

CYBER SECURITY
Gazette

2020: the impact of Covid-19 on cyber security professionals



**“Cyber security
requires a
proactive
approach
at any time”**



Dear members,

2020 has been an unusual year with a big impact on both our private and professional life. Like many other organisations the Cyber Security Coalition had to be agile, reshuffle its calendar of events and activities and adapt to the new normal of online meetings. Nevertheless, I consider 2020 to be a positive year for our Coalition.

Due to the Covid-19 pandemic companies, public institutions and the academic world had to face a series of new challenges, on top of the ongoing and accelerating digital transformation. For our members and for the whole Belgian economy the pandemic gave rise to new cyber risks. Most organisations were not or only partially prepared for a massive deployment of remote working on short notice. They needed new devices, new systems, more bandwidth, changes in their IT-architecture, etcetera...

This crisis emphasizes once more the importance of being prepared, having a thought-out security and continuity architecture, and elaborate response processes that are tested upfront. Cyber security requires a proactive approach at any time, in order not to be forced to act quickly and make mistakes under time pressure. This is where the Coalition with its cross-sectoral collaboration continues to prove its added value. By uniting our members to exchange information, knowledge and best practices in a trusted environment, we further strengthen the Belgian cyber security ecosystem.

We had hoped to throw a party in 2020, on the occasion of our first lustrum, but unfortunately we had to postpone it. Nevertheless there are reasons to celebrate: in five years' time the Coalition has grown to become the largest Belgian network of cyber security experts, uniting close to 100 member organisations. On LinkedIn, over 2900 people are following what we do. And in 2020 we organized nearly 50 successful events, activities and training sessions. This demonstrates that we are on the right track.

I would like to take the opportunity to thank our operations team – Cathy, Sofie and Christian – for their commitment and efforts to digitalise our operations. A special thank you to Sofie De Moerloose, who left the operations team to fully focus on her role as cyber security awareness specialist at Proximus. Thank you Sofie, for helping to build our community. We wish you well and hope to see you soon as chair of the Awareness Focus Group.

I am looking forward to 2021, where we will further develop our community, activities and value proposition for our members; will increasingly become the reference partner for our governments and policy makers; and will further develop our collaboration with both public, private and academic partners.

Wishing all of you a very happy and healthy new year,

**JAN DE BLAUWE,
CHAIRMAN OF THE CYBER SECURITY COALITION**

TABLE OF CONTENTS

THE CYBER SECURITY COALITION IN A NUTSHELL	4
2020: A YEAR LIKE NO OTHER KAREL DE KNEEF, JAN PAREDIS, CARINE LUCAS	5
STRATEGIC PILLAR EXPERIENCE SHARING JAN LEONARD, JEROEN VANDELEUR	8
STRATEGIC PILLAR PEER-TO-PEER COLLABORATION PETER SPIEGELEER, JAN VAN LINDEN	10
STRATEGIC PILLAR POLICY RECOMMENDATIONS SÉVERINE WATERBLEY, KURT CALLEWAERT	12
STRATEGIC PILLAR AWARENESS ALEXANDRE PLUVINAGE, KATRIEN EGGERS	14
A GROWING COMMUNITY TACO MULDER, CHRIS ROIJENS, CHRISTOPHE ROME	17
OUR BOARD OF DIRECTORS	19
OUR MEMBERS	20

ABOUT THE COALITION

The Cyber Security Coalition is a non-profit association (ASBL/VZW) that provides a neutral, non-commercial forum where cyber security professionals can freely exchange in confidence. The Coalition is a member-funded initiative. The membership fees cover the operating costs and deliverables, such as awareness campaigns, information kits or the publication of guidelines. All members are represented in the General Assembly.

The Cyber Security Coalition is governed by a Board of Directors, consisting of Jan De Blauwe (Chairman), Miguel De Bruycker and George Ataya (Vice-Chairmen) and Directors Anneleen Dammekens, Fabrice Clément, Bart Preneel, Bart Steukers and Séverine Waterbley.



COLOPHON

The Cyber Security Gazette is a creation of Comm2B, the content company, commissioned by the Cyber Security Coalition.
Editors: Björn Crul and Roeland Van Den Driessche | Editor-in-Chief: Cathy Suykens | Photography: iStock, archives | Design: Anais Hoornaert
All rights reserved | © 2020 Cyber Security Coalition

Cyber Security Coalition
Stuiversstraat 8, 1000 Brussels | info@cybersecuritycoalition.be | www.cybersecuritycoalition.be
Release Date : January 2020

THE CYBER SECURITY COALITION IN A NUTSHELL

OUR MISSION

The mission of the Cyber Security Coalition is to bolster Belgium's cyber security resilience by building a strong cyber security ecosystem at national level. We do so by bringing together the skills and expertise of the academic world, the private sector and public authorities on a trust-based platform aimed at fostering information exchange and implementing joint actions.



OUR NETWORK

The Coalition takes pride in bringing together the largest Belgian network of cyber security experts. They regularly meet in a trusted environment to exchange knowledge and best practices.



94 MEMBERS

ACADEMIC ORGANISATIONS : 11
PUBLIC INSTITUTIONS : 22
PRIVATE SECTOR : 61



FOLLOW US ON SOCIAL MEDIA:

TWITTER: @CYBER_COALITION | LINKEDIN: BELGIAN CYBER SECURITY COALITION



2020: A YEAR LIKE NO OTHER

”We had to face a completely different situation and assess the new risks”

2020 has been quite a challenging year for all. Every organisation needed to adapt to a new situation where remote working, virtual meetings and doing business online grew to be the new normal. As a result, many companies had to make a giant leap into the digital world. Simultaneously cybercriminals altered their tactics, which led to a rise in attacks aiming at homeworkers. We asked two of our members how they look back at 2020 and what were their biggest challenges.



KAREL DEKNEEF

“One of the most obvious changes for us is that staff have been staying away from their secure office environments and working remotely, mostly from home. We already had remote working practices and plans in place and were able to scale those successfully”, Karel De Kneef, CSO at SWIFT, says.

The VUB University was well prepared too. CISO Jan Paredis: “In 2019 we renewed and upgraded our VPN capacity. For me this was an essential element in our business continuity plan, which we started to develop after the 2016 terror attacks in Brussels. Following the cyber-attacks that hit the University of Antwerp and Maastricht at the end of 2019, our ICT department had launched a series of new cyber security measures. When we moved into a lockdown, all was ready to work remotely. But of course the IT-team had to put in an extra effort to adapt the infrastructure to the increased remote teaching.”

Entering into unknown situations

Still, like all other organisations, VUB and SWIFT entered into unknown situations. Karel De Kneef: “Sibos, our annual global financial services event which usually sees thousands of people from all over the world attending, had to be hosted fully digital in 2020 for the first time. This presented an increase in cyber risks from a technology and threat landscape perspective. I am pleased to say that thanks to the tremendous work of many colleagues we met this challenge and the event ran smoothly.”

“One area the pandemic forced us to pay particular attention to was the ▶



2020: A YEAR LIKE NO OTHER

remote on-boarding of new employees. The challenge was continuing to hire people while maintaining robust security in the process. This meant assessing the unique risks associated with remote onboarding – such as shipping a laptop and providing initial credentials – and putting controls in place to mitigate these risks.”

“Our laptops were shipped to the end users, but they had to do the configuration and registration on the VUB network themselves”, Jan Paredis adds. “Some problems could not be solved remotely. So we are well aware that not everything will have been done in accordance with our requirements. When staff will be returning to the campus we will definitely need to address this issue. But the advantage is that we know the risk and it is under control.”

Revising and increasing awareness communication

In order to counter the increased risk of cybercrime, both organisations revised and

increased their communication. “We had to face a completely different situation: our IT security was more than ever depending on individuals and on the (cyber) safety of their home environment. We considered our staff to be more vulnerable as they were operating out of their comfort zone and without the usual informal support of colleagues working side by side”, Jan explains. “That’s why we set up a new awareness campaign focusing on phishing and vishing and how to work safely in a home environment.”

Karel De Kneef: “As the industry moved to remote working and adapted new engagement tools, we had to assess the risk of each of these and figure out how we could continue collaborating without adding any unnecessary risk. It is important that staff at levels, from graduates right up to Board members, are aware of the threat landscape and the risks and actions they can take to protect themselves and the business.”

The challenges of security officers

For Jan Paredis one of the challenges is to maintain the cyber security level in a decentralised environment. “Our university and all of its research groups is an assembly of 100 SMEs that all need to move in the same direction. There is no rigid top-down management, it’s more about convincing peers of what they need to undertake. Informal contacts are key in my approach and I do admit this is something I miss currently.”

“Things are constantly changing. Although we’ve been in cyber security for 40 years, we need to keep focusing on the evolving threats that are out there”, Karel De Kneef describes his challenge. “We have gradually evolved into an approach of prevention-detection-response-recovery. We need to keep investing in business resilience and ask ourselves: in the event of a breach, how can we contain it and recover our systems and data.”

An inspiring community

Looking back on the achievements of the Cyber Security Coalition over the past five years, both Jan and Karel are delighted with the network that has been created: “As security professionals we need to make our colleagues aware of cyber threats and equip them with the right tools to protect themselves. The Cyber Security Coalition has built a truly inspiring community of professionals, which is a major achievement. The quality of the exchanges within the focus groups and of the awareness campaigns that have been developed is excellent. We are looking forward to the Coalition’s activities in 2021.”



JAN PAREDIS

“2020 was a wake-up call”

Digitisation has more than ever become a high priority for Belgian manufacturing companies. “We noticed that Covid-19 was a wake-up call for a lot of companies: either they had to adjust instantly or they used the time freed up due to the lockdown to deep dive into their digital and cyber challenges”, says Carine Lucas, digital innovation expert at Agoria. “We hope this will lead to more companies investing in a full digital transformation.”

Agoria takes the lead in supporting digitisation in the manufacturing industry. In early 2020, it launched the DigiScan, an online questionnaire which companies can use to benchmark the digitisation of their processes and offerings, and their digital culture. Carine Lucas: “More than 600 companies have completed the scan. In the period before Corona, operational efficiency proved particularly to be an incentive to invest in digitisation. Now we notice that companies are looking more at how they can leverage technology to improve staff training as well as their communication with customers and partners.”

An important evolution when it comes to cyber security is the increasing need to focus on Operational Technology. “New machines are equipped with intelligent technology and monitoring tools. But there are still a lot of older machines on the shop floor that function fine, yet were not intended to be connected to other systems,

or that function with operating systems that are no longer supported and thus pose serious security risks. The further we evolve towards Factories of the Future, the more the need will be to include such older machines in smart processes and enhance security. This can protect us from new vulnerabilities. One of our initiatives is setting up a learning network on this topic.”

Cyber awareness must be higher on the agenda

There is no question that Covid-19 has led to more attempts to hack company IT systems in the past year. Agoria has also launched extra campaigns on cyber-safe working. “The need to raise awareness and encourage SMEs to take preventive action remains high. From a recent survey of manufacturing companies in Belgium that we conducted together with Howest, we know that only half of the respondents provided cyber-awareness training to staff and that 35% had not yet developed an action plan in the event of an incident.”

“This is precisely why we think our cooperation with the Cyber Security Coalition is very important”, stresses Carine Lucas.

“We can join forces and exchange expertise so as to reach as many companies as possible. We want to convince SMEs that they should view cyber security as a form of fire protection: if you invest a little in it each year, you will continually reduce the risks. Moreover, together with the Coalition, we want to ensure that the theme remains high on politicians’ agendas, at all levels of government.” ■



STRATEGIC PILLAR

Information sharing is essential to protect our information assets and critical infrastructure. In the past five years, the Cyber Security Coalition has launched a wide range of information sharing initiatives. The growth of the community and of the number of topics has of course increased the experience sharing among the participants. Two of our members explain why they participate in these interactions.

“We want to create a universal roadmap for cloud security”

For many companies, the cloud has become a foundation of their digital strategy. However, a migration to the cloud involves much more than the commissioning of a new digital solution. “We notice that there is still a lack of knowledge to migrate successfully and safely. That is precisely why it is important that we share experiences. Within the Cyber Security Coalition everything can be discussed”, says Jeroen Vandeleur, Service Line Lead at NVISO.

Jeroen Vandeleur is one of the driving forces of the Cloud Security Focus Group. At security company NVISO he assists clients in the field of information security and helps them with complex information security issues. “Now that remote working is the new normal, companies rely on cloud applications. But nowadays setting up a cloud application is very easy and we have noticed the risk of Shadow IT is increasing.”

A lack of control mechanisms often leads to misconfigurations and incidents. “Cloud developers dance on a thin rope. On the one hand, they are tasked to create a manageable and safe environment. On the other hand, they need to keep it accessible and easy to use. But in the cloud your protective walls are gone, so you need to look at new cloud native features to build the same level of security. By choosing the right service model, we are already taking a step in the right direction and we can avoid problems.”

The easiest transfer is one without any adjustments. “With a ‘lift & shift’, for example, the entire architecture and data are just virtualised and moved to the new cloud environment. The advantage is that it can happen quickly. But as little or no changes

are being made, you miss the opportunity to thoroughly analyse, optimise and secure your infrastructure.”

Virtual Experience Sharing Day on security issues of remote working

In the ideal scenario a migration is planned well in advance. “This allows a company to develop the ideal architecture with the cloud provider, and to eliminate problems with legacy systems and intermediate solutions. Whatever model is chosen, it is important to clearly define the responsibilities. We strongly emphasise this aspect within the Cloud Security Focus Group”, Jeroen Vandeleur continues.

“We fill the gaps in knowledge by giving experts a forum and sharing experiences with each other. Most cloud security concepts are so similar that we can perfectly learn from colleagues in other sectors or across borders. This will speed up the knowhow on how to operate safely in the cloud.”

The Cloud Security Experience Sharing Day was a virtual event in 2020. “Sessions on cloud governance, visibility and legislation provided a lot of interesting insights, but participants mainly had questions about

remote working and the security issues it implies. Personally, I mostly remember Timelex’s presentation on what to do when a cloud provider leaks data abroad. Their legal argument was an eye-opener in every way.”

The Focus Group is ambitious for 2021. “By regularly meeting up, ideas are being developed faster. We hope to draw up a cloud security framework by the end of the year. This should become a guideline for both Belgian and foreign organisations that want to operate in the cloud. One of our recommendations will surely be multi-factor authentication, which is still not used enough”, Jeroen Vandeleur concludes.



JEROEN VANDELEUR



EXPERIENCE SHARING

The protection of privacy was a hot topic in 2020. The launch of a contact tracing app and other sanitary measures resulted in lots of discussions about where the boundaries lay between privacy and public interest. The general public is well aware of its right to privacy. And companies must comply with the GDPR legislation. In the Privacy Focus Group of the Cyber Security Coalition DPOs and data protection practitioners meet to exchange information and best practices.

“By joining forces our Focus Group can take up a pioneering role in Europe”

The introduction of the GDPR legislation in May 2018 forced many companies to appoint a Data Protection Officer. He or she assumes a neutral role within the organization and advises management on how to ensure that data is processed in compliance with the data protection rules. Jan Leonard, DPO at Orange Belgium and chair of the Privacy Focus Group: “In a company like Orange, counting 3 million customers and over 1,500 employees who generate data, keeping control over the data flows and data usage is a challenge. We can create a lot of value based on that data but we must at all time respect the privacy of the customers and employees.”

Privacy also applies to the employer-employee relationship. “Unfortunately, due to the corona crisis, we see that some companies are operating in a grey zone when they try to check on staff working remotely. We have noticed attention for privacy is slacking”, Jan states. “The balance between what is allowed and what is prohibited seems lost. As a result, tensions arise between the employee and the employer. If a company wants to roll out a restrictive measure today, I recommend evaluating the pros and cons, limiting the measure in time, communicating transparently about it and treating everyone equally.”

One of the challenges for DPOs is informing all employees correctly and getting everyone in the company on the same page. Jan Leonard: “After all, a lot depends on the company policy and awareness among staff about it. Financial institutions, for example, tend to have a very strict compliance approach. But being 100% compliant is difficult as the current regulation leaves room for interpretation. The Cyber Security Coalition offers the ideal forum to discuss these matters with peers and hear their opinion. It’s very interesting to see how each company deals with the data privacy rules.”

The Coronalert app is a good example

The Privacy Focus Group gathers best practices and invites experts to talk about concrete topics such as shadow IT, contractual clauses or data breaches management. In 2020 most sessions were held virtually. “During one of the sessions, we examined the Coronalert app. It’s actually a very good example of how the right balance between privacy and public interest has been found and how privacy by default was implemented. Personally I also liked the discussion on human rights. It reduced the debate to the essence: we have the right to privacy and must continue

ensuring that this universal freedom is guaranteed.”

In addition to exchanging experiences, the Focus Group provided a video and brochure for the “Data Cleaning” campaign. The chair wants to continue strengthening cooperation among companies and provide them with concrete best practices: “Our success depends on our members. They are our driving force. We can really be proud of what we have achieved in this crisis year. We are one of the few countries in Europe where experiences are being shared across sectors. In this way we can achieve unseen results and even be a pioneer in data protection.”



STRATEGIC PILLAR

OPERATIONAL COLLABORATION

“Peer-to-peer exchange leads to the most valuable insights”

One of the main goals of the Coalition is to develop and facilitate the sharing of information and best practices among cyber security experts from the private sector, public authorities and academic institutions. The Focus Groups provide a neutral forum where peers can exchange in confidence, develop their skills and improve their level of cyber security maturity. We asked the chairs of the CSIRT-SOC and Enterprise Security Architecture Focus Groups how peer-to-peer collaboration contributes to their daily operations.



JAN VAN LINDEN



YOUNES FOURIR

CSIRT-SOC Focus Group

The CSIRT-SOC Focus Group gathers experts from Cyber Security Incident Response Teams (CSIRT) or Security Operations Centres (SOC). Members share their findings concerning recent incidents, their incident response processes, technical indicators, their experience with vendors and tools, etcetera.

Chair Jan Van Linden is responsible for the CSIRT at BNP Paribas Fortis: “The bank has a large global security department, which monitors all international threats and attacks. Specifically for Belgium, we map local issues ourselves. The CSIRT-SOC Focus Group is an ideal forum to share information about possible threats and experiences with, for example, detection systems. Because we have representatives from a wide variety of industries, we get a good idea of what’s going on.”

“Being a telecom operator, we are an important target and we see many attacks on our network,” adds co-chair Younes Fourir, security analyst in Proximus’ CSIRT team. “By sharing information about attacks we observe, we can help limit or mitigate the impact on other organisations. Furthermore, if a member shares information about an attack or a vulnerability, other members don’t need to perform the same research. So we can all save time and benefit from each other by sharing.”

Openness is the key to success in this community. Younes: “As chairs we have to ensure that everyone within the group participates actively. One way I try to inspire others to share is by sharing as much relevant information with the group as possible myself.”



“We are open-minded, but there is also a clear code about what is said within the Focus Group. It is and will remain an environment where trust is very important,” Jan adds.

Covid-related topics on the agenda

In the past year, the group’s agenda featured threat hunting, ransomware, VPN security, DDOS attacks and Emotet malware. Younes Fourir: “We always discuss very diverse topics. We give members the opportunity to talk about what is relevant to them at that time. Last summer, for example, the Centre for Cyber Security Belgium gave a presentation about the impact of Covid-19, and Orange Cyber Defense shared the results of their investigation on the cyber risks of VPN.”

As a result of the pandemic, the CSIRT-SOC Focus Group had to shift to digital meetings. Jan Van Linden: “We have switched from all day physical meetings, once a quarter, to video conferences of two hours every two months. This has a number of advantages in terms of mobility and to maintain the bond. But we hope to meet in person again really soon, because we notice that physical gatherings are a better forum for discussion and exchange.”

“The challenge also lies in the fact that our group has grown strongly since the start of 2020. We must ensure that everyone is equally engaged and that we continue speaking in the same atmosphere. Ultimately, the interaction in the group provides the most valuable insights”, Younes states. “To me, a positive development was the opening to consultancy companies such as Nviso. There is no denying consultancy companies have a lot of expertise, it is great to welcome them in our group.”

2021 will be a year in which the group interaction will continue evolving. Jan: “I hope that we can combine physical and virtual meetings. We want to maintain a high quality of discussion. At the same time, our goal is to share more things online via an Office365 environment. And we also hope to broaden our exchange of technical indicators with for example MISP. As you can see, there’s plenty of work on the shelf!”

ESA Focus Group

The mission of the Enterprise Security Architecture (ESA) Focus Group is to promote architecture management as a key enabler for consistent security strategy definition and execution, a sound security governance and overall Business-to-Security alignment.

The growing dependency of enterprises on ICT has led to an unprecedented complexity and loss exposure. Many companies struggle with the spread between adhering to formal procedures and standards, and the need to deliver swiftly along their digital transformation journey. Peter Spiegeleer, enterprise security architect at Proximus and chair of the ESA Focus Group: “The greatest challenge of the architect is to combine thought leadership, guiding the realisation of the enterprise’s target architecture and enabling emerging business capabilities with agility and control.”

The ESA Focus Group gathers four times a year and is co-chaired by Benoît Moreau (ING Belgium) and Pascal Mathieu (BNP Paribas Fortis). “We embrace a risk-driven, systems engineering approach to security management, with a pragmatic and agile touch. Our focus is on design decisions that shape the enterprise’s security posture, effectively embedding security into solutions by design”, Peter explains. “Our ambition is to raise the members’ maturity in architecting for security. In a typical session we elaborate on strategies and architectures in recent or ongoing member projects, sharing experience and work products.”

The group is open to treating any risk domain, its unique selling point being the architectural approach: working their way down in stepwise refinement, from objectives, requirements and constraints to infrastructure models that make security effective, manageable and measurable. “We are in continuous search of the sweet spot between the traditional school promoting holistic frameworks, and leveraging simple yet effective defence tactics, while still relying on abstraction.”

The deep-dive presentations were richer than ever

The ESA Focus Group has grown from 15 to 40 active participants over the past year. This was not the only challenge ; due to the Covid-19 pandemic the format had to be changed as well. “Instead of having our traditional lunches and networking opportunities, we switched to webinars. On the one hand, it made group interaction more difficult because we had a larger group of people who did not know each other yet. But at the same time the deep-dive presentations were richer than ever.”

Topics that have been tackled so far, among other, are container security, API security, microservices security, the secure development life cycle, identity federation and delegation, adaptive authentication, data lake security, zero-trust architectures, endpoint detection and response, and threat hunting.

The chair is ambitious for the new working year. “I hope to organise a real-life marketplace, mimicking ‘buyers’ and ‘sellers’ of architectural assets. Such an event gathers a large offering in one place and whoever wants to, can go home with a package of useful material. But the success of this fair depends on the possibility to meet in person. In addition, we will initiate several co-creation processes in 2021. As a first concrete deliverable, we will publish a whitepaper to clarify the role and value of the security architecture practice in today’s enterprise”, Peter Spiegeleer concludes.



PETER SPIEGELEER

STRATEGIC PILLAR

POLICY RECOMMENDATIONS

Issuing recommendations for more efficient policies and guidelines is an important objective for the Cyber Security Coalition. The Focus Groups within the strategic pillar “Policy recommendations” provide a source for upcoming regulations and implementation methods, and thus help the members to achieve regulatory compliance. We asked the federal public service SPF Economie and Howest to give their opinion about the added value of these Focus Groups.

“The Coalition serves as a think tank”

“As a public service we want to have our finger on the pulse of the economic world. It is one of the reasons why we have joined the Coalition from the start”, Séverine Waterbley, director general at the SPF Economie explains. “Having close contacts is even more important today, in the midst of the crisis, where our service is involved in a broad range of projects to relaunch the economy. Due to Covid-19 we see that the digital transformation is accelerating. It’s a positive transition and the European Union has asked its member states to facilitate that transition.”

When it comes to policy-making, the director general sees a lot of advantages in the collaboration with the Coalition and its Focus Groups: “I see the groups that are working on policy recommendations as a public-private cooperation. To develop good policies we like to hear the views of both the private sector and the academic world. These interactions often serve as a think tank or a laboratory of ideas: we hear which topics are important for companies, we can identify their needs or determine opportunities together. Sometimes it also helps us to act upon specific issues.”

A concrete example is the transposition of the European NIS directive, which provides measures to achieve a high common standard of cyber defense in the EU. “We were one of the departments involved in

the process of transposition. Within the Focus Group Network & Information Security we carefully listened to the concerns of the different sectors involved. We used this information during meetings with the other departments and to keep our minister up to date.”

Raising awareness among SMEs

One of the important actions for the SPF Economie is boosting the cyber awareness among small and medium enterprises, which are still very vulnerable for cybercrime. Séverine Waterbley: “Together with the Cyber Security Coalition and the Centre for Cyber Security Belgium we have launched several campaigns to inform

and raise awareness about the risks. We developed a cyberscan that SMEs can use to check their readiness to counter incidents. All these things are published on our website too.”

The future is bright for the Coalition. “I would urge SMEs to join in this initiative and benefit from the knowhow of bigger organisations. It offers a broad network full of information and knowledge that you don’t need to search for yourself. I have seen how my colleagues have learnt so much from peers and experts within different groups”, Séverine Waterbley states. “Let’s hope that we can meet in person again in 2021 and fully reap the benefits of encounters during the coffee breaks!”



“A platform to clarify rules and interpretations”

Kurt Callewaert, lecturer and research manager at Howest University of Applied Sciences, is chair of the NIS Focus Group: “The NIS Directive obliges operators of essential services from the energy, transport, water, health and finance sector plus digital infrastructure and digital service providers to comply with the new regulation. As this is still a relatively new domain, it is important to bring representatives from these companies together to share their insights and experiences. But our platform also offers the opportunity to discuss with the Centre for Cyber Security Belgium and policymakers, in order to clarify some of the rules and interpretations.”

In Belgium there is still work to be done to put some aspects of the Directive into practice. “We have to move to the next level of implementation. How do we set up internal audits? What about the external auditor? What will be the methodology and process of an external audit? These are some of the questions that we need to answer”, Kurt Callewaert explains. “In order

to find answers we are looking abroad : we want to learn from the best practices that are internationally available.” The Focus Group will also communicate about new EU developments, such as the proposal for a revised Directive on Security of Network and Information Systems (NIS 2 Directive).

The Focus Group also wants to broaden its perspective to a wider range of companies. “We think it is crucial that all partners and suppliers of the organisations that have to comply with NIS are aware of the regulation, and – preferably – prepare themselves to comply as well. In future this could prove to be a big advantage in their collaboration with bigger companies. That’s why we will target this segment of enterprises too.”

Continuously learning about new developments

Howest has been involved in the Cyber Security Coalition since the early days and has found a lot of added value in the community. “It is vital that our courses and programmes

evolve with the needs of the industry. As a member of the Coalition I am continuously learning about the new developments in different sectors and we take this into account when adjusting and updating our Cyber Security Professional course”, says Kurt.

“Moreover, our students need internship positions or companies to work with for their bachelor’s thesis. Until a few years ago it was very hard to find organisations willing to offer an internship or work with our students. But the Coalition has provided a trusting environment, where I hear from fellow members when they need interns and then we can find matches and help one another.”

For his research activities too Kurt Callewaert sees the benefit of the Coalition’s cross-sectoral platform. “We are developing several initiatives to which the Cyber Security Coalition is contributing.

For instance, we are teaming up in a Living Lab on innovative cyber security technologies for Industry 4.0. We are looking into industrial security based on Artificial Intelligence. The project focuses on the development of new technologies, their implementation in the workshop and the policy recommendations that are required to make all of this possible. It’s a great example of collaboration.”

“Another project, supported by the European Social Fund and Vlaio, aims at raising cyber security maturity among non-IT professions, such as operators, accountants, etcetera... We want to develop specific training for these people. I have high hopes for this particular project, where the trainings will be developed in collaboration with and disseminated by the Coalition too”, Kurt Callewaert concludes.



STRATEGIC PILLAR

The fourth strategic pillar of the Coalition is awareness creation. The Awareness Focus Group plays an instrumental role in the implementation of this strategy. The objective is to increase cybersecurity awareness among both public and private organisations and citizens, by means of various initiatives such as running campaigns, publishing best practices, sharing tips & tricks and organising information sessions.

2020 was an extraordinary year for the Awareness Focus Group, too. Switching to working from home had a major impact on the business world and for SMEs, in particular, which had hardly any experience with this way of working. “Creating awareness and drawing attention to the inherent risks within a home environment were high on the agenda,” according to Alexandre Pluinage (ING) and Katrien Eggers (Centre for Cyber Security Belgium). “Fortunately, our group has a lot of experience and we have been able to rely on each other for five years. There is no competition in this matter and everyone likes to help each other.”



Working from home thus played a decisive role in what this focus group achieved during the past year. Alexandre Pluinage: “The fact that people are working remotely is nothing new on its own, but it is the scale at which it suddenly happened. Even at ING, where we already had a lot of experience with working from home, we still had to adapt our IT network and some applications to enable people to work comfortably and safely.”

“A second problem is the big difference between working remotely for one day a week and working from home every day. There are psychological and practical concerns. We have seen that people feel safer at home, so that, for example, they do not lock their screen when they leave their computer unattended. Or one computer is used by several members of the family, such as children doing their homework or downloading items on the same computer that is used for work purposes. These are very specific security risks within the home environment.”

Toolkit now includes a chapter on working from home

“There were also new challenges in terms of data privacy and protection”, notes Alexandre Pluinage. “I’ll give an example from our bank: if I print a document at work that contains sensitive data, I can

AWARENESS

“When it comes to boosting cyber security awareness, there is no competition”

throw it away afterwards in special rubbish bins, so that it is safely disposed of. This is not the case in a home environment, which means you have extra risks in terms of document security and privacy-sensitive information.”

The Awareness Focus Group has responded quickly to the new circumstances by adding a new chapter to its Cyber Security KIT, ‘How to work safely from home?’. Alexandre Pluinage: “We developed this toolkit in 2018 together with the Centre for Cyber Security Belgium (CCB). It helps organisations and companies to raise awareness about cyber security among their employees. The toolkit contains a roadmap, a planning tool and all the necessary materials to set up your own awareness campaigns as an organisation, including with regard to working from home.”

Successful national campaign on two-factor authentication

The annual Safeonweb campaign, which is also organised by the Cyber Security Coalition in close collaboration with the CCB, focused on the protection of digital accounts using two-factor authentication. “The theme was already well established before Covid-19 broke out and we kept it because it continued to be relevant irrespective of the situation”, says Katrien Eggers. “We believe that two-factor ►

Safe homeworking

- Download verified apps
- Set-up anti-virus software
- Protect your router
- Protect your home network
- Ensure wifi is secure
- Keep private and work tools separate

ONCE UPON A TIME, THERE WAS A PEACEFUL KINGDOM THAT BROUGHT HAPPINESS TO ALL TELEWORKERS.

www.cybersecuritycoalition.be

CYBER SECURITY COALITION





Working from home safely too



Passwords are a thing of the past.

Protect your online accounts with two-factor authentication. Check out safeonweb.be

MAKE YOUR ONLINE ACCOUNTS DOUBLY SECURE WITH TWO-FACTOR AUTHENTICATION (2FA). IT'S EASY AND SAFER. MORE INFO AT [SAFONWEB.BE](https://www.safeonweb.be)

authentication is the best way to secure safe access to various online systems. Some people still have doubts, but within five years, we will probably not be using traditional passwords anymore.”

Thanks to the ‘Passwords Are Out-of-Date’ campaign, Internet users were advised to switch to two-factor authentication and to spread this message to others. “The campaign was hugely successful. We reached 2 million Belgians using social media. Via the Cyber Security Coalition, the campaign also resonated within many organisations. Based on a retrospective survey, we learned that almost 6 in 10 people saw the campaign - the largest number ever. And half of them also took action.”

“People surfed to our website, looked up specific information on two-factor authentication, talked about it with their friends, colleagues and family, and advised them to switch”, explains Katrien Eggers. “10%

decided to change their passwords and 4% effectively installed two-factor authentication for one or more accounts. That means that at least 200,000 people have started using this form of online security. An exceptionally good result!”

A busy year in all areas

For the rest, it was a busy year for the focus group. Alexandre Pluvinaige: “We have about 40 active members who work in subgroups on various initiatives. Every month, we draw up a report on the state of affairs and, on a bimonthly basis, we also focus on a specific topic. We discuss the latest problems and experiences in the group and look for solutions together.”

In addition to the Cyber Security KIT, the SME Cyber Security Scan and the Cyber Security Basics for Starters guide were updated, as well. “And in September,

we launched an interactive e-learning course via the online platform Kahoot. In this way, we are responding to the needs of organisations to ensure their employees become more aware of cybersecurity topics related to working from home. The course is a gamification tool that also provides feedback on the results that participants achieve”, adds Katrien Eggers.

“And last but not least, we should also mention our certification project. It was developed to be given in a traditional classroom, but we gradually adapted it to an online format this year. It is actually quite a unique concept, as we certify both the cybersecurity awareness manager and the action plan he or she develops during the programme. As a result, people can start implementing their plan within their organisations immediately upon certification. We will of course continue this in 2021”, concludes Alexandre Pluvinaige. ■



A GROWING COMMUNITY

Nearly 100 companies, public services and educational institutions take part in the community of the Cyber Security Coalition. In 2020 over 20 new members and associate members joined. As a result of the digital transformation of our society, more and more organisations see the benefits of joining forces to increase their level of cyber security.

“The exchange within the Coalition brings value to every member”

Hospitals invest heavily in innovation, for the benefit of the patient. One of the examples is the patient’s personal health record, used to digitally record and implement care pathways. A wide range of e-health applications are also breaking through. These developments have radically changed the field in which information security officers of hospitals are operating.

The CHU-UVS Brugmann and HUDERF hospital network in Brussels has been strongly committed to digitisation for years. Taco Mulder, CISO of the group: “We invest in technology to improve the comfort of our patients. Cyber safety is of course an important part of these solutions. That’s why we strictly monitor our information perimeter and try to protect it as good as can be.”

The hospital is one large network in which doctors, nurses and administrative staff operate. “It is not easy to keep an overview. Especially in these times, when just about everyone has their own tablet. All these devices pose a potential threat. This is why it is important to make everyone aware of the possible dangers.”

The hospital organises training courses for staff on how to secure their home environment too. “In September, a major ransomware attack on a German hospital may have resulted in the death of a patient. That’s every hospital’s nightmare. We must be able to carry out our operations at any time. Fortunately, no data leaks have occurred yet and our management understands the importance of information security.”

The hospital group joined the Cyber Security Coalition in 2020.



“We are now taking part in the Governance, Risk & Compliance and NIS focus groups and have already learned a lot. For instance, we are now looking at our organisational structure in a different way and check whether our strategic vision is in line with our operational activities and the applicable legislation.”

“Within the Coalition we also meet peers of other hospitals with whom we can exchange ideas. But it is as interesting for us to see what challenges e.g. a financial institution faces. We can learn a lot from these different perspectives”, Taco Mulder concludes.



Today's students are tomorrow's computer scientists. Schools need the right tools to train them properly and especially in the field of cyber security, they need to tap into specialised knowledge. With its Professional Bachelor in IT course, PXL University of Applied Sciences and Arts wants to prepare youngsters for a digital future.

The Professional Bachelor in IT course at PXL pays a lot of attention to cyber security. "For three years now our students have been taught the 'security essentials' programme. We introduce them to phenomena such as cryptography, malware and different types of attacks. In the second bachelor we also let them penetrate systems, for example through red & blue teaming, or they are given assignments to develop a better protection. We see this as the perfect foundation to enter the professional world", lecturer Chris Roijens says.

Chris is conducting his own research into the status of cyber security in secondary schools. A steering committee with experts from the academic and business world is guiding his research. "It is interesting to bring the experience of students and teachers together in one study. Later on we want to use this knowledge in our own training."

As part of this research and its IT course, the PXL University of Applied Sciences chose to join the Cyber Security Coalition. "We attach great importance to community-driven teaching, in which we work in close cooperation with businesses. We get better insights and a company immediately sees what our students have to offer. We find the same kind of knowledge exchange within the Coalition. It brings value to every member."

Creating awareness among schools is a challenge. "They should not be asking themselves if, but when they will be the victim of a cyberattack. Studies are showing that the number of cyber incidents in the private sector has increased by 9% during the corona crisis; among educational institutions this was even 24%. Cyber safety in schools is a burning issue and we must act now. We need uniform guidelines and tools to better arm the ICT coordinators in their fight against hackers."

HOGESCHOOL PXL



More and more companies shift their freight transport from road to rail. Lineas, the largest private rail freight operator in Europe, optimises its use of the rail infrastructure through digitisation of internal processes and thus actively contributes to a more sustainable logistics network. In 2020 Lineas engaged a CISO to monitor the progress of all digital processes, and decided to join the Cyber Security Coalition.

In 10 years, Lineas has transformed from a Belgian public company into a fast-growing European private company. Digitisation supports its growth, but security is a key concern. Christophe Rome, Chief Information Security Officer: "Our security policy consisted of virus scans, a spam filter and firewalls. Today, this is no longer enough to counter a ransomware attack that – in a worst case scenario – could bring our operations to a halt. So now our focus is mainly on detect & respond capabilities, to ensure that we become cyber resilient."

As a part of its new safety policy Lineas wants to engage its employees and increase awareness. "Almost half of IT security incidents happen unintentionally at the hands of staff. They are therefore crucial in the security of the company. We need to make them more aware of the risks. Getting this message across to everyone is quite a challenge."

Soon after his appointment, the CISO decided to join the Cyber Security Coalition. "Any company can be a target. In order to better protect ourselves, we must exchange experiences with others. That is the real added value of the Coalition. It helps to test whether a certain strategy is useful", Christophe continues.

Lineas also wants to take up an active role within the Coalition. "A new generation of employees, that works in a completely different way, is arriving. Data that was centralised until recently, can now be found scattered in cloud applications. How will we deal with this in the future? I want to work with the Coalition to find answers to these questions. Especially for companies that want to take their cyber safety to the next level, the collaboration with peers will immediately prove its added value."

LINEAS
YOUR FREIGHT FORCE



OUR BOARD OF DIRECTORS

CHAIRMAN



Jan De Blauwe

VICE-CHAIRMEN



George Ataya



Miguel De Bruycker

DIRECTORS



Anneleen Dammekens



Fabrice Clément



Bart Preneel



Bart Steukers



Séverine Waterbley

OUR OPERATIONS OFFICE



Cathy Suykens
cathy.suykens@cybersecuritycoalition.be



Christian Mathijs
christian.mathijs@cybersecuritycoalition.be



our members

A.S.T.R.I.D. • AG INSURANCE • AGENCE DU NUMÉRIQUE • AGORIA
ALLEN & OVERY (BELGIUM) LLP • ALLIANZ BENELUX • APPROACH BELGIUM • ARGENTA
ASSURALIA • AXA BELGIUM • BEKAERT • BELFIUS • BELGIAN DEFENSE • BELNET • BELTUG
BELV • BIPT-IBPT • BNP PARIBAS FORTIS • CHU / UVC BRUGMANN • C.R.E.G.
CENTRE FOR CYBER SECURITY BELGIUM • CERT.EU • CIRB-CIBG • COLRUYT GROUP
COMEOS • CONFEDERATIE BOUW • DIGITRIBE • DILACO • DNS BELGIUM • EASI
EE-CAMPUS (EUROMETROPOLITAN E-CAMPUS) • ERIC DE SMEDT • ETHIAS • EURID
EUROCLEAR • EUROPEAN COMMISSION • FEBELFIN • FEVIA • FOD JUSTITIE/ SPF JUSTICE
FOD / SPF BOSA • FOD / SPF ECONOMIE • FOD / SPF FOREIGN AFFAIRS • GBA - APD
GRAND HÔPITAL DE CHARLEROI • HÔPITAUX IRIS SUD - IRIS ZIEKENHUIZEN ZUID
HOWEST UNIVERSITY OF APPLIED SCIENCES • HRZKMO - HOGE RAAD VOOR ZELFSTANDIGEN EN KMOS
HUAWEI TECHNOLOGIES BELGIUM • IBZ / SPF INTÉRIEUR • ICHEC BRUSSELS MANAGEMENT SCHOOL
ING BELGIUM • INNOCOM • INTIGRITI • ISABEL GROUP • JAN YPERMAN ZIEKENHUIS
JUNIPER NETWORKS BELGIUM • KBC GROUP • KPMG ADVISORY • KU LEUVEN • LINEAS
LSEC LEADERS IN SECURITY • MARC DECAFFMEYER • NATIONAL BANK OF BELGIUM • NEXTAUTH
NMBS-SNCB • NVISIO • ONZE-LIEVE-VROUWZIEKENHUIS AALST-ASSE-NINOVE • ORANGE BELGIUM
ORANGE CYBER DEFENSE • PARLEMENT WALLONIE • PROXIMUS • PXL HOGESCHOOL • RHEA GROUP
SECUTEC • SENIOR LIVING GROUP • SIRRIS • SOLVAY BRUSSELS SCHOOL OF ECONOMICS & MANAGEMENT
SOPRA STERIA BENELUX • STIB-MIVB • SWIFT • SYNERGICS • SYNERGRID • TELENET GROUP
THALES GROUP BELGIUM • UCL • UGENT • ULB • UNISYS BELGIUM • UNIVERSITÉ DE NAMUR
UWE - UNION WALLONNE DES ENTREPRISES • VBO / FEB • VLAAMSE OVERHEID
VUB - VRIJE UNIVERSITEIT BRUSSEL • ZETES BELGIUM

Special thanks to our Premium Members

