Digitization on Boards

6th Edition

High Performance Insights

CIOs and CISOs: Managing Tensions and Working Together Effectively

Amrop

Leaders For What's Next

JM SEARCH

Amrop Mission

Shaping Sustainable Success Through Inspiring Leaders

JM Search

To be the leading executive search firm for private equity, and other growth-oriented private and public organizations

Foreword

Many organizations have pursued large-scale digital transformation in the past years and are now under even more pressure to make consequential business decisions - not only at a faster pace, but also with much more attention to the organization's information, cyber, and technology security.

While the CIO oversees all the IT and Digital systems required to support the organization's unique objectives and goals, the CISO's responsibilities include developing, implementing, and enforcing security policies to protect critical data. The tension between the priorities of enabling business objectives through technology and maintaining a robust security posture can be especially challenging when it comes to CISOs reporting to CIOs.

JM Search and Amrop's Global Digital Practice have collaborated in this study and interviewed a number of CIOs and CISOs in Europe and the USA about their approach to managing the CIO's and CISO's sometimes competing priorities and relationships.

We asked them about the pros and cons they see in the CISO reporting to the CIO vs. working as peers, ways of effectively addressing the tension, and the governance standards which need to be in place to make sure that a cybersecurity framework aligns with organizational goals and industry security requirements – and we are excited to offer you the results of this study!

In summary, this study report contains:

+ Eight in-depth interviews with four CIOs (two US-based who also previously served as CISOs and two Europe-based) and four CISOs (two US-based and two Europe-based)
+ An article containing study conclusions based on the eight interviews, analyzed in four categories:
  1. Root causes and main areas of tension between CIOs and CISOs
  2. Reporting structure preferences (pros and cons of the CISO reporting to the CIO vs. working as peers)
  3. Best practices for managing the CIO/CISO relationship
  4. Best practices for CIOs and CISOs to collectively communicate a unified message about the security program and cyber risks to Boards and Executive Leadership Teams (ELTs)

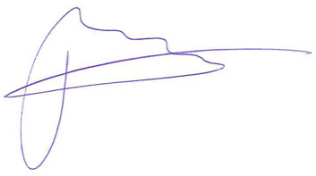
As strategic partners, JM Search and Amrop are privileged to have an extensive network and global expertise. We are excited about our strategic partnership and the opportunity to continue our dialogue with you through it, as we believe in the importance of developing digital leadership and digital literacy – and the great connectivity of the digital community. We're also excited about the opportunity to present to you these key learnings from high-performing tech leaders, especially considering the rapidly changing security landscape, where threat actors invent new approaches every day and trying to stay ahead of them is an ongoing challenge.

We and our fellow practice members would love to help you on your journey to digitize and secure your business – to make it more focused, efficient, sustainable, and successful! Please reach out to us with your needs!

Best regards,

Jamey Cummings

Partner at JM Search

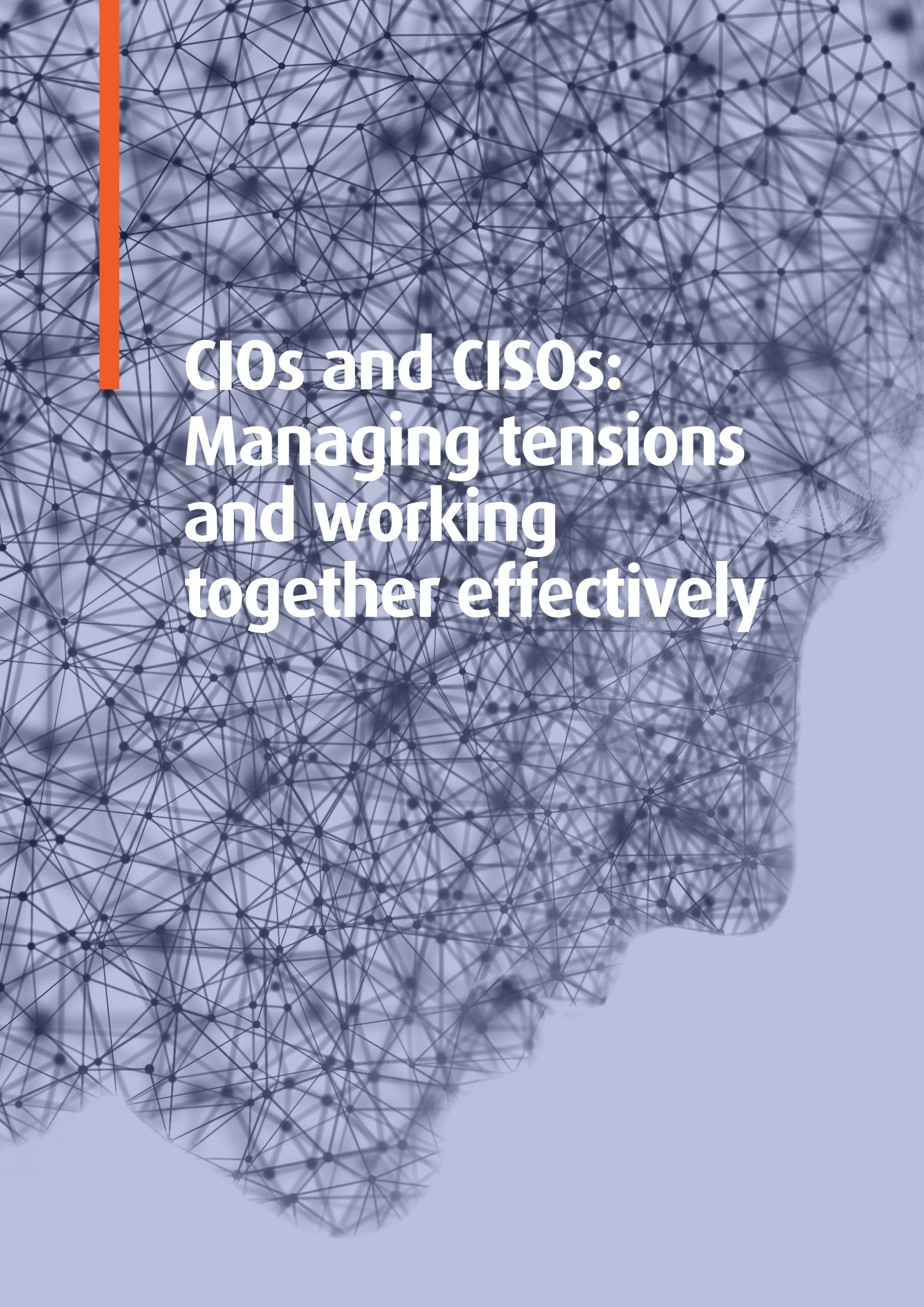


Job Voorhoeve

Leader of Amrop's
Global Digital Practice

Contents

Contents



CIOs and CISOs: Managing tensions and working together effectively

CIOs and CISOs: Managing tensions and working together effectively

A conflict of competing priorities can exist in any reporting structure, but the tension between the priorities of enabling business objectives through technology and maintaining a robust security posture can be especially challenging when it comes to CISOs reporting to CIOs. Many CIOs and CISOs work together effectively and have found a way of balancing technology enablement and security, while some CISOs have said they will never report to a CIO again.

The primary areas of focus for the CIO are to provide seamless technology infrastructure, facilitate business initiatives to drive revenue, and avoid downtime, among other expanding and competing priorities, while the weaknesses and vulnerabilities, which it is the CISO's job to uncover in the organization's security, often indicate different budget priorities.

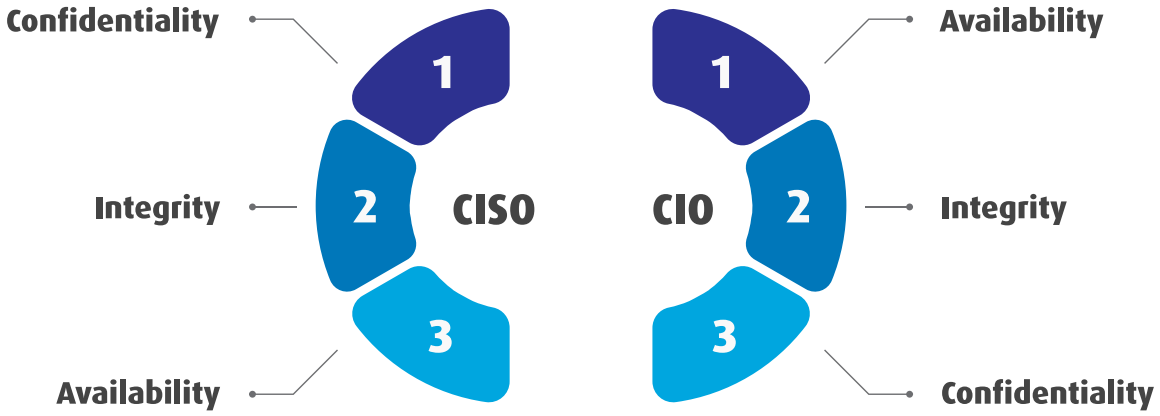
Amrop's Global Digital Practice and their strategic partner in the USA JM Search spoke to a number of CIOs and CISOs in Europe and the USA about their approach to managing the CIO's and CISO's (sometimes) competing priorities and relationships. They talked about the pros and cons they see in CISO reporting to the CIO vs. working as peers, ways of effectively addressing the tension, and the governance standards which need to be in place to make sure that a cybersecurity framework aligns with organizational goals and industry security requirements.

For this study we have interviewed four CIOs (two in the US who also previously served as CISOs and two in Europe) and four CISOs (two in the US and two in Europe), who have provided their unique perspectives and valuable insights in what the collaboration between a CIO and a CISO entails. **We've analyzed and compared their insights in four areas:** 1) root causes and main areas of tension between CIOs and CISOs; 2) reporting structure preferences (pros and cons of the CISO reporting to the CIO vs. working as peers); 3) best practices for managing the CIO/CISO relationship and 4) best practices for CIOs and CISOs to collectively communicate a unified message about the security program and cyber risks to Boards and ELTs.

Causes and main areas of tension between CIOs and CISOs

Many CIOs and CISOs have demonstrated that they can work together effectively and have found a way of balancing technology enablement and security, however, the tension between the priorities of enabling business objectives through technology and maintaining a robust security posture can often be very challenging. We asked four CIOs and four CISOs to identify the main areas and causes of tension between these two positions.

A US-based multi-time CISO, who works for a multi-billion organization in the industrial sector, found it helpful in this context to consider the CIA triad – confidentiality, availability, and integrity, which, according to him, causes natural tension: "From the CISO's perspective, confidentiality is at the top, integrity is a very close second, and availability,



though important, comes third. For the CIO typically availability is the most important factor, integrity – a close second, whereas confidentiality, while not unimportant, becomes the third."

His experience is echoed in the statement of Felix Voskoboynik, CISO at A.S. Watson Group, which is the largest health and beauty retailer in the world, when he reports that the retail space is growing incredibly fast and you need to be on top of things as an organization – the tension has to do with the speed: "It is a very competitive business, and what we feel and face when it comes to the constraints which exist between IT departments, marketing departments and security, is that the business needs to move at such a fast pace are really challenging to keep up from a security perspective."

This remains an issue, even as new roles are introduced in the configuration. Harvey Ewing, a CISO turned CIO, who is now a COO at Specialized Security Services, Inc., sees more and more companies move towards a structure which includes CTO, CIO, and CISO. "The CIO and CTO roles are typically predicated on delivery – delivering infrastructure, services, application feature functionalities, and so on, in a timely manner which, I believe, can create a direct tension between these roles," he says. "This tension is typically due to the CISO being seen as an inhibitor instead of an enabler."

Jan Joost Bierhoff, the CISO at Heineken, suggests that CISO being seen as an inhibitor creates a kind of false conflict: "The way it's presented is that the CIO is being hindered by the CISO in some way, and the CISO is always presented as either hindering the CIO's organization or being ineffectual because they don't get the support or the buy-in that they need, while actually they're both working towards the same objective." At the same time, in Bierhoff's experience, the CIO's focus is on building the future of the technology of the company, so they're a lot more forward-looking. The CISO's work is more about taking care of keeping "the old house" in shape, where many of the risks are and which could hamper the future. "So, there will sometimes be clashing agendas on priority."

On the other hand, it is not just the business requirements that create the race and, consecutively, the tension between CISOs and CIOs. According to Martin de Weerdt, CIO at Randstad Global, security too is a very rapidly changing field, since threat actors invent new approaches every day, and trying to stay ahead of them is an ongoing challenge: "There are things that definitely need to be done immediately, while other things might require a bit more time, and the tension can arise when trying to identify them."

Scott Howitt, currently a CDO at UKG (previously SVP and CIO at McAfee Enterprise, and SVP and CISO at MGM Resorts International) points out that the CISO often has to face a challenge where the CIO gets singularly focused on technology and focused on it for a while: "In the meantime the CISO has to worry about everything, and that can cause internal friction because the CIO has a big deliverable to deliver, while the CISO has many more things to keep track of."

Emily Heath, a former CISO at Docusign, United Airlines, and AECOM, touches on the possible reason for CIO's often singular focus. "The cloud has changed everything, including the CIO's role: they're not creating networks anymore like they used to, so the weight of the CIO's role has gone heavily into enterprise applications and PC desktop support," she states. "The CIO traditionally used to have a CISO as head of infrastructure, but now for the most part it's split out, and the CISO has more relationships to juggle." Like Ewing, Heath too sees more companies gravitate towards incorporating more roles, like CTO and CDO, in the mix: "I'd say there's exponentially

more headaches between a CISO and a CTO these days than between a CISO and a CIO."

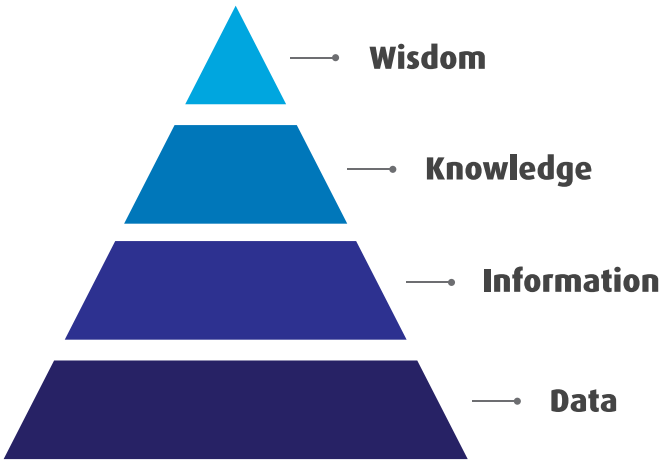
Aloys Kregting, Head of Global Enabling Services at ASML and the former CIO at AkzoNobel, however, sees the main cause of the tension between CIOs and CISOs within the larger relational framework of the organization: "You get this tension when the CIO or the CISO are detached from the rest of the organization, from the stakeholders, and start doing too many things in isolation." He uses the information pyramid: it shows that IT needs to be aligned with the governance, the organization, the master data, and the business process – the context needs to be made congruent. "To make it concrete: if the CISO is not able to explain how relevant the information security risks are for the business propositions, you will have this friction."

Reporting structure preferences (pros and cons of the CISO reporting to the CIO vs. working as peers)

The preferences among our interviewees, when it comes to the reporting structure, unsurprisingly depend very much on their personal experience with regards to what contexts and situations have facilitated or hindered their work and professional development.

A number of interviewees claimed that the reporting structure doesn't matter too much in itself, but each had particular conditions in mind that need to be in place for successful collaboration, nevertheless. Bierhoff, the CISO at Heineken, said that he doesn't care much for the reporting structure as long as there's good communication, besides: "Being within the CIO's organization has the benefit of working together, not being isolated." Similarly, de Weerdt, CIO at Randstad, didn't think the reporting line was important, but thought it was crucial for CISO to have a possibility to "raise alarm if the CIO doesn't listen, so there's balance in the relationship". Based on the specific global structure of their organization, he also notes that "his job as global CIO is to make sure that the local CIO organizations deliver on the things agreed to with the CISO, because they report to him and not to the CISO."

In Ewing's experience as CISO turned CIO, a mature enterprise risk mechanism needs to be in place – the tenor needs to be set from the Board and senior executive level. According to him, "the risk needs to be accepted at the right level of the organization, and if it is, the reporting structure doesn't need to become an issue." Heath, a former CISO and now a Board member, emphasizes the CISO's responsibility saying



that "as a CISO your job is to be a business leader first and a security leader second", which is why, for 90% of her career she "never really cared about the reporting structure". In her experience, the reporting structure started to matter at the end of her career: "I wanted to be on public boards and knew that I would get paper-sifted if I hadn't been either part of the C-suite or at least an SVP, so in my last role as a CISO it was important that I reported to the CEO."

Kregting, SVP Global Enabling Services at ASML and a former CIO, echoes the idea of the CISO needing to be more business-minded, mentioning that they must have good storytelling capabilities, to be able to tell an emotionally engaging story: "A CISO who is outgoing can influence the rest of the company including the CIO. In that case the reporting structure doesn't matter, and then things actually work much better." In his view, the different scenarios around a functional reporting structure are directly related to people's characters and insists that good communication is key.

At the other end of the spectrum are CISOs for whom, like for the previously mentioned US-based multi-time CISO, who works for a multi-billion organization in the industrial sector, "shifting the CISO out of the CIO's structure has been a game-changer". He explained that for him it meant that security was no longer viewed as an internal issue of the CIO's structure that can get deprioritized. He added, however, that generally more "tension can be observed where there's a lack of investment historically". Likewise, Voskoboynik, CISO at A.S. Watson Group, sees a lot of conflict of interest when the CISO reports to the CIO, such as budget constraints: "I think that a direct line to the CEO is needed; at the same time, it is important to be connected to the IT organization, to be aligned with business goals."

Howitt, a CISO turned CIO/CDO, has had different experiences with regards to reporting structure: "If you have a CIO who understands and cares about security, then it can be okay for the CISO to report to the CIO, but often nowadays the CISOs' security concerns are broader, and CIOs can be singularly focused on technology." For him there came a time when he said that he as a CISO will no longer work under a CIO, only as peers, so there's no conflict – and it worked for him. "However, this can create a different kind of conflict, where both are even less involved and aware of what the other is working on," he admits.

Best practices for managing the CIO/CISO relationship

It is often not possible to influence the reporting structure, however, each of the CIOs and CISOs we spoke to has generously shared their best practices for managing a sometimes strained CIO/CISO relationship and ways they've attempted to alleviate tension both privately and structurally – on an organizational level.

The US-based multi-time CISO, who works for a multi-billion organization in the industrial sector, invites everyone to focus on the common goals of CIOs and CISOs: "I don't know of any CISO that says: I'd like to see all the services be unavailable more often, or a CIO who says: I wish I could make things less secure. Everyone has the same objectives; the priority and the waiting shift a bit, but there's a common ground that can be negotiated. And that's where I see success as opposed to entrenched positions." For him, the most important thing he's always done, is to establish an exception process so that there's a consistent, informed way to approach and document a risk: "This way, if there really is an operational need that trumps a security need, which happens frequently, we make an informed decision, and move forward. But without that governance approach, without that consistent method of saying: this is how we will deviate from the ideal security state, or, at least, our desired security state, you really end up with a lot more conflicts."

Both Voskoboynik, CISO at A.S. Watson Group, and Bierhoff, CISO at Heineken, emphasize the educational role of the CISO, the need of the CISO to communicate their concerns clearly, in line with the business goals in order to alleviate the tension. "The CIO won't be an expert in cybersecurity – they're going to be missing that education, so it's crucial to provide it. That way the CIO will better understand the risks and opportunities in the security area and be able to take responsibility for it," states Voskoboynik. For him it is also about finding a way to make cybersecurity engaging and simple: "I have seen that many tend to complicate things and make it worse than it could actually be. But if you find a way to align with the CIO, to make it more simple, streamlined, and educational for them and for others in the team, if you form the right relationships with your stakeholders, I think that can really simplify things and make them better." Bierhoff agrees that it's crucial that the CISO continuously keeps the CIO informed about why he's concerned about either the CIO's legacy or his future states: "As a result, in my experience, the CIO will never overlook things which I'm truly concerned about. He might say: "Let's not do this now, rather next month," so it's about balancing priorities."

Both Ewing, CISO turned CIO, and Heath, a former CISO, emphasize the need for the CISO to be equally focused on security and business needs. According to Ewing, "the CISOs must overcome the traditional stigma associated with their role and must position themselves as strategically aligned to meeting the business's needs. That doesn't mean reducing security, but it does mean approaching best practices and all that goes into an effective cybersecurity program through collaboration and communication." According to Heath, the political capital of CISO in the relationship with CIO (as well as CTO) is highly important. She also offers practical solutions when it comes to CISO's relationship with engineering teams: "As a CISO you have to take time with these relationships and bring the engineers in when you're buying technology. The trust that you build is everything – because the minute they trust you, you're saving a massive amount of time. What happens then is you slowly start to get out of the way. Eventually you can tell them: you know the methodology – why don't you operate it yourselves? Now they're the captain of their own ship!"

The CIOs see communication as key too. Kregting, a former CIO, is convinced that if both the CIO's and the CISO's communication skills, drive and capabilities are good enough to come out and show themselves, share the risks and make their story an integral part of the overall picture, then there is no issue: "If the business really understands the information risks for their own environment, there won't be such tension." Similarly, de Weerdt, CIO at Randstad, states that there needs to be a very sensible conversation between the CISO and the CIO, as well as the business that eventually needs to pay for everything the CISO and the CIO does – about where we place the priority: "You're never going to be

100% watertight – it's impossible, because there are threats arising every day; there will be areas where we need to work hard to keep up and balance risk and investment very thoughtfully, but this is also a way to be as good as we can be." He also mentions that it's crucial that the CISO has an opportunity to raise the alarm if the CIO doesn't want to listen, to make sure there's balance in that relationship.

Howitt, CISO turned CIO/CDO, sees the advantage in increasing each role's practical understanding of the other: "I would encourage cross-pollination – the CISO could run security and one middleware for the organization. That would make them a little more cross-functional, and same goes for the CIO – they could run certain aspects of security, especially in the three lines of defense mode. The CIO could run operational security, while the CISO runs governance, security and oversight."

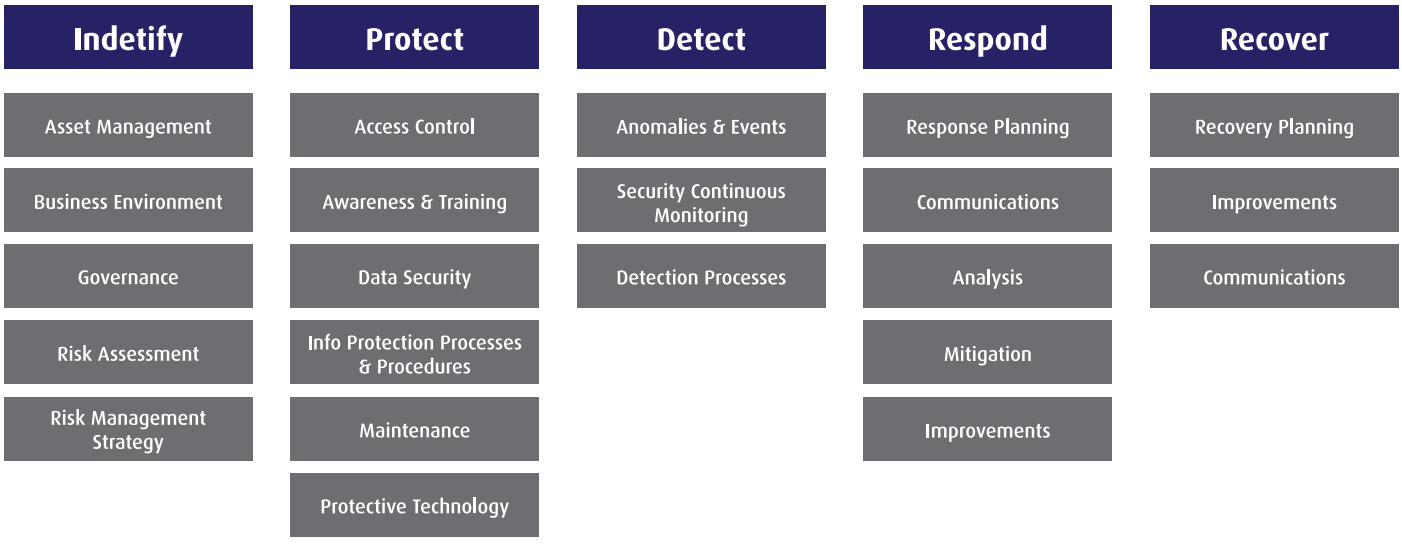
Best practices for CIO and CISOs to collectively communicate a unified message about the security program and cyber risks to Boards and ELTs

It is not only crucial for the CISOs and CIOs to alleviate the tension and arrive at the best practices in their own collaboration, but to also be able to collectively communicate a unified message about the security program and cyber risks to Boards and ELTs. We've asked the interviewees to share what's worked best in their experience and what the responsibilities of each involved party have been.

Direct Board access for CISOs, regardless of the reporting structure, is stated as a clear necessity by both some of the CISOs and CIOs. The US-based multi-time CISO, who works for a multi-billion organization in the industrial sector, stated: "I've had the good fortune throughout my career to always have direct access to the Board – even when I reported to the CIO, we would both be in the room having a conversation together. So, if the Board had a direct question, they could ask me, and they would always get a straight answer. When I used to report to the CIO, I would prepare all my presentation decks, and the data to back it all up, and present that to the CIO. So, if there was any point of conflict, which, again, I've typically been lucky not to have, and if something was changed or adjusted, I had at least some auditable record. Today I get to share with everybody beforehand, and everyone's aware of the metrics, aware of the calculations and wherever the data sources come from, which means everyone has an equal opportunity to control that narrative by taking appropriate action."

Bierhoff, CISO, who attends the Board meetings along with their CIO, states: "During the meetings with the Board and ELT we do a one-pager, where we show what our current risk profile is, given that the gross risk on the outside world is growing. We show them how our net risk is reduced by the initiatives that we embark on, and that really makes it tangible for them, because they understand that the gross risk is really there – they read newspapers, they talk to their peers, they know that e-commerce sites and B2B apps are going down, factories are being hacked. And we explain what we're doing to lower that risk, make sure they understand the terminology, and we talk in more detail about the top 5 activities that we're doing."

NIST Cybersecurity Framework



Similar approach is used by de Weerdt, CIO, who attends Board meetings along with the CISO who reports to him. He states: "We have a regular quarterly update, which works very well, because it's a mixture of what happens in the word in terms of security – it's basically a refresher about the constant attacks that are happening – and an update about the issues we've had. We talk about how we've handled those issues, and we mention issues that partners we work with have experienced too. Last but not least, we report against our strategic plan on how we want to improve our security posture in line with the NIST model."

Voskoboynik emphasizes CISO's responsibility in getting a place at the table by proving themselves to their CIO: "The CIO is very likely not going to be an expert in cybersecurity, so, if they have trust in the CISO, if they understand what you're trying to achieve and if you both have a good working relationship, the CIO will put you in front of the Management." That's his situation: he reports to the CIO but interacts directly with the Management team. But it doesn't end there: "Once you're there, you need to be able to sell and align, and keep everybody informed in the right way. Because if the CIO would see that you're somehow in conflict, that you're reporting about how bad the IT organization is in general, that you're making them look bad, they're quickly going to pull you down. So, as CISO you need to develop a way to keep the Management aligned, interested, engaged, and yes, you're reporting to the CIO because that's the structure, but they need to also see you as the leader, as someone with the know-how, who will provide them with the right information."

Both Ewing, CISO turned CIO, and Kregting, a former CIO and now Head of Global Enabling Services at ASML, emphasize the importance of CISO's communication skills. Kregting suggests that the CIO can be of help to the CISO when it comes to developing these skills: "Some of the CISOs really prefer to work in isolation, doing the brilliant things nobody knows anything about. So, that requires some work, helping them in that journey. As a CIO you can help the CISO by taking the rest of the organization along on the journey, which means different types of communication. For example, one piece of advice I've given to CISOs, and which has actually worked quite well, is to use real incidents in their storytelling."

Ewing states: "What's really worked for me is translating technology into business language – the Board will want to see and understand exactly what the level of risk is, but they want to see it with regard to its impact on strategic initiatives, top line revenue, EBITDA – they want to understand the business logic and math behind what the CISO is really trying to convey. Early in my career I made the mistake of being too technical to the point where the Board said: look, we love it, you're a technical guy, that's great. But what does it really mean for me?" According to him, a Board member providing guidance to the company wants to understand the following: are we driving to the level of risk where I'm comfortable? Have we enumerated those risks? Have you communicated those risks in a business format? Is it going to impact top-line revenue?

Interviews with CIOs and CISOs from the USA and Europe

You have to be comfortable with being uncomfortable – and having a healthy conflict!

Interview with Harvey Ewing

CISO turned CIO; former Chief Operating Officer at Specialized Security Services, Inc.; Mercy Technology Security Board Member at Mercy

Q: Harvey, you've been a CISO and are now a CIO, so you're in a position to offer a very interesting perspective on the subject. There often appears to be tension between CISOs and CIOs – the priorities of enabling business objectives through technology and maintaining a robust security posture. What have you found to be the specific areas where this tension most clearly manifests itself? Is it mainly about technology, ownership and accountability of technology and delivery, or budget priorities and constraints, perhaps others?

A: First, I'd like to expand this to include the CTO – at least in my experience I'm seeing companies move towards more of a CTO, CIO, and CISO type of configuration.The CIO and CTO roles are typically predicated on delivery – delivering infrastructure, services, application feature functionalities, and so on, in a timely manner which, I believe, can create a direct tension between the roles. This tension is typically due to the CISO being seen as an inhibitor instead of an enabler. In my opinion, an antagonistic relationship between these three roles can be very problematic to the business, so culture and reporting relationships become incredibly important. The tenor of the relationship can be positively influenced by the CISO through direct communication. The CISO must overcome the traditional stigma associated with their role and must position oneself as strategically aligned to meeting the business's needs. That doesn't mean reducing security, but it does mean approaching best practices and all that goes into an effective cybersecurity program through collaboration and communication. If the CISO becomes a business partner instead of a competitor, the tension is significantly reduced and all, especially the business, benefit.

Q: It seems that this way there's also not enough discussion around security happening.

A: Yes, I believe that cybersecurity should be discussed at senior executive and Board level. When risk acceptance is shifted to the senior executive team (away from the CISO), the decision as to how much risk will be accepted, how much risk must be mitigated and at what cost, will assist in aligning the CIO, CTO, and CISO. I've seen too many companies that allow risk decisions to be made at various levels of the organization which creates risk for executive leaders and the Board. It also creates friction between teams, especially cybersecurity and delivery, because decisions are made in silos. Every business takes risks, but, as long as the risk is defined, quantified and communicated, delivery and cybersecurity can drive towards one goal and know how far they need to go.

This aligned posture will reduce tension and increase delivery - in the right way. One other very important aspect of this discussion is culture. Leaders need to be business-focused, business-first, including the CISO. That can be rare, but they need to be able to speak the language of business, and they also need to lead without ego. If the CIO, CTO and CISO are all pragmatic, the tension is reduced, because now they're focusing on where the business is driving them, and the decisions are made without emotion.

Q: But, as you said, the tone needs to be set from the top.

A: Yes, and the risk needs to be accepted at the right level of the organization. The CIO, CTO and CISO are typically not empowered to accept or reject risks on behalf of the CEO, COO, CFO, or the committee at the Board level that's actually responsible for managing those risks and providing guidance.

Q: Is there anything else that, in your opinion, can affect the relationship between that triumvirate?

A: Large companies typically have in-house teams that are tasked with delivering the strategy for business from a technology perspective. One additional way to reduce stress is, instead of focusing on DevOps, to focus on DevSecOps, but in a very specific way. The cybersecurity team should have application security developers that are embedded in the software development teams. And when I say embedded, it is not for delivering vulnerability information, but to actually assist in remediation. The application security engineers should evaluate code and then assist in resolving issues. When that type of partnership exists, the security function is now seen as an enabler. Even though the team may iterate a little more during development, you'll accelerate as the code is inspected and moves through the combined process, so you truly "shift left". This type of process will, in my experience, reduce development and delivery cycles and truly position the cybersecurity team as a partner. It's a very powerful catalyst for creating aligned teams.

> "The CISO must overcome the traditional stigma associated with their role and must position oneself as strategically aligned to meeting the business's needs.

Q: It's one thing to have the best possible relationship between the CIO and the CISO, but how about when it comes to communicating risks to the Board? You've briefed the Board as both the CISO and the CIO. How can you best ensure that Boards and ELTs are informed on enterprise cybersecurity programs and risks?

A: I've had a lot of trial and error with this, but what's really worked for me is translating technology into business language. The Board will want to see and understand exactly what the level of risk is, but they want to see it with regard to its impact on strategic initiatives, top line revenue, EBITDA – they want to understand the business logic and math behind what the CISO is really trying to convey. Early in my career I made the mistake of being too technical to the point where the Board said: look, we love it, you're a technical guy, that's great. But what does it really mean for us? If I'm a Board member providing guidance to the company, I would like answers to questions such as: are we driving to the level of risk where we're comfortable? Have we enumerated those risks? Have we communicated those risks in a business format? Is it going to impact top-line revenue? Is it a third-party aspect that could have a negative impact on the company? Are we covering the bases for our responsibility as Board members to this company, and are we protecting our shareholders? That's the equation that we have to come up with, and again, the risk has to be accepted at the right level of the organization, that risk mechanism needs to be in place. And then there has to be a business justification and quantification on how those risks are mitigated. So, there's no sensationalism. There's no: hey, I'm going to go in and

show all my technical value to the company. Instead, I'm going to translate all of these challenges into business language and let the Board say: We're not willing to accept that particular risk for whatever reason. And here's what you've presented how much it's going to cost us to mitigate that risk. Is that acceptable to the business from a financial standpoint? If not, let's go back and forth to where we drive to an acceptable level of risk, and an acceptable level of spending to mitigate that risk to our understanding and our liking.

Q: One of the consistent themes for you seems to be that, regardless of the reporting structure, relationships matter. But how do you work through tensions if the relationship is not so great? Do you have any tips for your fellow CISOs and CIOs on how to navigate that – from personal experience or that of others?

A: That's a difficult situation to be in, and the CIO is likely put in that position by the pressure to deliver. Again, the question I would ask is: is the CIO being expected to accept or reject the risk on behalf of the entire executive team, is that CIO being put under significant pressure to meet business goals? As a CISO I would go to that CIO and say: look, I've got a job to do, as do you. How can I help support you and get the required delivery done? I understand you're under pressure, and here's what I want you to be careful of. Here are the things that we should work on together and which you need to be aware of, and if we need to elevate those risks higher in the organization so that it removes some of the pressure from you, let's do that together. If I report to you, if you're my colleague, then these are the items that we need to counsel the other executives on to see if they agree with where we're at and on how much risk we want to or don't want to accept. It may be seen as a roadblock, but you have to communicate to the CIO that you are business-aligned, and you want to help deliver all of the projects they're being tasked with, so it's really all about collaboration.

Q: And taking out the emotion…

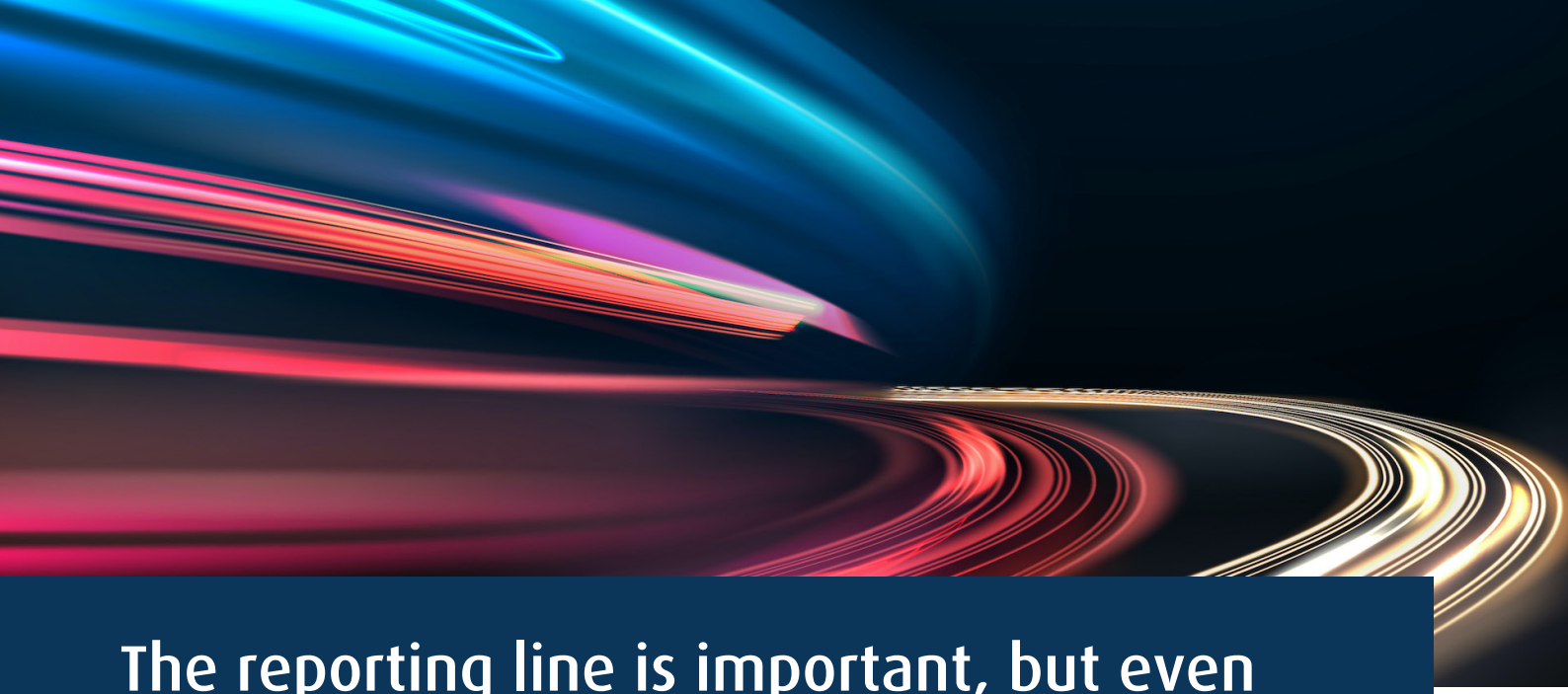
A: Exactly. Because you're going to get pushback, because people are going to say: look, I'm under pressure, I have to deliver, I know you want to do your job, but I see you as a roadblock. When you hear that, you really need to take the emotion out and ask: why do you see me as a roadblock? What's happened in the past? And, if they're new to the role, how can we work together on this? Let me prove to you that I'm a business-enabler, that it's not security for security's sake, but security for business's sake! When you remove the emotion, you approach cybersecurity and delivery pragmatically, and you shift the risk-acceptance or rejection to the appropriate place in the organization, it really helps repair the relationship, and then creates a true partnership.

Q: These are such universal themes, but it feels like they still have to be constantly reminded of…

A: Everyone tends to envelop themselves in a silo when there's contention, but I like to talk about healthy conflict. That's removing emotion and you need to be able to push each other appropriately saying: hey, I'm going to challenge you and here's why. I'm not just going to sit back and say: I'm going to make your life harder. We know that we have a common goal and that's to support the business, so, if we both want to succeed, we need to develop that relationship, because a divided house is always going to fall. So, if the CISO and the CIO can't develop that relationship, the ELT will have to say at some point: hey, you two are going to have to figure this out, because you're negatively impacting the business. And you have to be comfortable with being uncomfortable, with having that healthy conflict and challenging that relationship positively.

Q: Thanks a lot for that. Is there anything you'd like to add, any final tips to any of those involved in this equation?

A: One thing I find really important is the cultural fit. To have ego-free leaders who are there to support the business and who can develop that high-functioning team. That's the "secret sauce". There are tons of people with good technical expertise – that's why they're in that particular position at that stage of their career, but they must be willing to partner and to be challenged by the team. I also think that it's good to have that direct relationship with the Board, especially for the CISOs. The Board member can say: here's what's truly important to me. Here's how you can deliver that data. Don't make CISOs try to feel their way around to getting the Board, their peers and other senior executive leaders the data they need – give the CISOs that information upfront!



The reporting line is important, but even when that's in order, the CISO needs to do the hard work!

Interview with Jan Joost Bierhoff

CISO at Heineken

Q: Could be great to hear how you started your career and became a CISO?

A: In my first years with Deloitte I spent nearly 60-70% of the time as Auditor mainly in Africa, with the more up-coming countries to help them with their IT security. I started in one of the breweries of Heineken dealing with their IT security, satellite connection at that time. After I joined the IT department of Heineken to work on lowering the risk profile. I am now globally responsible for the whole security function of Heineken; present in 190 countries with breweries in over 80 countries. Currently reporting to one of the Board members, the Chief Digital and Technology Officer – before this year I reported to the CIO.

Q: There often appears to be tension between the priorities of enabling business objectives through technology and maintaining a robust security posture. What have you found to be the specific areas where this tension most clearly manifests itself? (e.g., Technology, ownership and accountability of technology and delivery, budget priorities and constraints, other?)

A: For Heineken it's mainly about gaining trust in the supply chain domain. It's the heart of our existence. Of course, we're super good brand managers. That's the other power of Heineken. So, our brands are super strong. But you can only do that if your product actually is reliable, and its quality is always exactly the same. So, the breweries became more automated over time. Even at this moment in time one of our breweries in India is not automated at all. There's no automation, there's no technology. So, it used to be how we worked. And over time more and more IT got into our operational technology sites. Also, our hand in IT security became stronger and stronger. And there are, of course, the brewers – they're not distrusting us, but in the end, it's their domain. Some of them are already getting a bit further in their career, less flexible to changes and also less flexible to technology changes in particular. So, we've needed to step up massively to take them by the hand and say: we're not a threat. We're here to protect your breweries even better, but really, it's about gaining trust, and even at certain moments we might need to take control of the brewery from a technological point of view, while they do the delivery of the products. That needs to go hand in hand. So that's where the biggest gap to fill is – in gaining trust, in taking over when needed.

Q: How is that done when it comes to setting priorities and from a budget perspective? I can imagine that it's going to cost them, right? One thing is gaining trust and being open for a discussion, but, at the same time, it all comes down to the budget. What, in your experience, is the key to success when it comes to dealing with those tensions?

A: Credit for success in this respect definitely goes to the CEO and the executive team in shaping the "Evergreen" strategy, which provides very clear goals as to how we, as Heineken, want to grow. There's a whole set of activities which need to be done. These are called the top 25 programs which need to be done, but 80% of these are supported by technology, and all of them have an IT component. One of them, for example, is the OT security, and from the funding perspective, it's really almost equal to what's dedicated to our B2B agenda. Thus, while we, of course, also have central pockets with funds available, the breweries are requested to allocate between 2% and 8% of their budget, depending on the country, to OT security. We set them on course, the program is spread over three years, but the request to allocate the budget is set by the executive team, thus making it relatively easy to make sure it happens. And then it's a matter of delivery, which is, of course, hard enough in itself.

Q: Were you involved in setting the percentage and scoping that? How did you do it?

A: It is a massive jigsaw, of course. So, for example, some operating companies don't have a brewery and only have a sales office, so in their case the project is not applicable, and the security budget is zero. But in the 80 sites residing in the 40+ operating companies it is really a matter of how many firewalls are still out there. It means really breaking it all down.

Q: So you've basically done an audit for all of them?

A: Yes, my audit background has helped a lot. But it is also our HR team, which has done a great job identifying what Heineken is. So, if I go to the HR system, I can really zoom in on the operating companies and see, for example, how many people work in a brewery, and even that gives you a flavor of what it might need in terms of security awareness campaigns. Also, my IT colleagues have helped a lot by getting us more insights into the assets and classifying them per brewery and per country. So, from a central point of view, I can already see how large a brewery is.

> "We could, of course, secure everything and achieve a certain level of security everywhere – build a very high fence around the house, so to speak. But, in the end, the houses that we really need to work on now are the next level.

Q: So, it's really about being able to gather the data on the local situation which then helps you define what needs to be done and to scope it. And then there's probably a dialogue because perhaps the local brewery puts in a minimum, the 2% and then you need to go in and say that, well, the bracket was 2% for those who are at a certain maturity but 8% for those who have to start from zero.

A: It's always the game, where in the end we always ask them to reserve €5K, but, again, security is not the whole amount of money for doing a new brewing line, which also happens, and then we often stay within the limits of the €5K and they have some extra money to play with.

Q: You can put it in the shared service center, so you can help them be efficient on certain elements, you can help them by scale.

A: But also, we could, of course, secure everything and achieve a certain level of security everywhere – build

a very high fence around the house, so to speak. But, in the end, the houses that we really need to work on now are the next level. We've put the fence everywhere now, which was the minimum, and now it's up to our procurement colleagues to see what blocks are the ones that matter the most. What's the top 10? And the top 50 and 100? Of course, I start with the top 10. What are the supply connections and the supplier engagement with the set-up, the safety on the core side? Which customers really matter globally and which regionally? The company money needs to be invested while keeping the priorities in mind, so I'm going one mile further to the operating companies, the customers, the suppliers, or even employees, which matter the most.

Q: So, for you the connections are really important, right? Because you're in the systems connecting with one another, and that's high-risk, right?

A: Exactly. So, if we look at the hacks, which happened on a macro level, those led to warehouses that needed to close. So, we have already sold our beer to them, but then it stays there, and, while it has a shelf life of multiple months, if they don't sell, we still miss out on the revenue. So, we need to help them as best we can to recover and perhaps even send people to help them recover as soon as possible. In these cases, we step in as a neighbor to help out the next-door family to recover from the blow.

Q: And that's, I would say, also typical for the CISO community, because you really see this as a global threat. And you also go in because you see the key learnings for yourself, so you can update your teams on the latest insights. There's a kind of win-win situation really.

A: That's true. I'm also exchanging information with a CISO who is a friend; their organization is a friendly competitor, so to speak, because we've done some joint acquisitions – we bought an asset together and split it up afterwards. The CISO community really works together. If we see something happening in the Nordics, where they're active, we inform them if we've bumped into a threat – we quickly check in saying that we assume you've seen this as well, but if not, please check it out. So that's really where we're teaming up.

Q: What from your perspective are the pros and cons of the CISO reporting to the CIO vs. working as peers?

A: It all depends on the CIO. I'm blessed with my CIO, who is, first of all, a great guy, but also has a background as an IT auditor. So, in the end, he understands me and my previous role as an auditor. We can have sufficiently heated discussions, but they're always productive, and we have a very good trust relationship. But he can also help me set priorities and I go to him when there's really an issue. For example, if we're moving from one system to another and afterwards I need to start chasing the ones who are running behind, the CIO sometimes needs to stand up and say to everyone that moving is a must if we're to take our work seriously, if we want to make sure we're not being attacked. We, of course, take in the feedback and concerns, and then the CIO can direct them to me should any problems occur. The tone needs to be convincing. At the same time, if he were my peer, I would need to take time to convince him, and we might have clashing agendas,

> “
>
> **The CISO community really works together. If we see something happening in the Nordics, where they're active, we inform them if we've bumped into a threat – we quickly check in saying that we assume you've seen this as well, but if not, please check it out.**

but now my agenda is automatically his agenda as well. So, this is a typical example where he's fully briefed, he stands up, tells the story, takes away all the ammunition from other people before there's fire.

Q: What from your perspective are the pros and cons of the CISO reporting to the CIO vs. working as peers?

A: It all depends on the CIO. I'm blessed with my CIO, who is, first of all, a great guy, but also has a background as an IT auditor. So, in the end, he understands me and my previous role as an auditor. We can have sufficiently heated discussions, but they're always productive, and we have a very good trust relationship. But he can also help me set priorities and I go to him when there's really an issue. For example, if we're moving from one system to another and afterwards I need to start chasing the ones who are running behind, the CIO sometimes needs to stand up and say to everyone that moving is a must if we're to take our work seriously, if we want to make sure we're not being attacked. We, of course, take in the feedback and concerns, and then the CIO can direct them to me should any problems occur. The tone needs to be convincing. At the same time, if he were my peer, I would need to take time to convince him, and we might have clashing agendas, but now my agenda is automatically his agenda as well. So, this is a typical example where he's fully briefed, he stands up, tells the story, takes away all the ammunition from other people before there's fire.

Q: So, reporting to the CIO for you is an advantage, because you have a good working relationship, and you're part of his team. So, you also understand the technical implications of that strategy, and that's really important. Because if you wouldn't, you would be less connected to the OT, to the networking issues and certain levels of infrastructure, which is so important for you to be able to get it all fixed.

A: Yes, that's exactly why it works. I definitely wouldn't classify myself as a peer to the CIO because, after all, he's a couple of positions higher than me. But in the end, when it comes to the reporting line, we're sharing the same executive team member. So, the CIO is a lot more important in the company but we're still in the same layer. His focus is really on building the future of the technology of Heineken, so he's a lot more forward-looking so to speak. Of course, he's also taking care of keeping "the old house" in shape, where many of the risks are and which could hamper the future. But also, the new initiatives, the new structures, for which we literally use the #CoolShit, model2, so we are not directly secured by design. So, it's crucial that I continuously keep him informed about why I'm concerned about either his legacy or his future states. So, there will sometimes be clashing agendas on priority, but he will never overlook things which I'm truly concerned about. He might say: "Let's not do this now, rather next month", so it's about balancing priorities.

Q: That's very interesting. So, if you have a mature IT organization and the CIO is focused more on the future direction of the technology, you as a CISO are more focused on the legacy of the organization, especially on the OT side, to see if there are issues that still need to be addressed. Could you say that?

A: Yes, exactly. Two of the pillars of "the house" are really about modernizing our front ends, while three pillars are about simplifying and automating the back ends, which, we could say, are more connected to the legacy of the organization. So, about 60% of my focus, and not only mine, is about simplifying and automating the back ends, and, by doing so, making it all smaller and smaller, while broadening the other pillars. Three years from now we hope that all our sales reps and restaurant owners will have 1 to 3 apps to communicate with Heineken – for doing the orders and all other necessary things. That's the future.

Q: Do you have anything to add with relation to the scope of the responsibility, the goals and the philosophy when it comes to technology security? Can you share anything about the frameworks and best practices, considering that you've developed such strong and successful relationships?

A: I'm really blessed with the set-up we have, because our executive team really considers cybersecurity to be important. And I have unfiltered access, while some of my peers, other CISOs, sometimes have an issue with even getting into the boardroom, or when they do, there are filters. Of course, I still get my coaching on how to do the best storytelling (laughs), but I am able to have unfiltered sessions with the Supervisory Board members, where my previous role as an auditor helps a lot. Also, budget-wise, Heineken really takes security seriously, not being penny-wise and pound-foolish at all. Besides, I have access to our CFO, our CTO and, of course, our CIO. So, the only thing I can say to my fellow CISOs is, yes, the reporting line is important. But even when that is in order, the hard work needs to be done! See if you can get informal moments with all the people who you would want that with – for your cyber insurance you need to talk to the CFO and other colleagues in insurance, and see what's important for them, so you can get more aligned, more focused with your own

agenda; and by doing that you get to connect! Find moments to approach your commerce colleagues, see which apps and which customers are the most important to you, and approach also your supply chain people, which in my case is the brewery staff – see which 15 breweries are the most important. And yes, the supply chain colleagues might not always prefer that you're talking to the same people as them, but, in the end, it's also your own responsibility to connect – just ask them if they can join for a coffee if you feel like there's still some possible hostility there. But really, make those informal connections, and from those you can start building formal moments throughout the year – from the informal beers and coffees you can get to, perhaps, formal biannual connects. And by doing that you gain your place at the meeting room table.

Q: Excellent advice, thank you! Let's now talk a bit about Enterprise Information Security and Board and ELT Communications. What governance standards need to be in place to make sure that a cybersecurity framework aligns with organizational goals and industry security requirements? How can you best ensure that Boards and ELTs are informed on enterprise cybersecurity programs and risks?

A: So, during the meetings with the Board and ELT we do a one-pager, where we show what our current risk profile is, given that the gross risk on the outside world is growing. We show them how our net risk is reduced by the initiatives that we embark on, we show them what's happening. And that really makes it tangible for them, because they understand that the gross risk is really there – they read newspapers, they talk to their peers, they know e-commerce sites, B2B apps are going down, factories are being hacked. And we explain what we're doing to lower that risk, make sure they understand the terminology, and we talk in more detail about the top 5 activities that we're doing. And there are 150 more activities, but we don't need to bother them with that, we're just showing the big blocks. And if they want to know more about the other activities, then the informal connections can again help – colleagues from different geographies can explain what's happening in the region and so on. And then there's a discussion on the executive team level about how we can cover the site and do more. So, by using my moment to shine, I can also get other topics on the table. But we always show that the risk is fed by, let's say, the following 20 angles, and then these angles are cut away or narrowed by the following 5 or 6 initiatives.

> **"Make those informal connections, and from those you can start building formal moments throughout the year.**

Q: Yes, simplify, make it, being a point of view, almost. And it's also like a scorecard of where you stand and how you develop.

A: Yes. And I can say, if you want me to do more, even if you gave me a bag of money, I cannot do more. If you want to reduce the amount of money or, let's say, gain more time in spending that money, these are the three angles you can choose, that's the lever between these brackets in time and euros. So, it's up to them to decide if it's about the amount of money.

Q: Yes, so it's all really clear around where the budget is being spent, what is empowered, what is non-negotiable, what's okay – you can maybe spread that investment over a longer period of time, but then these are the risks. You talked a bit about the relationship between the CISO and the CIO, but is the CIO also involved in this part or is this kind of separate?

A: The CIO and I go to the Supervisory Board and executive team meetings together. It's always about a couple of topics which are on the top of our minds. These are usually about the largest investments and the progress we make out there, and they're usually chaired by our CIO and heavily supported by our CTO. And then we also discuss the biggest risks – and the budget which needs to be successfully spent. And when it comes to risk, one of the big risks is around cybersecurity, but, because I used to be the voice of risk on the other side of the table, they also bring me in to discuss the other risks out there. So, there are often three agenda topics, and the CIO does the overarching security story where we can zoom in on a couple of supervisory- or deeper questions.

Q: So, the CIO, CTO, and you go in together, right?

A: Yes, and the three of us are aligned, we do five or six slides in there. It's great to be part of the discussion, and the two of them have helped me immensely with the pitching, the storytelling – they sometimes coach me quickly, five minutes before we go to the Board meeting, they could say: it's good, but if you bring it in like this it's even more powerful. That kind of support is priceless.

Q: That's really great, you've really been set up for success by your Board member and your CIO. So, it's all about the collaborative effort and bringing the awareness there, and, of course, you being the subject matter expert there. So, when it comes to really complex questions and they want to poke, you know that you are the one to have the answers for certain elements. And my final question: if we talk about the regulatory developments across Europe and the US, how does it impact your scope and responsibilities and also your necessary interactions with stakeholders?

A: The impact is enormous. When it comes to many of the regulations, we really welcome them, because, if we look at, for example, GDPR – because of the existence of GDPR it has become much easier to get data privacy out there in the rest of the world. We can have debate after debate about the European Union, and, sure, there are the good, the bad and the ugly components to it, but at the same time they're really making regulations that are going to rule the world, and we do welcome those. But yes, it means that there is a tsunami of activities that need to happen right now, some of which will help us massively, but to implement all that, I, for example, need to debate with some of my suppliers about why they're delivering old operating systems as part of their brewing line – in the future I could even sue them for doing that! So, it's going to be about calibration, because they also need our help in figuring out what to do, it's, of course, not done on purpose. I think it will involve a lot of collaboration with our large European companies to deliver state-of-the-art operating systems with our brewery or conveyor belts.

But there are also other things which I cannot foresee at this stage, like the law around the use of AI. Even yesterday we had a debate with the ethics committee about the use of AI. And it's going to be a big question for our company because some of the things are viewed as ethical in some geographies but not in others. So, what will be our ethical lens? Again, there is no good or bad, but in the end, we will have to choose our lens. We are active in a number of countries and are often really doing good for the local communities by raising welfare, uplifting the community spend. But the perspective in some other countries on this might differ. So, I'm welcoming the regulation, and I think that, as a global multinational, some of the low-hanging fruit will be easy, but there's going to be some debate on what's ethical, for sure. It will surely make our life spicy, and there will be debates, which we should have as a company over the edge of technology. It's not going to be easy.

Q: The cultural awareness element, the international component in your role is really becoming more important, right?

A: We always need to keep that lens in mind. Within the European Union, let's not lower our threshold, and be extremely harsh on the non-negotiables while implementing the legislation. At the same time, for the things where we simply don't yet know how they'll be implemented, let's give it more time to give some countries time to adapt. We don't want to stop the conversation.

Q: Great. Can I just try to summarize your approach to the reporting structure again: it doesn't really matter where you are positioned as long as you have the unfiltered capability to talk to the leadership team around the cybersecurity issues; and when working together with the CIO you need a very strong relationship regardless of whether you're reporting to them or working independently. Because you still need them to make things happen.

A: Yes, and another very important element is trust – because I'm not micromanaging my colleagues. I know that if they really have doubts they reach out to me, and if I need to come to them with a question they know it's been well thought-through. So trust is the one thing that's very important to gain on all levels – my level, but also on the level of the audit team and IT team, because if we do something they then know that we're doing it for a very good reason.

When I hire a CIO, having had an experience with a serious security issue is a must

Interview with Martin de Weerdt

CIO at Randstad Global

Q: There often appears to be tension between the priorities of enabling business objectives through technology and maintaining a robust security posture. What have you found to be the specific areas where this tension most clearly manifests itself?

A: Randstad is a people company – we hold a tremendous amount of information on people all over the world, millions of records, so for us security is very, very important. There's always a level of security to which you can get within reason and within financial boundaries. So, I think the key thing is to focus on where the risk is the highest. It all needs to be in balance, and there are things that definitely need to be done immediately, while other things might require a bit more time. Security is a very rapidly changing field, since threat actors invent new approaches every day, and trying to stay ahead of them is an ongoing challenge.

Q: So, it's about balancing priorities?

A: Yes, and I think there needs to be a very sensible conversation between the CISO and the CIO, as well as the business that eventually needs to pay for everything we do – about where we place the priority. What I've learnt from it is that you're never going to be 100% watertight – it's impossible, because there are threats arising every day, there's always something new and we are the leading talent company in many countries all over the world. So, I'm quite sure that there will be areas where we need to work hard to keep up and balance risk and investment very thoughtfully, but this is also a way to be as good as we can be.

Q: What from your perspective are the pros and cons of the CISO reporting to the CIO vs. working as peers?

A: In reality, one does not necessarily exclude the other. The key question is how understanding is the CIO of the CISO role, because mutual respect is crucial. They both have their own agenda, but, at the end of the day, both are working towards creating the best possible IT structure in a secure way. And what that exactly looks like, I think, can be worked out between the CISO and the CIO on both the central and local levels. I don't think that the reporting line is that important, but I think it's crucial that the CISO has an opportunity to raise the alarm if the CIO doesn't want to listen, to make sure there's balance in that relationship.

In our organization the CISO doesn't report to the CEO, but to me; however, they have an open door to the CEO anytime it's necessary, and same for the

> There needs to be avery sensible conversation between the CISO and the CIO, as well as the business that eventually needs to pay for everything we do – about where we place the priority.

Supervisory Board. I've introduced them, and they have a direct link now.

Q: What have you found to be the best practices to effectively address these tensions? How do you go about building that relationship?

A: In the case of our organization, we've created a measurable security strategy – where do we want to be great and where do we want to be good enough at any point in our journey. Of course, the CISO's role is basically to deliver the security strategy, but they need to do it together with my organization. So, once we've jointly established the plan, my job is to make sure that the local CIO organizations actually deliver on the projects we've agreed to improve and our CISO needs to ensure that we deliver what we agreed. So, it's very much a dance for two, a collaboration.

Q: Unfortunately, it doesn't always work out so smoothly, right?

A: I think, if you have a CIO who's diametrically opposed to the CISO, or the other way around, you're never going to be successful, because you'll spend more time debating and creating resistance, than just addressing the issues. And it's not an issue of beliefs or feelings – there's fairly particular measures you can use to check your security, and there's clear choices you can make with regards to the level of security which need to be a necessity. And once the choices are made, it's all a matter of execution, which I think you should do hand in hand.

Q: But from your perspective as a CIO, I think it's important to understand what the CISO is doing, right? Because in the case of your organization the CISO is dealing with a lot more political and global issues, considering there are requirements coming from NIST.

A: The CISO in this case could be called the process owner. What you need to specify is the definition of "good" – and not just in isolation but in cooperation with the rest of the business. That's the CISO's job. And their job is also to measure how well we're doing to achieve that definition of "good". The CIO's job is to deliver the work that's required to achieve that – it's a fairly simple split. And you don't want the CISO to own the security measures because then you get the butcher who's checking their own meat. So, the CIO's organization's job is to deliver upon the definition of "good". The CISO's role is to define "good" and measure how good we really are over time, and if there are any gaps. And then there's the long-term strategic approach. Of course, if there's an issue, or a challenge, or a threat, then the CISO very much controls the process of managing it, reminds us to control the resolution of it where we can, by technical means.

Q: So, make it available.

A: Yes. And I think there is a distinction between the functional hierarchy, which I find to be less of a relevance, and what I would call the hierarchy of expertise which, I think, should prevail, depending on the situation. So, if it is about security, I'll gladly follow our CISO's guidance, and if it's about how we deliver what is required, I presume, they will gladly follow mine. It must be a symbiosis of skills, knowledge, and experience.

Q: Thank you for that! What advice would you give to your fellow CIOs and/or CISOs to best manage this relationship?

A: To simply treat the CISO as your critical best friend. I think working with a CISO is almost like your relationship with your doctor. Either trust the

doctor on medical issues, or do the surgery yourself... You need to trust the person's knowledge, and if you're not willing to do that, then I think you need to find a different CISO, or the organization needs to find a different CIO.

Q: Interesting, because we were talking just before with one of the other interviewees that in the US a couple of CISOs are reporting to the Chief Legal Officer.

A: In that case the CISO becomes almost like a part of the audit committee, and that's, in my opinion, a very risky situation. In our case the CISO is very much part of the IT management team, we're in this together, and it's far more fruitful. It's not just because we share the understanding of the technology but also because we share KPIs. Then they are like a friend, who has an expertise in a particular area much more than having someone who checks your homework.

Q: What governance standards need to be in place to make sure that a cybersecurity framework aligns with organizational goals and industry security requirements?

A: We've created this CISO organization where we have a CISO in every region. They all report to the global CISO, and we pay for them from the central budget – the line of reporting is very clear. They of course work closely with the local CIOs, but they don't necessarily report to anyone other than to the global CISO, which is very deliberate due to the independent role that they need to have. It actually goes against what I just explained to be the dynamics between our CISO and me, but, at our level, we're able to handle that. And we've created a very clear issue escalation process, where we described in detail what needs to be done in case of an emergency.

Q: So, you have implemented a more solid line of reporting - from the local CISOs to the global CISOs.

A: Yes. Just like the local CIOs report to me, the local CISOs report to our global CISO.

Q: So, when we talk about going up a level, what are your best practices when it comes to you, the CIO and the CISO communicating in a unified way to the Board and the Executive Leadership Team?

A: We have a regular quarterly update, which works very well, because it's a mixture of what happens in the world in terms of security – it's basically a refresher about the constant attacks that are happening – and we also give an update about the issues we've had. We talk about how we've handled those issues, and we also mention issues that partners we work with have experienced. Last but not least, we report against our strategic plan on how we want to improve our security posture in line with the NIST model.

> "It helps if you have a CIO who has gone through a security issue at least once - to know how painful it really is. It certainly gave me a better understanding of why security matters.

Q: It means that the CISO really needs to also understand the complexity the CIO is dealing with within the IT organization. On the other hand, the CIO really needs to understand the risk audit side or the process, right?

A: It helps if you have a CIO who has gone through a security issue at least once – to know how painful it really is. It certainly gave me a better understanding of why security matters. Let's put it this way: I would not hire a CIO who has never had a security issue, because it is a daily situation these days.

CISOs are encouraged to do knowledge-sharing among their peers, and the CIOs could really learn that from them!

Interview with Scott Howitt

CISO turned CIO; CDO at UKG; previously SVP and CIO at McAfee Enterprise; previously SVP and CISO at MGM Resorts International

Q: There often appears to be tension between the priorities of enabling business objectives through technology and maintaining a robust security posture. What have you found to be the specific areas where this tension most clearly manifests itself? And what from your perspective are the pros and cons of the CISO reporting to the CIO vs. working as peers? Some people have also included the CTO when talking about how these structures function. But you've been in both seats before – CIO and CISO, so your perspective will be very valuable.

A: If I look at how the world worked 5 -10 years ago, the CIO was a well-established tech leader, and oftentimes the CISO would come in and be yet another person under the CIO's purview. And if you have a CIO who understands and cares about security, that's a fine relationship to have; because, of course, there are conflicting drivers for what the CISO does and what the CIO does, as there are conflicting drivers in every business. But often the CISO has to face a challenge where the CIO gets singularly focused on technology and focused on it for a while. The CISO in the meantime has to worry about everything, and that can cause internal friction because the CIO has a big deliverable, while the CISO has many more things to keep track of. So, at one point when I changed companies I said: I won't work for a CIO. If I'm coming here, I'm going to be a peer, that way there's no conflict. It worked for me, but it can create a different kind of conflict: the CIO and CISO can have even less understanding when it comes to the projects the other one is working on. One of the CIOs I was working with as CISO, which I thought worked really well, said: you can be a CISO, but at some point you'll own capacity management, and network engineering, and database administration too, so you can really learn all of it. So, I think there's value in getting the CIO to be the CISO at times and the CISO to be the CIO. I know that's hard and you're not always going to have leaders that are mature, but, I think, playing different C-suite roles certainly helps.

Q: What are the main things each of them needs to learn about the other's job?

A: Typically, the CIO has a better relationship with the business, they understand the business drivers a little better. The CIO could sit down with the CISO and say:

here's all the controls you're trying to put into place, but let's prioritize against the business outcomes that we're trying to achieve. And most of the times the CISO is a better technologist than the CIO because they have to understand every technology that's in the place, and they typically also understand the interdependencies a little better, because they see those hand-offs: they need to understand generative AI better than anybody in the organization before things get too far in implementing it, they have to understand the Cloud better than anybody and so on, so the CISO is always in the cycle of having to keep up.

Q: And having to do that also gives them a certain advantage.

A: Yes, and you can see it in the differences between the CISO community and the CIO community. CISOs are encouraged to do knowledge-sharing among their peers, so I think you get better collaboration and more rapid innovation out of the CISOs. And the CIOs could really learn those things from them. When you put these two people together, it can be a really strong partnership, but in a lot of cases organizations set them up in a way that it's almost like they purposefully want them to be in conflict. But oversight doesn't mean conflict. Sometimes the Chief Revenue Officer and the Chief Financial Officer don't agree about how the sales motion and revenue recognition should work, and they have to battle it out and come together and decide what's right. But you shouldn't set them up to be in conflict all the time, the same is true for CIO and CISO – they should complement each other. Occasionally they should debate and come up with a better way of doing things. But now it's very much also about the complexity of technology – it's so complex that it's very rare to find somebody who is conversant in all spaces.

Q: Yes, it's overwhelming and moving very fast right now.

A: Yes, because for the CIO, most of what he deals with is fairly well established. So you find the CIO concentrating more on the business, and the CISO more on the technology, because they have to try and figure it all out on their own and pull it all together. But, like I said, you can't have one without the other. If you have a well-seasoned CISO, then the CIO can talk about the business outcomes and the CISO can talk about the risks to the outcomes, and better decisions can be made. So, it's about who are the players that you have – knowing that you organize your business around that. And then I would encourage cross-pollination – the CISO could run

"CISOs are encouraged to do knowledge-sharing among their peers, so I think you get better collaboration and more rapid innovation out of the CISOs. And the CIOs could really learn those things from them.

security and one middleware for the organization. That would make them a little more cross-functional, and same goes for the CIO – they could run certain aspects of security, especially in the three lines of defense mode. The CIO could run operational security, while the CISO runs governance, security and oversight.

Q: Do you have any final remarks with regards to what we've discussed?

A: At the end of the day, all businesses work the same way – you maximize EBITDA, and you grow revenue. That's just the basic premise of how you run a business, and then you figure out what the key levers are to make that happen. So, technology evolves, and just like during the COVID-19 pandemic, the resilient businesses survive and the fragile ones do not. And if you have the ability to be resilient in your role, you will be a fine technologist. At the rate things are changing, your job might be going away soon, but good technologists are resilient.

Align, educate and simplify!

Interview with Felix Voskoboynik

CISO at A.S. Watson Group

Q: There often appears to be tension between the priorities of enabling business objectives through technology and maintaining a robust security posture. What have you found to be the specific areas where this tension most clearly manifests itself? (e.g., Technology, ownership and accountability of technology and delivery, budget priorities and constraints, other?)

A: If you look at the retail space, at the moment it's growing quite fast, and you need to be on top of things as an organization. It is a very competitive business, and what we feel and face when it comes to the constraints which exist between IT departments, marketing departments and security, from a security perspective, it's really challenging to keep up with the business needs moving at such a fast pace. So, they move fast, they want to roll out new projects, there are different innovations, especially when it comes to ways of simplifying things, and all that comes with complications from the security perspective. They're working with many different vendors, and that also makes things complicated – there's a large supply chain with many parties involved, so the scale becomes immense. And then the question from a security perspective is: how do we get a hold and on top of all this? That starts the debate in which there can be tension, and it has to do with the speed...

Q: Would the security prefer things to go slower?

A: No, not so much slower, but security wants it to be done right. And sometimes going fast and having it done right doesn't align. Driving the car really fast is not always the best idea, because you need to see the picture ahead, assess the risk. And in our organization and from the management's perspective, the idea of "faster, faster, faster" is pretty much what's imprinted on everybody's minds today. Because if you're not the one going "faster, faster, faster", somebody else will be. And if you look at a lot of these organizations, you notice that many don't actually have a CISO organization in place, and it tends to be that the IT person is responsible for the security (I met someone who is both HR and IT, holding some responsibility for the organization's security). So, at the end of the day, the scope of cybersecurity in retail is not that large yet. And, the way I see it, it's because a lot of times the management of these businesses think that if they'll add more layers of complexity to the organization, it will be much harder to move on the "faster, faster, faster" route, and somebody else will be faster and get there first.

Q: But what about the risks, haven't there been that many breaches in retail?

A: There have been big breaches in retail, so I do believe that retail is a risky area. But it's a

low-margin industry, and investing in security is costly, so I believe that sometimes businesses would rather take losses, because retail will always come back up – people need to go to the stores and buy products. So, they tend to accept the risks, and sometimes they'll have a breach or lose some data. They'll then pay whatever they need to pay. And a lot of retailers pay ransom.

Q: What from your perspective are the pros and cons of the CISO reporting to the CIO vs. working as peers?

A: If there's to be a proper CISO organization and good cybersecurity then the CISO needs to have that enforcement factor, the upper hand, so he needs to have a direct link to the management and the ability to make these decisions. And, I believe, when you have the CIO in the middle, there can be a conflict of interests, because they're responsible for the budget. And, in their view, the budget needs to be allocated properly to the IT space, to innovate – large projects.

> "When it comes to risk aversion, cybersecurity has a big risk management perspective, and the CIO department will want to work faster, while the security, from their perspective, will be what's causing that slight delay.

And, of course, security will also have considerable budgetary needs, but, if the CISO reports to CIO, they cannot go directly to the CEO, which would also cause a conflict. So, the reporting structure needs to be clear, but in such a case the security might not get the budget it needs. And, I think, when it comes to risk aversion, cybersecurity has a big risk management perspective, and the CIO department will want to work faster, while the security, from their perspective, will be what's causing that slight delay, and this too can be a source for conflict. So, when it comes to budget and risk, these are the main hurdles that the CISO needs to overcome when working closely with the CIO.

Q: Are there any pros, in your view, when CISO reports to CIO?

A: There are, of course, pros too, and I think the main one is that as CISO you're closely connected to the IT department, working in that environment, because, if you look at some other areas, say, data privacy, today that tends to be run by legal – and reporting into legal would be something I see as disadvantageous. They're not really connected to the business; they don't understand how IT works and the issues it's faced with. Without having full awareness of the larger picture, they would deal with the different regulations, controls, and measures. But when the security department is reporting into the IT department and working closely with the CIO, they understand the business, they understand the project, and that way they will have a closer visibility of the strategy. Which is why it's really worth looking at the pros and cons of this: because sometimes it could be that you're the CISO, reporting directly to the CEO, having a large budget, but at the same time you might be investing in things which are not aligned with the strategy, the bigger picture. And, at the end of the day, the bigger picture sits with the CIO, s/he's responsible for the IT strategy, and the security needs to be part of that. When you're fully independent, you're going to have a visibility problem.

Q: What do you see as best practices, from your perspective? How to manage these tensions? For example, do you think that company culture or the personalities of the CIO and CISO can be an important factor?

A: I think it's about finding that common divide. Of course, the CIO won't be an expert in cybersecurity, s/he's going to be missing that education, so it's crucial to provide it. Because that way the CIO will better understand the risks and opportunities in the security area and be able to take responsibility for it.

It's also about finding a way to make cybersecurity engaging and simple. I have seen that many tend to complicate things and make it worse than it could actually be. But if you find a way to align with the CIO, to make it more simple, streamlined, and educational for them and for others in the team, if you form the right relationships with your stakeholders, I think that can really simplify things and make them better. And you don't put fire out with water, right? There's a way, a tactical approach for doing things.

Q: Can you give an example?

A: Yes, it's about not making it more complicated than needed. For example, the CIO department needs to roll out an application for the HR system. The old-school CISO would probably come in with hundreds of controls and insist that we need to do all these things, which will probably take them ages to implement, and it will slow down the project. In this case the CIO will probably say: hold on, we need to think about this, it will cost us a lot of money and a lot of time; we don't have time for this! So, instead of doing that, you as a CISO need to look and see what the key risks are in this application, what could happen? So, you've got a couple of things. There's the employee data, you want the application not to be ransomed, for example. So, you think about the highest risk controls – you need to control the server that the application is sitting on, just be a bit tactical to protect the data. And you find ways to minimize the work necessary, because a lot of the aforementioned activities can be easily automated. So, you cover up the key risks, and then, overtime, you might want to look at the bigger picture, but don't make it too big, don't over-amplify it right away, just control the key risks without slowing down the operation, and let the CIO work fast. So, that's the divide, you can't have everything, but this way you make things work.

Q: Great. And what other advice would you give to fellow CIOs and CISOs to best manage their relationship?

A: Managing this relationship is very much about understanding each other's priorities, and the three processes, which I mentioned earlier – aligning, educating, and simplifying, are also playing an important role in this relationship. Aligning is much about understanding each other's strategic direction, as in: what's my approach? What's your approach? What's your plan? It's important to work in the same environment, the IT department, and when it comes to educating, I think the relationship will improve a lot if and when people understand what you need from them. Because you can go around screaming all day about needing cybersecurity, but if the CIO, your main stakeholder, which is technically your boss, has no idea what you're trying to do – good luck with that! And the streamlining, when it comes to the relationship, it's about finding ways to make it simple, finding ways to meet both my and their objective in a way that we can get our jobs done, to control the risk as much as possible, and to allow the business to operate at the same time. And the relationship will develop from there because it's the confidence factor. Most CIOs need to feel confident that you as CISO are going to help them. But you also need to keep the company secure. And it's ultimately the CIO's responsibility because of the reporting line, so s/he needs to ensure that you are a part of her/his team,

> "It's really worth looking at the pros and cons of this: because sometimes it could be that you're the CISO, reporting directly to the CEO, having a large budget, but at the same time you might be investing in things which are not aligned with the strategy, the bigger picture.

while you also need to do your job. But do it in a way where everyone's aligned with how you do it.

Q: How can you best ensure that Managements and ELTs are informed on enterprise cybersecurity programs and risks?

A: The CIO is very likely not going to be an expert in cybersecurity, so, if s/he has trust in the CISO, if s/he understands what you're trying to achieve and if you both have a good working relationship, the CIO will put you in front of the Management. That's how it is in my case: I report to the CIO, but I'm interacting directly with the Management. But then, once you're there, the important aspect is that you need to be able to sell, and align, and keep everybody informed in the right way. Because if the CIO would see that you're somehow in conflict, that you're reporting about how bad the IT organization is in general, that you're making her/him look bad, s/he's quickly going to pull you down. So, as CISO you need to develop a way to keep the Management aligned, interested, and engaged. And yes, you're reporting to the CIO because that's the structure, but they need to also see you as the leader, as someone with the know-how, who will provide them with the right information. As an example, we have something called "The Heat Map". In "The Heat Map" I'm able to show, across every business unit, where we are from a cybersecurity perspective, what's our risk: are we red, yellow, or green? They don't need to know all the details, just the colors. So, if the CIO sees that the Management likes the idea of what they're presented with, they align and listen; then the confidence factor is there. But you need to build that gradually: no organization will give you that from day one. And this is also the CIO's way of ensuring that you make her/him look good by being able to present credible information to the Management.

Q: I think that's a great example. What about when it comes to governance frameworks, industry standards, and requirements? There are a lot of European and US regulations coming. How are you dealing with that?

A: I think, in retail we experience it a lot less, since we're not exactly critical infrastructure. Though, in case of some of our businesses, like pharmacies for example, we had to stay open during the COVID-19 pandemic. But, while there's, for example, PCI compliance, which is very much focused on protecting customers' information, as well as others, we really deal with it as part of our day-to-day operation. In the cybersecurity space there's not so much focus on the regulations, but if your cybersecurity organization is in order and you're able to show compliance, it's going to be pretty much business as usual.

Q: But you're of course looking at Artificial Intelligence (AI), and you're probably already using that type of technology. And I can imagine that with profiling bias in the systems, you will run into regulations, which are coming from the EU.

A: Yes, this is going to be key for the retail industry, because there are still a lot of questions about what levels AI will reach, how dependent retail will be on it and how customers will perceive it – how much interest will come from customers in this field. But it can also be another potential area of tension between the CIO and the CISO, because if the CIO will see this as an opportunity to run at 100 miles per hour, then the CISO needs to find a way to be there and support them and know how to deal with that. But I think that the level that AI will be used still needs to be determined. There's a lot of AI in the military space and in cybersecurity – it's been around for many years, and we use a lot of AI too to protect our systems and so on, but it still needs to be determined how the customers will require it and how retail space will use it, as well as how that's regulated and controlled. It's surely going to be part of the normal way we approach things, our way of working.

Q: Is there anything more you'd like to add?

A: For me it's all very much built on relationships, simplification, and clear alignment. The CIO won't be an expert in cybersecurity, but s/he needs to know in a simplified way, what you are going to do, how you are going to do it, and, in the end, how you are going to help her/him to deliver what needs to be delivered.

We're all in the people business!

Interview with Emily Heath

Former CISO at Docusign, United Airlines, AECOM; General Partner, Cyberstarts; Board Member

Q: There often appears to be tension between the priorities of enabling business objectives through technology and maintaining a robust security posture. What from your perspective are the pros and cons of the CISO reporting to the CIO vs. working as peers?

A: My general philosophy about reporting structures is that for 90% of my career it never really mattered to me so much about who I reported to because as a CISO your job is to be a business leader first and a security leader second. If you're truly a business leader, you spend time with your business partners and the reporting structure becomes just a formality. The important thing is that you have the space, the freedom to do your job and complete access to everybody you need access to. Somebody with a strong political capital can navigate any organization and being given the freedom to go and do that, to do your job, is more important than any reporting structure.

Q: You said that was 90%. What's the other 10% about?

A: That's the part where the reporting structure starts to matter. In my last role as a CISO I reported to the CEO, and that was very important to me personally – not because of hierarchical influence or anything that made any difference to how I did my job, but because I knew it was going to be my last operating role. I needed to be part of the C-suite because I wanted the opportunity to be on Boards later. The reporting structure can matter a lot when you're at the end of your career and you're looking to be on public boards, because you will get paper-sifted if you've not been either part of the C-suite or at least an SVP. That opens different doors for you because having a seat at the table allows you to see how the whole company operates, and in order to be a well-rounded Board member you can't be a one-trick pony that only knows security; you need to understand the whole business.

Q: What reporting models do you see more often these days?

A: The world of the CIO has changed a lot over the years. I think now we only really see the traditional CIO role in very large organizations. I have seen CIOs become Chief Digital Officers by taking on some of the digital initiatives and some take on larger COO roles and have both the CISO and the CIO report to them. That goes to show that even larger companies are now sometimes pulling the CISO out of the CIO organization, but you need to look at the profile of the company. If it is a very large enterprise company that has a more traditional structure, it's highly likely that the CISO will still report to the CIO. There are now also a lot more CISOs reporting to the legal, which has pros and cons too.

> For 90% of my career it never really mattered to me so much about who I reported to because as a CISO your job is to be a business leader first and a security leader second.

Q: What are these pros and cons, in your opinion?

A: I would say the pro is that when legal tells you to do something you generally do it: you leverage that relationship very carefully and pull those cards out when you need them – and you get things done faster. The con is that the lawyers are not operators, they're not technologists – so they really have very little understanding of what you actually do every day. They're brilliant at what they do, and we need them to be our partners – we need them in the trenches with us, but reporting to them, in my opinion, is inhibiting. Of course, it depends on the company – if the company has been massively breached, often the CISO will report to legal, because legal wants to have a firm eye on everything that's been said and done, but, for the most part, they're just not operators, and they also don't have large budgets, so the security budget for them can often appear excessive.

Q: Indeed. But let's go back to where you said that the role of CIO has changed a lot.

A: The cloud has changed absolutely everything, and business units are a lot more self-sufficient than they've ever been before – they're spinning up their own technology. And when you think about the CIO's role, they're not creating networks anymore like they used to, so the weight of the CIO's role has gone heavily into enterprise applications and PC desktop support – unless you have a large, traditional organization which does a lot of in-house development. But most organizations run on SaaS, so it's more about managing the SaaS relationships. The CIO traditionally used to have a CISO, a head of infrastructure, who also did desktop support, then a leader for enterprise apps, and they probably had a PMO that reported to them. Now it's becoming more prevalent that there's a CISO, CTO and CIO who are all peers. In very large organizations, the CTO used to report to CIO, but that practically doesn't happen anymore. For most part it has split out, and the CISO has more relationships to juggle across the business. What they juggle with the CIO is normally corporate IT stuff – anything to do with the PCs or the corporate cloud or the data that's stored in the SaaS applications, the finance systems, the legal systems, the HR systems. In companies that have CTOs and engineering shops that's a very different relationship for the CISO to manage. And I'd say there's exponentially more headaches between a CISO and a CTO these days than between a CISO and a CIO. And there are a lot of companies which operate like tech companies, because they have their own engineering shops with a separate organization.

Q: So, you could say that CISO's role has become more challenging too.

A: The dials have shifted a lot. CISOs are wearing many hats. The CISO has a very unique vantage point across a company – they're responsible for understanding each business unit, the critical operational processes and the risk it entails. They don't get to just sit in a digital world, or in an IT world anymore, they need to understand how business operates. Even in the technical realms, the landscape has changed a lot. Most CISOs and their teams spend a lot of time on vulnerabilities, and the definition of that word has changed over recent years. People used to think that a vulnerability was just a missing patch – you just had to go and patch it, and that was it. But now, because you've got this completely automated CICD pipeline that's pushing code out all day every day, a vulnerability can be a misconfiguration, a password or a secret that's not rotated, it could be a container that hasn't been set up properly, or something more traditional like a patch. And it is the CISO's job to look across all of them, add business context to them, and to understand what needs to be fixed first. It is not

uncommon for companies to have tens of thousands or hundreds of thousands of vulnerabilities in their environments. So how do you organize that in a way where you inspire somebody else to do something that needs to be done to reduce the risk? As a CISO you are 100% reliant on somebody else doing something for you to be successful in your organization.

Q: And how does one make it work?

A: The CTO organization and the CIO organization, they've got their jobs, they've got code to ship, product to ship, back office and revenue generating initiatives to attend to, and you have to work with them in order to have them drop what they're doing and go fix something. Therefore, the political capital of the CISO in the relationship with theCIO and the CTO is highly important. Those relationships can make or break your security program. If you've got friction there and the CTO says, yes, I see all of those issues, but we're busy right now, there's no way you are going to get things fixed. Security teams don't fix stuff, they're the governance. Historically they used to go to the person running the infrastructure and say: hey, you've got 10,000 vulnerabilities, here's your report, you need to fix them. But that doesn't do anything, when this person is not going to get off their seat. So now we're evolved more, and we say: hey, you've got 10,000 vulnerabilities, these 5,000 are critical or high, but only 20 of them are unique vulnerabilities, and only 10 of them are actively being exploited right now. So, of all these 10,000 you really need to fix only these 10 things for us. Then that's a very different type of conversation. So, there's massive friction with engineering teams that often sit under the CTO, because the first thing engineers do is try and discredit any data that security teams give them. We end-up spending too much time talking about the source of data, instead of talking about what needs to be fixed.

> “
>
> **The CISO has a very unique vantage point across a company – they're responsible for understanding each business unit, the critical operational processes and the risk it entails. They don't get to just sit in a digital world, or in an IT world anymore.**

Q: How do you counter that?

A: You have to take time with these relationships and bring people in when you're buying technology. Let's say we're bringing in a vulnerability scanner. If you don't bring the engineering team along for that ride, the first thing they'll do once you've purchased it and given them the first report, is say: well, why did you buy this one? It doesn't do this and that! They'll discredit everything. So, to avoid that, you have to make them part of the process from the very beginning. And then the security teams work through the output, and it's up to them to curate the data, and tell the story – and you need to make sure you tell the right story. You have to walk the engineering teams through it – and it's a very delicate dance. In the first few months where you're bringing data together, you have to go through and demonstrate to them where your data comes from, why you've made a decision that this or that vulnerability is important. The trust that you build is everything – because the minute they trust you, you're saving a massive amount of time. What happens then is you slowly start to get out of the way. The best implementations are where I implement, I do the dance, I build the trust and then I get my team out of the way, and say – you know what, let me give you access to this. You don't need to wait for me to tell you that something's wrong. You know the methodology – why don't you operate it yourselves? And should you need us, we're absolutely here to help you. Now they're the captain of their own ship! It takes time to build this kind of partnership. You have to meet people where they are and bring them along with you. 90% of what security teams do is all about

people – we're all in the people business. But it takes a certain kind of influencer to make that happen.

Q: At the end of the day a CISO is really influencing and selling ideas and concepts to other stakeholders.

A: The thing for the CISOs to remember is that they should anchor their decision-making and what truly matters to the business. Like I said at the very beginning – the CISO needs to be a business leader first and a security leader second. They need to have a very strong understanding of what matters most to their business, what makes their business operate, how they drive revenue, and parts of technology which are crucial for the business. First three or four months at a company I'm spending large amounts of time with business leaders talking to them about how their business actually works – I need to know the nuts and bolts of what drives us, what drives revenue; if things went down what the impact would be. It's very much about understanding the inner workings of any organization and CISOs often don't take enough time to do that – they jump right at the technology. My five questions are: What matters most? Where is it? How are we protecting it? Where are we most vulnerable? How prepared are we for when something goes wrong? That's how I run a security program. But it all comes back to that very first question. And I think it's part of the storytelling with the CIOs and the CTOs because if you take the time to do that work, they know that you understand them. But a lot of CISOs don't get off on the right foot – they're already discredited because they don't take time to understand the business, and ask questions, and listen. Just go to the CTO and say: Hey, if you were me, what would you be worried about the most? What parts of your infrastructure would you need us to help you protect more than others? But a lot of times it's the wrong wayround – there's a bit too much of dictatorship: here's what we need you to do, go do it, we'll check if you've done it, and we'll tell you if you've not. But that's just not the way to do it. I think it all starts with truly trying to understand your business partners, including the CIO, and the tough job they have keeping their business happy and operating – as a CISO you need to understand them and meet them where they are. All in all, I think it's getting better and there are a lot more business-minded CISOs out there than there ever used to be. Besides, those are the people who will be in high demand for Boards. Public companies are not going to give them a precious Board seat, unless they really have this mindset.

“First three or four months at a company I'm spending large amounts of time with business leaders talking to them about how their business actually works – I need to know the nuts and bolts of what drives us, what drives revenue.

Q: With the increasing regulatory scrutiny in Europe and increasingly across the US, what impact have you seen on the scope of CISO's responsibilities and necessary interactions with other stakeholders to strike an effective balance between security and privacy?

A: Most of the businesses, including their CTOs and CIOs, really lean heavily on CISOs and their legal partners to help them navigate the regulatory issues. I think that CISOs are becoming subject matter experts in the regulatory landscape because it's so embedded in their day-to-day job – the other technology teams are coming to them a lot more, which is a really positive thing. At the same time, I've bumped my head with lawyers quite a lot around the operational side of privacy. We do need lawyers to help us interpret the law and understand the guardrails, so I can go build programs around them and make sure that everybody's doing what needs to be done. But the friction for me comes when lawyers want to take on privacy operations – own the

operational side of privacy, because they tend to want it, but they're not operators and often don't do well with those roles. We need our legal expertise to guide us and to be impartial and counsel us, but they shouldn't be running privacy incidents in my opinion. Privacy is a gray area which sits between security and legal – sometimes the CISO owns it, sometimes legal owns it, sometimes both do, but it's often a hard one to navigate.

Q: What are your views on a Privacy Officer, is that going to be a more prevalent role? And where do you see it sitting ideally?

A: Privacy is not going away, if anything, it's on the rise. I've seen CISOs as Privacy Officers and I've also seen somebody from the legal team be the Privacy Officer. I'm in favor of it being from the legal team – they can help govern that as well, but not take on the operational side, as I've said before. Just because you're a Security Officer or Privacy Officer doesn't mean you have to own everything. As a CISO we don't own everything, we don't want to own everything! We actually want to own less, because the less we own, the more it's embedded in the business. It's a question of accountability versus ownership. You get friction when those parameters are not well-defined.

Q: Yes, on the one hand you don't want to be too rigid about who owns what but also the legal team can help you set barriers – you need to stay within this guardrail to keep the company safe, so they really act almost like a Risk Officer at the end of the day.

A: True, and it's helped me countless times especially where there's new laws and regulations – I need the legal team to help me dissect what that means for us. And once they've done it, it helps also when I need to go talk to the CIO or the CTO and say: these are the new guardrails. They might not agree with that, and I don't necessarily agree with that either, but the legal team has determined this in conjunction with outside counsel, and that's how we must operate, the conversation stops there. So, it's helpful to have them be the overarching guidance and counsel – that actually helps people get the job done. And, to avoid any potential friction, you need to know who owns what – it just takes a bit of time upfront to make sure everybody knows who does what and then you stick to it.

You need to have good storytelling capabilities!

Interview with Aloys Kregting

Former CIO at AkzoNobel; head of Global Enabling Services ASML

Q: There often appears to be tension between the priorities of enabling business objectives through technology and maintaining a robust security posture. What have you found to be the specific areas where this tension most clearly manifests itself?

A: I think you get this tension when the CIO or the CISO are detached from the rest of the organization, from the stakeholders, and start doing too many things in isolation. I use the information pyramid a lot: it shows that IT needs to be aligned with the governance, the organization, the master data, and the business process – the context needs to be made congruent, and then you won't have this problem. So, to make it concrete: if the CISO is not able to explain how relevant the information security risks are for the business propositions, you will have this friction. But if the business really understands the information risks for their own environment, there won't be such tension. Generally, the tension is mostly related to the fact that people have an asymmetrical set of information and background. So, if both the CIO's and the CISO's communication skills, drive, and capabilities are good enough to come out and show themselves, share the risks and make their story an integral part of the overall picture, then there is no issue. You get the misery you deserve, so to speak (laughs).

Q: Now you mainly refer to the CISO's area of expertise and responsibility, but it's also an element when it comes to the CIO post, right?

A: Exactly the same applies in this case. The CIO needs to be able to explain its challenges, for example, that they need to do the maintenance of their ERP landscape or the data center, because nobody will care about it as long as it runs, nobody will otherwise worry about the fact that the CIO has trouble making sure that it runs properly. So, the CIO needs to be able to explain risks. In general, if you're too introverted and have no storytelling capabilities, you will have a very difficult life these days. But to be able to tell a good, compelling story, it needs to have two components: it must be rationally sound and emotionally engaging. If you have that, you will be able to make things work, and it is true for many functions, but surely it applies to both the CIO and the CISO.

Q: You mentioned the information pyramid and governance, and, from what you're saying now, it becomes clear that you take a kind of governance approach to the CIO role. So, it's framed your thinking in the sense that you're doing something like an internal auditor, and that's also an asset when it comes to the alignment of the CIO and the CISO, because the CISO is also very much working from a governance perspective.

A: Absolutely. I've seen and experienced it in the past – when people don't follow that logic, it's very difficult, near impossible to do their job, and they often pursue projects with zero chance of success. And that's the case in many organizations where the governance is very much dispersed. I've experienced it myself in the past, where finance was organized for each business group, and I was tasked with creating a single finance solution. It's not going to work, and you can easily draw parallels with what's happening in the government here in the Netherlands. Every ministry has their own CIO, and they share one tax authority which executes all the demands and functionality requirements from at least seven ministries. They have no chance of creating an integrated system, and, of course, everybody complains about the way the tax authority works, which is actually unfair, because they have some quite brilliant people working there – but they've allowed that seven different sources steer one single authority. It's not aligned and there's no way it can be successful – unless, by accident, all seven ministries give aligned requirements to the tax authorities. What are the chances of that happening?

Q: That's a great example. And what from your perspective are the pros and cons of the CISO reporting to the CIO vs. working as peers?

A: I have a slight preference to CISO reporting to the CIO, but, of course, there are also negative aspects to that. The positive effect of such a reporting line is that your ability to execute on the technical side is much higher. But the complete scope of the CISOs work normally contains three levels: technology, process, and people. These are the lines of defense when it comes to information security. If we look at the level of technology, the best chance for that to function well is when the CISO reports to the CIO – in this scenario they just need to make the decision, as the CIO would never want to be caught in a situation where he's failed to have basic protection in place. If we look at the process level, which is about, for example, how certain things are done, how people throw away papers etc., both types of reporting structure are fine, there is no difference. If we look at the people level, how reporting structure influences the company culture – I would say in this scenario the CISO reporting to the CIO is a bit disadvantageous, and it's better if the CISO would be reporting higher up in the ranks. But both scenarios have pros and cons that even one another out. What I think has more influence are the characters of the two individuals. So, if you have an introverted CIO and also an introverted CISO then the reporting structure makes no difference either way, because

> "If the CISO is not ableto explain how relevant the information security risks are for the business propositions, you will have this friction. But if the business really understands the information risks for their own environment, there won't be such tension.

they won't be able to influence what happens on the people level. When it comes to the process level, they will both withdraw themselves completely into the technology, and do potentially brilliant things which nobody else will know about. So, I would say that a much more powerful mix is where you have a CISO who is very outgoing and can influence the whole company. And that could be perfectly combined with an introverted CIO, who makes sure that the technology works perfectly. And in such a scenario they would work better as peers.

Q: Right, because then the extroverted CISO will help the CIO to have more influence on the culture level?

A: Yes, that way they will work together better on the process and the people level. I have done lots of the

so-called "red team" exercises where you let the security be compromised by ethical hackers. And 100% of the time, without exception, the people level was the weakest link. With social engineering, with pressuring people the ethical hackers always got what they wanted, while the technology usually worked quite well – the intrusion systems were picking up on certain things. So yes, looking back on that I also have to conclude that the most important distinctive factor which could determine how well everything works is to have a CISO who actually knows what they're talking about and knows also how to influence the organization, including the CIO. And then it actually doesn't matter whether they're reporting to the CIO or if they're working as peers.

Q: Do you perhaps have some suggestions for a successful collaboration?

A: It is definitely crucial to follow a common framework. I've often worked with the NIST framework because it perfectly highlights not only the technology side but also the response side, which is a form of process – for example, if it goes wrong, how do you respond to that? Then you can grow in maturity and use the language which everybody can compare to the rest of the market. Plus, the NIST report is something that you can send to, let's say, the key stakeholders on a monthly basis. If you do that you build tension around this which is necessary because often the senior management has a form of plausible deniability. But when you report out of the NIST framework on a monthly basis, you take them along for the journey, and they have no reason to say that they didn't know something. Especially if that's combined with the good storytelling capabilities of the CIO or CISO. Because, again, you have to have a rationally sound story, real content, and you can use the NIST framework for that, but you also need your story to be emotionally engaging. So, you basically need to have impact on both halves of the human brain – then the people will follow. Communication is key – not just because we now work in a global environment, but also because the different components of the risks are really complex. There are so many levels and layers, and parts of the organization and technology where it can go wrong! So, the ability to tell a story in a very simple, engaging way is really an art in itself, and cannot be taken for granted.

Q: Simplicity does work really well, but it's not in itself simple at all!?

A: Yes, and the challenge is to find CISOs who not only know security well but can also tell a compelling story. It's a rare species, I would say.

Q: But things are getting better! What advice would you give to your fellow CIOs and CISOs to best manage this relationship?

A: Even if the CISO reports to the CIO, there needs to be a clear demarcation on who does what. So, for example, just like an internal audit director, the CISO needs to have a form of independence to not be overruled by the CIO for budget reasons or others that would be risky. So, there must be a direct link between the CISO and the CFO, as well as the chairman of the audit committee, for example, so that the independence of the CISO is safeguarded.

> "I have a slight preference to CISO reporting to the CIO, but, of course, there are also negative aspects to that. The positive effect of such a reporting line is that your ability to execute on the technical side is much higher.

Q: What about managing the relationship, the personal side of it – what would you do and what would you expect from the CISO towards you? What has worked well in the past when you're working with the CISOs?

A: I think, just like with every working relationship, you need to understand what makes them tick. How do they want to develop themselves? Just like with every direct report and a colleague, give them

respect, give them constructive feedback, help them develop. Working with CISOs in the past I've had to spend a lot of time working on the communication, and getting them out of the dark, so to speak, because some of them really prefer to work in isolation, doing the brilliant things nobody knows anything about. So, that requires some work, helping them in that journey.

Q: So, I think, what you're saying is that you could also challenge them and challenge yourself as well in the process, right?

A: Definitely.

Q: My final question is related to the collective communication and messaging towards the Board: what have you found to be best practices for CIOs and CISOs to collectively communicate an unified message about the security program and cyber risks to the Board and ELT?

A: It's similar – help them by taking the rest of the organization along on the journey, which means different types of communication. For example, one piece of advice I've given to CISOs, and which has actually worked quite well, is to use real incidents in their storytelling. As a CIO, I once experienced a situation where we were having a sales meeting and the whole sales team would get new laptops while being off-site. So, one of the IT team members would drive to that site the evening before and would install 26 laptops the next morning, but they got stolen from the boot of his car. And then we can remind everyone that the corporate policy dictates to never leave the laptop unsupervised, or in the boot of your car. Or somebody went to China and their laptop was ripped by the Chinese government when they used the Wi-Fi of a building. Always use real examples, make it very real, rather than talk about vague, generic security risks – make them very specific to your company. Many companies don't like to do this because there's this natural tendency to sweep information security incidents under the carpet, pretending they didn't happen, but I think it's much better, much more powerful to be more open about them. Of course, we need to respect privacy in that too, but sweeping everything under the carpet – that's unhealthy.

Q: Thank you, that's very insightful. Do you have any final remarks?

A: Make sure that the CISOs are not IT security officers, but really information security officers – they need to consider things on paper, on whiteboards, on social media, not just in the ERP systems and the R&D environment. They really need to think about innovation in the broadest sense of security.

Shifting the CISO role outside of the CIO has been a game changer to/for me!

Interview with a US-based multi-time CISO

Who works for a multi-billion organization in the industrial sector

Q: There often appears to be tension between the priorities of enabling business objectives through technology and maintaining a robust security posture. What have you found to be the specific areas where this tension most clearly manifests itself?

A: To answer that I think I need to go back to what CISOs typically look at, which is the CIA triad. When you look at it from the CISO's perspective, there's confidentiality, which is the top thing you need to protect at all times. A very close second is integrity, and the third, which is, of course not unimportant, is availability. For the CIO typically availability becomes the most important factor, integrity – a close second, while confidentiality, again, is not unimportant, but becomes the third. So, there's a kind of natural tension between the two roles, where the CISO is responsible for ensuring that information is appropriately protected and reviewed, and appropriately accessed and used, while the CIO is responsible for making sure that information is available, easy to consume, and that it enables the business. Both are, of course, complementing the same goal: to deliver an efficient service for the organization; they look at how the organization uses and consumes data, and do so in a manner that supports business objectives, but there's a kind of false sense of conflict between the two.

Q: Does this sense of conflicting priorities often manifest, in your view?

A: The way I see it there's three generations of C-suite within information technology and cybersecurity spaces. You have the first one, which was very much business and cost-focused, which would see IT more like a cost center, but, of course, information is not a cost, it's an asset to the organization. With the second one, it all became about whatever the business wanted, as quickly as the business wanted, however the business wanted it. And those were, I think, the kind of sales and marketing CIOs and CISOs who were focused on making everybody happy, but that's a short-sighted approach. And the third generation, which I see popping up more and more and to which I selfishly think I fall, is one that takes a balanced approach – because we need to understand what those risks are both from a CIO and a CISO perspective. We need to understand the business value of something and what's the risk that's taken, and an informed decision needs to be made by the appropriate authority. And that's what I've seen to be successful, and such an approach has been effective for me too in multiple organizations.

Q: Can you also expand a bit on the false sense of conflict when it comes to the components of the CIA triad?

> We need to understand the business value of something and what's the risk that's taken, and an informed decision needs to be made by theappropriate authority.

A: It seems that the CIOs often think that the CISOs are opposed to them, and there's that concept of the Culture of No, and one of the things I've been advocating for my entire career is that it's not a "no", it's "know" – we want awareness; we want to have an understanding of what risk is out there. And so there's a kind of false conflict that's presented where the CIO is being hindered by the CISO in some way, and the CISO is always presented as either hindering the CIO's organization, or being ineffectual because they don't get the support or the buy-in that they need, while actually they're both working towards the same objective. I don't know of any CISO that says: I'd like to see all the services be unavailable more often, or a CIO who says: I wish I could make things less secure. Everyone has the same objectives; the priority and the waiting shift a bit, but there's a common ground that can be negotiated. And that's where I see success as opposed to entrenched positions.

Q: Let's talk a bit about the reporting structure. You as a CISO have been reporting to the CIO in the past, but over the last year or so you've been working in an organization where you're reporting into legal and working with the CIO as your peer. There are of course different organizational cultures and different personalities that can always come into play, but what have you found to be the most prominent differences with regard to the different reporting structures?

A: The most significant is that there's a balance that was not there before. Previously, when reporting to a CIO, even the best of CIOs, who had the right intention and the right approach, security was still only one aspect of their job across the spectrum. If they looked at where they had to meet, and they had to choose to sacrifice security to meet a compliance need, for instance, or to meet a legal demand or operations requirement to generate more growth, all of it was balanced over internal requirements. The external requests would always have more weight than internal requests because the people making them are the people who provide direct feedback on the CIO's performance and can directly impact their success at the organization. Everything below them can be to some extent controlled and managed because it is their responsibility. Therefore shifting the CISO role outside of the CIO to me has been a game-changer – both in terms of balancing the conversation between IT personnel, objectives, and approaches, and the risk profile of the enterprise, which gets a much more prominent voice that way, but also just in terms of shifting security from being something that can be internally prioritized or de-prioritized according to need to it being ranked on the same platform and to the same degree as operational growth and delivering new infrastructure at plants. It all must come into the same discussion, rather than being part of that kind of background IT approach that often gets deprioritized.

Q: In the past few have been in positions to report to the CIO. Considering that one CIO to the next might have had different ways of viewing security and different styles when it comes to how they operate, what have you found to be some of the best practices, the key factors in successfully managing that relationship?

A: The single most important thing I've always done is establish an exception process so that there's a consistent, informed way to approach and to document a risk. So, if there really is an operational need that trumps a security need, which happens frequently, we make an informed decision and move forward. But without that governance approach, without that consistent method of saying: this is how we will deviate from the ideal security state, or, at least, our desired security state, you really end up with a lot more conflicts. With that structured approach all the discussions become much easier

because, as a simple example, our password policy says we need 20 characters, and there's an application that can only do eight characters, and it's going to take us $5 million to do that, or we can apply some additional controls. It's a much simpler decision when you can go to a table and say: okay, that means that the CFO needs to sign off on this risk because of the financial impacts, but we can move forward, rather than entrenching positions of the CIO or IT saying - we have to do this, this is untenable, you're being unreasonable, and the CISO is saying – I don't have to address this challenge, I have to be compliant. Then you start getting a "he said, she said", an adversarial position in boardroom and executive discussions, and that's never helpful.

Q: I hear that first and foremost you want to establish some good governance practices and documentation, set those standards so you can minimize emotions and opinions as much as possible and make things more objective and fact-based just so, at least, if nothing else, you can minimize some of the noise and friction that way.

A: Absolutely. If you look at the program I've established and am using for the last four organizations, the factors that go into the assessment criteria are all clearly defined and quantifiable. So, when a decision is made, if there's a concern that it needs to go through the CEO, versus the CFO, versus the CIO, versus another senior manager, that decision is driven purely by the data points, and the data points related to what we discuss and work on, not with regards to who has the authority in the organization. It's predefined ahead of time, so we can avoid conflict. And then we're back to discussing where something falls on a chart, and not what we want to do as a company. That really helps get us to the minimum point of conflict, which is simply the individual who makes the choice.

Q: Another theme that has come up in discussions about the reporting structure and governance, is that some organizations have a CTO, whose job relates more to infrastructure and product orientation. So, all of a sudden you have not only the internal infrastructure and technology, but also customer-facing technology, which adds another element to the mix. Have you experienced such a set-up and does that add any more friction or complexity, or is it just another stakeholder who needs to be involved in the governance process?

A: No, for me that's the exact same stakeholder, whether it's CIO, CTO or a CEO, the difference is what they have the authority to approve. Treating all as standard inputs and standard outputs, impersonal as it may sound, actually allows for more personal relationships, because then you're having conversations about risk profiles, rather than what somebody wants to do or doesn't want to do.

Q: When you were reporting to a CIO, how much did that reporting structure impact, if at all, your direct communications with the Board of Directors, compared to the way it is now that you're on the same level as a CIO? Did it have an impact on how you were able to communicate the risks to the organization?

A: There are two factors there. First is that I've had the good fortune throughout my career to always have direct access to the Board – even when I reported to the CIO, we would both be in the room having a conversation with them. So, if the Board had a direct question, they could ask me, and they would always get a straight answer. The big thing that's changed is, when I used to report to the CIO, I would prepare all my presentation decks, and the data to back it all up, and present that to the CIO. So, if there

> "There's a kind of false conflict that's presented where the CIO is being hindered by the CISO in some way, and the CISO is always presented as either hindering the CIO's organization, or being ineffectual.

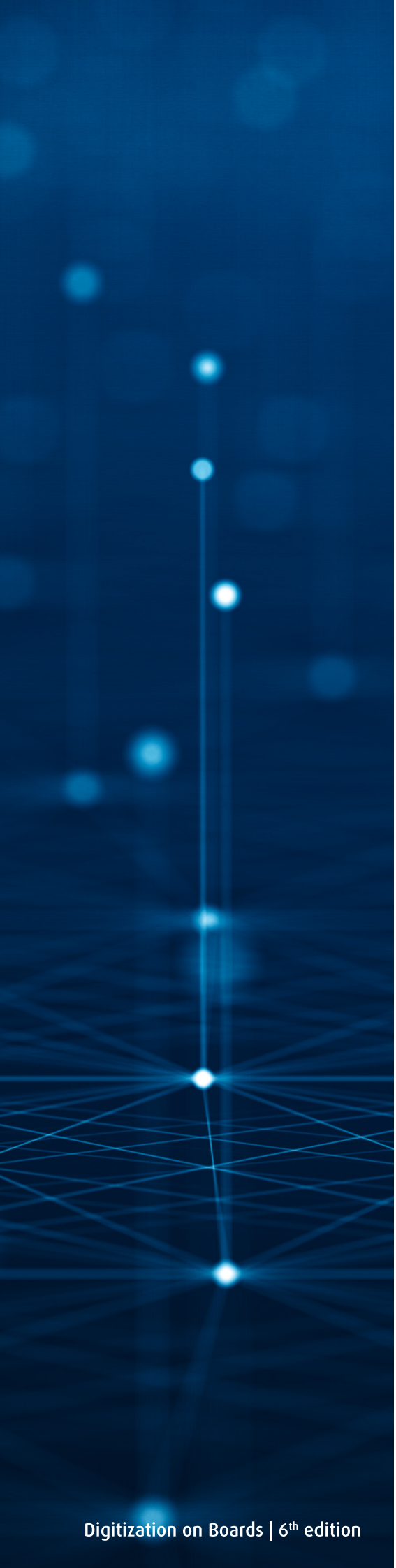
was any point of conflict, which, again, I've typically been lucky not to have, and if something was changed or adjusted, I had at least some auditable record. So, I always had it in the back of my mind that I need to be aware of how this is going to be presented. Today I get to share with everybody beforehand, and everyone's aware of the metrics, aware of the calculations and wherever the data sources come from, which means everyone has an equal opportunity to control that narrative by taking appropriate action.

Q: The privacy laws are expanding even here, in the US, so they seem to be impacting pretty much every organization to different degrees. Have the conversations around privacy been relevant for your organization, and your and the CIO's work? What has been the impact?

A: It's very significant. I established the privacy program in a company I worked for in 2016, worked on our GDPR compliance and got us into an operational state; that then became a kind of standard direction. When I moved to another company I worked very closely with the Legal Officer and the Chief Compliance Officer in selecting who became the Chief Privacy Officer, working through that entire process, building up the training and the awareness, and, of course, implementing the controls. Now, in my current role I've been working very closely with the Chief Privacy Officer: we're building out a new privacy program, and I'm heavily involved in that. Privacy is a foundational component, and it really comes down to understanding the way data is used. People often look at privacy in terms of – this is my information, rather than – what will happen to it, how will it be used? And those are slightly different concepts. So, a lot of what we do is look at how information is stored. Does it still pass as private information? And how can we minimize the flow of that information – that's very much in the realm of CISO's duties. It's all very much aligned to security programs, and I see myself involved in privacy on a daily basis.

Q: Do you have any final suggestions, advice to your peer group out there, the CIO and CISO community?

A: Open governance and communication is always the first step – you have to be communicating, you have to be collaborating. One of the things I preach to my teams and in development sessions with my future leaders, is that it's more important to find common ground and agree and move forward together, than be right about the individual item – because that way you'll get further in the long run. So, make compromises, make them often, negotiate, be aware of what you're doing and document it, but really take a collaborative approach, because anything else is just shooting yourself in the foot. There's another thing I keep seeing in the relationship between CISOs and CIOs – the tension in it often comes from a lack of investment historically. In places where there are more mature organizations, I don't typically see the same degree of friction and the CIOs and CISOs are more aligned because they built the infrastructure, processes and foundation together to be successful, they've included security into that. So, there's a much lower level of friction and much lower barrier of entry for new services. The organizations where I see the most challenge are places like manufacturing, where there's traditionally been hesitancy to commit resources to build out those kinds of core foundations, to create the more dynamic and agile computing infrastructures. There tends to be conflict around information security, because IT is trying to use its very limited resources to address very urgently presented business needs, and information security is always trying to catch up to that, always trying to add things to that, which is perceived as an additional cost. Whereas if we spend the time building the foundation, spend a few years, which is, of course, a massive undertaking, prioritizing and building foundations that are agile and scalable, it becomes much, much easier to work together going forward. And it's really a question of how much time you dedicate to building that – and if you do it, you can be agile and efficient going forward, and the pain disappears.



About Amrop's Digital Practice

Amrop's Global Digital Practice combines deep sectoral knowledge with local market expertise, backed by global resources and integrated cross-border key account management. We have long-term partnerships with our clients on the digital transformation journey. Not only delivering critical assets – the Leaders For What's Next – but in digital competency assessment for Boards and management teams, implementing succession planning and talent management solutions.

We have experience in these sectors and key functions:

- Cloud, Software, SaaS, Apps
- AI/Machine Learning & Data Analytics
- Chief Information Officers (CIO), Chief Digital Officers (CDO) and Digital NEDs
- Cyber Information Security Officers (CISO)
- e-Commerce
- Scale-up, Venture Capital, Private Equity
- Media & Entertainment
- Fintech
- Telecom
- Leadership Advisory, Digital
- Chief Revenue Officers (CRO), Chief Sales Officers (CSO), Sales Executives

Looking for Advice?

If we can help you with any further information or can be of assistance to your organization, don't hesitate to contact any of the members of Amrop's Global Digital Practice for a dialogue on your Technology, IT and Digital priorities or any struggles you may have transforming your organization! We are more than happy to offer advice and share our experience in these sectors, as well as put together a team, if necessary, to help you create sustainable success!

Reach out to us or contact the Amrop's Global Digital Practice member in your country!

digital.practice@amrop.com

www.amrop.com/industries/technology

Amrop's Digital Team

Every organization requires a customized solution, and customization requires specialists. Members of Amrop's Global Digital Practice have the capability to serve you locally, globally and overseas.

Job Voorhoeve
Partner, Global Practice Leader - Digital
Netherlands

Miloš Đurković
Managing Partner
Serbia

Paulo Aziz Nader
Partner
Brazil

Mikael Norr
Managing Partner
Sweden

Bo Ekelund
Partner
Sweden

İrem Yüksel Göğüş
Managing Partner
Turkiye

Christian G. Hirsch
Managing Partner
Germany

Caroline Søeborg Ahlefeldt
Partner
Denmark

Jesper Brøckner Nielsen
Partner
Denmark

Florian Jummrich
Partner
Germany

Mika Suortti
Managing Partner
Finland

Jan Kirkerud
Partner
Norway

Oana Ciornei
Managing Partner, Member of the Global Board
Romania

Fiona Getty
Partner
Australia

Sampo Syväoja
Partner
Finland

Paolo Clemente
Partner
Italy

Matej Taliga
Partner
Slovakia

Daniëlle van der Horst
Assistant
Netherlands

Jamal Khan
Managing Partner
Australia

Ewa Baranek
Partner
Poland

Viesturs Liegis
Managing Partner
Ukraine

Manuel Barthe
Partner
France

Samiron Ghoshal
Partner
India

Luke Henningsen
Partner
Australia

Ebru Esmen Mete
Partner
Turkiye

Gabriela Nguyen-Groza
Managing Partner
Luxembourg

Yannis Zafeiropoulos
Senior Consultant
Greece

Agra Liege-Dolezko
Marketing
Netherlands

Benoit Lison
Managing Partner and Global Practice Leader - Professional Services
Belgium

Steve Meynen
Partner
Belgium

About IT, Cybersecurity & Risk Executive Recruiting at JM Search

Top performing IT executives are in high demand and many companies are struggling to secure talent to fill critical roles. Likewise, the need for security and risk executives has never been so high. Cybersecurity attacks from a variety of threat actors are increasing at a rapid speed, forcing companies of all sizes to defend against threats that are becoming more widespread and commonplace by the day.

That's why at JM Search, we've built a highly experienced and deeply connected team of IT and information security recruiting experts dedicated to matching exceptional technology and data leaders with high-growth and transformative businesses across private equity-backed, private, and public companies.

Likewise, our specialized recruiting team includes former cybersecurity CEOs and other deeply experienced technology search consultants who know first-hand the critical importance of getting it right when hiring executives to lead security and risk functions and are dedicated to supporting the ever-evolving needs of our clients. Since 1980, we've expected nothing less and neither should you.

Looking for Advice?

As the number of jobs in the space continues to outpace the supply of professionals, organizations across all industries partner with JM Search to access our extensive networks of top-flight CIO, CISO and other security executives with proven track records of leading businesses through dynamic, rapidly changing environments.

Reach out to our IT, Cybersecurity & Risk Executive Recruiters at JM Search!

https://jmsearch.com/function/technology-product-data/

https://jmsearch.com/function/security-risk/

IT and Cybersecurity Executive Search Recruiters at JM Search

At JM Search, we've carefully built a considerable, highly experienced, and deeply connected team that is collaborative and accountable, by design and by culture.

Jamey Cummings
Partner

Bill Hogenauer
Partner

Ben Millrood
Partner

Chris Radigan
Partner

Ryan Gilligan
Principal

Doug Bower
Principal

Brent Lamb
Principal

Notes

Notes

Credits

We warmly thank all the participants, CIOs and CISOs who took their time to share their experiences, perceptions and observations with us and our readers. We also thank all members of Amrop's Digital Practice and IT and Cybersecurity Executive Search Recruiters at JM Search who were involved in the brainstorming of ideas, and are always striving for excellence in their daily IT and Cybersecurity recruitment work.

Data Analysis, report writing and study design by Agra Liege-Dolezko, Jamey Cummings and Job Voorhoeve.

About Amrop

With over 60 offices in all world regions, Amrop is a trusted advisor in Executive Search, Leadership and Board Advisory. It is the largest partnership of its kind. Amrop advises the world's most dynamic organizations on finding and positioning Leaders For What's Next: top talent, adept at working across borders in markets around the world. Over the past 45 years, we have built a reputation for our focus on quality, talent and agility. At the heart of our business is a deep connection with our clients. Our goal is simple - to help our clients shape sustainable success and be prepared for 'what's next'.

Our consultants blend entrepreneurship with solid business experience and are able to recognize the opportunities and challenges you face. Our partnership is distinctive, created over many years by bringing together top local independent search firms across the world. Our strength lies in our collective expertise and track record, rooted in local responsibility and spanning a global network of senior consultants. All united in a shared framework: our Mission, Vision, Values and Code of Professional Practice.

About JM Search

JM Search is the leading retained executive search firm for private equity, and other growth-oriented private and public organizations.

With over 40 years of experience, our partners are immersed in your search every step of the way, supported by a passionate, cohesive team of recruiting experts. With deep sector and functional-specific expertise, our partners have built expansive professional networks from decades of firsthand experience to ensure the best possible outcomes for our clients and their businesses.