CYBERSECURITY MONITOR 2023

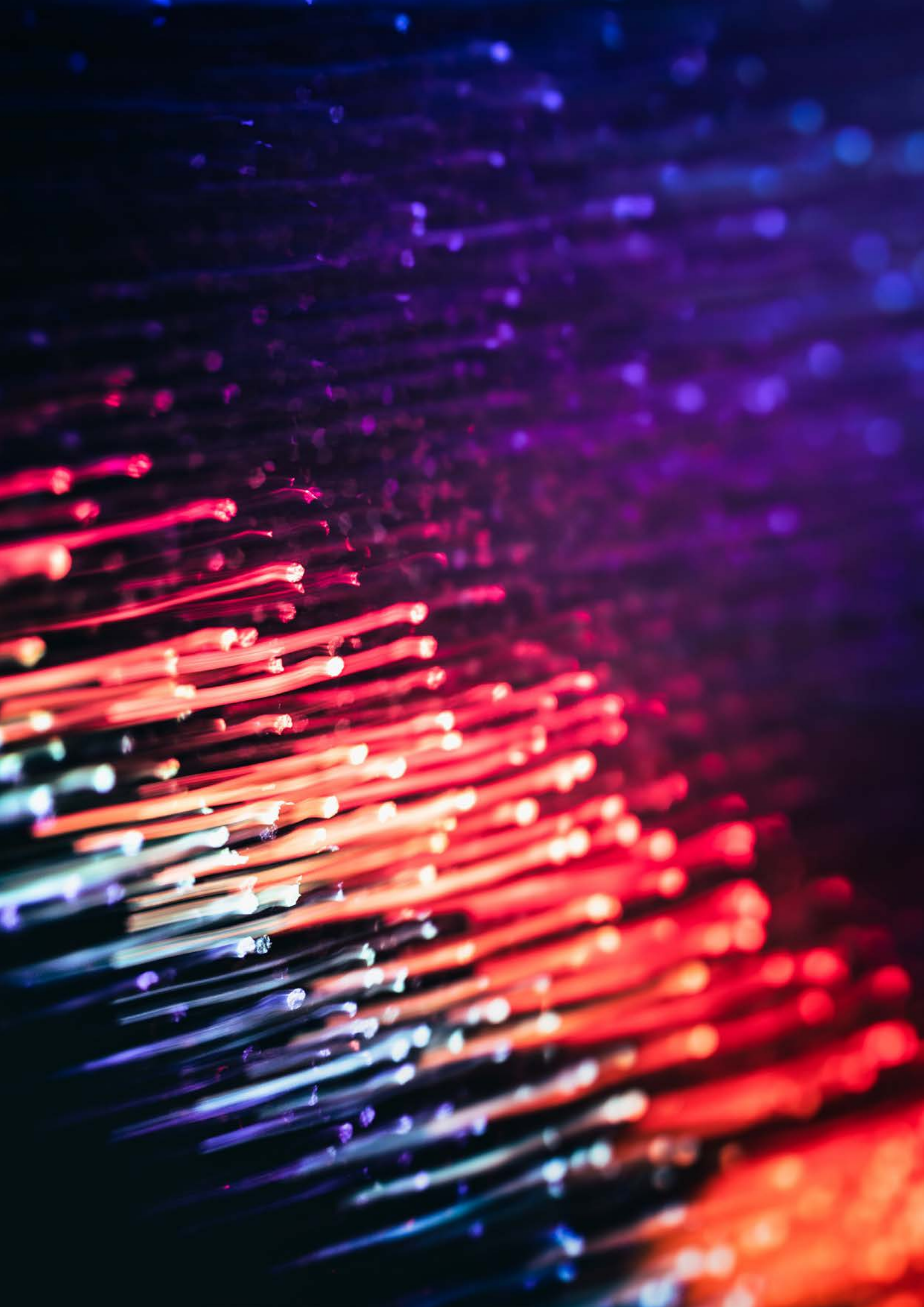
The Status of Cybersecurity Management in Belgium

Research Report

October 2023

CIONET What's next.

INNOCOM.



Contents

Introduction

Why did we perform this study?

As the complexity of technology is on the rise, so are the tactics, techniques, and procedures used by adversaries. While novel technologies such as cloud, AI, and IoT enable increased productivity and efficiency, they also lead to a larger attack surface. Maintaining a resilient organisation in this context requires a mature cybersecurity posture and awareness throughout. This places cybersecurity on top of mind for many business leaders.

In last year's study *"CIONET Agile Monitor: What's the deal with your agile transformation?"*[1], we looked at the adoption of the Agile methodology. That study presented a few key findings, such as the strong relation between Agile success, organisational alignment on initiatives and priorities, and the early involvement of HR to shape the company culture. DevOps also has shown to be an accelerator for successful Agile transformations.

In this study, we shift our focus to organisational cybersecurity and how it integrates with Agile. DevSecOps, the practice of blending cybersecurity into the software development lifecycle and operations, in particular is a hot topic. We ask which factors are key in shaping and maintaining a resilient but Agile organisation in the face of an increasingly complex cybersecurity landscape.

By doing so, we aim to determine the current state of cybersecurity throughout the Belgian industry.

How did we do it?

To check the pulse of cybersecurity within the Belgian industry, we applied a two-pronged approach. Firstly, we reached out through CIONET to the leaders of 250 companies via a voluntary survey. 35 of these provided us with responses, forming the quantitative part of our study. Secondly, we invited a subset of these members of CIONET for an in-depth interview on cybersecurity. This resulted in 9 interviews, forming the qualitative part of the study, providing us with a deeper insight into which topics occupy the minds of executive leaders in cybersecurity.

Both the qualitative and quantitative parts of the study covered the following topics:

1. Overall State of Cybersecurity in Belgium
2. Cybersecurity Awareness on Board Level
3. Transparency and Collaboration among Senior Leaders
4. DevSecOps: Where do things stand?

With these topics, we aim to gain insight into both the strategy and maturity of cybersecurity management within the Belgian industry, as well as the interactions between organisations in this domain. To what level is the board involved with the cybersecurity of their organisations? Finally, we want to establish what the progress is on DevSecOps initiatives.

The response rate to our study amounts to 14%. We believe our sample to be representative for the Belgian industry as our correspondents are distributed across multiple sectors, including retail, finance, manufacturing, and government. This provides us with a cut-through of the Belgian industry.

What's in it for you?

Unlike other cybersecurity reports, this study considers the Belgian industry its prime focus. This way, we can provide insights into our local industry, identify common pain points, and provide guidance on how to navigate them.

The information contained in this report is relevant for business leaders regardless the sector their organisation is active in, due to both the diversity in the study population and the universality of cybersecurity.

[1] This monitor, as well as last year's AI monitor, is available for download on our website through the link cionet.com/reports.

Executive summary

Overall, cybersecurity budgets are rising at 79% of correspondents, with a sharp increase of more than 10% for a third of the correspondents. However, cybersecurity budgets are becoming less distinguishable from other IT spend. The size and the way these budgets are spent depend on the board's engagement for cybersecurity initiatives. To grab their attention, organisations should avoid reporting on operational metrics, such as the number of incidents, and instead focus on highlighting the value at stake, the quantified risks that were mitigated and the successes gained with cyber initiatives (e.g. what impact did our protections have).

Due to the war on talent in the cybersecurity industry, cybersecurity departments and teams are understaffed and not adequately skilled to deal with the sophisticated attacks they need to defend against. As a result, organisations are shifting towards leveraging automation to increase the value per capita, holding teams accountable for the security of their products with support of security champions, and managed security service providers to staff and run cybersecurity operations. At the same time, organisations adopt a risk-based approach to select which cybersecurity concerns to deal with based on their overall risk impact.

The perception of cybersecurity is positive in almost two-thirds of organisations. However, in over a third of organisations, the security department is perceived negatively due to insufficient insight into the necessity and benefit of security measures. Staff tend to only perceive the downsides of security, such as dealing with multifactor authentication. In organisations where the cybersecurity department successfully responded to incidents, the appreciation for the department is much higher.

We observed that the top initiatives being tackled include identity and access management (IAM), operational technology (OT) security, cybersecurity awareness training, and business continuity in the context of cybersecurity (i.e. cyber resilience).

Many of the participants to our survey see value in the collaboration with their peers, especially across sectors. Being able to discuss cybersecurity with peers provides new insights for cybersecurity leaders.

Setting up a successful, secure software development life cycle forms a challenge for many of our correspondents. In general, insufficient documentation around the organisation's security architecture is holding back progress. Though the roles and responsibilities involved have become clearer, the adoption of the required automation forms the next frontier.

Eight key takeaways are identified:

1. Cybersecurity maturity stems from solid cybersecurity foundations.
2. Strong partnerships can mitigate cybersecurity talent acquisition challenges.
3. Resilience strategies need to be sufficiently tested.
4. Third-party risk and supply chain management remain a challenge.
5. Board engagement is essential for effective cybersecurity governance.
6. Collaborating openly and fully with peers ensures maximum engagement and value.
7. Implementing DevSecOps in an incremental process ensures sustainable progress.
8. Approaching cybersecurity in a holistic way helps to keep perspective.

Responses and Trends

Theme 1: Overall State of Cybersecurity in Belgium

Rising cybersecurity budgets

A clear and expected trend in cybersecurity budgets is their prospected growth for the years to come. Overall, 79% of correspondents expect an increase in their organisation's cybersecurity budget. 31% even expects a significant increment beyond 10% growth compared to last year's budget. (Figure 1)

The budget dedicated to cybersecurity varies significantly across the correspondents, ranging from very small budgets up to a fifth of the IT spend. These budgets include cybersecurity initiatives, staffing, tooling, and hardware. Some participants indicated during the interviews that the IT and cybersecurity budgets are becoming indistinguishable. This shows a higher maturity level towards cybersecurity within the organisation as the playing field between IT and cybersecurity is levelled.

Structural cybersecurity understaffing

On average, correspondents dedicate about 7% of their IT FTEs to cybersecurity. Compared to the overall size of the organisation, less than 0.5% of staff is dedicated to cybersecurity on average. As a result, cybersecurity teams are vastly and structurally understaffed.

This trend is evident not just within Belgium but on a global scale. The core issue is a genuine struggle for talent, stemming from the shortage in the worldwide cybersecurity talent reservoir. As this resource becomes increasingly depleted, organisations are compelled to employ ingenuity.

Organisations dealing with this shortage of cybersecurity talent use a two-pronged approach. Firstly, for cybersecurity capabilities that lend themselves to outsourcing, such as the security operations centre (SOC), managed security service providers (MSSPs) can provide relief.

Secondly, responsibility and accountability for cybersecurity is shifted towards the product teams. However, expecting the product teams to have the required cybersecurity skills overnight is a fallacy. Having security champions in the product teams who function as a proxy for the security team helps to overcome this obstacle. The dedicated cybersecurity team is involving them where their expertise is required, freeing the first up to support a larger part of the organisation. (Figure 2)

Perception of Cybersecurity

When asked how cybersecurity is perceived in their organisations, participants overall expressed that cybersecurity is seen as a positive force. However, many still perceive the department to be a burden or even a complete roadblock.

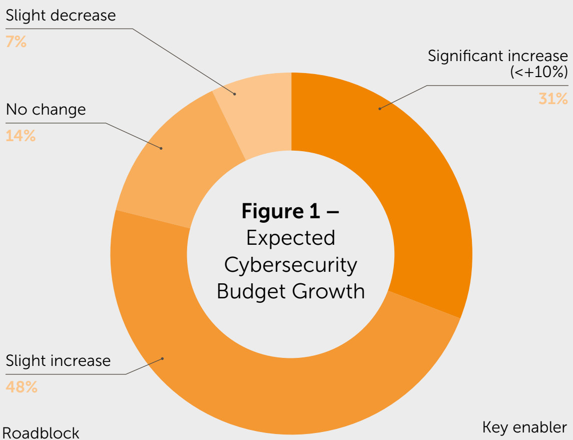


Figure 1 – Expected Cybersecurity Budget Growth

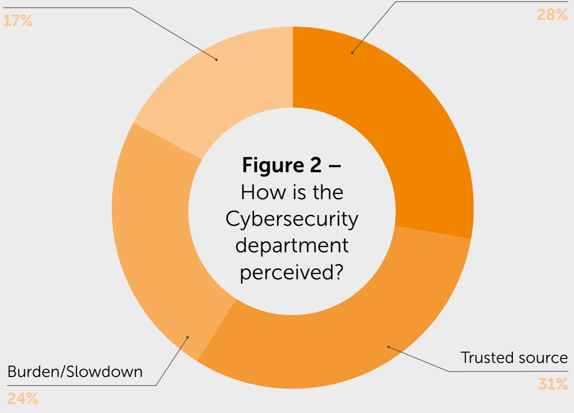


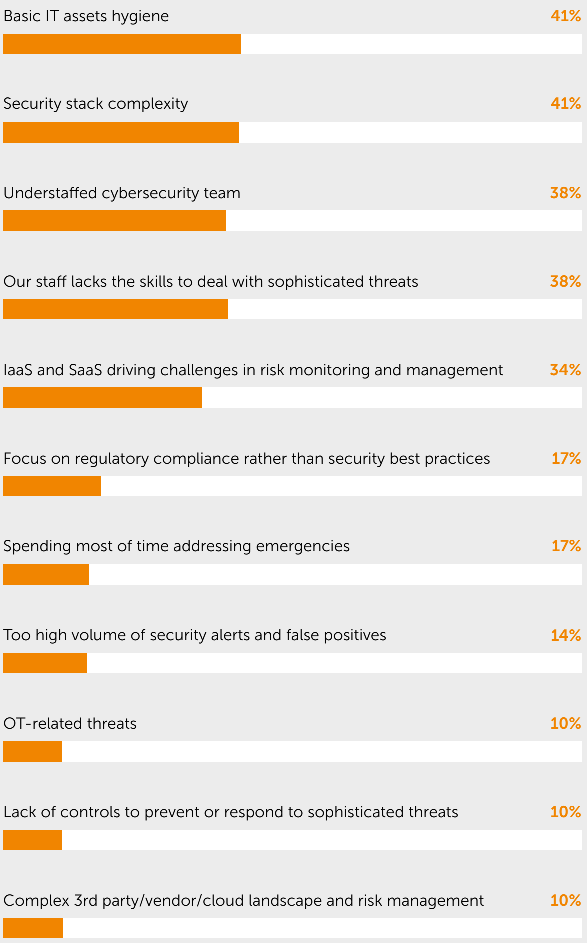
Figure 2 – How is the Cybersecurity department perceived?

This is mainly due to a lack of understanding of the security measures taken, both on board level and within the product teams. Implementing security measures requires changes in people's habits and how they work on a day-to-day basis. Having to perform additional verifications, providing multifactor credentials, and being restricted to access any piece of data, all without an understanding of why these measures are needed, results in resistance within the workforce. On the board level, this is perceived as slowdowns and delays in progress along with employee dissatisfaction, ignoring the protection and assurance offered by the security measures.

Regulation

Several of the interviewees indicated that regulation, to a large extent, drives their cybersecurity adoption. This is apparent in sectors with strict regulations, such as Finance, where the processing of online payments and risk management have been cornerstones for the past decades. These sectors have a clear advantage over those that are just starting to become regulated for cybersecurity. Recent directives such as the European GDPR, have made regulation more stringent and harder to fully comply with.

Figure 3 – Top Cybersecurity Challenges



In the case of NIS 2, the number of entities in scope has exploded from 100 to 2500 organisations. This prompts organisations to more than ever shape their resilience strategy.

Challenges

In terms of challenges, the top 5 challenges are neck-and-neck. (Figure 3)

When drilling down on these topics, we see that the staffing issue we discussed earlier is readily apparent, both in sheer headcount and required skills. Often, a single person, be it a developer or a member of the security team, is expected to perform the roles that an entire team should perform.

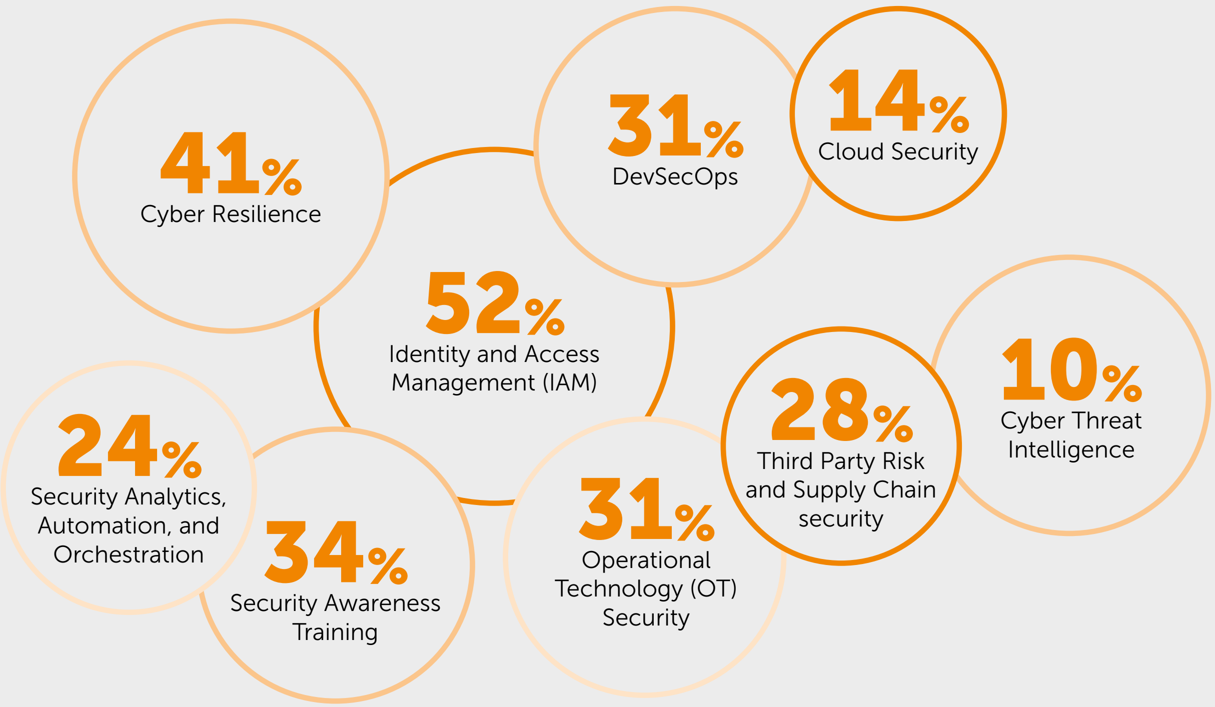
Next to staffing, the complexity of the cybersecurity, supply chain, and cloud landscapes is a hurdle to security programmes. It is not feasible to expect staff to be able to deal with all the complexities of the cybersecurity stack. Just as developers can only be experts in a subset of programming languages, with skill and knowledge that transcends languages, so too can security staff only be experts in so many security technologies.

Regarding basic IT asset hygiene, our correspondents noted that staff members often do not apply the same discipline towards cybersecurity as they do for their private devices. Additionally, with the diversity in devices that are used in organisations, keeping track of, and patching all assets is a vast challenge.

> *“There is so much evolution in the technology that even the engineers who use it daily have a hard time keeping up, let alone security staff. Likewise, we cannot expect engineers to know the latest vulnerabilities.”*
>
> *Mark Van Tiggel - Telenet*

On the other end of the spectrum, only a few correspondents indicated challenges related to OT security. When asked, some correspondents specified that the maturity of their OT environments is at a lower level, consisting only of a few disconnected devices. As these environments modernise expand, and mature, we foresee this challenge to gain importance in the years to come.

Figure 4 – Top Cybersecurity Initiatives



Initiatives

Next, we asked correspondents their top initiatives they are focusing on for the upcoming year. (Figure 4)

Immediately, we see that IAM takes the top spot with over half of the correspondents indicating it as an ongoing focus point for the period to come. It remains a complex security domain, as it requires the cooperation of stakeholders throughout the organisation. Some organisations stipulated that this problem has been tackled before and, therefore, no longer is a top initiative.

Cyber resilience comes in second, as a result of both the increase in cyberattacks globally and the emergence of the NIS 2 directive. 63% of correspondents indicate they currently have not sufficiently tested their cyber resilience strategy, or even do not have a formal one making this initiative even more pressing.

However, for many participants, prevention is at least as important as resilience, as can be seen by security awareness training and DevSecOps taking the subsequent spots while security analytics and operations are further down the list.

Both automation and circumventing the talent shortage will play an important role in these initiatives, attempting to optimally leverage the cybersecurity workforce.

While OT security only reaches 10% as a challenge, almost a third of correspondents mention it as a top initiative for the year to come.

28% mention third-party risk and supply chain security as a top initiative, as they have become increasingly dependent on parties external to the organisation.

Important to note is that even though cloud security was listed as a challenge by about 44%, it is only a top initiative for 14%. Some correspondents include this in their SDLC initiatives, other see it as part of their management of third parties, both of which rank higher on the list.

Theme 2: Cybersecurity Awareness on Board Level

Board meeting frequency

Over half (58%) of the organisations in our research meet with their boards to discuss cybersecurity topics on a quarterly basis. Over a quarter has monthly meetings. On the flipside, the other 42% of organisations meets with their board on cybersecurity topics on a less than quarterly basis. Over a quarter indicates not having structural meetings at all, but rather having them on an ad-hoc basis. (Figure 5)

Cybersecurity savviness at board level

When asked about the cybersecurity savviness at board level, 93% consider their board to be insufficiently equipped to perform decision-making. This results in difficult conversations in which more time is spent on explaining cybersecurity concepts rather than addressing the topics on which decision-making is required. This does not mean that the board does not have a keen interest in cybersecurity, though they are lacking experience on the matter. (Figure 6)

Risk Appetite Discussion

As a result, 70% of organisations is not able to decide on a crisp definition of risk appetite. In over a fifth of organisations, the topic is not even being discussed with the board. (Figure 7)

> *“Translating the quantitative protection level of the organisation into the right KPIs that represent the effort and time required to reduce the vulnerability window is challenging but essential.”*
>
> *Stefan Van Gansbeke - CM*

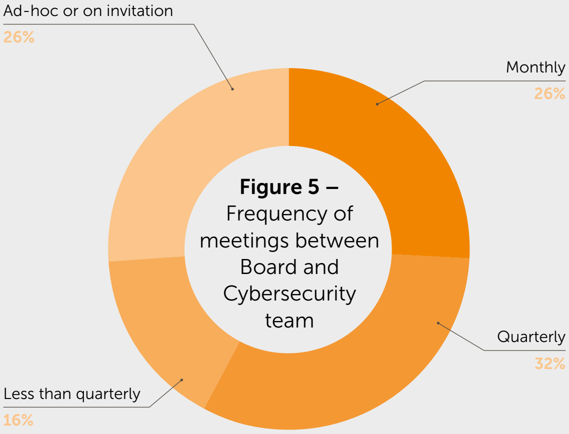


Figure 5 – Frequency of meetings between Board and Cybersecurity team

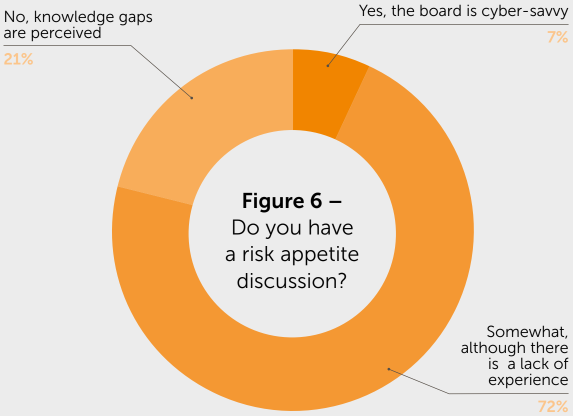


Figure 6 – Do you have a risk appetite discussion?

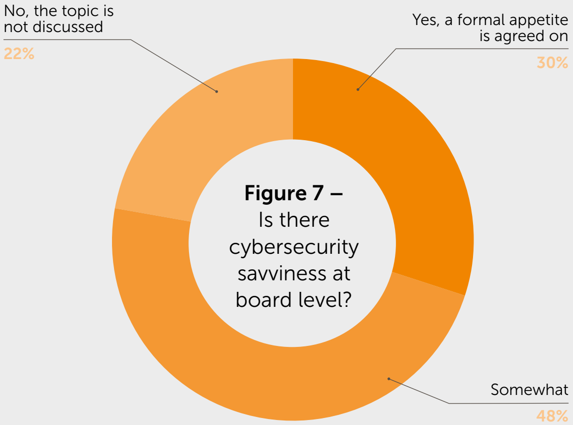


Figure 7 – Is there cybersecurity savviness at board level?

Metrics

About 18% of respondents indicated that they do not use formal metrics to report on cybersecurity to the board. Instead, they inform the board through status updates with context-dependent and informal metrics. Especially highlighting ongoing critical security programmes is popular among correspondents. (Figure 8)

Board meeting outcomes

When asked which outcomes our correspondents perceive from meetings with the board on cybersecurity topics, we received the following responses. (Figure 9)

Figure 8 – Top Metrics Used to Communicate with the Board

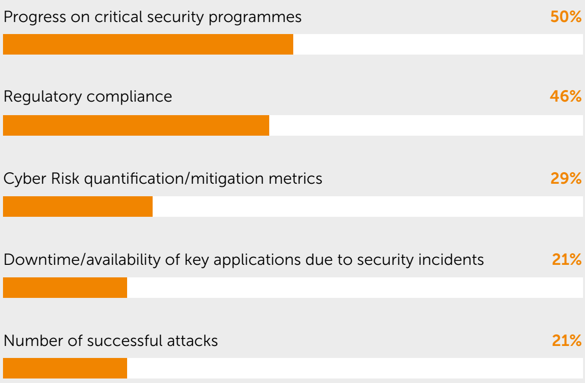
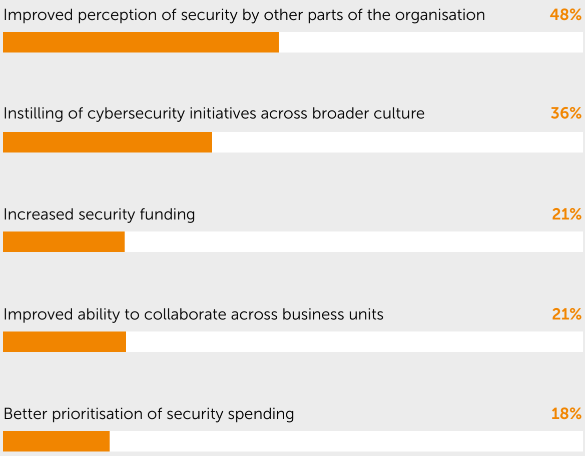


Figure 9 – Top Board Meeting Outcomes



Conclusion

Putting these results together paints the picture that the engagement of the individual board members plays an important role. In organisations where the board is engaged and interested in cybersecurity, the topic is discussed more often, more in depth, and questions from the board members are more frequent. These discussions greatly influence the available cybersecurity budgets and how these are being spent.

We observe that alignment on cybersecurity initiatives at an organisational level is paramount, especially when unpopular or investment-heavy measures need to be implemented. When there is a common understanding on the risks involved and the organisation's risk appetite, this reflects throughout the organisation. Cybersecurity is included in the organisation's objectives, leading to increased collaboration across departments.

Theme 3: Transparency and Collaboration among Senior Leaders

Cybersecurity peer organisations, like the *Cyber Security Coalition*, are an integral part of cybersecurity exchange. They offer insights on how cybersecurity is approached across sectors and organisations. Though only 44% of participants indicated to actively participate in collaborative communities on cybersecurity, it is nearly universally understood that value is to be found in exchanges with peers (89%). Over a quarter of correspondents indicated not to be able to find the time to participate in these communities.

> *“Every organisation understands that they not only need to collaborate internally, but externally as well.”*
>
> *Nilesh Gade - Bekaert*

From the viewpoint of openness, over three-quarters of the interviewees notices increased sharing of information within communities. The remaining quarter disagrees, indicating that there is still much resistance in what and how much information is shared.

Further, we observed a clear difference for financial institutions, as legislation compels them to release information to the authorities on cybersecurity incidents, whereas this is often not yet the case for other sectors.

Often, senior leaders are willing to share information on cybersecurity directly with their peers, while being prudent in doing so in a more public context, such as a workgroup. Interviewees indicate a fear of potential business impacts, such as loss of trust, as one of the causes for this behaviour.

> *“Openness can be a good thing and sharing has its benefits, though it hurts in the moment.”*
>
> *Stefan Van Gansbeke - CM*

A specific aspect that our correspondents indicated is that interactions with peers across sectors are often more open than those within communities, as the former are ties on a personal level, based on mutual trust.

> *“What I appreciate in the interaction with my peers is that every topic is up for debate.”*
>
> *Mark Van Tiggel - Telenet*

Theme 4: DevSecOps: Where do things stand?

Gaps in DevSecOps adoption

As mentioned in the introduction, DevOps, the blending of Development and Operations, has been identified as an accelerator for Agile organisations. When introducing cybersecurity to this mix, DevSecOps is born. Adopting this methodology is essential but challenging. Our participants indicated a few top gaps in their journey to implement their continuous integration and continuous delivery (CI/CD) pipelines. Important to note is that three-quarters of participants describe their DevSecOps initiatives as still in an early stage. (Figure 10)

As we can see, documentation on security architecture is lacking for many correspondents. Enterprise security architects are hard to come by as the field is relatively new and highly specialised.

In terms of testing, we see that organisations follow the natural flow of the DevSecOps model. As static analysis precedes dynamic testing and penetration testing, it can have a greater impact and as a result, receives a higher priority. This is the so-called "shift left" trend we see in action.

Vulnerability management also scores highly, with asset management and basic asset hygiene often stated as the underlying cause.

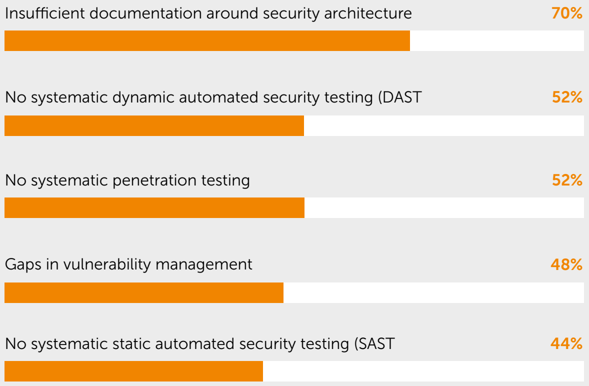
One area that nearly all correspondents indicated to have mastered is instilling clear roles and responsibilities, including those for cybersecurity, within their teams.

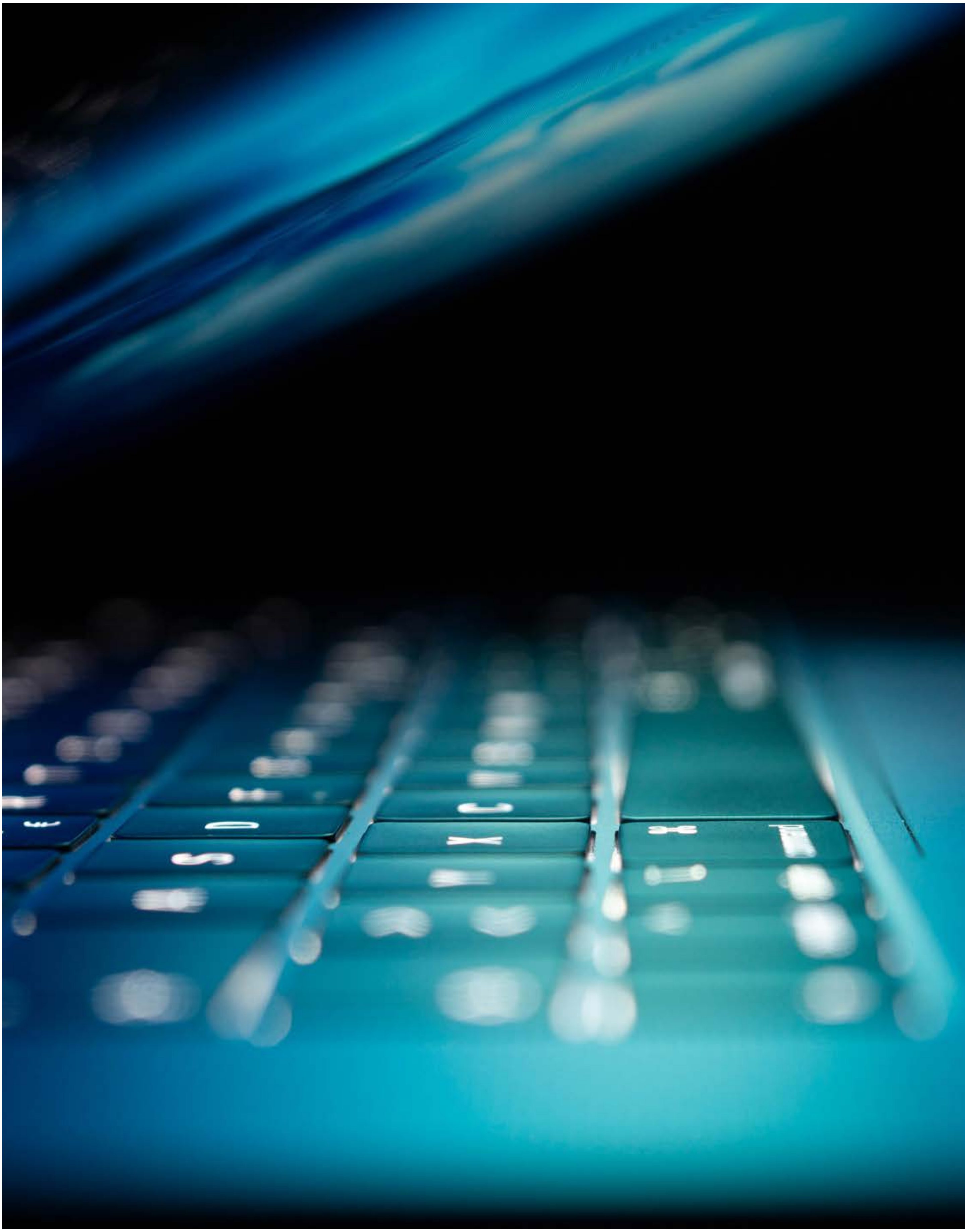
Threat modelling

From the responses, we see that threat modelling is not widely adopted, with two-thirds (63%) of correspondents not being aware of any threat modelling activities taking place during product or solution design.

During the interviews, it became apparent that threat modelling is a great concept that brings value, but often does not outweigh the substantial cost in practice. This is due to it being a largely manual process and its dependency on an existing view of the system. Often, the organisation does not have this view readily available due to factors such as churn in the workforce and lack of enterprise security architects. In those cases, investing this effort and budget elsewhere makes more sense, such as documenting the system's architecture.

Figure 10 – Top CI/CD Gaps





Part 2

Recommendations & Key Take-aways for Cybersecurity

Key Take-away 1: Fix Your Basics First

As the first step of threat modelling states, you must know what you are protecting. Having a clear view on the critical assets within the organisation and how these are exposed to adversaries plays an essential role. Without this insight, it becomes hard to identify where to focus cybersecurity efforts, further aggravating the talent shortage issue.

As we saw in the first part of this report, basic IT asset hygiene remains a challenge for many organisations. Equally, we observed that many organisations currently have IAM as a focused initiative, both partially due to the low quality of HR data and insufficient frequent updates. Having a firm grip on high-quality data related to assets within the organisation is a critical success factor for cybersecurity initiatives.

Mature organisations that have mastered asset management for all asset types enforce stringent data policies and hold the data sources responsible and accountable for the data provided. They understand that data quality forms the foundation for many capabilities that build on top of it, such as their IAM and privileged access management (PAM). As a result, capabilities can focus on fulfilling their security objectives rather than pushing data quality maturity.

> *“With a relatively small team, prioritisation is key.”*
>
> *Stefan Van Gansbeke – CM*

Key Take-away 2: Mitigate the War on Talent

Building and maintaining a fully capable internal cybersecurity team is becoming less and less obvious. On the one hand, the war on talent forms a big obstacle not just to find cybersecurity talent, but also to retain it. On the other hand, even if that talent can be found, a lot of time, energy, on the other hand resources goes into setting up and operating cybersecurity teams.

What we see in mature organisations is a collaboration with managed security service providers (MSSPs) for the operational areas of cybersecurity. The provider manages and operates these capabilities, taking on the challenges of finding suitable staff members and guaranteeing specific service levels (e.g. 24/7 security monitoring). This way, the organisation can focus on defining the cybersecurity strategy in accordance with its risk appetite.

Other areas of cybersecurity are more challenging to outsource as they pertain to the risk appetite and resilience strategy of the organisation. If no candidate can be sourced internally, external consultants can be suitable for roles such as enterprise security architects and CISOs.

Important to note in this scenario is that, even though trust needs to be present between the organisation and the MSSP, this trust should be verified. Just as for any third party, clear agreements need to be made including a mechanism to verify the security claims made by the MSSP (e.g. through independent auditing). Other parameters to clarify include service level agreements, the use of subcontractors, and reporting processes. Such due diligence gives the partnership all chances to last, resulting in an even better service over time due to the knowledge build-up and increased integration of teams.

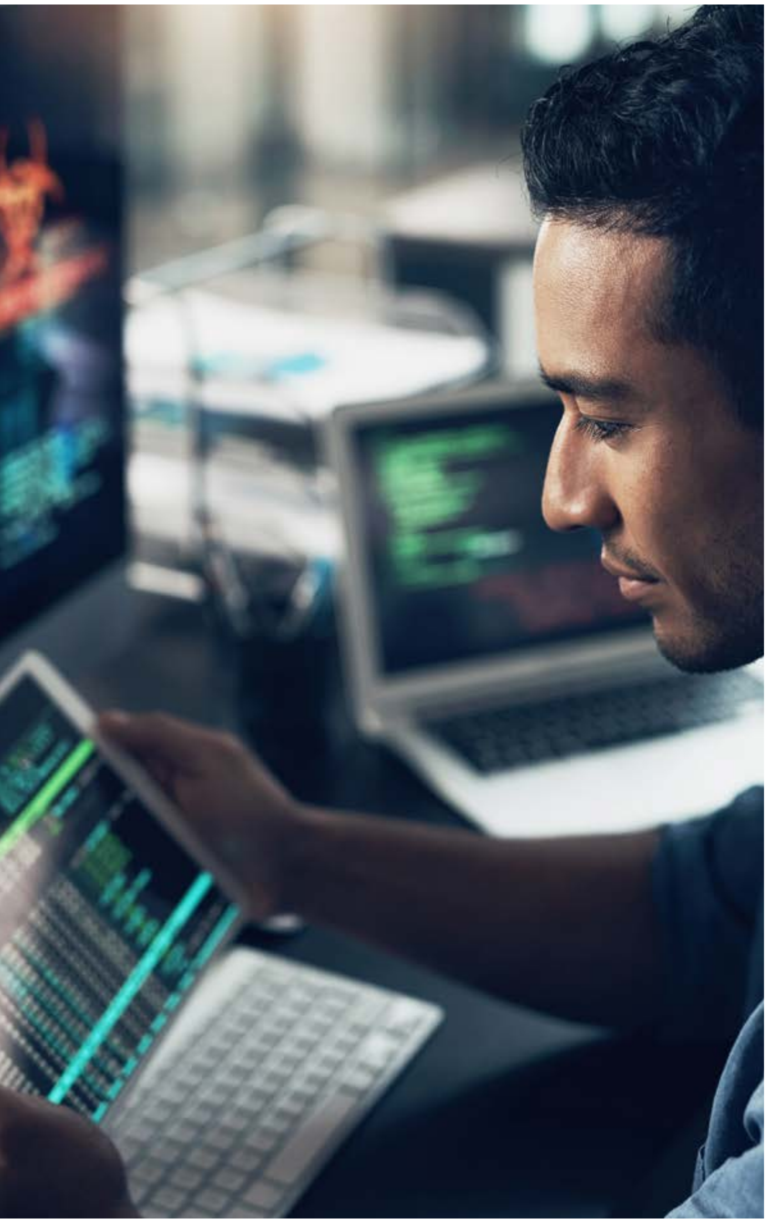
On the organisation's side, consider the creation of a CISO office in which the CISO is supported by a team of cybersecurity experts and enterprise security architects. This office then sets out the cybersecurity requirements and policies, shaping the organisation's cybersecurity strategy, based on the board's risk appetite. The final responsibility remains with the CISO, but this role no longer forms a bottleneck for operations as the work becomes decentralised. This way, the CISO team can service more security needs, become more available, and better connect with the rest of the organisation.

For cybersecurity at the level of product teams, cybersecurity champions are essential to enable cybersecurity throughout the software development life cycle. They interact with both the CISO office for guidance and the MSSP for operational support (e.g. to discuss specific security vulnerabilities and learn about the underlying weaknesses), while being a single point of contact for the product team.

Key Take-away 3: Test Your Resilience Strategy

An organisation's cybersecurity posture can be well-documented and complete on paper, only to fail when push comes to shove. Cybersecurity, and cyber resilience in particular, should be provable and tested property of an organisation. As we saw in Part 1, most organisations in Belgium either have not tested their resilience strategy or even do not have one altogether. This is a veritable sword of Damocles as no organisation is exempt of becoming the target of a, potentially targeted, cyberattack.

Our recommendation is to ensure your resilience strategy is not a paper tiger. Instead, test the strategy under controlled situations, so that you are confident your organisation knows how to respond when an attack occurs.



Key Take-away 4: Manage Your Third-party Risks

In Part 1, we saw third-party risk management and supply chain security popping up as both challenges and initiatives. In our first key takeaway, we suggested that service providers be essential to reinforce security operations. As mentioned, it is important to vet these providers sincerely to ensure their trustworthiness and ability to deliver qualitative services. After all, the organisation is reliant on these providers to remain secure.

However, any other third party the organisation relies on should receive the same treatment. Any weak link in your supply chain may lead to disastrous effects. They should be seen as part of your organisation's attack surface as attacks often leverage the accesses granted to suppliers or external staff.

One crucial pitfall is the temptation to rely fully and solely on third parties. As is the case with cloud providers, blindly relying on them creates a false sense of security. It is therefore paramount to vet third parties and supply chains for their cybersecurity posture. The CISO office plays an important role in this process, as indicated by Stefan Van Gansbeke:

> *"It is important to not blindly trust suppliers, but to have the necessary skills in-house to check what is delivered."*
>
> *Stefan Van Gansbeke – CM*

Requirements for third parties (e.g. IAM procedures, secure development maturity, and internal security awareness), should be explicitly negotiated at the start of an engagement and periodically renegotiated to ensure the third party provides and keeps providing the required cybersecurity guarantees.

Maintaining a precise inventory of engaged third parties is a basic, just like asset management. As mentioned in the first key takeaway, if this capability is not under control yet, it should be addressed with high priority.

Key Take-away 5: Get the Board Onboard

As explained in Theme 2, attracting interest in cybersecurity within the board is essential for a successful cybersecurity programme, both in terms of funding and direction. However, due to a language mismatch and gap in cybersecurity experience, it is hard not to get bogged down in definitions and details. Operational metrics do not speak to the board members as it is hard to gauge the impact and return on investment. Instead, use success stories and updates on security initiatives that speak to your board, highlighting the positive impact of cybersecurity spending and referring to trends in the organisation's sector.

Once the board warms up to the topic of cybersecurity, shift the conversation towards a common understanding of risk appetite and the identification of critical business objectives. This appetite will then drive the cybersecurity strategy, defining critical business objectives as a guide to selecting the critical assets to protect.

In the end, attempting to close the knowledge and experience gap at the board level is worthwhile, as correspondents experience that having a cyber-savvy board entails smooth interactions in which both sides are engaged and aware.

Key Take-away 6: Collaborate Openly and Fully with Peers

The overall sentiment of our correspondents is that collaboration with peers yields value. To maximally harness this value, one should take an open stance in this collaboration, creating a context in which participants feel safe to share security-related information.

Creating this open sharing culture starts with you. Participating in peer events, both as an attendee or speaker, creates connections between peers. These connections, in combination with openness on cybersecurity topics, results in an ecosystem in which organisations lift each other towards a higher cybersecurity maturity level.

> “We are not competing on cybersecurity”
>
> *Rik Bobbaers - ING*

Key Take-away 7: Incrementally Build Your DevSecOps

Like Rome, the perfect DevSecOps pipelines are not built in a day. Trying to get everything right at once is not in line with the Agile spirit and puts stress on the teams. Instead, aim to build up your DevSecOps practices gradually and incrementally, focusing on automation and ease of use. This way, DevSecOps is not a burden but rather an enabling factor. By working with an incremental approach, gradual, lasting progress is ensured. In short, retaining control over a limited initiative is better than losing control of a big bang. If issues arise during the adoption and implementation of DevSecOps stages, consider involving external experts.

A common pitfall for DevSecOps initiatives is to get caught up in chasing regulatory compliance or blindly following frameworks, such as the OWASP Top 10. Instead, initiatives should be tackled according to the impact they have on the overall cyber risk.

> “Too often, the OWASP Top 10 is used as a checklist, while we need insights into and awareness of the vulnerabilities.”
>
> *Mark Van Tiggel - Telenet*

From the challenges identified earlier, we see that insufficient documentation around the security architecture poses a gap in DevSecOps initiatives. Getting enterprise security architecture right is no mean feat and can easily occupy entire cybersecurity teams. Therefore, it is essential to split up this effort into smaller increments so that the security architecture can grow alongside the initiatives, instead of hampering the progress. The prioritisation of these smaller increments, again, should be performed in a risk-driven manner.

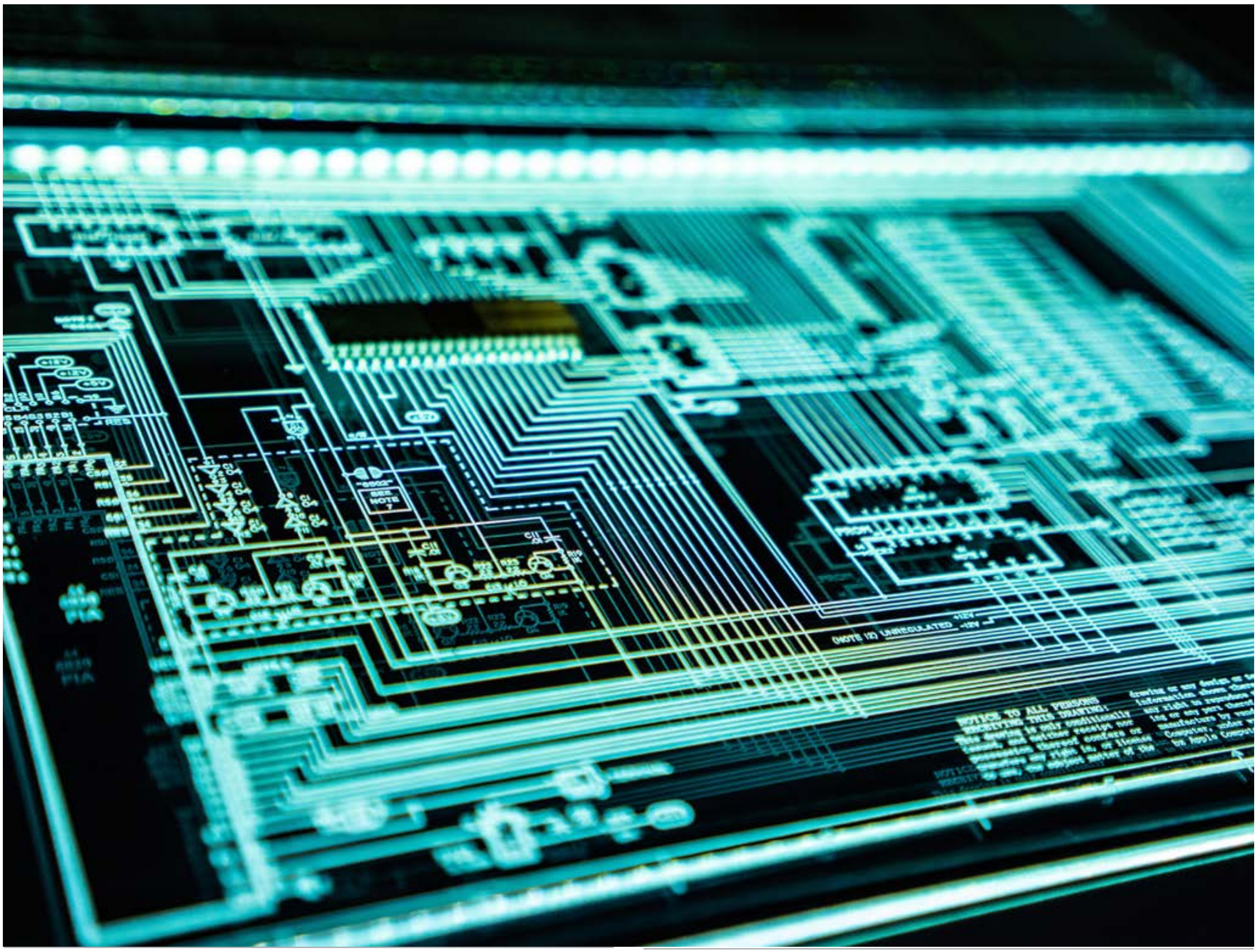
Key Take-away 8: Approach Security in a Holistic Way

As we saw throughout this study, cybersecurity is increasingly breaking free of its silo and becoming part of every department within organisations. This should not come as a surprise as organisations increasingly embrace technology throughout their operations. Hence, cybersecurity should be counted as an enterprise business risk.

As a result, the approach to cybersecurity should be risk-driven and holistic. We already mentioned the basics in the first key takeaway and mentioned the prioritisation of initiatives in the previous one. Beyond these, the organisation needs to identify where it is vulnerable, which assets to protect, what the risks and trade-offs are, and how to act accordingly.

Keeping track of risk appetite, attack surface, and decisions made can become a daunting task if not performed structurally and well-documented. Adding an enterprise security architecture capability to the organisation ensures that the approach to cybersecurity remains structured, in line with best practices, and holistic.

> *“Cybersecurity is one of the critical enterprise business risks”*
>
> *Gunter Van Craen – Bekaert*



WORD OF THANK

We want to thank the CIONET members who devoted their time filling out the questionnaire. An explicit shoutout goes out to the correspondents who reserved their time and attention to participate in the face-to-face interviews. Furthermore, we want to thank CIONET for the collaboration in and opportunity for conducting this research.

Thank you for your participation and collaboration.

Sincerely,

Hans and Nick

Interviewees in order of appearance:

Mark Van Tiggel, Telenet

Gunter Van Craen & Nilesh Gade, Bekaert

Chris Borremans, Komatsu

Peter Decock & Dirk Beynaerts, Colruyt Group

Rik Bobbaers, ING

Luc Verdegem, Vlaanderen Connect.

Pascal Kieboom, Aertssen

Stefan Van Gansbeke, CM

Tom Wouters, SD Worx

ABOUT THE AUTHORS

Nick Van Haver
Associate Cybersecurity Consultant

Nick is an INNOCOM consultant with over 7 years of combined experience in all fields of cybersecurity. He has a strong background in both software engineering and application security. His professional passion lies in bridging the gap between cybersecurity architecture and its execution.

nick.vanhaver@inno.com

Hans Hujoel
Cybersecurity Consultant

Hans is an INNOCOM consultant with over 20 years of experience in cybersecurity, IT and risk management in both industry and consulting. Throughout this time, he has build up extensive experience in securing Critical Infrastructures and has been involved in complex Change and Transformation Management. His interests lie in aligning security strategies with IT and Business strategy.

hans.hujoel@inno.com

CIONET
What's next.

About CIONET

CIONET is the leading community of IT executives in Europe and LATAM. With a membership of over 10000 CIOs, CTOs and IT Directors, CIONET has the mission to help IT executives achieve their aspirations. CIONET opens up a universe of new opportunities in IT management by developing, managing and moderating an integrated array of both offline and online tools and services designed to provide real support for IT executives, so they can do more than just keep up with change but ultimately define it.

www.cionet.com

About INNOCOM

INNOCOM is a fully independent Belgian company that has been guiding organisations through large and complex, strategic changes for over 25 years. We take on the challenges that keep our clients awake at night and strive to achieve the desired results with outstanding commitment. We do this by applying our expertise in agile organisation, enterprise architecture, IT strategy, and cybersecurity architecture. We share and strengthen our knowledge through our IC Institute, which offers various training programs, master classes, foundation classes, and on-the-job coaching.

www.inno.com

CIONET What's next.

INNOCOM.