybercriminals are accumulating encrypted data in the hope of decrypting it later when they have quantum computers at their disposal."*

Last but not least: VSEs and SMEs. Even if small firms may be more aware than before, many of them continue to think that investing in IT security is far too expensive, even though reasonably priced solutions exist (see the interview with Jean-Guy Roche, p.xx). Many managers still wrongly believe that their structure is too small to be attacked, and do not appreciate how disastrous the consequences of a cyberattack could be. An attack could seriously damage the image of the company, lead to a loss of customer confidence and ultimately force a company out of business. The financial damage can also be very significant: court and lawyer costs, drop in sales, depreciation of the brand which can go as far as the revocation of the operating license, etc. Without forgetting the legal issues: in addition to the legal sanctions specific to each sector, a company can be heavily penalised if it has not put in place a personal data protection system within the framework of the General Data Protection Regulation (GDPR).

In today's digital world, experiencing a cyberattack has become almost inevitable. The question is therefore no longer whether we will be the victim of a cyberattack, but when it will occur. Sometimes, a company may suffer an intrusion without ever realising it - a "*stealth attack*". Cybercriminals can infiltrate systems and networks without raising alerts and remain undetected for months or even years, during which time they can steal information, disrupt operations or cause other damage.

Faced with this reality, it is imperative that all companies, whatever their structure and size, adopt a proactive cybersecurity attitude that does not stop just at prevention. Not only must a strict security policy be implemented, but also an incident response plan to minimise damage in the event of a successful attack.

In short, the guiding principle regarding cybersecurity remains unchanged: "*Maintain constant vigilance and be prepared to face all eventualities*".