

Celebrating

1



YEARS

CYBER SECURITY COALITION

A DECADE OF
COLLABORATION



BOARD OF DIRECTORS



FROM LEFT TO RIGHT: BART PRENEEL, KARINE GORIS, NATHALIE RAGHENO, VICE-CHAIR PHÉDRA CLOUNER, STÉPHANE VINCE, SASKIA VAN UFFELEN, VICE-CHAIR GEORGES ATAYA, SÉVERINE WATERBLEY, FABRICE CLÉMENT AND CHAIRMAN JAN DE BLAUWE.

OPERATIONS TEAM



FROM LEFT TO RIGHT: CHRISTIAN MATHIJS, HENK DUJARDIN, CATHY SUYKENS, GUY HOFMANS, PASCAL CHAMPAGNE

Dear Members and Partners

How time flies! This year, the Cyber Security Coalition celebrates its 10th anniversary. What began as a 'coalition of the willing' - a small group of committed companies - has grown into an active community of over 1,000 cyber professionals, policymakers, and researchers, all eager to exchange information, share knowledge, and strengthen their professional networks.

Over the past decade, our organisation has evolved into a respected and integral part of the broader ecosystem working to enhance our nation's cyber security and resilience. This achievement is a testament to the contributions of every one of you: founders, board members, focus group chairs, active participants in our activities and, of course, dedicated members of our Operations Team. By building a professional organisation with a solid structure, we've ensured the Coalition's lasting presence and impact.

The results are unmistakable: year after year, we see steady membership growth, the emergence of new focus groups, and increasing collaboration with partners and other organisations to raise awareness and implement targeted cyber security initiatives. While growth is not a goal in itself, the principle holds: more involved members mean greater expertise available to all, and richer interactions within our network. We aim to continue to be a relevant and valuable sounding board for all our members.

At its core, the Cyber Security Coalition remains dedicated to the exchange of information and the sharing of knowledge and best practices. In cyber security and information protection, there is no competition: when one of us is hit by an incident, we all lose. Therefore, to make real progress in the fight against cyber criminals, we must tackle these challenges together. The environment we foster allows cyber security professionals to connect in confidence, share experiences and best practices, assist one another with issues, and seek inspiration from each other. In other words, if two members connect outside the Coalition and support each other as a result, we know we've done meaningful work.

After a decade, our mission is, of course, far from complete. As a leading network, we will continue to keep a close eye on developments in the cyber world and take action accordingly. We aim to address the specific needs of sectors that are particularly vulnerable to cyber attacks, such as energy, chemicals, biotech and pharma, logistics and transport. Additionally, we are exploring ways to ensure that SMEs can also benefit from the Coalition's added value.

Finally, I want to thank all my colleagues for their dedication and commitment. Here's to the next 10 years!

Warm regards

JAN DE BLAUWE
CHAIRMAN



TABLE OF CONTENTS

6 THE EVOLUTIONS
IN CYBER SECURITY
LEADERSHIP

9 HISTORY &
OUTLOOK

20 FORENSICS &
LAW ENFORCEMENT

13 FACTS &
FIGURES

23 AWARENESS

14 THREAT
INTELLIGENCE

25 PRIVACY & DATA
PROTECTION

17 CYBER INCIDENT
DETECTION &
RESPONSE

27 REGULATIONS &
STANDARDISATION

30 PICTURES OF
KEY EVENTS

COLOPHON

THIS BROCHURE IS A CREATION OF THE CONTENT COMPANY, COMMISSIONED BY THE CYBER SECURITY COALITION.
EDITORS: BJÖRN CRUL, BAVO BOUTSEN, ANSE KEISSE, FRANK SIMKENS AND ROELAND VAN DEN DRIESSCHE
EDITORS-IN-CHIEF: CATHY SUYKENS AND HENK DUJARDIN
PHOTOGRAPHY: ISTOCK, ARCHIVES. DESIGN: ANAÏS HOORNAERT
CYBER SECURITY COALITION · STUIVERSSTRAAT 8,1000 BRUSSELS · WWW.CYBERSECURITYCOALITION.BE
ALL RIGHTS RESERVED | © 2025 CYBER SECURITY COALITION · RELEASE DATE : FEBRUARY 2025



32 CLOUD SECURITY

35 CRYPTOGRAPHY

37 ENTERPRISE SECURITY ARCHITECTURE

39 GOVERNANCE, RISK & COMPLIANCE

42 OT/ICS SECURITY

44 APPLICATION SECURITY

47 CYBER SECURITY FOR HEALTHCARE

49 IDENTITY & ACCESS MANAGEMENT

52 TALENT DEVELOPMENT

54 CYBER SECURITY RESEARCH

57 CYBER SECURITY PERSONALITY OF THE YEAR 2023

58 CYBER SECURITY PERSONALITY OF THE YEAR 2024



the evolution of cyber security leadership

RIK BOBBAERTS · XAVIER PAULUS · YURI BOBBERT
PHILIPPE MICHIELS · XAVIER NEERDAELS

The CISO must be a multifunctional leader

Every week Belgian companies face over 1,000 cyber attacks. This illustrates the growing importance of the Chief Information Security Officer (CISO) role. As businesses grapple with the mounting threats, the CISO function has evolved beyond its traditional scope, and demands a clear redefinition. Rik Bobbaers (Tech CISO INC Global), Philippe Michiels (CISO Cegeka Group), Xavier Neerdaels (CISO BNP Paribas Fortis), Xavier Paulus (CISO Solvay) and Yuri Bobbert (Global CSO ON2IT and cybersecurity programme lead at Antwerp Management School) discussed how CISOs can best tackle the challenges while adapting to their new responsibilities.

“As a CISO, you are essentially accountable for the trust in the brand,” begins Rik Bobbaers. “Businesses want to bring new functionalities to market. A CISO ensures these innovations can continue to thrive. Interestingly, companies that recover correctly from an attack often inspire more trust than those that have never been attacked at all.” Xavier Paulus provides an even simpler analogy: “If I had to explain my job to a seven-year-old, I would say: I make sure I know which games in the cupboard are really important and ensure they don't get broken or stolen.”

A communicative chameleon

The CISO's role thus increasingly involves shaping public perception, maintaining continuity, and ensuring resilience. “You must be a multifunctional leader, while acting as a communicative chameleon,” says Bobbaers. “You need to switch contexts seamlessly and adjust your message for your audience - whether it's the coder or the Board. And for the latter, in

particular, you must clearly show where your added value lies and why investments in this area are absolutely essential.”

Paulus echoes this point: “When communicating with the Board, it's critical to articulate the CISO's contributions in terms of business value and risk mitigation, making it clear why cyber security is not just a cost but an enabler of trust and innovation.” Michiels emphasises alignment with business goals: “A security program must align with shifting business objectives, so you need to understand where the business is headed in order to build support for security initiatives and foster a safety-first culture. In practice, this means embedding security by design into every process and architecture.”

Inspiring leadership

The CISO must first and foremost be able to inspire and to get people on board with their story. “The central question today is: how do we build an organisation that can withstand challenges? For one thing, this involves building mental resilience within the team, which requires the CISO to have well-developed soft skills,” says Yuri Bobbert. “Certain training programmes should therefore focus on this aspect as well.”

The balancing act between security and business demands clearly requires strong interpersonal leadership. Philippe Michiels: “Security teams often work in a friction zone. On the one hand, they want to improve security; on the other, they face a business eager to move forward, often without prioritising security. That's why a CISO must be a supportive leader and a strong people manager.”

Creating this balance also requires a grasp of the company's critical assets, risks and processes. "For example, regular testing of incident processes ensure you are ready when things go wrong," says Xavier Neerdaels. "But it also has educational benefits, while making everyone in the company accountable. The human factor remains crucial," Xavier Paulus adds.

CISOs are expected to maintain close contact with decision-makers while preserving their independence. But as Neerdaels warns, "In smaller companies, IT management is often fully outsourced. This can create serious security risks, because you need to make quick decisions in an incident." In such a dynamic environment, technical expertise must be combined with in-depth strategic understanding.

"Expanding the talent pool ensures that security teams can meet the growing requirements of the digital landscape"

Regulations and recruitment

One of the biggest hurdles the CISO faces is the increasing number of regulations. "It takes a lot of effort to prove that security measures are effective," says Xavier Paulus. CISOs can find themselves pulled too deeply into the details of compliance, leaving less time for strategic initiatives. Bobbaers therefore advises, "Use established frameworks and policies as a foundation—not just for compliance but to build security maturity."

Global operations further complicate compliance efforts. "Many companies operate across multiple continents, beyond Europe where most regulations originate, creating geo-

political issues," Xavier Neerdaels notes. The complex regulatory environment demands a flexible, proactive approach to compliance that doesn't detract from a company's overall security strategy.

Adding to the struggle is the difficulty in finding the right talent for such a demanding role. "Given the current war for talent, the security sector needs to better understand what attracts people to this field," the panel agrees. To this day, recruitment for CISO positions often emphasises highly technical profiles, potentially alienating talented individuals with complementary skills. "We need to open up to candidates from non-IT backgrounds, which can also attract a more diverse talent pool," suggests Rik Bobbaers.

Diversity in recruitment is not just about inclusion; it's about necessity, the panel explains. "The current demands of cyber security require a broader range of perspectives and skill sets," says Yuri Bobbert. "Expanding the talent pool ensures that security teams can meet the growing requirements of the digital landscape. For instance, there remains significant room for improvement in achieving gender balance."

Promoting the position of CISO

As a result, what the evolving CISO function needs most is greater visibility to attract top talent. Bobbaers argues, "We have to actively promote what it means to be a CISO today. This is a job that involves strategy, leadership and shaping the future of business. And looking ahead, the CISO's role will continue to broaden. AI, for example, will make us more efficient, but it also increases security risks. Similarly, ransomware is increasingly advanced and invasive. These developments add new dimensions to the already complex responsibility." But the flip side is that this complexity also makes the position more rewarding. "To current IT or security students, I would say: the role of CISO is incredibly challenging and will continue to broaden in the future," says Xavier Neerdaels. "It's an exciting, ever-expanding field with vast career opportunities. You can choose your specialisation. Honestly, a CISO today could use their own marketing department," Rik Bobbaers concludes. ■

HISTORY & OUTLOOK

10 years of Cyber Security Coalition **We'll continue to enhance our outreach**

A decade after its establishment, the Cyber Security Coalition has grown into a respected partner both within and outside the sector. Its focus on knowledge-sharing and strengthening the ecosystem has proven invaluable in navigating years of rapid technological innovation and evolving regulations. Founding members Georges Ataya (Solvay Brussels School of Economics & Management), Fabrice Clément (Proximus), Christine Darville-Finet (VBO FEB), Jan De Blauwe (NVISO) and Bart Preneel (KU Leuven) reflect on the journey and look ahead.

"The Cyber Security Coalition grew out of the Leuven-based Belgian Cybercrime Centre for Research, Training & Education (B-CCENTRE), which had been promoting the importance of cyber security since the 1990s," Bart Preneel starts. "But even then, we were building on knowledge accumulated long before that. My own work, for instance, goes back to 1978. Thus, Belgium was indisputably a pioneer in this area, and the industry continues to benefit from that legacy today."

The catalyst for the creation of a private network organisation was a large-scale cyber incident that telco operator Belgacom fell victim to in 2013. "This sparked a year-long discussion on how to unify the cyber security landscape and enhance Belgium's overall resilience, based on a sense of shared responsibility. In 2015, this led to the creation of the Cyber Security Coalition", says Christine Darville-Finet, who became the first chair.

These efforts helped foster awareness at all levels of society, including the government.



BART PRENEEL



THIS PHOTO WAS TAKEN ON 26 JANUARY 2015 WHEN THE BELGIAN CYBER SECURITY COALITION WAS FOUNDED AS A PUBLIC-PRIVATE PARTNERSHIP BY SEVERAL LEADING BELGIAN COMPANIES AND ORGANISATIONS.

While it initially lagged behind, slowly policy makers started to recognise the importance of national cyber resilience. “The Coalition was established around the same time as the Centre for Cybersecurity Belgium (CCB), the public point of contact for our sector,” Preneel continues. “The timing was fortuitous for both organisations, enabling them to grow together in a complementary and collaborative manner. That synergy continues today,” adds Georges Ataya.

Building bridges

At its core, the Coalition was created as, and still is, a unique contact point between the government, academia and the private sector. “Our aim was to create something that could exist in the long term, which is why we deliberately structured it as a non-profit without commercial interests,” notes Fabrice Clément. “Initially, our focus was on fostering team spirit, as collaboration among such diverse groups was unprecedented. Achieving that goal, mainly by organising successful experience-sharing days, was our first major milestone,” Darville-Finet adds.

Since 2016, Jan De Blauwe has been leading the organisation. “Based on my experience in the peer group of cyber security professionals across major banks, I strongly believed in the added value of the model. Consequently, I didn’t need much convincing when they asked me to take up this responsibility,” he says. “The unique strengths and expertise each partner

brings, allow us to address challenges more effectively. For example, awareness campaigns can only succeed when supported by government communication channels.”

Spectacular growth

The Coalition’s rapid growth underscores its value. What began with five founding members - Proximus, KU Leuven, VUB, VBO-FEB and Belnet - has expanded to a network of over 200 members. A major driver of this growth has been the Coalition’s swift integration into the international community, marked by its early membership in the European Cyber Security Organisation. “Belgium is not an island. It’s vital to keep an eye on developments in neighbouring countries. Moreover, the Coalition has undeniably bolstered Belgium’s standing as a leader. The fact that we can represent the sector as a whole at the European and international levels greatly enhances our influence on the global stage,” Preneel remarks.

From the beginning, the Cyber Security Coalition also established itself as a creator of practical output. “For instance, we quickly published two guides: one on implementing cyber security as an SME and another on incident management. These are still available and updated regularly. Later, in 2017, we launched the Cyber Security Kit for SMEs, which clarifies basic IT infrastructure hygiene,” Darville-Finet explains. “This demonstrates our efforts to offer practical added value to our community. This goal has only become more prominent since then.”



IN 2016 CHRISTINE DARVILLE-FINET RELINQUISHED THE CHAIRMANSHIP TO JAN DE BLAUWE, WHO IS STILL CHAIR OF THE COALITION.

A context of trust

Perhaps most importantly, the Coalition's numerous working groups address issues ranging from incident response to sector-specific challenges. "One of the first was the Focus Group on Incident Response. This subdomain, just like everything within cyber security, benefits significantly from information sharing among members," says De Blauwe. "To achieve this, however, companies must be willing to be vulnerable and share sensitive information with third parties. That's where the Coalition makes a clear difference: we foster a context of trust. An environment in which people know each other and within which there is an equal distribution of information exchange."

The number of focus groups has grown significantly over the past decade. Today, there are 12. De Blauwe and Darville-Finet explain: "We've essentially opened our operations more and more to society. Our recent expansion with a specific group for healthcare institutions is just one example. For hospitals, cyber security isn't their core business, but they've become attractive targets, making enhanced security and resilience essential."

Regulation, translation, and implementation

Throughout this period, regulation has been a significant driver of cyber security advancements. "Academic research has clearly shown that there is market failure in this area, necessitating government intervention," says Bart Preneel. "Due to the domain's technical intricacy,

however, this is a very complicated story and has led to a veritable tsunami of regulations in recent years. Regulations like the NIS (Network and Information Security), the Cybersecurity Act, and DORA have created a robust framework, but they also introduce complexity."

"The mandatory framework, however, has given the Coalition's professionalisation a strong boost," adds Georges Ataya, pointing to initiatives like the Belgian Anti-Phishing Shield (BAPS), directly aimed at enhancing citizen safety. In other words, navigating this regulatory landscape is one of the Coalition's key roles. "We translate dense, technical regulations into practical guidance, ensuring our members can comply effectively," Jan De Blauwe states. "This is a critical aspect of what we do: bridging the gap between policy and practice."

2020 and the pursuit of greater visibility

A key milestone for the Coalition was the COVID-19 pandemic, which undeniably highlighted the role of digital technologies—and thus cybercrime—in our society. The Coalition has since focused heavily on virtual events, a trend that continues today. "Consequently, we also enhanced our digital presence through social media, podcasts, blogs and our Cyber Pulse-newsletters," says De Blauwe. "In the latter, we want to highlight our members as much as possible. Because we believe that their achievements, which are often particularly impressive, can act as a source of inspiration for the rest of the ecosystem."



GEORGES ATAYA



FABRICE CLÉMENT

These efforts align with the Coalition's mission to attract new talent. "Our participation in the Cyber Security Challenge Belgium, which inspires young people to enter the field, is one example. Another is the Cyber Security Personality of the Year award, which we introduced in 2021. Since 2024, this recognition has been divided into different categories. "It celebrates professionals who make significant contributions to the sector. Moreover, we hope to raise more awareness on the importance of these efforts," Fabrice Clément continues. "After all, security officers are often rare assets in an organisation."

Simultaneously, the Coalition is committed to groups at risk of exclusion due to increasing digitisation. This active engagement in digital inclusion is reflected in participation in initiatives including DigitALL, BeCode, Passwerk and DigiSkills Belgium, which they also aim to spotlight. "As society becomes increasingly digital, it's crucial to ensure no one is left behind," says De Blauwe.

A glimpse into the future: a continued focus on societal value

While the mission – enhancing cyber resilience across all levels of society – remains unchanged, the Coalition today bears little resemblance to what it was 10 years ago. Jan De Blauwe: "The growth is spectacular, and we want to continue focusing on it, particularly in sectors where we aren't yet represented. For example: chemicals, pharmaceuticals and logistics. These industries are vital to our economy and bringing them into the Coalition

will strengthen our overall network. That's why we'll continue to enhance our outreach."

"Had you told me 10 years ago where we'd be today, I wouldn't have believed it. We've created something that functions efficiently and meaningfully, capable of responding to changes in context," states Christine Darville-Finet, pointing to the dynamic nature of the cyber security sector, where knowledge evolves rapidly. Consider, for example, the stormy developments in Artificial Intelligence (AI) and large language models (LLMs). "You then inevitably find yourself in a societal narrative. In Europe, we agree that we don't want to end up in a dynamic where technology dictates how we live. That's why we must build a digital society that reflects European values," concludes Bart Preneel. ■

Over the past 10 years, the Cyber Security Coalition has strengthened ties, set up collaborations and entered into partnerships with numerous organisations from the Belgian cyber security ecosystem.

- » Academia: Cyberwal, KU Leuven, Solvay Brussels School of Economics & Management, SANS Institute
- » Governmental entities: Centre for Cybersecurity Belgium, Agence du Numérique/Digital Wallonia, Belgian Defence/Cyber Command, Vlaio
- » Sector federations: Agoria, VBO FEB
- » Other strategic partnerships: Beltug, DigitAll, ECSO, Flux50, Isaca Belgium Chapter, Women4Cyber Belgium

FACTS & FIGURES

members



15%
GROWTH
IN 2024

134 PRIVATE | **34 PUBLIC**
13 FEDERATIONS | **18 ACADEMIC**

focus groups

12 FOCUS GROUPS - 2024



50 PLENARY MEETINGS
1103 PARTICIPANTS IN PLENARY MEETINGS

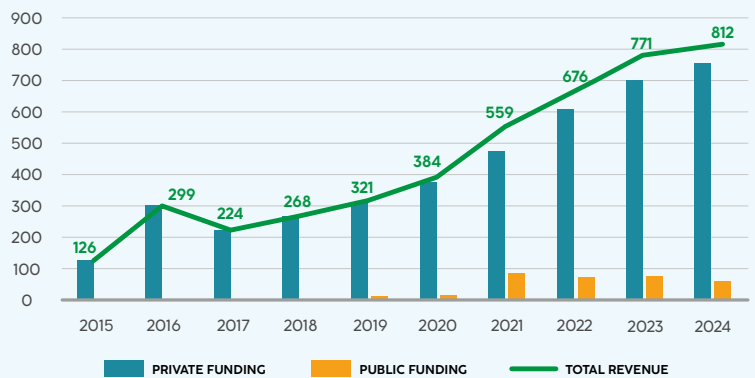
9 national awareness campaigns

- 2016 TAKE BACK THE INTERNET
- 2017 IDENTIFY SUSPICIOUS MESSAGES BEFORE IT IS TOO LATE
- 2018 BOOST YOUR DIGITAL HEALTH BOOST YOUR DIGITAL HEALTH
- 2019 RELAX! AND THINK TWICE BEFORE CLICKING ON A LINK
- 2020 PASSWORDS ARE A THING OF THE PAST
- 2021 BE SMARTER THAN A HACKER
- 2022 CLICKING OK IS NOT ALWAYS OK
- 2023 PHISHING, THE DEVIL'S IN THE DETAILS
- 2024 TWO-FACTOR AUTHENTICATION: A SIMPLE STEP TO A SAFER DIGITAL WORLD

events 2016 - 2024



funding (in € 000)





Threat intelligence

We are continuously exchanging information to respond to new threats

Modern warfare is increasingly taking place in cyber space, and attacks can have as significant an impact as physical conflicts. Monitoring all cyber threats is a task for the Cyber Command, the fifth component of the Belgian Defence. "Attacks and techniques are becoming increasingly sophisticated. Using cyber threat intelligence, we can map out tomorrow's threats today," states Major General Michel Van Strythem.

No sector is immune to the growing threat of hackers. Cyber threat intelligence (the process of collecting and analysing information about current and potential cyber attacks) is helping the Belgian Defence to respond more quickly to cyber threats. "The task is not getting any easier, because the techniques used against us are more advanced every day," says Major General Van Strythem, who leads the Cyber Command.

A complex threat landscape

The most visible incidents are DDoS attacks. Last autumn, several Belgian municipalities fell victim to this type of attack. "Because many local authorities use the same hosting partner, the servers became overloaded and their websites were inaccessible for a while." Although the impact of these attacks was relatively limited, they still stirred up emotions. "And that is what some criminal groups are after. They want to incite fear and

create a breeding ground for anti-Western feelings."

Other threats also require attention. "Next to ransomware, phishing attacks and cyber intrusions with data exfiltration, a fourth major threat is coming our way: the abuse of our own infrastructure to carry out attacks on third countries," Van Strythem continues. Such attacks can significantly undermine allied interests. "But they are very difficult to detect, especially in an increasingly complex landscape with ever-more advanced techniques. We have long since passed the point where traditional security measures could protect us."

The Major General emphasises the importance of vigilance and cooperation in the fight against cyber threats. "We work closely with the academic world and the technology industry to strengthen our resilience. We continuously exchange information with European colleagues and with national authorities, such as the Centre for Cybersecurity Belgium and other partners. This allows us to respond more quickly to new developments and threats."

Stronger through collaboration

By working together, Defence also aims to stay one step ahead in assessing future threats. "We make predictions based on hypotheses and by drawing out possible consequences. This analytical work

is performed by a team, based on our own knowledge, public information, and input from our partners." It's an approach that has delivered results for Defence. "To name one, we exposed a network infrastructure that was being abused to launch attacks. After this discovery, we took action with the security services to better shield the network. In this way, we were able to avert an attack."

This example illustrates the intense battle to stop cyber criminals. "The fight is certainly not getting any easier," says Major General Van Strythem. "We are receiving an increasing volume of data and with everything being interconnected, we must take account of a growing number of variables. Artificial intelligence can be a valuable ally, but there as well it is crucial to share experiences via joint platforms. That is where the future lies, and as a country we will not shirk our responsibility."



MICHEL VAN STRYTHEM

AI helps us to detect suspicious transactions faster

Payment companies are a popular target for cybercriminals. To better protect itself against these attacks, Mastercard announced the intent to acquire the threat intelligence company Recorded Future. This way the company aims to detect and address suspicious transactions and security threats more quickly. "Collecting information about cybersecurity is one thing, the trick is to also link the appropriate action to it."

In addition to obtaining data, money remains the biggest driver for cybercriminals. And as their attacks become more sophisticated, the financial sector is doing everything it can to identify potential threats. "Technology plays into the hands of cybercriminals, because with AI it is easier than ever to carry out attacks," says Rigo Van den Broeck, EVP Cybersecurity Product Innovation of Mastercard. The rise of AI-driven phishing is particularly worrying. "After all,



RIGO VAN DEN BROECK

criminals know all too well that people are the weakest link in an organization and with AI they can now also write convincing, truthful emails."

Turning intel into action

To gain a better understanding of the behaviour of criminals and the vulnerabilities they exploit, Mastercard announced its intent to acquire the threat intelligence company Recorded Future. "This company excels in collecting and analysing threat intelligence and translating it into actionable insights," explains Rigo Van den Broeck. According to Van den Broeck, that is exactly where many companies fall short. "Collecting data is only the first step, but it's about what you do with that information."

Mastercard links that information to certain fraud cases. "It is precisely by making these connections that we can set priorities and take more targeted action within our security policy." In doing so, the company is also taking a close look at its entire supply chain. "After all, criminals are increasingly targeting suppliers. We therefore advise organisations not only to take a critical look at themselves, but to make a risk analysis of their entire ecosystem. Based on that analysis, it can then be decided which investments need to be made."

AI as an ally

In doing so, organisations should also take a look at what AI can do

for them. "In any case, the technology helps us to detect suspicious transactions faster. The downside, however, is that criminals also have access to it and use it to set up new attacks."

Despite this evolution, Van den Broeck mainly sees the advantages of AI. "I sincerely believe that thanks to AI, we can stay one step ahead of criminals, even though there are also attacks that cannot be detected yet." Fortunately, these attacks are the exception rather than the rule, and the number of criminals who have the knowledge to set them up is also limited. "Logically, most stick to the more classic phishing and ransomware attacks. However, where large companies have extensive resources and expertise to defend themselves against this, smaller companies are much weaker."

To close that gap, Van den Broeck argues for more cooperation, such as the Cyber Security Coalition is offering. "By sharing knowledge and resources, we can also make every organisation more resilient. After all, no one can be completely cyber secure on their own," he emphasizes.

In addition, a collective approach helps to get a better grip on the enormous amounts of data that come to organisations. "And if we only keep data to ourselves, we are playing into the hands of criminals, while we need to make our AI models more powerful. If used wisely, I see technology more as an ally that can make an entire organisation stronger." ■

INCIDENT DETECTION AND RESPONSE

People must be able to share without fearing negative consequences

As society becomes more deeply intertwined with digital technology and the threat landscape shifts at lightning speed, a solid approach to identifying and managing cyber incidents has become indispensable. Freddy Dezeure, the founder of CERT.EU, Jean-Luc Peeters, head of the Cyber Emergency Response Team CERT.BE and Rutger Saelmans, managing partner at nFuse (part of the Cronos Group) share their views on the complexities of detecting and responding to cyber incidents and the inherent challenges of this work.

A zero-risk approach to cyber security is simply not realistic, making effective incident handling the cornerstone of any cyber security strategy. It is no coincidence that the roots of the Cyber Security Coalition lie in this domain. In fact, the organisation was founded in direct response to a large-scale hacking of the Belgacom network in 2013. This event underscored the need for enhanced reactive and proactive knowledge-sharing within the cyber security sector. It led to the establishment of the very first Focus Group within the Cyber Security Coalition, that created the Incident Management Guide, which remains a useful guideline.

Logging, data and geopolitics

Since 2013, incidents have grown more complex, causing ongoing technological develop-



JEAN-LUC PEETERS



RUTGER SAELMANS

ments in detection and the increasing role of threat intelligence to remain a constant focus. “Continuous monitoring is the foundation of a solid incident response strategy that ensures you’re prepared to respond and initiate a recovery process without delay,” Jean-Luc Peeters opens.

Effective detection and response depend on the quality and availability of data to support these processes. With proper insights from log files, organisations are empowered to detect anomalies, trace issues to their source, and proactively strengthen their defences. “However, this is becoming increasingly challenging,” Freddy Dezeure explains. “With hybrid work setups, IT resources are often used for private and professional activities. Due to the increase in cloud usage, log files are not always comprehensive. Consequently, it can be more difficult to detect and remediate incidents quickly.” The response process typically involves five phases: detection, containment, eradication, resolution, and then a rebuild phase to restore systems. “Above all, today’s approach needs to

“Criminals are working more professionally than ever, and it’s naive to think they lack the resources to carry out complex attacks”

be flexible. You must be able to quickly determine who the presumed attacker is (such as a criminal or a state) because the response will differ fundamentally,” notes Dezeure, highlighting the geopolitical layer inextricably linked to these processes.

Rutger Saelmans, who has 18 years of expe-

rience within the Dutch defence, adds: “We increasingly see this trend in conflict zones and wartime contexts. Criminals are working more professionally than ever, and it’s naive to think they lack the resources to carry out complex attacks. Incident response teams must therefore be aware of technological risks and broader geopolitical threats.”

Incident coordination and complexity

Choosing the right response path is only possible in an open culture where people feel free to communicate with trusted parties. “A blameless root cause review is essential ; i.e. focusing on how something happened without immediately assigning blame. This helps the team openly communicate mistakes. People must be able to share without fear, particularly when there are financial implications. This is the only way forward,” Saelmans clarifies.

For this reason, incidents must be managed as projects within the crisis management framework, with strict communication lines and priorities defined by a few key people. “Ideally, you work with a technical layer for forensics and log analysis, and a management layer to keep an overview. Without this division, there’s a risk that managers will ask for continuous updates, undermining the technical work and ultimately making thorough handling of the incident impossible,” explains Freddy Dezeure.

Tools, technology and AI

The experts agree on the necessity of advanced tools. “Previously, manually checking thousands of log files was the norm—a painstaking and time-intensive task. AI automates these routine processes, allowing companies to tackle threats more efficiently and freeing up time and personnel for higher-level tasks,” Dezeure explains.

However, our interviewees caution against over-reliance on these tools. “You still need experts. Sometimes we see expensive tools adding no value because they are misused,” they note.

“Many organisations rely too heavily on technology, forgetting that people’s behaviour remains the greatest vulnerability”

The technology also creates new challenges, including vendor lock-in and integration-related security risks. The three experts emphasise that cloud applications and baseline security by default are increasingly important for safeguarding data in complex environments.

The human factor

This illustrates how detection and response teams need both the right tools and the right skills. “Purple teaming, where both offensive and defensive skills are developed and combined, is essential for effective collaboration,” says Jean-Luc Peeters. This should also contribute to creating a larger culture of knowledge sharing. “Every incident presents learning opportunities, but these are only realised when the commu-

nity commits to documenting and sharing their experiences,” Dezeure notes, implicitly highlighting the vital role of an organisation like the Cyber Security Coalition.

In other words, technical skills alone aren’t enough. The human element is pivotal in shaping the future of cyber incident response strategies. “Many organisations rely too heavily on technology, forgetting that people’s behaviour remains the greatest vulnerability. By focusing on training personnel, much can be gained. This prevents situations where confidential information, such as secret keys, is inadvertently shared on public platforms,” Rutger Saelmans concludes, after having briefly – and perhaps fittingly – interrupted the interview to respond to a new cyber incident. ■



FREDDY DEZEURE

Research leads to results: cyber criminals are being convicted every week

The Belgian law on computer crime is almost 25 years old. In that time, cybercrime has grown exponentially and changed drastically. In response, the police and the Justice department have stepped up the fight. Investigating judge Philippe Van Linthout is an expert in cybercrime. He observes that more cooperation is needed, especially internationally, to catch the perpetrators of cyberattacks.

Belgium's original computer crime law dates from 2001. At that time, Belgium was one of the first countries to implement the European Convention on Cybercrime. In 2015, under the initiative of Minister of Justice Koen Geens, the cyber legislation was re-written. Philippe Van Linthout contributed to the drafting. "The law itself remains solid, but requires updating. We are being confronted by new online phenomena that cannot immediately be classified into an existing legislative box: banking, crypto and telecom claims, or claims based on the economic law code. That makes it difficult for us to draw up a good claim."



PHILIPPE VAN LINTHOUT

"If we are quick enough, we can sometimes recover money in the crypto world"

It's worthwhile to file a complaint

Another challenge for the Justice Department is that too much remains hidden beneath the surface. "People sometimes report a fact to the Centre for Cybersecurity Belgium or to the FPS Economy, but a report is not an official complaint," says Van Linthout. "We must therefore convince victims that it is worthwhile to file a formal complaint. In our Mechelen-Antwerp district, for example, there are judgments every week on bank card fraud. And if we are quick enough, we can sometimes recover money in the crypto world."

The investigating judge is all-too aware, however, that this is just the tip of the iceberg. "Perpetrators usually spend their profits very quickly, or the loot is immediately transferred to tax havens. We must be able to penetrate deeper and tackle the organisations behind all these cyber phenomena."

International cooperation and instruments such as the European search warrant have made it possible to track down international gangs. However, things can still be improved, notes Van Linthout: "A new European regulation should make it possible for me, as an investigating judge, to request information directly in other EU countries. Because the slowness of the administrative mill unfortunately often means that we are struggling to keep pace. For example, we are a popular target for Dutch cybercriminals. But the Netherlands is unable to meet our information requests, as our files are not a top priority for the police and judiciary there."

Justice needs tech profiles

Over the past 25 years, Belgium has invested in capacity and expertise to detect and prosecute cybercrime. These efforts must continue

unabated. "To give a simple example, as an investigating judge I am allowed to hack a computer or a mobile phone. But am I able to? We need the help of tech profiles if we want to keep up with developments. Recruiting additional competencies remains urgent," says Van Linthout. "And we must certainly tap into the knowledge of Belgian researchers. Our country is top in cryptography; why can't we use that expertise more in our field?"

The delicate balance with privacy

There is also the delicate balance between privacy and cybercrime investigation. "The right to privacy is important, but it must be proportionate. We cannot build a case without data. Belgian legislation works to our disadvantage there. The 12-month retention period for terrorism crimes and 9 months for most other serious crimes is very short, while the limitation period for criminal offenses is much longer. So much evidence is thrown away, à charge and à décharge. I hear privacy lobbyists proclaim that the government is becoming too invasive in private life. But no one has a problem sharing their data online with giants like Google. If we want to tackle (cyber)crime, we must be able to access victims' data so that we can solve cases."

Finally, Van Linthout makes a passionate plea to increase awareness: "I am still amazed every day by the files that we receive and the amounts involved. We must make the population fully aware of the risks and prevent them from falling into the trap of phishing and hackers. Organisations such as the Cyber Security Coalition are doing a good job in this area, but we must scale up those efforts even further. After all, prevention yields the greatest benefits for all parties involved."

Make sure you file a complaint so we can investigate each incident

The Belgian police services operate at multiple levels to tackle cyber crime. Commissioner Caroline Frère, who heads the Federal Computer Crime Unit (FCCU) and also represents our country internationally, explains: “We are constantly recruiting to further expand our investigative capacity and bring on board additional expertise.”

Since 2001, the Federal Judicial Police has maintained a specialised section dedicated to serious online crime. The FCCU focuses on investigating attacks on critical infrastructure, organised international ICT crime and other cyber threats. “We work closely with the federal prosecutor and policy makers. And for ‘alpha cases’, where cyber criminals are testing a new modus operandi, we look into which investigation method is most appropriate,” Frère explains.



CAROLINE FRÈRE

In addition to the federal investigators, each judicial district has a Regional Computer Crime Unit (RCCU), which is also part of the Federal Police. “These colleagues focus mainly on hacking and ransomware at companies, in close cooperation with the local public prosecutors. We work hand-in-hand with the regional investigators. In principle, the investigation starts after a complaint is made to the local police. It is investigated by the RCCU; if it concerns a more widespread phenomenon, the FCCU will coordinate the investigation.”

One major achievement has been the creation of a Quick Reaction Force (QRF) in 2019: a pool of regional and federal experts who can be deployed on an ad hoc basis. “In cases such as the wave of attacks on hospitals including CHWAPI and Vivalia, the RCCUs may not have sufficient personnel to investigate quickly enough. Then, the QRF can provide support on the ground in terms of analytical capacity, technical expertise and coordination.”

Collecting traces and data is crucial

Frère notes that companies often hesitate to file a complaint: “Understandably, this is not their first reflex. People are mainly concerned with getting their activities up and running again, and recovering as much data as possible. Some fear our actions will delay the reboot. But this is not the case: we do not seize servers and we work closely with incident response companies. Our goal is

to collect the right traces, so that we have the data needed for further investigations. This is also very relevant for policy makers: what is not mentioned in the statistics, does not exist!”

To ensure that the right information is collected for each report, the Federal Police has developed the CyberAid tool for the first-line police services. “Whether someone makes a report at the front desk of a police station or an officer documents a complaint during an intervention, we now have a structured method. We provide a manual and flowchart, as well as a form for the victims indicating what elements they need to collect to enable the investigation.”

Because cyber crime is a significant cross-border phenomenon, the FCCU is in close contact with Europol and the Joint Cybercrime Action Taskforce (J-CAT), an international platform for exchanging information with countries inside and outside the EU. “We bring our intelligence to the table and receive relevant information from other countries, such as ransomware trends or impending attacks,” Frère explains. “We also participate in joint investigations. Last year, for example, Operation Magnus led to two data theft programmes being taken offline. A collaboration between the Belgian Federal Police, the Dutch police and the US FBI, it offers further proof that we are indeed achieving successes in the fight against organised cyber crime.” ■

AWARENESS

There's no competition in awareness

The Awareness Focus Group is one of the oldest groups in the Cyber Security Coalition. Through collaboration with experts from various sectors, it aims not only to raise awareness, but also to drive behavioural change and help organisations protect themselves from cyber threats.

The Awareness Focus Group began as a small group of cyber security professionals. Jan Populaire, one of the group's founders, recalls: "We started with just 25 members, who would meet regularly to share best practices and experiences." Jan co-chaired the focus group until end 2023, when he was a marketing and communication specialist at the cyber security competence centre of BNP Paribas Fortis. Today he is director of Psybersafe BV, which focuses on online cyber security awareness trainings based on behavioural science.



JAN POPULAIRE

From a small group to a national movement As the Coalition grew up to 200 member organisations, it brought together participants from IT, HR and communications. This fostered a multidisciplinary approach essential in addressing the human side of cyber security: an often overlooked yet critical factor in a tech-driven world.



SOFIE DE MOERLOOSE

One of the Coalition's first achievements was developing the Cybersecurity Kit. Sofie De Moerloose, a cyber security awareness & communication specialist at Proximus and co-chair of the Coalition's Awareness Focus Group: "The kit was tailored for SMEs, offering practical tools such as customisable email and PowerPoint templates and tests.



ARNAUD RECKO



STÉPHANE VINCE

This allowed companies without dedicated IT teams to easily integrate cyber security into their daily operations.”

Taking security beyond IT

Sofie describes the shift toward creating a cyber security culture: “It’s not just about facts and threats – it’s about guiding people toward better behaviours and building a culture where security becomes second nature.” To support this vision, Jan led the development of a behavioural framework that enables organisations to measure and improve security practices among their employees. Expanding the focus beyond IT has been one of the Focus Group’s most notable accomplishments. Arnaud Recko, sustainability coordinator at DNS Belgium and a board member of Digital for Youth highlights that in recent years the Group has launched initiatives to educate the wider public. “During the COVID-19 pandemic, for example, the Coalition quickly introduced tools such as the cyber security quiz for remote work, helping both organisations and individuals adapt to the new reality.”

Reaching SMEs: challenging but crucial

Among the Coalition’s standout initiatives is the annual national cyber security campaign, organised in collaboration with the Centre for Cyber security Belgium (CCB). Jan Populaire explains that the campaign gains momentum by engaging both private companies and public institutions: “When 180 organisations use the CCB’s materials in their own campaigns, it creates a powerful multiplier effect.” This year, the campaign focusses on two-factor authentication, an important step toward improving online security.

Despite the successes, reaching smaller businesses remains a challenge. Sofie De

Moerloose points out the difficulty of convincing these companies to also focus on cyber security, as they often have other priorities. “We understand that it’s tough, because their core business naturally comes first. Security awareness training and budgets might then feel like a luxury,” she says.

Stéphane Vince, director of technology at L’Agence du Numérique offers three practical points: “First, always prepare to be hacked. Second, if you are hit, be transparent about it. And finally, if your teams think you aren’t at risk, that’s when you should be most worried.” Stéphane leads the CyberWal programme to boost Wallonia’s cyber maturity and joined the Coalition’s board of directors in March 2024.

Security as second nature

The ultimate objective of the Awareness Focus Group is to embed cyber security as a habit in the minds of all stakeholders. Arnaud Recko compares cyber security training to driving a car: “There are many beautiful places you can drive to, but if you don’t stay alert, you’ll crash. Cyber security is the same ; it’s a journey that requires constant vigilance.” Through new educational programmes and ever-evolving tools, the Coalition aims to make cyber security second nature.

The successes of the Coalition demonstrate that collaboration, practical solutions and lifelong learning are key. By uniting organisations and providing them with the right tools, the Awareness Focus Group plays an important role in building a more secure digital future for everyone. As Sofie concludes: “There’s no competition in awareness. Everything we do makes a difference, and the more we support each other, the stronger we become.” ■

PRIVACY & DATA PROTECTION

We provide tools to deal with the dangers of data misuse

Even as privacy and data protection concerns have surged, Belgian citizens and businesses remain vulnerable to data breaches. Recognising the ongoing challenge, the Cyber Security Coalition, alongside the Belgian Data Protection Authority (DPA), continues to prioritise this issue. We spoke with Nathalie Ragheno, chair of the Privacy Focus Group and board member of the Coalition, and Cédrine Morlière, DPA president since 2022, to discuss their achievements, challenges and road ahead.

Privacy protection and data protection regulations form a consistent thread throughout the ongoing digitisation, datafication and digital transformation of our world. "We must keep focussed on this matter because there is a significant power imbalance in the digital realm between citizens and individual users on the one hand, and governments and tech companies on the other," Cédrine Morlière remarks. "Just as

crucially, data breaches are an inherent part of our digital reality." Examples include the 2017 Equifax breach, which exposed the Social Security numbers of nearly half the U.S. population, and the 2018 Marriott breach, which compromised data from half a billion guests, and the Cambridge Analytica scandal, in which data misuse impacted U.S. elections.

Promoting GDPR awareness

"It was precisely this realisation that led to the establishment of the Cyber Security Coalition's Privacy Focus Group in 2017, making it one of the oldest focus groups," Nathalie Ragheno continues. "We scan the landscape for interesting and relevant topics. For example, we previously created a dedicated track on the European Digital Wallet. Last year, we welcomed world-renowned privacy activist Max Schrems to one of our events. Since 2024, we have also selected the Privacy Professional of the Year, to give more exposure to key



NATHALIE RAGHENO



CÉDRINE MORLIÈRE

advancements in this field.” Unequivocally, the EU’s General Data Protection Regulation (GDPR) from 2018 serves as the foundation for these initiatives. “One of our primary goals is to raise awareness about this framework and its implications, and we can definitely say we’ve been successful in this regard. Overall, I believe Belgian businesses are quite compliant with GDPR requirements,” Raghenò states. “Of course, there are exceptions. For smaller SMEs, it’s often much harder to allocate the necessary resources.”

Building a data protection culture

Both experts emphasise the need for a robust data protection culture. “In Belgium, we’re still in the early stages, partly because we are a nation of SMEs, but also because the culture of data protection is still very young. Compared to France, for one, we still have a long way to go. The first data protection laws in France date back to the 1970s; as a result, they have had dedicated professionals in this field for much longer. In Belgium, the concept of a Data Protection Officer (DPO) has only gained traction in recent years. Hence, there’s still a lot of work to be done, particularly in terms of training for the role,” Raghenò explains.

It’s within this landscape that the Belgian DPA focuses first and foremost on raising awareness. “When

we detect a data breach, we work with the affected organisations to guide them through the necessary steps, rather than immediately contemplating sanctions,” Morlière elaborates. “We also provide guidelines for both citizens and businesses. For instance, in our recent report on Smart Cities, we explain the interplay between adequate security measures and data architecture in urban areas where technology is used to collect and analyse large amounts of data for city management purposes. Our main takeaway: the more centralised the data, the more caution is needed to avoid creating single points of security failure.

“We’ve also drafted a list of best practices on cookies, and participated in the elaboration of a data protection guide for small businesses at European level. We distribute our guidelines through our own channels, while also making an effort to engage with the press. Another example is the EDUbox on data and privacy which we launched in collaboration with public broadcaster VRT and other partners among which the Coalition,” Cédrine Morlière continues.

Empowering citizens and businesses

The DPA also enforces the GDPR through its litigation chamber, and offers practical advice

through its Authorisation and Opinion Service. “To give one example, in 2023, we recommended that smart meters update data every 15 minutes to avoid excessive data disclosure,” explains Morlière. Similar guidance was given in 2021 on Brussels’ Smart Move kilometre charge, which initially overstepped privacy boundaries.

While these measures help minimise privacy risks, sanctions remain an essential part of the DPA’s work. “We have to balance empowerment and enforcement. When an organisation disregards the dangers of data misuse, we move toward penalties,” Cédrine Morlière states. “But we always aim to empower both organisations and citizens by providing them with tools to address the dangers of data misuse in the digital world.”

“This clearly illustrates the complementarity between the missions of the DPA and of our focus group,” Nathalie Raghenò adds. “Our goal is also to equip the business world with the means to handle the challenges of data protection, both in terms of raising awareness and implementation. In practice, despite the commendable efforts of DPOs, it’s still all too often like ‘fishing’ among the many different guidelines and potential implementations. The growth of AI in the coming years will further increase the need for clarification and support.” ■

The Cyber Solidarity Act is an engagement to fight cybercrime together



CHRISTIANE KIRKETERP DE VIRON

Over the past 10 years, the EU has put in place a legal framework with the purpose of achieving a higher level of cyber security. The implementation is ongoing and will culminate in the Cyber Solidarity Act. This new piece of legislation, approved by the European Council in December 2024, aims to improve the preparedness, detection and response to cyber security incidents across the EU. It is accompanied by an investment budget of 100 million euro.

Europe's legislative efforts have been setting the example since the NIS1 entered into force in 2016, as the first EU-wide cyber security legislation. Christiane Kirketerp de Viron, Acting Director for Digital Society, Trust & Cybersecurity at the European Commission, explains, "Our internal market is intrinsically connected. This implies that the weakest link can pose a risk for the whole market. Therefore, we needed to agree on what a good level of cyber security entails and how to achieve it."

The regulatory efforts have yielded noticeable results. "The NIS1 has led to most critical entities adopting risk management procedures and other measures, increasing cyber security maturity. We also see a clear impact in incident reporting. The NIS2 introduced Boardroom responsibility, prompting C-suite level interest. As a result, the demand for training is on the rise."

Because the threat landscape and risks continue to evolve at a rapid pace, the EU has taken multiple legislative initiatives to better protect critical infrastructure, businesses, public institutions and citizens. "The Cyber Resilience Act, for instance, is a legal framework published at the end of 2024 that focuses on product security. Everyone agreed that security was not at the

heart of product development and innovation, which instead focussed mostly on speed and getting to the market as quickly as possible. Now the cyber security requirements for both hardware and software are clear, imposing security by design, after-sales patching and a lifecycle approach, to name a few," Kirketerp de Viron states.

Keeping up with and complying with new regulations is a tough job for SMEs and other smaller organisations. "There is a lot of good will among SMEs, who acknowledge they need to do better to protect their businesses. This is the reason we have foreseen transition periods to comply with new rules, and why we insist on standardisation. The latter plays an extremely important role in making things simpler and more straightforward for companies. So, my advice is: use the standards and take advantage of all the tools the Member States have put in place for SMEs - with financial help from the EU."

The final piece of legislation that is currently being rolled out, the Cyber Solidarity Act, is meant to better protect the EU as a whole in times of very sophisticated attacks. "We want to improve the detection, analysis and response to cyber threats. To deal with this in an efficient way, we need to work together. That is why the Cyber Solidarity Act includes a proposal for a European alert system, composed of national and cross-border Security Operations Centres and the use of advanced technologies such as AI to identify threats faster and better. Furthermore, we want to enhance our preparedness for and response to cyberattacks. And we have foreseen a mechanism of mutual support when a Member State is affected by an incident," Kirketerp de Viron concludes.

REGULATIONS AND STANDARDISATION

We help companies implement the NIS2 step by step



PHÉDRA CLOUNER

Over the past decade, the European Union has launched numerous regulatory initiatives to promote cyber resilience. This coordinated approach was necessary due to the strong digitalisation of the economy and society, coupled with the significant increase in cross-border cybercrime. The Centre for Cyber security Belgium (CCB) is responsible for the national cyber strategy, implementing EU regulations and coordinating the monitoring and follow-up of cyber threats.

The CCB was founded at the end of 2014. Managing Director General Miguel De Bruycker and Deputy Director General Phédra Clouner were tasked with developing this specialised organisation. "Today, the organisation counts approximately 125 employees. Policymakers are now acutely aware of the need to invest in cyber resilience," says Clouner. "And the impact of cyber criminals on the economy and on our society has become clear. While a lot of money is at stake, successful phishing among citizens can also lead to more personal impact."

The NIS1, the first major step

To limit this impact, the EU has issued a host of regulations. "The 2016 NIS Directive was a first major step in increasing the cyber security of the Member States. It obliged organisations from six sectors providing essential services to take measures and arm themselves against cyberattacks. We already see a much higher cyber maturity in e.g. the financial sector, the energy sector and the ports. But as Member States implemented the directive in their own ways, this has led to complex situations, especially for multinationals."

The NIS2 Directive was issued in 2022. Clouner: "Some vital sectors, such as the public sector, remained outside the scope of the NIS1. The NIS2 solves this, with a much broader target group of

essential service providers. The approach has been made more coherent, too. For instance, the same criteria are now used throughout the EU to determine who must take these regulations into account, based on sector, number of employees and turnover. And the cooperation between the cyber security authorities of the Member States is also more formalised."

A framework for certification

The NIS2 came into effect at the Belgian level at the end of 2024. "We started very early to raise awareness in the sectors involved about what was coming. We did this, for example, through our presence in Cyber Security Coalition focus groups, which offer a very interesting forum for discussion. Moreover, we developed the CyberFundamentals Framework, a series of concrete measures that organisations can implement step by step to be compliant with the NIS2. They will be able to be certified based on this Framework, just as they can with ISO 27.001. In addition, the Deputy Director General of the CCB also refers to the GDPR privacy regulation (2018), the Cyber Security Act (CSA, 2019), the Digital Operational Resilience Act (DORA, 2022), the Cyber Resilience Act (CRA, 2023), and the upcoming Cyber Solidarity Act and AI Act (2025).

"We realise that companies are subject to a lot of regulations and that it requires great effort to implement all of it in your organisation. The EU is also aware of this, and aims to give companies time to do what is necessary. But with the cyber threat still increasing we must all accept that cyber security has to be a priority for every public institution, for every company and for every citizen. The CCB will continue to fully play its role in increasing Belgium's cyber resilience, by offering services such as Safeonweb@work. And we have the ambition to expand our capacity even further in the coming years," concludes Clouner.

REGULATIONS AND STANDARDISATION

The challenge remains to convince SMEs to invest in cyber security



SÉVERINE WATERBLEY

For more than 10 years, the FPS Economy has been taking initiatives to raise awareness among companies and independent professionals about cyber security. Due to widespread cyber attacks and the increase in European regulations, this mission remains highly relevant. “In close collaboration with the Belgian ecosystem, we will continue to focus on raising awareness among SMEs and the self-employed.”

Séverine Waterbley is President of the FPS Economy and a Cyber Security Coalition board member. Her many contacts give her a solid perspective of the evolution in cyber security awareness in our economy: “It is clear that our companies are much more aware of the risks than 10 years ago. But with more than 100 incidents reported every day, we must continue to convince self-employed people and SMEs to better prepare.”

Recovery plan: 13 projects, €12 million

The FPS Economy has therefore launched the website mijnzaakcyberveilig.be / mapmecybersecurisee.be, with an online QuickScan for SMEs that helps them identify the first steps they can take in cyber security. For personalised advice to further improve their cyber security, they can turn to the CyberScan. “More than 600 self-employed people and SMEs with fewer than 50 employees have already carried out the CyberScan,” says Waterbley.

“In addition, as part of the post-COVID recovery plan, we have invested 12 million euros in 13 projects that contribute to increasing the cyber security maturity of our SMEs.” The selected projects include a training programme from the NSZ/SNI and Safeshops.be on webshop cyber security, a programme for Brussels-based SMEs from CyberWayFinder, and a basic cyber security training for contractors developed by the federation FABA/FECC.

Standardised approach for SMEs

European directives, such as the NIS2, CRA and CSA, are imposing a growing number of rules, with the aim of increasing our economy's cyber security. “We need to give the private sector the necessary time to implement it all. It's critical that they develop strategies and cyber security action plans now. Sometimes it seems a bit far-fetched for SMEs, but if they act as a supplier to a larger organisation that is subject to certification and audit under NIS2, they will be confronted with these rules too.”

Introducing a standardised approach will therefore also prove useful and necessary for smaller companies. Waterbley: “For public institutions and large companies, ISO-27001 has become the standard. However, this approach can be difficult to achieve for smaller organisations. To address this, they can call on a service provider to help them, or set up the necessary measures themselves via the CyberFundamentals Toolbox from Safeonweb@work.”

She shares this message annually at numerous congresses and conferences that specifically target the self-employed and SMEs. “This group has little time, so you have to address them specifically, and show them that they must not only invest in protection, but also in a recovery plan in case they are affected.”

She concludes, “In the coming years, we will focus our awareness campaign more on specific sectors, such as construction, energy and pharmaceuticals. The Cyber Security Coalition can play an important role in this, with its broad network and the practical expertise at its disposal.” ■

10 years of experience sharing and networking events



2018 | BELGIAN CYBER SECURITY CONVENTION



2024 | KEYNOTE DAVID HICKTON



2024 | BE-CYBER EXPERIENCE SHARING EVENT



2022 | CYBER SECURITY AWARENESS & CULTURE MANAGER TRAINING



2023 | BE-CYBER EXPERIENCE SHARING EVENT



2021 | CYBER SECURITY PERSONALITY OF THE YEAR



2024 | CYBER SECURITY PERSONALITY OF THE YEAR



2022 | CYBER SECURITY PERSONALITY OF THE YEAR



2023 | WOMEN4CYBER BELGIUM



2023 | GRC: BE CONNECTED!



2023 | CYBER SECURITY PERSONALITY OF THE YEAR



2023 | GOODBYE SUMMER EVENT @ CEGEKA

CLOUD SECURITY

Seize the momentum of the cloud to create a continuous interest in cyber security

While the rise and growth of cloud computing has fundamentally transformed technological development, its impact has also created numerous challenges in data and resource management and security. These will require the Cloud Security Focus Group to stay vigilant and up-to-date in the coming years. Permanent chair Ulrich Seldeslachts is well aware of the scale of the task.

Delivering benefits from agility, availability and elasticity to cost savings, cloud computing leverages leading-edge technologies to meet the information processing needs of many organisations. But it also introduces a new set of challenges, such as a shift in the dynamics of IT resource control, both in terms of ownership and management. Faced with this context, the Cyber Security Coalition established the Cloud Security Focus Group in 2018, with LSEC and KBC taking on a driving role.

From perimeter defences to zero trust architectures

“Our group’s objective is to identify current security issues in cloud computing service implementation, and to equip our members with the tools to address them,” explains Ulrich Seldeslachts, CEO of LSEC and permanent chair of the focus group. “We provide practical security management approaches for cloud operations, guidance on applying risk management to cloud-based systems, and support for re-evaluating organisational processes to facilitate cloud migration. We also offer training to enhance maturity in this area.” Fulfilling this role requires close monitoring of the latest technological developments. “We gather knowledge from both inside and outside the Coalition, and explore meth-

odologies for assessing cloud security,” Seldeslachts continues. Emphasising how much the group has evolved since its inception, he adds: “Initially, the focus was on perimeter defences and compliance, but the rise of advanced threats shifted our attention to zero trust architectures and continuous monitoring.”

Adapting to multi-cloud strategies and advanced threats

One important trend has been the increasing use of multi-cloud strategies. “This approach requires unified and proactive security policies across different environments, embedded in the software development lifecycle,” he notes. “To achieve this, we must keep stressing the importance of knowledge sharing, and continue our ongoing efforts to attract new members and insights.”

The central challenge for cloud security lies in Belgium’s highly heterogeneous cyber security landscape. “There is a large and even growing group of companies with a low level of cyber security maturity. This means we need to have enough different focal points within each group. As Chair, I have noticed that here, too, there is an opportunity to seize the momentum of the cloud to create a continuous interest in cyber security maturity improvements. This will remain key in the upcoming years,” he concludes.



ULRICH SELDESPOCHTS

CLOUD SECURITY

Assume that you will have a security breach. And be prepared!

Walter Adriaens (KBC) and Frederik de Ryck (Accenture) are both optimistic yet realistic about cloud security among Belgian companies. While work remains, Belgium is certainly not lagging. They discuss 'assume breach' thinking and how to maintain security without undermining trust within your organisation.

Frederik De Ryck is a Cyber Security Senior Manager at Accenture Security, focusing on Cloud Security. He actively contributes to the Cloud Security Focus Group: "The Belgian market is diverse. Some institutions - such as financial players, defence organisations or EU bodies - use top-tier practices, but others remain unaware of major pitfalls. Belgian firms can also be conservative, adopting a 'wait-and-see' approach before investing significantly in cloud security. Our reliance on major international cloud service providers (CSPs) forces us to carefully address data sovereignty, regulatory compliance and potential geopolitical risks."

What are the biggest technology-related threats currently and how do they affect cloud security?

Walter Adriaens is Delivery Manager at KBC Bank & Verzekering, overseeing on-premise servers and public cloud teams. He chairs the Cloud Security Focus Group within the Cyber Security Coalition: "Organisations must realise that advanced technology - AI for analytics or IoT for smart devices - also introduces new vulnerabilities. For example, I know of a pilot programme for an AI tool that automatically generated meeting minutes. The users discovered that any participant, even someone invited briefly and then removed from the session, could later access the entire set

of notes, including confidential information. The tool had to be disabled to avoid exposing sensitive data. That's why at KBC, we emphasise a 'zero-trust' mentality.

Frederik: AI and IoT can expand your attack surface if deployed without proper security baselines. For instance, IoT devices often ship with weak default configurations, leaving them wide open to malicious actors. Quantum computing, on the other hand, has the potential to break current encryption schemes, though it may not be an immediate large-scale threat. Additionally, while confidential computing and hardware-based encryption offer promising ways to keep data secure even during processing, they are often expensive or still not robust enough for widespread adoption. Nevertheless, organisations should keep an eye on such technologies to future-proof their security.

"Organisations must realise that advanced technology also introduces new vulnerabilities"

How do criminal threats like ransomware or insider breaches rank among your concerns?

Walter: These are major worries. Ransomware attacks can cripple an entire company, whether your IT runs on-premise or in the cloud. Insider threats also deserve attention, because anyone with valid credentials can



FRED DE RYCK



WALTER ADRIAENS

cause data leaks. That's why we train people extensively, limit privileges where possible, and keep robust monitoring in place. We also try to manage these restrictions in a positive way: we explain that minimising access protects each user, should their account get compromised.

Do political and regulatory factors, such as Schrems II or the GDPR, create additional challenges?

Frederik: Absolutely. European companies must comply with the GDPR, and Schrems II places more scrutiny on data transfers outside the EU. With the major CSPs largely based in the US, questions on data sovereignty arise. It's not just about criminal hackers but also about potential state-sponsored access to sensitive data.

Walter: For a bank like KBC, compliance is non-negotiable. We must align with the European Central Bank's guidelines, national and EU regulations like DORA, and internal standards. This can become complicated, but it also drives us to maintain the highest levels of security in our cloud strategy.

Where do companies most need to improve on cloud security?

Walter: First, establish a clear cloud strategy. Define your goals and requirements. Second, invest in the right people. Your staff must understand configurations, monitoring, security and incident response. Third, assume you will

be breached. So, make sure you can detect, contain and recover quickly.

Frederik: Start with secure defaults. Many CSP features arrive wide open by default. This is why the Cyber Security Coalition has signed the Manifesto advocating for vendors to integrate baseline security controls into their user infrastructure by default. And if you're an SME, you don't have the luxury of large security teams. Hence, adopting best practices and limiting permissions will greatly reduce risk.

What are its next steps for the Cloud Security Focus Group within the Cyber Security Coalition?

Frederik: We've been collaborating to push CSPs to improve default security settings, especially for smaller businesses. We are working on a baseline that ensures essential protections are enabled by default, reducing accidental misconfigurations. Next year, we plan to finalise that baseline and continue raising awareness throughout Belgium's cyber security community.

Walter: The group brings together experts from both large and small organisations, pooling knowledge on legal, technical and operational aspects. By uniting our voices, we can influence providers more effectively than if we each approached them separately. We'll focus on practical tools, industry-wide standards and knowledge-sharing to strengthen cloud security across the board. ■

cryptography

It's all about preserving a fundamental individual right

In today's rapidly evolving digital landscape, cryptography is an essential pillar of robust security architecture. With the rise of sophisticated threats and emerging technologies, Bojan Spasic and Johan Kestens, co-chairs of the Cyber Security Coalition's Cryptography Focus Group, delve into the challenges and opportunities shaping the future of cryptography. They highlight its fundamental role in preserving privacy and security in an interconnected world.

Anyone looking to outline today's main cryptography challenges and trends will encounter quantum computing. "It's been clear for several decades that quantum algorithms offer a performance advantage for a specific class of problems," explains Bojan Spasic, who combines a position as cyber security technology partner manager at Swift with his role at the Coalition. "Once an adequate quantum computer is built, we could potentially see a devastating impact on the cryptography that is being used around the world to guarantee data confidentiality and integrity. Malicious actors would have the power to

break widely used cryptographic algorithms such as RSA and ECC." While such large-scale quantum computers are still hypothetical, how far off they truly are remains a matter of intense debate. Most predictions suggest 10 years, "but it is obvious that the adoption of post-quantum cryptography (PQC) should already be high on the agenda of every organisation involved in cyber security. Bad actors can collect encrypted information today, then wait to decrypt it once a cryptographically-relevant quantum computer is available," Spasic continues. "Recent milestones, such as NIST's pioneering standardisation of PQC algorithms in August 2024, are the first step forward, but I think the potential impact of this cryptographic change is underestimated."

An inherent trade-off

Adding to the complexity of cryptography is its inherently challenging nature. In the face of this, the migration to cloud systems - without a doubt one of the most significant developments of recent years - can be seen as a benefit. "As an organisation, you are



JOHAN KESTENS



BOJAN SPASIC

essentially choosing to outsource your data because it allows you flexibility. This also applies to cryptography management. However, this introduces security risks (such as with key management) that, in my opinion, are sometimes taken too lightly,” Johan Kestens states. He is an independent consultant who advises companies on designing and implementing cryptographic policies.

“I take a very conservative stance on this. I believe you should always be attentive to what happens to your data in the cloud provider space. Considering the challenges imposed by the PQC migration,

“Privacy is, after all, the reason we do this work”

however, this can have a positive aspect. In particular, we are seeing these providers beginning to play a leading role in this area. But again: this implies you see them as allies when in fact you should always remain careful when en-

gaging. On the other hand, there are cryptographic techniques enabling computation on encrypted data that can help there, and the cloud providers are slowly but increasingly recognising the benefits”, Kestens continues.

Key management is - and will remain - critical

The exponential growth of smart devices and IoT creates yet another difficulty. Bojan Spasic: “Even though cloud services can help structure and manage cryptography, it remains challenging. Due to their small size and low energy use, IoT and smart devices can only handle lighter forms of encryption.”

A sufficiently high degree of security can in this case only be achieved through proper key management. “Too often, solid key management is undervalued. Especially with wireless smart devices, managing keys is no simple task. In my view, the relevant legislation is not strict enough. The all-to-frequent use of generic passwords by manufacturers should be banned. Conversely, the benefits of structured key management in the cloud only apply if you make the keys available to the cloud platform, and you may or may not be comfortable with that,” Johan Kestens clarifies.

A story for us all

While cryptography is the workhorse of today’s interconnected world, enabling secure business transactions, the human side cannot be ignored. “Privacy is, after all, the reason we do this work: it’s about preserving a fundamental, individual right,” says Bojan Spasic. Although we rely on high-tech innovation for protection, at its core, it is fundamentally a human story. Thus cryptography is essentially about ethical and societal issues that impact everyone.

Discussions on the role and use of cryptography can therefore never be entirely detached from the cultural and societal contexts in which they occur. People’s perceptions on (the enforcement of) privacy rules and their implications will always vary depending on cultural and political circumstances. Consequently, this field will increasingly need professionals who can explain to the business world and the public what cryptography does and what effects it has. “That’s why we need communicators who can understand the technology and then translate it,” Johan Kestens concludes. ■

ENTERPRISE SECURITY ARCHITECTURE

Just because you are compliant does not mean that security is guaranteed

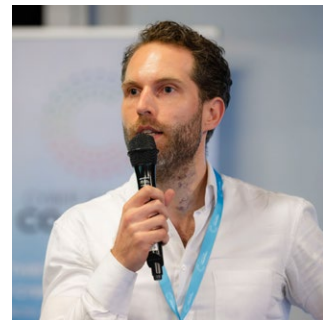
The more complex IT networks and infrastructure become, the more difficult it is to protect that architecture against cyber attacks. The job of enterprise security architects has therefore become simultaneously more challenging and more strategically important. “We oversee the bigger picture and must ensure that security is taken into account in all domains.”

With the switch to the cloud, as well as the increase in Operational Technology (OT)-related assets and new technology platforms, organisations’ digital footprints are growing larger and more difficult to manage. “At the same time, attackers are using increasingly sophisticated methods, such as AI malware. In terms of defence, the job of the enterprise security architect (ESA) is becoming more difficult; in terms of offence, things are evolving very quickly,” says Hans Hujuel, ESA at Innocom and Cybersecurity Program Manager at the Belgian Cyber Command.

“The focus in what we do has therefore shifted from protective controls to include detection and recovery controls,” adds Michael Boeynaems, co-founder of Splynter and chair of the Cyber Security Coalition’s Enterprise Security Architecture Focus Group. “Our customers often have many legacy systems and applications that are still important. The question arises as to how you can define security mechanisms that consistently secure both modern cloud environments as well as these legacy environments where, for example, implementing network segmentation or multi-factor authentication may be much more challenging.”

Know your assets

The security architecture must close as many doors as possible to potential attackers. The more complex the IT landscape becomes, the more important it is to have everything properly mapped out. “Know your assets. That’s what it’s all about today: having an



MICHAEL BOEYNAEMS



HANS HUJUEL

accurate and up-to-date picture of the IT, network infrastructure and architecture, which assets are connected to each other, which applications the business uses... But keeping it all under control remains difficult," says Hujuel.

One positive development has been the introduction of standards and frameworks, along with the availability of quality documentation. Exchanges within the ESA Focus Group have played a contributory role in this. "However, we notice that smaller organisations in particular still struggle with risk management. Which assets are critical? What risks are you willing to accept? And how do you further

"Just because you are compliant does not mean that cyber security is guaranteed"

expand your architecture, taking into account the business needs? That is where the challenge lies," both experts indicate.

Seeing the bigger picture

Enterprise Security Architecture is on the one hand a fairly technical matter, but on the other hand it touches on strategically impor-

tant aspects. "We cover various domains and deal with governance, legislation and compliance, but also application security and cryptography. ESAs must be at home in many markets and see the bigger picture," says Hujuel. "They must also be able to explain things to senior management and the Board of Directors. But that assumes that these people have some knowledge of IT and the specific needs of the business."

Security buffers are built in to ensure a robust IT environment, but how do you reconcile that with an agile organisation and ease of use for end users? Boeynaems

comments, "Agility and security can go hand-in-hand. While there is often a perception that security slows things down, in fact we are perfectly capable of participating in a fast, iterative process. It's just a matter of appropriate organisation. By working closely with developers for example, we can ensure security by design as part of a robust devsecops framework."

Compliance must remain proportionate

According to both Hujuel and Boeynaems, the true tension is primarily between security and compliance, especially due to the sheer volume of regulations. "We see that the NIS2 and DORA are causing a real shift in companies," Hujuel explains. "But we have to be careful that it remains proportionate. The focus is in danger of shifting more to controls than to actual threats and risks. The risk of a fine is sometimes perceived to be higher than the risk of a successful attack. But just because you are compliant does not mean that cyber security is guaranteed."

The coming years are certain to remain challenging. "I see AI evolving into a specific security domain with specific security needs. In addition, quantum is also coming our way. But many organisations still struggle with the basics and often it comes down to keeping things simple and maintainable while prioritising securing the critical processes," says Boeynaems. "Geopolitical tensions will continue to fuel destructive attacks on critical infrastructure. And we also see the success rate of supply chain attacks increasing. This is often the weakest point of entry. So organisations will have to focus even more on that," concludes Hujuel. ■

This really is 'the brain' of your security

GOVERNANCE, RISK AND COMPLIANCE

Almost every cyber security challenge and issue can be traced back to the dynamic interplay of governance, risk and compliance (GRC). This explains the strong response to the Cyber Security Coalition's GRC Focus Group. Providing a comprehensive overview of developments in the field in the past ten years is a difficult task. In an attempt to address the complexity, Karine Goris, Laurie-Anne Bourdain and Tatiana Postil reflected on this question together. According to them, "The most important thing is that maturity continues to increase."

Whenever IT security is discussed, the terms 'governance', 'risk' and 'compliance' are quickly brought up. "GRC is fundamentally linked to the overall maturity level of your cyber security. I often call it 'the brain' of your security. Technical implementations serve as 'the heart', but of course, even this relies on the brain," explains Karine Goris, Chief Security Officer (CSO) at Belfius.

Growth in maturity

This GRC 'brain' has evolved significantly over the past decade. The growing complexity of cyber threats has, for example, led to the adoption of several important standards and frameworks, such as ISO 27002 and the NIST Cybersecurity Framework (CSF). Furthermore, there is increased adoption of an integrated risk management (IRM) approach, increased involvement of the supply chain, growing quantification of cyber risks, and increased integration of GRC platforms into business operations.

"The evolution in information security is like the evolution in IT, which was long seen as something that merely supported the business.

Today, however, it is recognised as a strategic asset and a topic for the management level,” adds Laurie-Anne Bourdain. Data Protection Officer, Information Security Officer and Business Continuity Manager of Isabel Group, a Belgian Fintech active in the BeNeLux and France. She is one of the co-chairs of the GRC Focus Group.

This shift has implications on the profile of professionals involved in this field. Previously reserved for technical profiles, today it also requires people with a strong understanding of business and leadership qualities. So, while a Chief Information Security Officer today may not need to be able to set up a firewall, GRC professionals must be able to analyse its operation and report on it to the organisation's board. “My personal career is an illustration of this. I started as a network engineer with a purely technical profile. Today, as CSO of Belfius, I am more involved with strategy and implementation than with the technical side,” continues Karine.

Safe space between carrot and stick

The key is to be able to translate GRC developments into business objectives. “This ability contributes to overall maturity growth, by increasing awareness that IT security is a fundamental building block for a company's success and not just a cost item,” Goris continues. The many legislative initiatives that have emerged in recent years at European level, including GDPR (2016), NIS1 (2016), NIS2 (2023), DORA (2023) and the Cyber Resilience Act (2024) have set the framework. “In the financial sector - which continues to play a leading role in GRC - the focus today is firmly on DORA,” Bourdain states. Cyber incidents are a very important driver for this cultural shift too. “Every cyber incident that a company or even a peer in the sector faces leads to increased awareness of the impor-

tance and potential impact of GRC. This can lead to additional budgets for GRC,” explains Tatiana Postil, GRC and IT risk consultant, and a member of the ISACA Belgium Chapter Board.

“Like most developments, this evolution - and the resulting discussions - is driven by both a carrot and a stick. Every event, whether new legislation or a cyber incident, forces people to adapt to a new context. This jumpstarts a negotiation phase on how to deal with the new reality, creating a context where much change is possible,” Postil continues. “By being transparent and learning from each other, everyone can achieve great gains. Our focus group aims to give this process as much tailwind as possible by creating a safe space for all participants to openly share their insights.”

“By being transparent and learning from each other, everyone can achieve great gains”

Not the most exciting profiles?

The focus group, which was established in 2019, aims to serve as a trusted platform for exchanging success factors and content that contribute to developing security policies, processes, and risk and compliance measurements. In other words, it provides a space to reflect on the ‘how’ and ‘what’ of building a strong security culture. As a result, focus group

membership has expanded from mostly technical experts to include a broader range of profiles. "For example, we expect to welcome more project managers, because the implementation of each new piece of legislation must in practice be managed as a standalone project," says Postil.

In light of this shift, the focus group is broadening its orientation towards the entire business world, including collaboration with ISACA. "By setting up collaborations with them and hosting events such as the annual GRC: Be Connected! experience-sharing event, organised with Solvay Brussels School of Economics & Management and ISACA Belgium Chapter, we aim to raise the awareness of people outside the profession about why GRC is important for business today," they agree.

This is the clear direction for the coming years. "The most important thing is that maturity continues to increase. I hope to see more positions with the job title of 'GRC expert', reflecting a growing recognition of GRC's importance for the business world overall," says Bourdain. "Audits will also play an increasing part in the constantly evolving threat landscape," Tatiana Postil, a certified auditor herself, adds.

Obviously, the demand for GRC profiles will also grow in the coming years. "This will be a considerable challenge because young people don't necessarily see 'GRC expert' as one of the most attractive profiles. By definition, a GRC expert tends to be a generalist, while young people are attracted to specialist jobs, such as programmer or hacker," says Karine Goris. Additionally, the role requires a lot of experience, making it necessary to look at profiles that have flown into the field from other sectors. "These people bring knowledge and skills that are much rarer in the sector," concludes Laurie-Anne Bourdain. ■



TANIA POSTIL



KARINE GORIS



LAURIE ANNE BOURDAIN

NIS2 isn't just about avoiding fines. It's about making our society more resilient

As industries become more digitalised and connected, the need for robust Operational Technology (OT) and Industrial Control Systems (ICS) security is growing rapidly. The introduction of NIS2 has brought the need to safeguard OT/ICS to the boardroom discussions. But how should organisations tackle the challenges ahead? Vincent Haerinck and Gert-Jan Wille, members of the Cyber Security Coalition's OT/ICS Focus Group, believe that Belgian companies urgently need to further secure their OT systems.



GERT-JAN WILLE

"Safeguarding OT/ICS is fundamentally different from traditional IT protection," explains Vincent Haerinck, who co-chairs the OT/ICS Focus Group and leads the OT Security practice at Toreon, specialising in risk management for the energy sector. "Many OT infrastructures are designed to last 20 to 40 years, while IT systems evolve much faster. Securing such long-lived machines requires a distinct approach." OT systems often interact with the physical world, and their failure can be catastrophic. "For example, an OT disruption in a nuclear or energy production facility could have massive consequences, affecting not just the entities involved, but society as a whole," he adds.



VINCENT HAERINCK

Gert-Jan Wille leads the cyber security research group at HOWEST University of Applied Sciences and advises both the Belgian government and the European Commission. He highlights the increased vulnerability caused by connecting OT systems to the internet. "Companies often see OT as 'just machines,' but once online, it becomes susceptible to cyber attacks," he says. "We've seen cases where outdated infrastructure,

“Imagine two weeks without electricity or clean water - that’s the level of risk we’re facing”

including a lock gate in northern France, has been left exposed online for years, allowing anyone to operate it remotely. This shows how critical and easily compromised OT networks can be.”

Collaboration is key within the OT/ICS Focus Group

The Cyber Security Coalition’s OT/ICS Focus Group aims to raise awareness and promote collaboration across sectors. “We bring together diverse industries, from energy to food production, to share experiences, tackle challenges, and explore solutions,” says Haerinck. “When requested by members, the group also provides a platform for certain vendors to provide more insights into innovative solutions.”

Belgium has been at the forefront of adopting and enforcing the NIS2 directive which strengthens cyber security for essential and important entities. The Centre for Cybersecurity Belgium (CCB) plays a key role in helping organisations comply, by providing resources, guidance and support. The government also works closely with industry entities to ensure that businesses, particularly SMEs, can access the necessary funding and expertise to bolster their cyber security.

“The NIS2 has been a game-changer, especially for C-level executives who now face personal fines for non-compliance,” notes Wille. “In the past, safeguarding OT was often an afterthought, but it’s now becoming a top priority for company leadership.” He explains that the new legislation has forced businesses to reevaluate their security strategies, particularly with a focus on the supply chain. “Even if a company is not directly covered by

the NIS2, they still may need to increase their cyber security efforts to remain a supplier for their client. This has increased awareness across various sectors.”

Starting today: Mitigating risks and seizing opportunities

Many organisations are still trying to figure out how to comply with the new regulations. “Some are just now realising the importance of asset management: knowing exactly what devices are connected to their OT networks. Without that understanding, it is impossible to secure the environment properly,” says Haerinck. The OT/ICS Focus Group plays a pivotal role in guiding companies by sharing best practices and fostering collaboration across sectors.

Both Haerinck and Wille believe that, while progress is being made, securing OT/ICS environments will be a long-term endeavour. “In five years, we’ll see some significant improvements, but it will take decades of investment to fully secure these systems,” says Haerinck. He again stresses the potentially devastating societal impact of OT failures, such as in energy or water treatment facilities. “Imagine two weeks without electricity or clean water—that’s the level of risk we’re facing.”

Wille echoes this sentiment: “Companies need to act now. Many incidents are caused by human error—such as using default passwords or incorrectly configuring networks. Awareness and training are key. Supply chain protection also needs attention, as the NIS2 and future regulations will demand that organisations manage the risks posed by their vendors.” ■

APPLICATION SECURITY

With a proactive approach of app security, we aim to create a safety net

The explosion of apps - including in-house applications, cloud applications and SaaS tools - marked a true revolution, in more ways than one. From a security perspective, it significantly expanded the potential attack surface: each app and device provide additional entry points for intruders. Sebastien Deleersnyder and Lieven Desmet - co-chairs of the Cyber Security Coalition's Application Security Focus Group - and Philippe De Ryck, organiser of SecAppDev and founder of Pragmatic Web Security, reveal how they are addressing these challenges head-on.

In 2023, the Cyber Security Coalition launched the Application Security Focus Group to address new security challenges stemming from the rapid proliferation of apps. Its primary goal is to strengthen security practices in order to detect, resolve and ideally prevent vulnerabilities within applications. "The group covers the entire application lifecycle, from requirements analysis, design, implementation, verification, to maintenance," explains Sebastien Deleersnyder, who is CTO of Tore-on and was named Cyber Security Personality of the Year 2022.



LIEVEN DESMET



SEBASTIEN DELEERSNYDER



PHILIPPE DE RYCK

“A central priority is building strong partnerships between developers and security teams”

The aim is to foster a shift toward a more proactive approach to application security. “Software vulnerabilities are common, which makes them frequent targets in attack chains. By identifying and fixing these issues early, we can significantly reduce an organisation’s attack surface. If we don’t, the organisation will sooner or later face an existential threat,” Deleersnyder points out.

The key principle is to map out the existing attack surface and identify the threats that might exploit it. The 2020 Threat Modelling Manifesto plays a fundamental role here, because “it treats security as a team effort involving multiple stakeholders. Therefore, Threat

Modelling (TM) should be as agile and iterative as possible, aligning the team around a shared security vision,” notes Lieven Desmet, Professor of Privacy & Security at KU Leuven. “In the past, security testing was typically carried out infrequently (e.g. as part of a half-yearly software release cycle). Now, it needs to be done much more frequently - even continuously - to keep up to speed with the fast-paced software release cycles and the continuous changing attack landscape.”

Connecting to broader trends

The overarching nature of these threats makes an emphasis on training and knowledge shar-

ing essential. “Through a close collaboration with SecAppDev, we organise an intensive week-long training session on this topic at KU Leuven,” says Philippe De Ryck. “Participants learn to prioritise threats and address risks in legacy applications, which is a frequent issue in application security. This reinforces the principle of security by design in application development.”

In essence, application security intersects with nearly every significant cyber security trend today. “Advanced threat modelling, blockchain for data integrity, post-quantum cryptographic algorithms and the expanding use of multi-factor authentication to secure user access are all developments closely related to application security,” notes Desmet.

“A central priority is building strong partnerships between developers and security teams. This could involve embracing security champions in the development team or facilitating the integration

of security tooling in the Continuous Integration (CI)/ Continuous Deployment/Delivery (CD) pipelines, to give a few examples. Over time, companies have tried out various tailored approaches, and their specific successes and failures provide extremely valuable insights for other members of the focus group. This open culture encourages members to freely share their experiences,” Lieven Desmet continues. This is also why the annual Application Security gathering, which will mark its seventh edition in 2025, has grown into one of the Coalition’s major events. “International experts and speakers share their insights, helping members of the field stay up to date on the latest technological advances,” describes Sebastien Deleersnyder.

Milestones and standards

The collective progress in this field is reflected in several major milestones achieved in recent years, such as establishing the Open Web Application Security Project (OWASP), introducing Secure Development Life Cycle (SDLC) models, adopting security-focused development methods such as the Lightweight Application Security Process (CLASP), and implementing Common Vulnerability Scoring System (CVSS) to standardise security risk severity ratings.

These advancements are largely driven by the maturation of security standards, which have “enabled everyone to build applications securely from the start.

By removing common pitfalls and challenges, we’re moving towards a secure-by-default approach that ultimately makes security easier to achieve,” says Philippe De Ryck. “In practice, however, implementing these standards raises extra challenges for the whole ecosystem. Companies must adhere to a secure software development lifecycle for their own development, and monitor the security posture of all their suppliers, adding complexity,” adds Desmet.

In the coming years, the focus will remain on supporting developers and architects to build secure software and to learn to test it

“We’re moving towards a secure-by-default approach that ultimately makes security easier to achieve”

themselves. “Our experience shows that it’s almost impossible for developers to keep up with every change. It’s unrealistic to expect them to never make mistakes. That’s why we aim to create a safety net. These are boundaries within which teams should operate. By staying within them, it’s relatively easy to keep the application secure – even when mistakes do occur,” Philippe De Ryck concludes. ■

CYBER SECURITY FOR HOSPITALS

We must constantly balance security with accessibility

With the increasing digitalisation of the healthcare sector, the risk of cyber attacks is rising in tandem. This concern prompted the Cyber Security Coalition to establish a focus group dedicated specifically to this sector. Wouter Danckaert, CISO at Jessa Hospital Hasselt, and Wendy Roodhooft, CISO of az Vesalius Tongeren, discuss the growing challenges, emerging technologies, and future vision for cyber security in the Belgian healthcare domain.

Greater digitalisation inevitably attracts more hackers, who know all too well that hospitals provide critical services. "Ransomware is currently the most significant threat hospitals face," Wouter Danckaert and Wendy Roodhooft begin by emphasising together. Hackers aim to block access to systems by encrypting data and demanding ransoms. This can severely impact patient care because when staff cannot access data, the result can be unpleasant and even life-threatening.

"During a cyber attack, we must continue providing services, even if test results are delayed or operating room staff are not adequately prepared," Roodhooft explains. "In addition, waiting times for patients can increase by as much as 50%, which underscores the urgency for hospitals to stay ahead of these attacks."



WENDY ROODHOFFT



WOUTER DANCKAERT

Data theft is another pressing concern. “Patient records contain extensive sensitive information, from medical histories to personal and financial details, which position us as an appealing target,” Wouter Danckaert notes. “While data in other sectors is also valuable, the sensitivity and volume of medical data in healthcare make us uniquely vulnerable.”

Balancing security and accessibility

“We must constantly balance security with accessibility,” Danckaert says. “In a hospital, information often needs to be instantly available to doctors. This is why we use role-based access in our electronic patient record system and apply the ‘break-the-glass’ principle, which removes certain access barriers in emergencies so that doctors can retrieve the information they need quickly.”

“Beyond AI, we see significant potential in machine learning”

He also highlights the challenges posed by third-party software systems. “Hospitals frequently use multiple systems that need to exchange data securely. Each system has different requirements, adding complexity, but we ensure that security does not compromise the speed and accessibility essential to healthcare.”

Awareness and training

Over the past five years, az Vesalius Hospital has invested substantially in a comprehensive security plan. “One of the most effective measures I implemented when I started this role in 2020 was multi-factor authentication (MFA),” Wendy explains.

Engaging healthcare staff has also been a priority. az Vesalius organises regular information sessions for staff and circulates articles on GDPR compliance, phishing and other key topics. “Our management then

receives tailored training to ensure they thoroughly understand the risks, so they’re aware of the impact of their decisions.”

Wouter Danckaert agrees: “Raising awareness is essential to our cyber security strategy. We plan to launch an awareness platform to help staff recognise cyber threats and respond appropriately.”

Trends and technologies in the future of cyber security

The first steps have also been taken towards implementing artificial intelligence. “AI helps us identify normal behaviours, such as typical browsing patterns in records, and detect anomalies,” Wendy Roodhooft explains. “Beyond AI, we see significant potential in machine learning to respond to threats faster,” Wouter adds. “These technologies can analyse vast amounts of data, recognise patterns, and identify attacks early on.”

She highlights the growing risks posed by wearables and mobile medical devices that move with users. To mitigate these risks, hospitals are implementing network micro-segmentation. “Micro-segmentation enables us to place vulnerable devices, such as medical equipment, in separate network segments, which isolates them and reduces the risk of contamination,” Wouter Danckaert explains. He also closely monitors advances in quantum computing. “Quantum computing will have a profound impact: on the one hand strengthening cyber attacks, but on the other enhancing encryption. We should already be considering quantum-resistant encryption.”

Inspiring pioneer

Both experts consider the Cyber Security Coalition to be a valuable platform. “For healthcare, the Coalition is an essential resource for strengthening cyber security. It provides a network where we can share experiences and learn from other sectors, allowing us to jointly develop solutions to our shared challenges,” describes Wouter.

Wendy Roodhooft concurs: “We are a smaller hospital, but we bear the same level of responsibilities as larger institutions. Collaborating with larger organisations gives us a voice. The Coalition also supports hospitals that are less advanced in their cyber security strategies.” ■

identity & access MANAGEMENT

Securing 31 million entitlements: how KBC leads the IAM frontier

For financial institutions like KBC, the stakes for Identity and Access Management (IAM) have always been high. Tom Swerts, product owner for IAM at KBC Group and chair of the IAM Focus Group, explains how managing millions of entitlements, navigating international regulations, and embracing innovative technologies demand a proactive and strategic approach.

IAM is a critical pillar of KBC's cyber security framework, given the scale and complexity of its operations. "We manage over 31 million entitlements for both human and machine identities. Internationalisation adds an additional layer of complexity; our operations span multiple countries, each with its own regulatory requirements and IT infrastructure", Tom Swerts explains. "Another major challenge is the lifecycle management of machine identities, which now outnumber human identities. These identities underpin automated processes, and their secure handling is simply non-negotiable."

Can you elaborate on the technological challenges? Do you rely on off-the-shelf solutions or develop systems in-house?

"Historically, we've built most of our IAM systems in-house. But the increasing demands from regulators, auditors and the business itself make it challenging to de-

velop new functionalities entirely in-house. Additionally, the market has matured significantly, offering robust vendor solutions. While we still maintain bespoke elements for specific requirements, we're more open to integrating commercial packages to execute our IAM strategy."

Why is a proactive IAM approach necessary?

"Reacting to regulatory demands or security threats as they arise often leads to tactical fixes, which can be costly and inefficient in the long run. By anticipating trends and potential requirements—for example, through conferences or market insights—we can implement strategic solutions. This foresight enables us to manage risks more effectively and allocate resources more efficiently."

What is the role of the IAM Focus Group within the Cyber Security Coalition?

"The IAM Focus Group provides a collaborative platform for organisations to share best practices and address common challenges. At KBC, we've contributed insights on managing privileged accounts, machine identities and large-scale access reviews. The group helps participants learn from one another, reducing duplication of effort and fostering collective security. Personally, I've found the networking aspect invaluable.

Engaging with peers at conferences and through the Coalition has enhanced our approach to IAM and keeps us aligned with the latest industry trends."

What can other businesses learn from KBC's centralised approach to IAM?

"Centralisation ensures consistency and reliability in access control across a diverse IT environment. While it's resource-intensive, the payoff is significant: streamlined compliance, enhanced security, and better alignment with strategic goals. However, centralisation isn't a one-size-fits-all solution. Organisations should evaluate their specific needs, but the overarching lesson is clear—proactive, strategic planning in IAM is more cost-effective and robust than reactive, tactical fixes."



TOM SWERTS

IDENTITY AND ACCESS MANAGEMENT

No secure online world without a safe digital identity

Stephanie De Bruyne and Roel Peeters of itsme discuss the critical role of Identity & Access Management (IAM) for consumers in today's digital landscape from a business-to-consumer perspective. "Every procedure must also be frictionless."

"IAM is about creating a secure bridge between the physical and digital worlds," starts Stephanie De Bruyne, CEO of itsme. "For consumers, it ensures they can authenticate and identify themselves online while protecting personal data." itsme, launched in 2017, has revolutionised consumer identification in Belgium through a close cooperation between the private sector (especially banks and telcos) and government entities to deliver a seamless and secure solution.

De Bruyne emphasises that a user identity system can only succeed with strong collaboration between all parties. "Banks provide consumer trust and frequent usage, while governments establish the regulatory framework that ensures legitimacy. Without this alignment, scaling a credential solution to meet diverse needs would be nearly impossible."

Zero Trust as a foundation for secure identity management

De Bruyne and Authentication Technology Architect Roel Peeters both emphasise the challenges

of balancing security and user experience for consumer IAM. "Identity theft and other cyber attacks often target consumer-facing platforms," warns Peeters. "Achieving the right equilibrium between security and user experience remains one of the toughest challenges."

The introduction of Zero Trust principles brings workforce-oriented IAM and consumer IAM closer together. "Requiring continuous authentication and logging ensures that no device or user is inherently trusted, and that accountability is guaranteed throughout the entire process. It's a proactive safeguard in today's interconnected world," explains Roel Peeters.

He further emphasises that consumer IAM needs to prioritise user experience to encourage widespread adoption. "Whether logging in, granting permission, or signing contracts, the procedure must be frictionless in order to build trust and engagement."

Europe must lead the digital identity revolution

Europe must take a leading role in digital identity, says De Bruyne. "This is a strategic geopolitical asset. If Europe doesn't unite and create robust, interoperable systems, we risk ceding control to global tech giants." Peeters adds that a unified vision across

countries is vital, "but it must also accommodate regional diversity to strengthen privacy and the broader digital ecosystem."

The IAM Focus Group within the Cyber Security Coalition was created to address fragmented knowledge in digital identity and access management. "By fostering collaboration between public and private stakeholders, between IT and business, we ensure solutions are practical and forward-looking," explains Roel Peeters. "That's why we want to engage more stakeholders and influence policy discussions to empower consumers and enhance digital security. For 2025, we are now developing new themes within the focus group to tackle the new changes and trends in IAM."



ROEL PEETERS



STEPHANIE DE BRUYNE

IDENTITY AND ACCESS MANAGEMENT

IAM enables a secure digital transformation

Identity and Access Management is one of the cornerstones of cyber security, as identity theft and access management vulnerabilities continue to underpin numerous incidents. Kameliya Stoeva highlights the critical role of IAM in organisational cyber security from a business-to-business perspective: “Success depends on user adoption and standardisation.”

“Identity and Access Management (IAM) is essential to cyber security,” Kameliya Stoeva begins. She is Manager Cyber Security at EY and the Lead for Identity and Access Management at EY FSO practice. “Up to 80% of data breaches result from compromised credentials, underscoring the importance of robust identification and access controls.” Yet, many organisations fail to prioritise IAM. In heavily regulated sectors like healthcare and finance, the stakes are even higher, with the sensitive customer data they handle making them frequent audit targets.

Striking the right balance between security and usability

One of the biggest challenges organisations face is aligning security policies with operational efficiency. Stoeva notes, “Businesses often struggle with balancing security management such as frequent access reviews against day-to-day operational de-

mands.” She stresses the importance of collaboration between IT and business units, and suggests phased implementation strategies: “Start with the most critical systems, gather feedback, and expand gradually.”

The Zero Trust principle of “never trust, always verify” is becoming central to IAM strategies, emphasising the need for continuous authentication and monitoring. Kameliya sees this as a proactive approach to modern cyber threats, but warns of implementation complexities, particularly when integrating legacy systems. Decentralised identity models also promise to reshape IAM by giving users more control over their data. However, Kameliya emphasises, “success depends on user adoption and cross-industry standardisation.”

Building a community of expertise

Launched in 2023, the IAM Focus Group brings together experts from diverse industries to share best practices and tackle common obstacles. Kameliya Stoeve underscores its role as a collaborative platform that enables organisations to navigate emerging trends including AI integration and compliance with evolving regulations. “IAM isn’t just a technical domain,” she concludes. “It’s a business enabler, driving secure digital transformation.” ■



KAMELIYA STOEVA

TALENT DEVELOPMENT

We need teams with diverse skill sets, knowledge and experience

THE SKILLS GAP IN THE INTERNATIONAL CYBER SECURITY LANDSCAPE REMAINS A HUGE CHALLENGE AND IS FORCING US TO RETHINK TALENT AND CAREER CULTIVATION. SIGNIFICANT PROGRESS HAS BEEN MADE IN RECENT YEARS TO ADDRESS THE CHALLENGE, WITH THE CYBER SECURITY COALITION PLAYING A PIVOTAL ROLE IN PROMOTING THE DEVELOPMENT OF CYBER SECURITY SKILLS. "IT'S MUCH EASIER IF YOU HAVE SEVERAL SUCCESS STORIES TO TELL."

The skills gap within the cyber security sector is not just a Belgian issue. "In all our neighbouring countries, there is a mismatch between the skills needed in the field and those currently possessed by the workforce. The speed of technological evolution means this gap is continuing to grow," says Saskia Van Uffelen, who leads the National Coalition for Digital Skills & Jobs for Belgium. In this role, she focuses on the upskilling/reskilling of talents to ensure everybody is equipped for the changing employment market (DigiSkills Belgium).

The mismatch can be partly explained by legacy factors. "For a long time, cyber security was seen as a career you entered only after gaining significant experience in IT. As a result, when we started in 2017, there were few young people

working internally in cyber security teams," explains Rosanna Kurrer, Co-founder & Managing Director of CyberWayFinder, a European platform that empowers and trains the next generation of diverse cyber security professionals. "This led to the misconception that attracting young people would solve the shortage of skilled professionals," adds Van Uffelen.

Cultural shift

To close the gap, a cultural shift is needed in talent development, competencies and skills. "Cyber security skills are essential in a digital world. We must continue to emphasise the importance of awareness, but even more importantly we must approach recruitment differently. A paradigm shift is needed that



SASKIA VAN UFFELEN



ROSANNA KURRER

prioritises skills and potential over experience. We must advocate for the development of a new talent culture. This is something we are actively working on, for example, through Agoria's Future Workforce programme."

This shift must be directed at business leaders, not just HR departments, as is still too often the case. "Cyber security skills continue to be perceived as important solely for the IT department, but in fact they concern everyone within the organisation. That is why initiatives that make this overarching effort visible, such as DigiSkills Belgium or the CyberBoost e-learning from Agoria, are so valuable," says Van Uffelen.

The educational world, of course, also plays a key role. "Steps are being taken in the right direction," states Van Uffelen, describing the growing formalisation of cyber curricula throughout Belgium, including specialised academic programmes, online learning platforms, government initiatives such as European Cybersecurity Skills Framework (ECSF) and the increase in cyber security certifications, as well as all the actions taken to attract more women to the sector.

Shifting the workforce

"Role models are also important," Kurrer adds. "My own background is in architecture. But there were no real opportunities in that field for someone like me, who moved to Europe as an adult with academic credentials and work experience. Even people educated locally often had difficulty finding work. So, I decided to pivot my career and build on the programming knowledge I acquired in my graduate studies in Engineering. And I found myself in the world of cyber security. Now, with CyberWayfinder, I help others take the same steps.

It is much easier if you have several different success stories to tell."

Such career transitions are highly valuable as the previous experiences that people bring diversify the available skill set within the cyber security workforce. "This enrichment of skills is exactly what we need, especially in the face of the tsunami of new legislation and technological developments around AI," continues Kurrer. "The increasingly complex challenges must be tackled by teams with diverse skill sets, knowledge, experience and problem-solving methods. We can only do this by building a strong ecosystem around talent development and innovative recruitment practices."

Initiatives like BeCentral demonstrate how career transitions are being made as accessible as possible. "The idea was to build a hub in a central, easily reachable location where everyone could attend classes, be part of a community, expand their professional network and develop the necessary cyber security skills. CyberWayfinder has greatly benefited from this community, which has been a key factor in our success," explains Rosanna Kurrer. "That's why we are working to replicate the model in as many other locations as possible," adds Saskia Van Uffelen.

By continuing this trend, our country aims to establish multiple hubs where talent from all corners can flourish. "We can't think in terms of regional or national borders, which would limit the spread of talent - the exact opposite of what we need. The same principles apply to policies on diversity and inclusion, which should focus on enabling as much talent development as possible, rather than disadvantaging or sidelining certain groups," concludes Van Uffelen. ■

CYBER SECURITY RESEARCH

Through our research, we want to make Flemish companies faster and more cyber secure



COEN DE ROOVER



PARIS VAN PAESSCHEN - © DEPARTMENT WEWIS

To strengthen research into cyber security innovation and encourage companies to take action, the Flemish government launched the Flemish Cybersecurity Policy Plan in 2019. A second five-year cycle of the programme was approved in 2024. It has led, among other things, to the establishment of a research consortium with KU Leuven, imec, Ghent University and VUB as partners. "Without governmental support, this strategic basic research is simply not possible."

Flanders ranks among the global leaders in research into cryptography and securing distributed IT systems. "To further deepen this basic research and maximise its potential for the benefit of industry and society, a grant of almost 9 million euros is awarded annually to a consortium of universities and research centres," explains Paris Van Paesschen. He is a cyber security policy advisor at Flanders' WEWIS Department (Work, Economy, Science, Innovation and Social Economy), which, together with the Vlaio agency, coordinates the implementation of the Flemish Cybersecurity Policy Plan.

The plan includes various instruments to strengthen cyber maturity in Flanders. "In addition to the research pillar, our Vlaio colleagues annually allocate 6 million euros for initiatives that help SMEs in particular become more resilient to cyberattacks.

“Our lab has about 40 researchers, five of whom are involved in the development of tools for static application security testing”

Vlaio also offers subsidies for companies that help organisations to increase their maturity and for companies that develop technology themselves or integrate cyber security into their innovation projects. Finally, the policy plan provides an annual budget of 3 million euros for awareness and training,” says Van Paesschen.

Very fast testing of application source code

The research component focuses on four domains: secure software and applications, security services, system and infrastructure security, and building blocks and secure hardware. Professor Coen De Roover of VUB’s Software Languages Lab is one of the consortium participants: “Our lab has about 40 researchers, five of whom are involved in the development of tools for static application security testing. They look for possible vulnerabilities in an application’s source code. We can thus warn developers and help them make their apps cyber-safe.”

Such tools are not new, but developers often find them too cumbersome and slow. “As a result, these systems are rarely integrated into development environments,” says De Roover. “We are therefore working on a very fast form of testing that can immediately provide signals to the developers after a change to the source code. We also bring automated security testing to new domains such as Infra-

structure-as-Code - Ansible and Kubernetes files, for example.”

From research to practical implementation

Thanks to the support of the Flemish government, the VUB researchers can continue their project over the next four years; they also hope to translate it into practical implementation within companies.

Coen De Roover: “Without governmental support, such strategic basic research is not possible. We want to further refine our prototypes, reduce the number of false positives, and continue improving the user experience. The next phase will include broader validation in industrial applications, for which we are naturally collaborating with companies. The Cyber Security Coalition network is a very interesting forum for me and many VUB colleagues to exchange knowledge and network with interested cyber professionals.”

Increasing EU regulations will intensify cooperation between companies and researchers in the coming years. “For instance, because of the Cyber Resilience Act passed at the end of 2024, companies will have to demonstrate that they control cyber security through processes, tools and techniques. We want to help them do that in an efficient and economical way. In the end, the goal of our research is to make Flemish companies faster and more cyber secure,” concludes Coen De Roover.

CYBER SECURITY RESEARCH

Belgium can be among Europe's top 5 cyber security leaders

Cyber security expert Axel Legay was named 2024 Cyber Security Researcher of the Year for his groundbreaking work and commitment to putting cyber security on the map in Wallonia. He notes that our Belgian cyber security ecosystem leads in many ways, but we must strengthen collaboration with other stakeholders to tackle future challenges.



AXEL LEGAY

Axel Legay started his career in the academic field, specialising in formal verification, testing and cyber security. As a pioneer in statistical model checking (SMC), he greatly influenced industrial verification practices. Today he coordinates CyberWal, bringing together Walloon researchers and economic stakeholders.

When Legay was named Cyber Security Researcher of the Year the jury cited his pioneering research, including advanced AI algorithms for malware detection. Reflecting on the honour, Legay states: "For me, CoronaAlert will always be my most important achievement, because it united people across regions, disciplines and institutions. It taught me that genuine progress arises when we collaborate, listen and trust one another, which requires different kinds of intelligence."

Belgium is increasingly being recognised for its cyber security efforts. How would you describe its current position in cyber security research?

"Belgium is among the leading players in Europe. We have made significant progress, thanks to strong digital foundations and a willingness to adapt. Although we face complex administrative structures across regions, we are aligning priorities and moving towards a more integrated approach. That's why we need to maintain political momentum as well as continue our investments in research and training programmes to produce skilled cyber security professionals."

What are the biggest priorities for Belgian cyber security research right now?

"In my opinion: cross-regional collaboration, strengthening public-private partnerships, and enhancing education at every level. We

need more structured, long-term investments to ensure that universities, businesses and governmental agencies work together efficiently. Bridging technical and legal aspects - ensuring that engineers understand regulations and policymakers grasp technology - is likewise crucial."

Why is cooperation between academia and the private sector so important?

"It ensures practical, impactful results. For example, when we worked with Cisco on malware detection, they provided real-world data and deep industry insight, while the university brought cutting-edge machine learning algorithms. By combining high-level academic research with immediate industrial needs, we created a valuable feedback loop that accelerated innovation on both sides."

Which threats do you foresee in the future? And how can we cope with them?

"The threats are both technical and human. Critical infrastructures (including hospitals, energy grids and transportation networks) are increasingly interconnected and vulnerable. As digital devices proliferate — from smart homes to connected cars — the attack surface grows. Educating citizens, professionals and policymakers is essential. Cyber threats aren't just technical challenges; they also stem from a lack of awareness and digital literacy."

Do you see Belgium becoming a top European cyber security leader?

"Yes, absolutely. We are on track, and I believe Belgium can be in Europe's top five for cyber security. By building an ecosystem that includes strong research, innovative companies, supportive public agencies and well-educated citizens, we can create a robust defence against evolving cyber threats." ■

CYBER SECURITY PERSONALITY OF THE YEAR 2023

We must remain very aware that cybercrime is an industry

Miguel De Bruycker, Managing Director General of the Centre of Cyber security Belgium, was elected Cyber Security Personality of the Year in 2023. Looking back on his 10 years at the helm of the Centre, he delves into the challenges ahead and the Centre's plans to bolster Belgium's cyber security posture.

The jury of the Cyber Security Personality of the Year awarded the 2023 prize to Miguel De Bruycker in recognition of his profound impact on both the Belgian economy and society throughout the years. The author of the first national cyber security strategy in 2012, De Bruycker was subsequently asked to develop the Centre for Cyber security Belgium, together with Phédra Clouner, who now serves as Deputy Director General of the Centre.

"In the beginning, it was just the two of us. The plan was to recruit and build a team of about 10 experts. But very quickly policy makers began to see the need for coordination and awareness in the field of cyber security. Investments were then made possible, and we grew to over 120 employees," De Bruycker explains. "I believe that our actions have contributed to strengthening the resilience of our economy and society. And many other organisations, such as the Cyber Security Coalition, have also done a great job in augmenting

the level of security. So it comes as no surprise that Belgium ranks among the top countries globally in cyber resilience."

Which achievement are you most proud of?

"One key achievement was achieving spiral development - starting with big ideas, and then developing in small, iterative steps - and thus deliver services to the general public, enterprises, governments and critical infrastructure. For instance, I am quite proud of the mail address suspicious@safeonweb.be, which stimulates involvement among the whole population. We receive around 30,000 notifications every day! And we have put in place multiple systems that really make a difference - all of them small steps towards a higher level of cyber security."

What do you consider to be the biggest challenge our country is facing?

"Cybercrime, and especially espionage and state-sponsored criminal activities, have been growing significantly. Although we are developing more resilient systems, building our capacity, and sharing more information internationally, we must remain very aware of the fact that ransomware, phishing, identity and money theft have become an industry that is still

evolving at lightning speed. This remains a big challenge."

International collaboration is key to counter cybercrime. Do you see a positive evolution?

"We are exchanging more and more information with our partnering nations. During meetings at the European level, we exchange ideas with our peers and we inspire each other. This is a key achievement of the past 10 years. Additionally, significant regulation has been implemented. We don't always appreciate this, but companies and public institutions have gradually been pushed towards securing their environment and adopting new technologies. This is a much better incentive than waiting until after an incident to take action." ■



MIGUEL DE BRUYCKER

Belgium has everything needed to grow into a creative hub

Europe's intrinsic sensitivity to data protection and privacy prompts constant reflection on the societal impact of technological progress. This reflex offers significant opportunities for the future, says Catherine Van de Heyning, Cyber Security Personality of 2024. "Belgium has everything it takes to become Europe's creative hub in technological advancements."

"I think my personal role is that I helped putting cyberviolence on the agenda. This is not like a traditional form of cybercrime. I hope that this will result in higher cybersecurity in our society," opens Van de Heyning, who combines her role as a public prosecutor with a position as a professor at the University of Antwerp. "For me, it is very important that human rights are not just an afterthought but really centre when thinking of cyber security and in particular cyber security solutions."

"This is crucial because a human rights approach to cyber security solutions will really balance those on the one hand protecting everyone from cyber criminals, but on the other hand also safeguard our human rights. And, as always, the solution is in the middle, and we need more people, not just lawyers, not just policymakers, but tech people that come into the

middle and try to figure out those solutions that keep us safe, but are also human rights centred," she continues.

Momentum and Future Potential

Van de Heyning views her recognition as a pivotal moment. "The Cyber Security Coalition's strength lies in its broad perspective. It's not just about keeping hackers out but addressing societal challenges. This award can therefore provide momentum to expand my impact and inspire others to invest in cyber-secure solutions for society. So, this award will obviously also even more impact and probably gather more people into my field to really invest in cyber secure solutions for society."

More importantly, she sees the growing attention to the interplay between cybersecurity and societal values as a future opportunity. "Here, we have a path for the future that will also set us as Europe apart from other regions where you have more focus on, most of the time, only cybersecurity without taking human rights along", she explains.

Belgium, she argues, is well-positioned to lead this effort. "We excel in creativity and have trailblazers who've paved the way, like our unique regulations on ethical

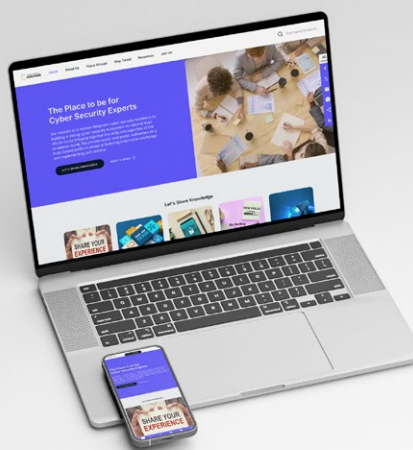
hacking. No other country has such a forward-thinking framework that balances progress and societal values. In contrast to the U.S., where the 'go fast, break things' mantra often ignores the impact of advancements until later, Belgium is proactive and can therefore develop into a creative hub."

To fully capitalize on this potential, Van de Heyning stresses the need to attract more talent and ensure accessibility. "We must lower barriers to entry and encourage talent development. Additionally, the government must prioritize the fight against cybercrime, especially in the SME sector, to harness the societal and economic opportunities this field offers." ■




CATHERINE VAN DE HEYNING

STAY INFORMED



visit our **website**
www.cybersecuritycoalition.be



CYBER PULSE
newsletter

Celebrating 10 Years of the Cyber Security Coalition

Belgian Cyber Security Coalition
13,234 volgers

30 januari 2025

Ten years ago, on 26 January 2015, the Cyber Security Coalition was created. What began as a 'coalition of the willing' - a small group of committed companies - has since evolved into a dynamic community of over 1,000 cyber professionals, policymakers and researchers. Our association has evolved into a respected and integral part of the broader ecosystem working to enhance our nation's cyber

subscribe to our **newsletter**
CyberPulse



Listen to our **podcast CyberTalk**

NEDERLANDS

Gehost door Danny Moerenhout,
podcaster en expert in cyberveiligheid



FRANÇAIS

Animé par Alexandre Pluvinge,
podcaster et expert en cybersécurité



follow us

LinkedIn: [Belgian Cyber Security Coalition](#)
Spotify of ApplePodcast: [cybertalk-nl / cybertalk-fr](#)

OUR MEMBERS

ACADEMIC	Antwerp Management School · EE-Campus (Eurometropolitan e-Campus) · Hénallux · HOGent · HOWEST University of Applied Sciences · ICHEC Brussels Management School · KU Leuven · PXL Hogeschool · Solvay Brussels School of Economics & Management · Syntra PXL · Technofutur TIC · Thomas More · UC Louvain · UGent · ULB – Université Libre de Bruxelles · Université de Namur · VIVES University College · VUB – Vrije Universiteit Brussel
FEDERATIONS	Agoria · Assuralia · Beltug · Comeos · FABA – Federatie van Algemene Bouwaannemers · Febelfin · FedNot · Fevia · HRZKMO CSIPME · LSEC · Santhea · Synergrid · VBO FEB
PRIVATE	Accenture · BNP Paribas Fortis · Cronos Security · ING Belgium · KBC Group · Mastercard · Proximus · SWIFT AG Insurance · A&O Shearman · AXA Belgium · Belfius · Byblos Bank Europe · Cegeka · Colruyt Group · Computacenter · Crelan · Delaware · Devoteam · DKV Belgium · Ethias · Euroclear · Exclusive Networks Belux · EY Advisory Services · Huawei Technologies Belgium NV · Isabel Group · Microsoft · Netskope · Nextensa · NRB · Orange Belgium · Orange Cyberdefense Belgium · Pluxee · PwC Enterprise Advisory · Schneider Electric · Solvay · SopraSteria Benelux · Telenet Group · Thales Group Belgium · Trend Micro Belgium · Wavestone Belgium · Zefes Belgium 2dehands/2ememain · AboutIT · Approach Cyber · Ataya & Partners · Capyx · Cranium Belgium · Cresco · Crimson7 · Cyber Security Management · DigiTribe · DNS Belgium · Doccle · EASI · e-BO Enterprises · E-Solutions · Elimity · EURANOVA · EURid · Expertware Belgium · Fox&Fish Cyberdefense · Innocom · Intigrity · itsme · Jarvis · L&S Registered Auditors · Link2Trust · Maiky · Nexova Cyber · NVISO · Passwerk TRPlus · Peopleware · Psybersafe · Secudea · Secure Code Warrior · Secutech · Sirius Legal · Sirris · The Key 2 IT · Toreon · Trustbuilder · Uniwan
PUBLIC	Agence du Numérique · ASTRID · Banque Carrefour d'Echange de Données (BCED) · Belgian Defence · Belnet · BelV · BIPT-IBPT · CPAS Bruxelles – OCMW Brussel · C.R.E.G. · Centre for Cyber Security Belgium · ENABEL · European Commission · FIA-FAI Federal Audit Fédéral · Flanders Investment & Trade (FIT) · FOD Justitie / SPF Justice · FOD Beleid & Ondersteuning / SPF Strategie & Appui · FOD Buitenlandse Zaken, Buitenlandse Handel en Ontwikkelingssamenwerking / SPF Affaires étrangères, Commerce extérieur et Coopération au Développement · FOD Economie, K.M.O., Middenstand en Energie/ SPF Economie, P.M.E., Classes Moyennes et Energie · FOD Financiën/ SPF Finances · FOD Sociale Zekerheid / SPF Sécurité sociale · FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu / SPF Santé publique, Sécurité de la Chaîne alimentaire, Environnement · Gegevensbeschermingsautoriteit / Autorité de protection des données · IBZ FOD Binnenlandse Zaken / SPF Intérieur · IDELUX – Association intercommunale pour le développement économique durable de la province de Luxembourg · iMio · IRISnet · MIVB-STIB · NMBS-SNCB · Paradigm.brussels · Parlement de Wallonie · Province de Namur · SCK-CEN · VDAB · Vlaamse Overheid
HEALTH CARE	AZ Delta · AZ Groeninge · AZ Maria Middelaars · AZ Oudenaarde · AZ Rivierenland · AZ Sint Jan · AZ Sint-Lucas Brugge · AZ Turnhout · AZ Vesalius · Broeders van Liefde · CHU-UVC Brugmann · Clinique Saint-Jean · CHU Saint Pierre · Clinique Saint Pierre Ottignies · Cliniques Universitaires Saint-Luc · GPN Son · Grand Hôpital de Charleroi · Hôpital Universitaire de Bruxelles · Imelda · Iris Ziekenhuizen Zuid · Jan Yperman Ziekenhuis · Jessa Ziekenhuis · Onze-Lieve-Vrouw Ziekenhuis Aalst-Asse-Ninove · Korian · Ziekenhuis Oost-Limburg (ZOL) · ZNA Ziekenhuisnetwerk Antwerpen · UZ Leuven · VITAZ Hospital
NON-PROFIT	Cetic · ISACA Belgium · Flux50 · Landsbond der Christelijke Mutualiteiten · Miris · Multitel · SAI · Shield
ASSOCIATE MEMBERS	Leila Abajadi · Patrick Bochart · Nathalie Claes · Olivier de Visscher · Filip Herman · Matthias Neuville · Gunther Penne · Clarence Pinto · Doshi Shreeji · Meenakshi Sundaram · Iva Tasheva

SPECIAL THANKS TO OUR PREMIUM MEMBERS


accenture

 **BNP PARIBAS**

 **cronos security**

ING 





proximus

