Solutions

The CISOs' New Dawn

An in-depth study of the year that changed everything. By the CISOs who were there.

WITH secure

Contents

Introduction

For many organizations faced with a sudden need to have their staff work from home in 2020, the CISO and their team became unlikely – or perhaps overdue – heroes.

Cyber security stopped being ‘just’ about preventing bad things. It helped companies survive – sometimes even thrive – by equipping organizations with the tools needed to stay productive under extraordinary conditions.

In mid-2020, WithSecure™ Countercept asked Omnisperience to interview CISOs around the world about their roles. What follows – the output of these conversations – is an unfiltered response, direct from 28 senior information security officers in the US, UK and Europe. The CISOs took part in lengthy, qualitative discussions that explored their challenges, hopes, fears and plans. The insights they shared paint a portrait of a group of experts getting to grips with immediate problems – and coming to terms with the rapid development of a role that is only 27 years old1.

Chapter 1 – An effective security leader: the year that changed it all

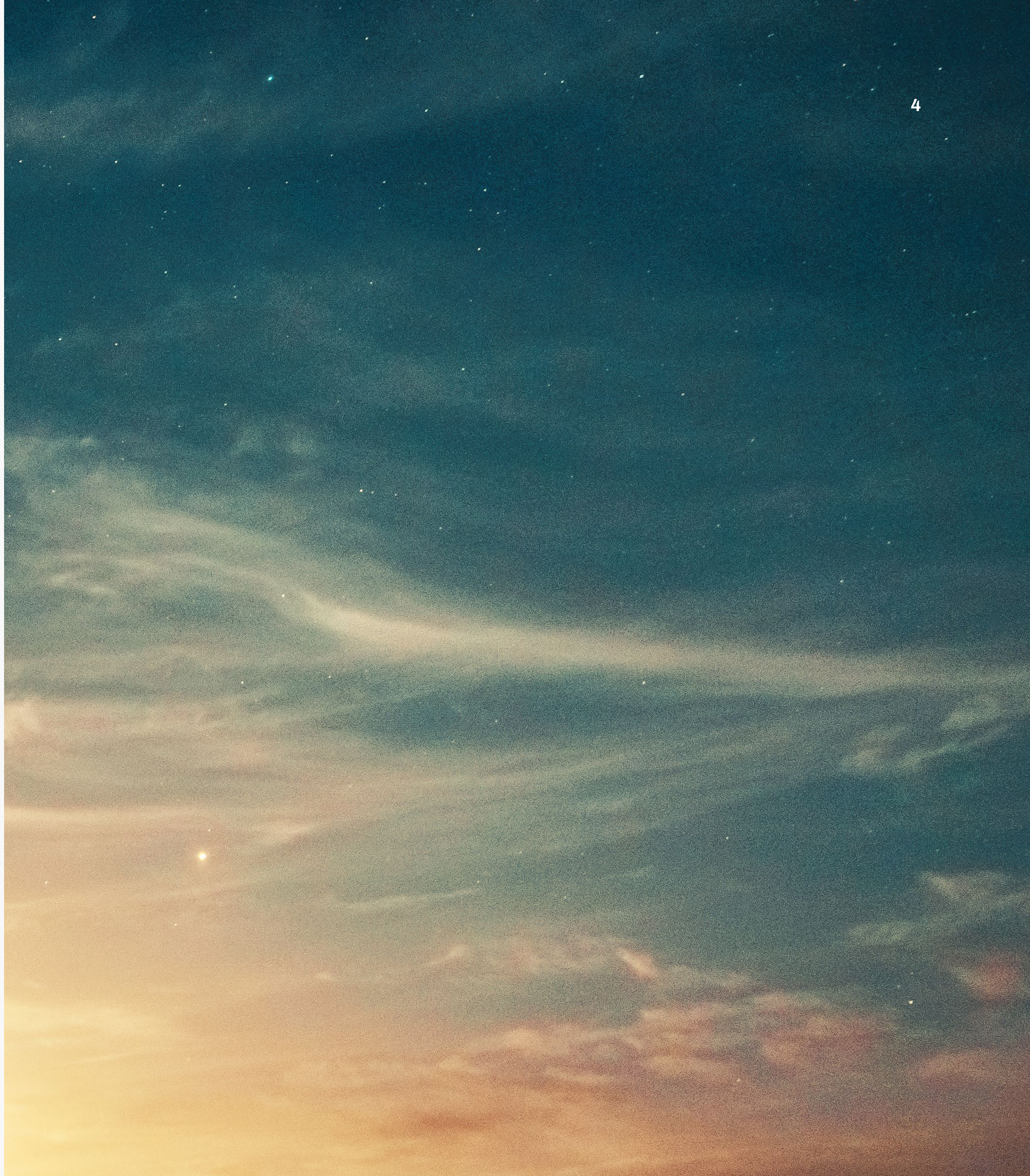
The Chief Information Security Officer’s (CISO’s) role has grown and matured fast from a standing start less than 30 years ago. Lately, this progress has accelerated.

Recent events have thrust information security – along with CISOs, their teams and suppliers – into the spotlight, and suddenly cyber professionals have started getting invites to all the right parties.

But this ascent to mainstream business relevance, trust and recognition comes with several burdens – not least changing priorities, a need to develop or refine soft skills, and a host of fresh responsibilities and accountabilities.

To maintain effectiveness as an operational CISO is, under current circumstances, one of the most challenging responsibilities they face. Recent events, it seems, have added further challenges: embracing and adapting to new pressures, requirements and requests that stretch the CISO’s traditional roles in several directions at once. This brave new world is one littered with personal, political and human challenges, as well as the technical ones.

In this chapter, our panel outline how their roles have changed over the past 12-18 months.



Question 1

Have your role's responsibilities changed in the past 12-18 months, and have you been required to learn new skills?

Have your role's responsibilities changed in the past 12-18 months, and have you been required to learn new skills?

Since the first cyber security officer was hired by Citi Corporation in 1994, the role of the CISO has matured significantly. The events of 2020 have demonstrated just how adept CISOs are at responding to the challenges to business operations and the increased need to embrace a wider security protection landscape.

While activities undertaken and skills employed by CISOs haven't changed dramatically over the past 18 months, their responsibilities and priorities have shifted away from security executed as an isolated practice to becoming coupled with day-to-day operations. CISOs consistently highlighted key change points as: 'risk' becoming the foremost responsibility, and the balance between technical capability and the ability/application to apply 'soft' skills in the role.

There are similarities of role changes and responsibilities on both sides of the Atlantic – any major differences are evident when it comes to organization size.

The size of a company is often a more effective predictor of the role of its CISO than the risks the organization faces. Cyber security leads for smaller firms are certainly more multidisciplinary beasts – and may even be the IT director. They must tackle roles that also touch on IT operations, help desk, as well as security. Bigger organizations mean more resources and the opportunity to specialize, ensuring the CISO stays focused on mitigating cyber security risks and remaining engaged with the senior management team.

The previous 18 months have compelled CISOs to strike an effective balance between – and alignment of – technical and business skills. CISOs of companies that handle volumes of personal data will be acutely aware of the responsibilities that come with this.

The same applies to those undertaking regulated activities: non-compliant organizations face significant exposure sentences2 for company principals in some cases. US (59%) and European (57%) CISOs see a clear increase in their role's responsibilities related to regulation and privacy. The potential penalties that come with some regulatory regimes create a powerful incentive for CISOs to strive for alignment of cyber security risks within an organization's enterprise risk management (ERM) frameworks.

The lack of consistent nationwide regulation and privacy controls in the US has added to the complexity of many of our respondents' lives. They must stay abreast of incoming state-level regulation such as the California Consumer Privacy Act (CCPA) and Illinois' Biometric Information Privacy Act (BIPA), as well as Federal Trade Commission (FTC) and industry-specific laws. In contrast, with a single source of regulation, our European CISOs said they had a slightly easier time implementing EU laws across multiple member states. Taking personal data laws as an example, under the EU's General Data Protection Regulation (GDPR), CISOs can proceed promptly to practical implementation. It's worth noting that this single source is often transposed into national laws in a slightly variable manner, and that supervisory offices often have different procedures.

Many of the CISOs have global responsibilities, highlighting that the Asia Pacific region has seen increased data protection enforcement: South Korea's Personal Information Protection Act (PIPA), Japan's Act on the Protection of Personal Information (APPI) and My Number, as well as the forthcoming Personal Data Protection Law (PDPL) in China all feature regular audits, with sizable penalties imposed for lack of compliance.

The increased responsibilities seen by our panel told us that the events of 2020 placed increased focus on business continuity planning (BCP) policies and their relation to the organization, operation and safety of the business. The CISOs we spoke with said they had increased their application of business impact analysis (BIA), taking a view of the dependencies that business has on technology and then appraising the necessary security controls.

Many CISOs we spoke with told us that their role was increasingly viewed by their organization as less of an 'internal security consultant,' focused on the protection of the organization's assets and people, and more as an 'operational security officer.' This has revealed a new challenge: peers within the organization assume CISOs have considered the needs of every department, without taking responsibility themselves to understand the implications of cyber security.

> **" It's about risk, and CISOs need to not make decisions that sit in other peoples' responsibilities."**
>
> Matt Stamper, CISO, Evotek

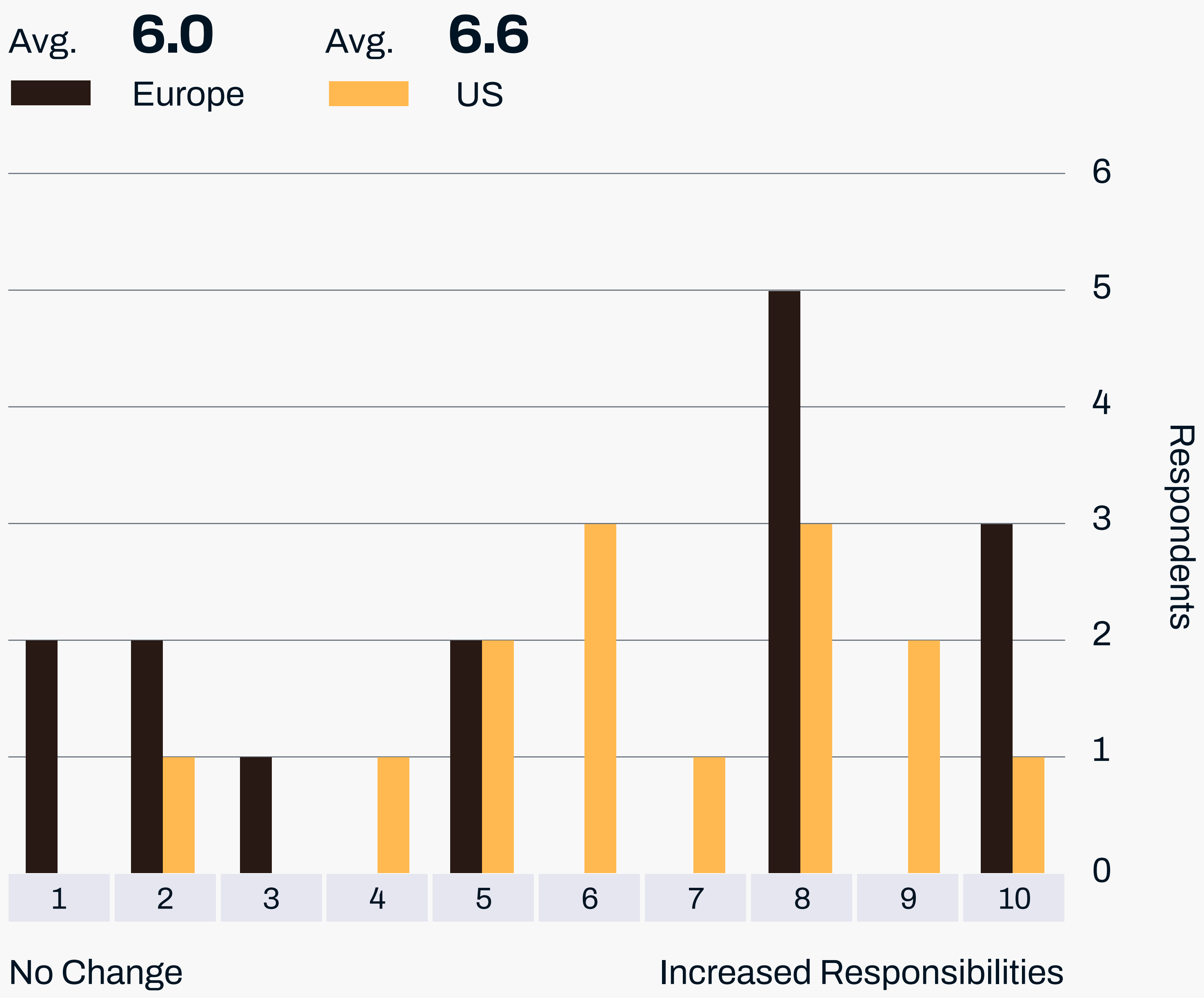
A glaring worry from many respondents was that the CISO role is not given the level of importance as a critical business function – continuing to be viewed as a middle-management function and, as such, could be 'crushed' unless they can be valued as advisors to the CEO. This could mean that the future of the CISO ends up combined within the role of a data protection officer (DPO), specific industry sector specialist (fraud, SCADA, etc.), or an operational role.

Our interviewees recognized that the security landscape has broadened, and that the expertise of cyber criminals has increased both in capability and volume. This has mandated that they keep close to the battleground and continually look to understand new and evolved threats.

Our panel are fully aware that cyber security specialists are a rare commodity, and this scarcity stretches from school and higher education leavers all the way through to industry veterans. In turn, this has obliged them to step up their skills when it comes to talent management, reflecting a growing imperative to enhance and retain their existing workforce – or risk losing knowledge, talent and experience that can be difficult to replace.

Depending on the size of the companies involved, our cyber leaders were being asked to contribute more at a business – rather than solely technical – level. A drive for cost efficiencies, increased capability and improved customer experience has encouraged or obliged CISOs to educate themselves outside the scope of cyber security, with the assistance of peers in understanding how their organization needs to compete in the digital market to serve existing and future customers. A large proportion of the CISOs we spoke with suggested this has compelled them to view cloud in a more positive light for both IT infrastructure and business applications – something of a must, given the surging importance of cloud to the success of many organizations.

Have your role's responsibilities changed in the past 12-18 months?



> " **What is starting to change is the business is starting to take more recognition and ask questions. As CISOs are used to talking tech, they are being asked to talk more business-speak."**

David Lello, CISO, Burning Tree

Question 2

Have you needed to upskill around cloud security, device sprawl, RPA, AI, ML, analytics, threat intelligence, etc?

Have you needed to upskill around cloud security, device sprawl, rpa, ai, ml, analytics, threat intelligence, etc?

Our interview subjects overwhelmingly (71%) said they had spent time reading up on emerging (digital) technologies. One of the more interesting topics: operational technology (OT) in manufacturing industries targeted as possible attack surfaces has been a keen interest for organizations, but also supply chain evolution and communication architectures used to run a business. There was little-to-no feedback regarding the need to understand the day-to-day impact from Internet of Things (IoT) devices. IoT seems to be a new territory for security teams and our panel acknowledged the need to ensure that they can interpret the signal/noise levels these devices generate.

The majority of CISOs are avid readers, using books and reports to widen their knowledge and increase the relevance of a subject matter, prior to considering technology or policy in their business. They revealed a variety of topics covering privacy, DevSecOps, incident response, preparation modeling, and data visualization.

The desire for continuous improvement also includes mapping new frameworks such as NIST and MITRE ATT&CK. Many of the CISOs we spoke with worried about failing to stay current – and the potential impact of that on their career. This concern is not just focused on technological change but also the cyber security implications for regulation and privacy that are key boardroom concerns.

The consistency from CISOs regarding their need to increase their familiarity and knowledge about cloud was a continual surprise to the author. In the past, many CISOs have regarded cloud as a loss of control, but this has changed dramatically. Much of the urge to understand cloud technologies was conveyed in three pragmatic areas:

1. The need to maintain the highest levels of threat detection and mitigation as attacker vectors grow in complexity, while reaping cost and operational benefits provided alongside a variety of managed security and cloud service outsourcing partners;
2. A realistic desire to appreciate the value of cloud as an architecture that will increase with the growth in digital applications;
3. Apply insights gained from the first two areas as they focus on cloud security technologies that can consistently enforce how to secure data and their operations outside of traditional boundaries.

> **“ We are diving heavily into security analytics to make informed decisions. In the past it was responding to alerts from SIEM, but we are now looking at a new skill set for analytics.”**

Leo Cronin, CSO, Cincinnati Bell

> **“ The way cloud works is different, so you need to go [back] to basics and get new skills.”**

Dave Thomas, Director of Security & Privacy Engineering, GoCardless

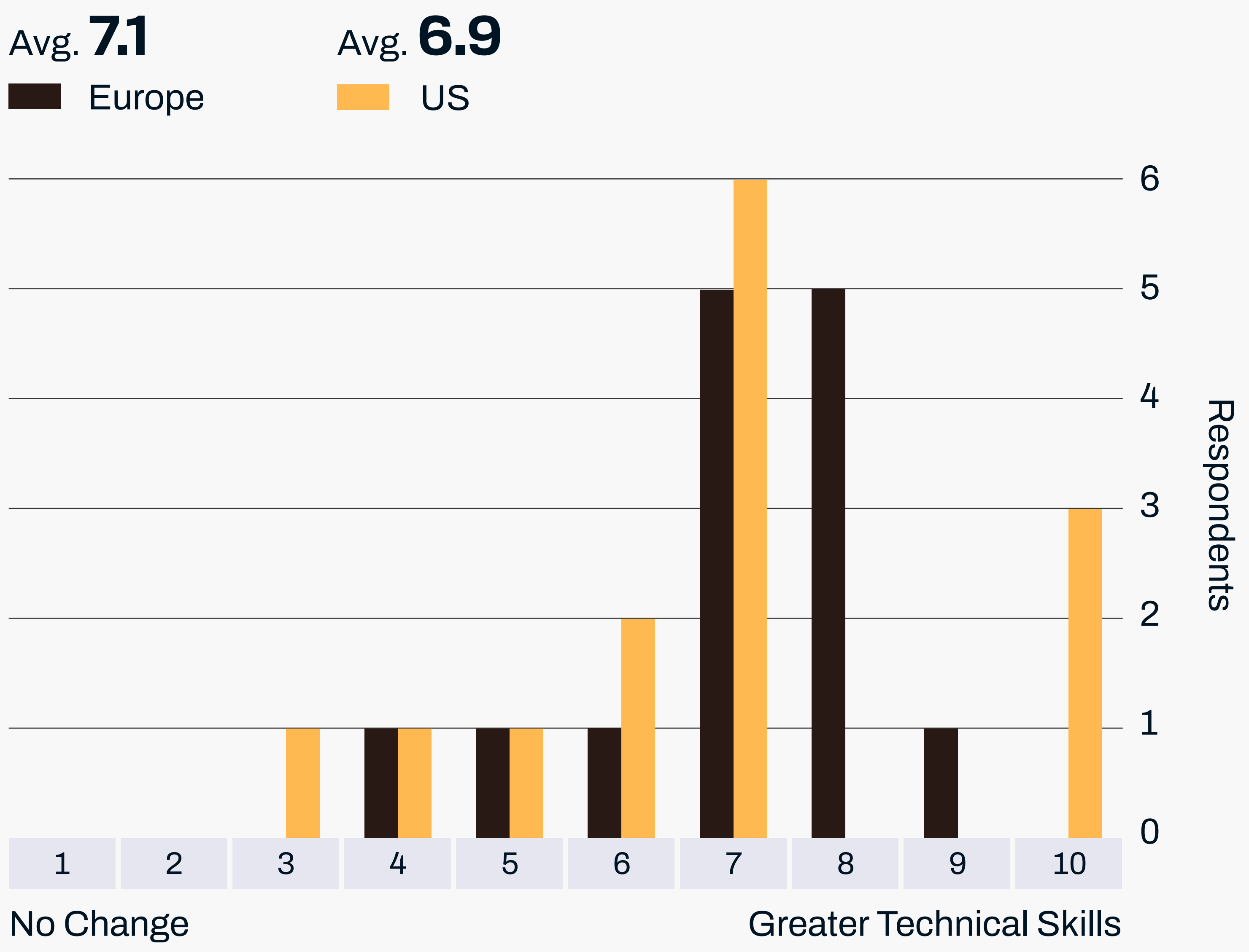
Our CISOs continue to understand and mitigate data risk. For many, the continual struggle to be a data-led cyber security practice has raised the visibility of analytics as they endeavor to understand where their business data is used, created and transferred. The panel believe that their security teams are more responsive if they employ security analytics, driving towards more predictive and real-time threat intelligence capability. The increased focus on mathematical analysis has raised the applicability of SOAR and more predictive (SIEM, MDR, NDR, EDR, etc.) offerings and their capability to deliver actionable insights. The CISOs told us they appreciate that they need greater supplementary data, requiring them to increase their knowledge of additional open source and third-party data feeds to increase their analysis of threats.

Our panel understand that humans alone are ill-equipped to manage the complexity and increased diversity of threats. CISOs recognize the growth of AI and machine learning (ML) in OT and IT, constantly reviewing the use of these technologies for cyber security to determine if they can really add demonstrable value – and, for that matter, whether these technologies have left their infancy. One area that appears to be gaining traction is user protection such as user and entity behavioral analytics (UEBA) and the incorporation of ML characteristics into identity and access management (IAM) controls to protect users of technology from themselves and also supplement the role of a security analyst.

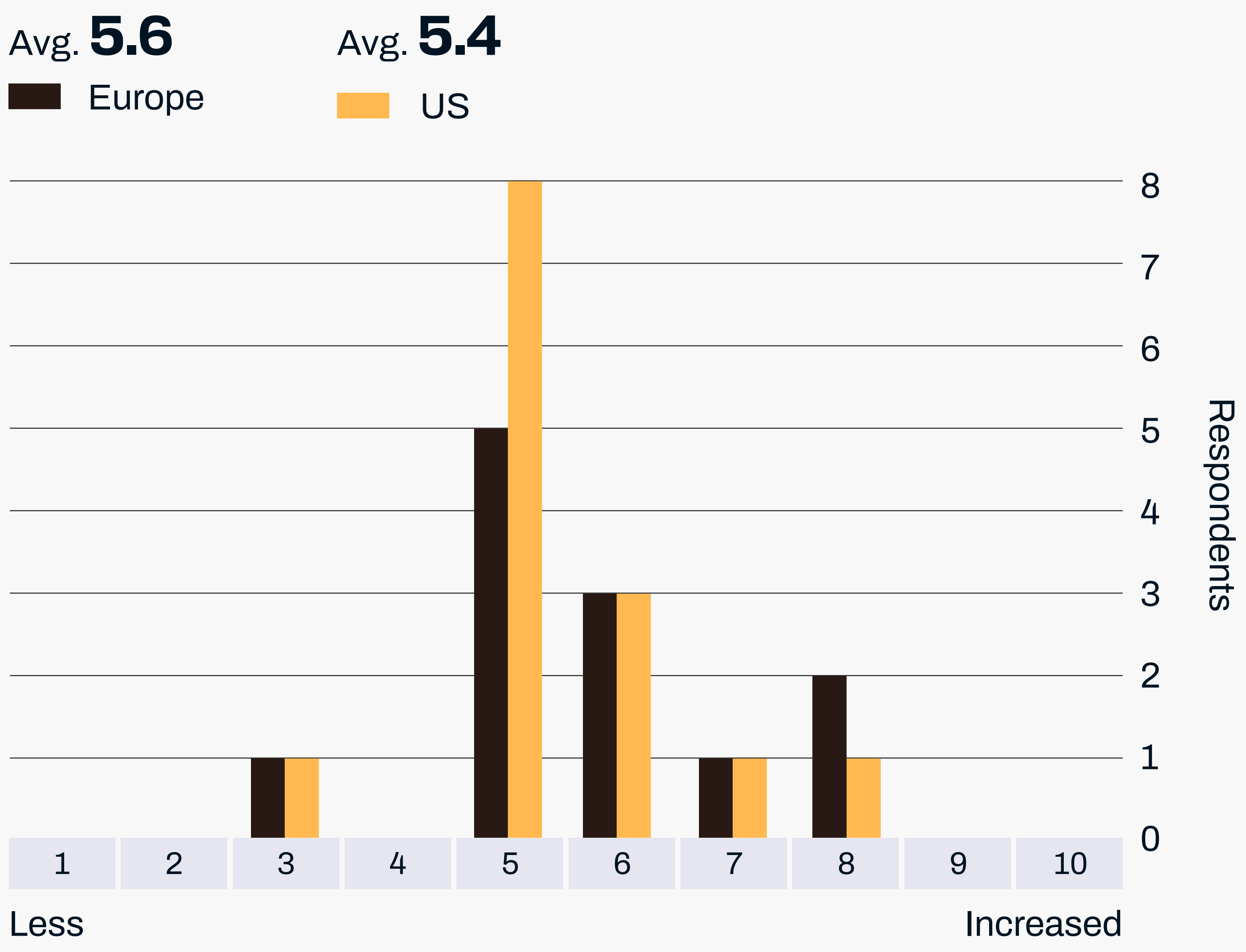
It was clear from our conversations with CISOs that a move to perimeterless environments is ushering in a new focus. Data, rather than assets, are the point of concentration, and where CISOs are working actively to build and renew skills and knowledge.

> “ **Humans alone are ill-equipped to manage this environment.”**
>
> Matt Stamper, CISO, Evotek

Have you needed to upskill around cloud security, device sprawl, RPA, AI, ML, analytics, threat intelligence, etc?



Do you have more funding available?



Question 3

Have you needed to increase your business skills and the impact you have on company achievements?

Have you needed to increase your business skills and the impact you have on company achievements?

Sixty-one per cent of the CISOs we spoke with strongly believe they need to up their business skills. Not only that, they felt they must now continually engage with others across the business, updating them on new developments and identified risks. A significant part of this engagement is to use their own skills and those of their teams, alongside potential technology in anticipating and conveying the impact on the business should it suffer a cyber incident.

Performing this level of interpretation and communication requires our CISOs to have both a strong understanding of the organization they protect and the ability to apply a technical perspective to operational excellence to fulfill their responsibilities.

Digital change and keeping up with the competition

Growing digital operations also obliged the CISOs we spoke with to understand a fast-evolving marketplace. Many of the respondents spend considerable time examining and researching how their competitive peers are using digital to reach their audience, as their own business will either be in the process of, or may shortly implement, similar engagement strategies. They expect to be asked to provide guidance on the technological and security risks and benefits of doing this work.

The largest challenge our CISO panel faced when attempting to demonstrate the impact they have on business achievements is their ability to, in the words of one respondent, “raise the profile of security to be a positive protective element of the business.” This is a significant turnaround from being seen merely as an internal security practice. Many believe that overall business risk remains the responsibility of the CEO, but when it comes down to security risk, “this is not the CEO’s responsibility: it belongs to the CISO,” to quote one of our interviewees. The role of the CISO as risk mitigator has meant that many have taken it upon themselves to understand what dependencies

> **“ I need to be positive about the competition and how they are becoming more digital.”**
>
> Hitesh Patel, Head of Cybersecurity, Cloud Computing & Digital Infrastructure Audit & Risk, Fidelity Investments

> **“ I don’t think you can separate the technical from the business anymore; you have to understand the business impact from a technical perspective.”**
>
> Scott Goodhart, CISO Emeritus, The AES Corporation

> **“ Absolutely. CISOs need to understand the company strategy and how cyber security could help with it.”**
>
> Gene Zafrin, CISO, Renaissance Re

The impact of working from home

‘Home working’ became ‘just working’ for many of us during 2020. This abrupt change to common working practices gave CISOs entry to task groups assigned to redefine the working environment and upgrade or introduce technologies that make the business more efficient, such as digital signatures and workflow validation. In the same way that face-to-face interactions have been overtaken by the leap to video conferencing, engaging with employees via new cyber security e-learning modules are helping businesses to secure themselves from attacks.

Has your role created a larger diversity of internal and external engagements?

Knowledge-sharing should be a major part of any individual’s day-to-day activities, and many CxO roles profess to have intrinsic learning and knowledge contribution across peer networks. CISOs take this to another level. Over 66% of our panel spend significant amounts of time with external communities of interest, such as CISO roundtable discussions and SME groups. These contacts allow them to exchange notes with peers on topics from day-to-day issues, business networking and the discussion of operational cross-CISO collaborations. There was a distinct difference in regions, where 78% of US CISOs scored almost 50% higher than their European peers when it came to professional contacts of this nature.

Around the world, raised awareness of cyber security has meant the CISO is now party to conversations and decisions previously closed to them – and this has provided them richer, more numerous relationships across the business, as well as earlier access to initiatives and projects.

Not surprisingly, our interviewees were pushed and squeezed into new working practices by the events of 2020. Stronger internal engagements and the provision of relevant security tools are proving critical as cyber security has added new responsibilities.

> **“ CISOs should engage widely with different parts of the business to understand what cyber security could do for them.”**
>
> Hitesh Patel, Head of Cybersecurity, Cloud Computing & Digital Infrastructure Audit & Risk, Fidelity Investments

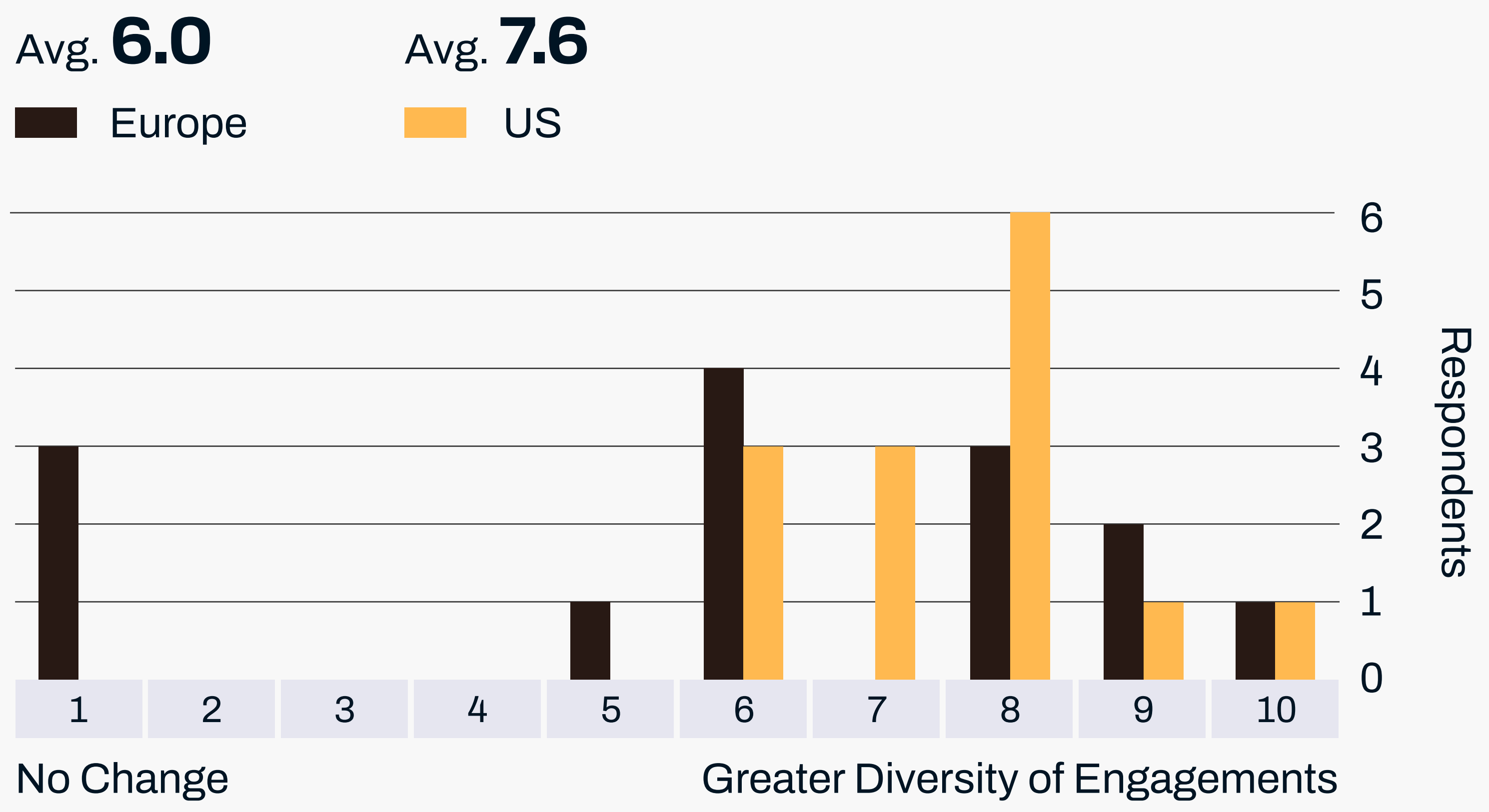
> **“ We need diversity to understand how cyber security fits into the company - international diversity on how things operate differentlyacross countries and industries and socio differences.”**
>
> Matt Stamper, CISO, EVOTEK

> **“ Before, the CISO was in a silo as the IT guy. Now he is the visionary of the new economy.”**
>
> Mauro Israel, Corporate CISO, ORPEA Group

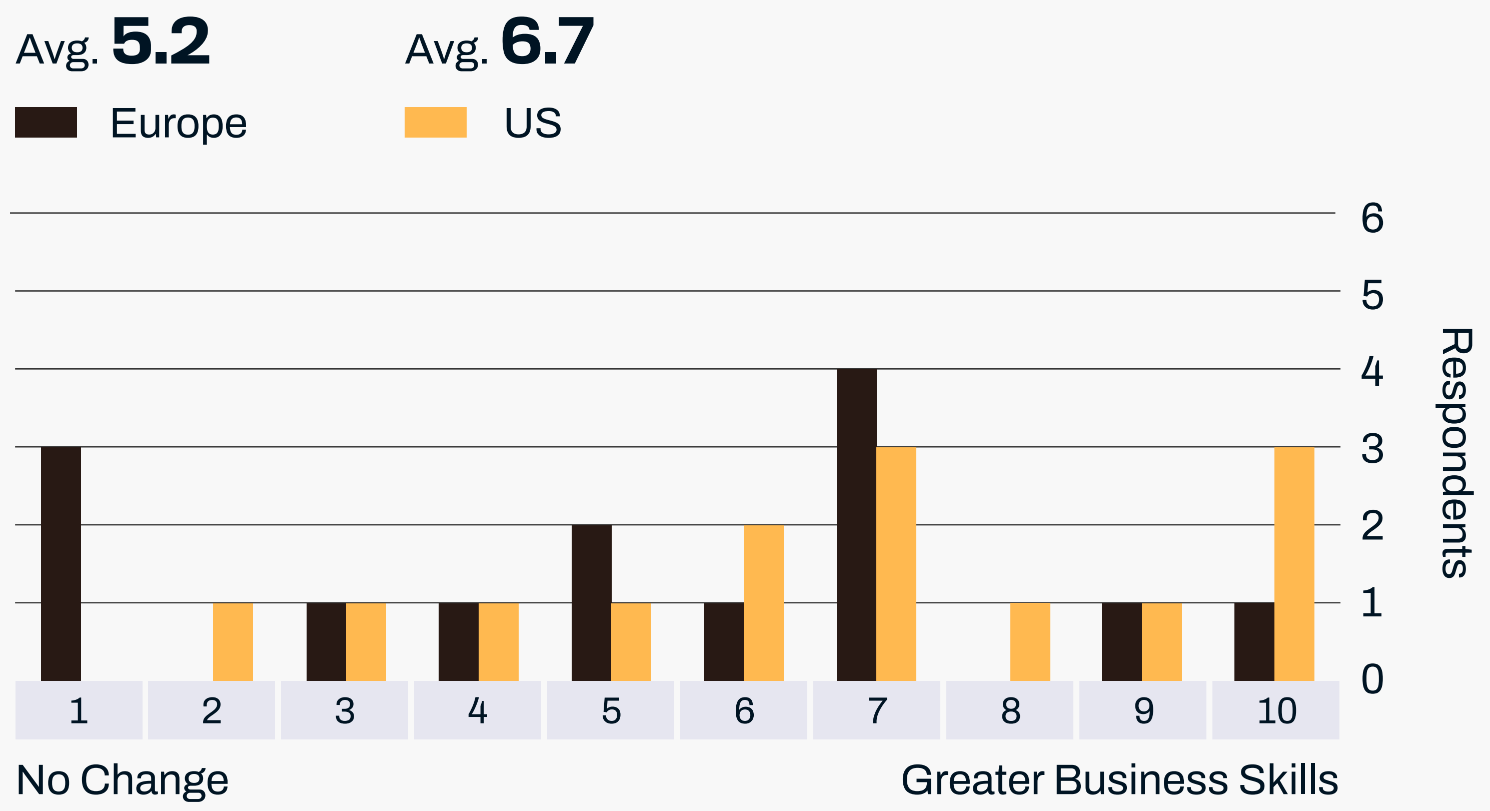
While engagements with peers across business units and functions are on the rise, some of our CISOs remain skeptical of the outcome of all this security knowledge-sharing within their own organization. Some were resigned to the fact that a minority of senior management will remain stuck in their ways and reluctant to embrace more inclusive, diverse and digital-led ecosystems. This mindset causes problems and challenges for both current and future operations. To avoid this, our panel recommended that non-IT-related senior management use their own network and conversations to appreciate how cyber security operates differently across countries, industries, and cultures. CISOs believe that their widening of engagements promotes communication based on openness, reality and facts instead of using role power to convey beliefs that may result in a more negative and less diverse approach.

External engagements are now more diverse and include regulators, government agencies and banking merchants to ensure that the CISO can hear directly what they need to consider and where other peers may have best practices to ensure compliance. In addition, many of the CISO's business contacts, suppliers and customers are reaching out for subject matter expertise for their own organizations. Mutually beneficial discussions have increased, as the growth in ransomware attacks has meant connected third parties need to understand the possible impact of such attacks from each other's perspective.

Has your role created a larger diversity of internal and external engagements?



Have you needed to increase your business skills and the impact you have on company achievements?



> " Core diversity across the central team. Seniority is not always the best; it's the idea that counts."

Hitesh Patel, Head of Cybersecurity, Cloud Computing & Digital Infrastructure Audit & Risk, Fidelity Investments

> " Yes, we have more external conversations with CISOs of most major customers and their boards."

Andrew Rose, CSO, Vocalink (A Mastercard Company)

Question 4

Do you believe your role will become more critical to your business?

Do you believe your role will become more critical to your business?

Regardless of their employer's scale, our CISO panel agreed that their role is now recognized as a senior management position. Of those CISOs already holding a seat on the board, there is confidence that their role is as critical to the business as other CxO positions. It is worth noting that, while this may appear to contradict the points made earlier in this chapter, it's more accurate to say this reflects a dichotomy. CISOs may be relied upon as senior managers, but they've not always been identified or rewarded as such. Almost two-thirds (65%) of the CISOs in this study believe that they are critical to the business. Respondents from the US scored their value perception as slightly higher (7.4 average) than European CISOs (6.1). Respondents on neither side of the Atlantic expect these numbers to change dramatically any time soon.

The recognition of strategic and operational value

CISOs are also confident in the value that they bring to their employer. They see the role they play as just as valid as that of other big functions, like human resources or finance.

Three-quarters (75%) of the CISOs we spoke with acknowledged that their role has significantly moved from a pure focus on network risk to cover every aspect of technology now being deployed. This was particularly evident from those respondents hailing from healthcare, manufacturing and retail – sectors that eagerly adopt all forms of IT to increase business value, including the digital security of employees, business partners and customers.

As cyber security becomes more recognized as a practice that enables the wider business, CISOs understand that they need to demonstrate value to risk management as part of the greater accountability and responsibility that comes with it.

Some of our panel believe that you cannot divorce the physical from IT security, so the term 'CISO' itself may evolve so that the individual's all-encompassing responsibilities are understood; one suggestion was chief security officer. Job title aside, our panel deemed that their role is unique in providing a perspective on business risk and conveying a probability that their company will, at some point, become a more interesting target to the plethora of cyber criminal personas.

> **"It depends on the business. As a security leader we have to practice what we preach! Enable businesses to create the right security culture, awareness and to build cyber resilience. Trust, resilience and good communication are critical."**
>
> Chani Simms, CISO, SHe CISO Exec

> **"There may be a new name for the CISO that more broadly represents the role's responsibilities collapsing into a chief security officer rather than CISO."**
>
> Scott Goodhart, Emeritus CISO, The AES Corporation

There is a caveat: some of the more skeptical respondents have concerns about the long-term value of their role. These CISOs believe that unless their work is truly understood – as part of the standard operating model – it could become commoditized or consumed into just another function, rather than recognized as a strategic asset.

New levels of confidence

Suppliers and clients of a business often turn to CISOs for the appropriate risk management knowledge needed to discuss, plan, implement and guarantee cross-organizational security. This level of confidence coincides with the increased integration of supply chains, triggered by digital and ecommerce growth.

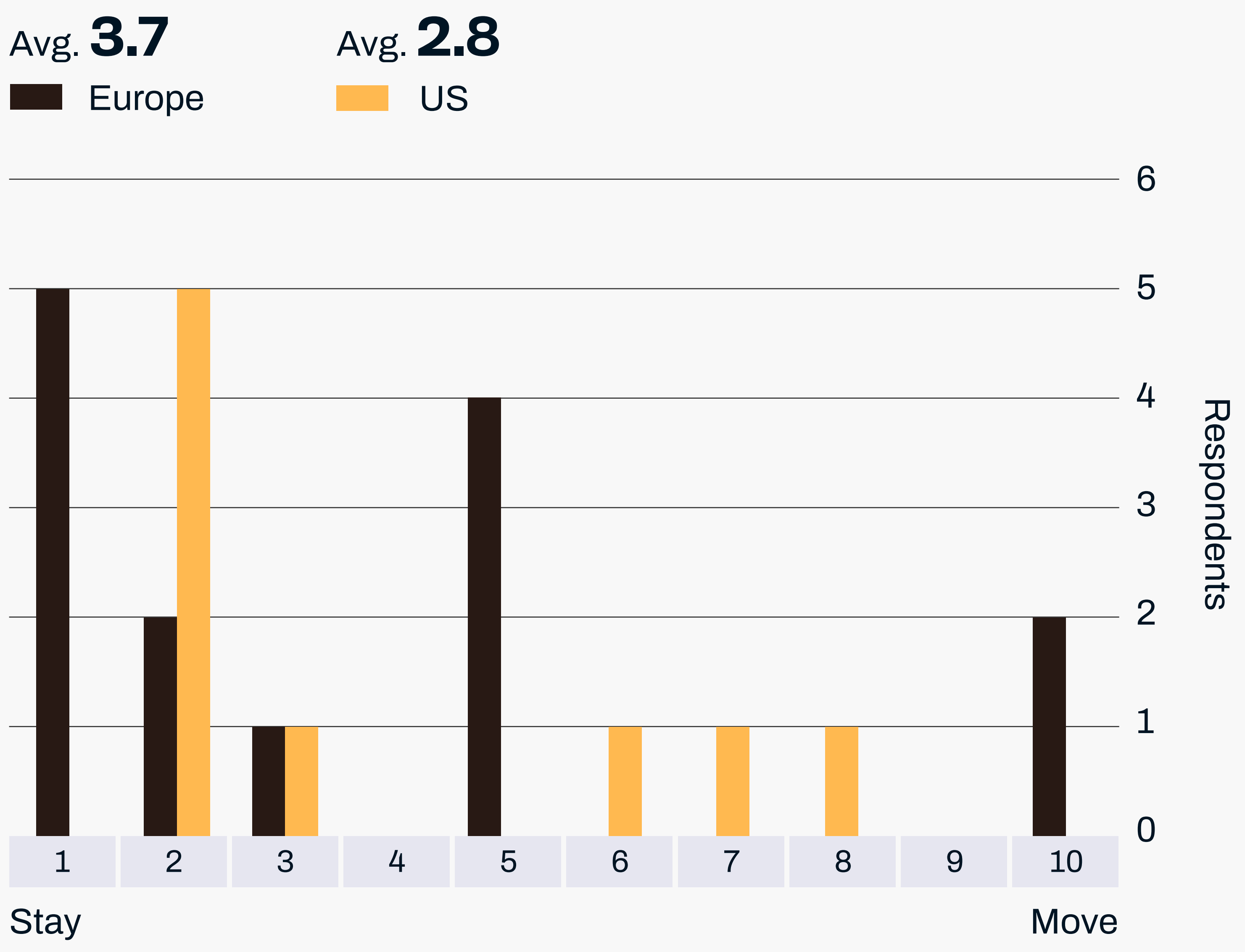
Some CISOs recognized that the data protection or compliance officer is a custodian of data. As a result of more privacy laws and regulation, many CISOs feel required to amplify their role and become custodian of everyone and everything that has a data association.

The quarter (25%) of CISOs that scored between 1-5 on the scale when asked if they feel their role was critical to the business could be regarded as being more cautious, believing that the role will probably stay the same. They were consistent, however, in conveying that 'staying the same' does not diminish the importance of that role.

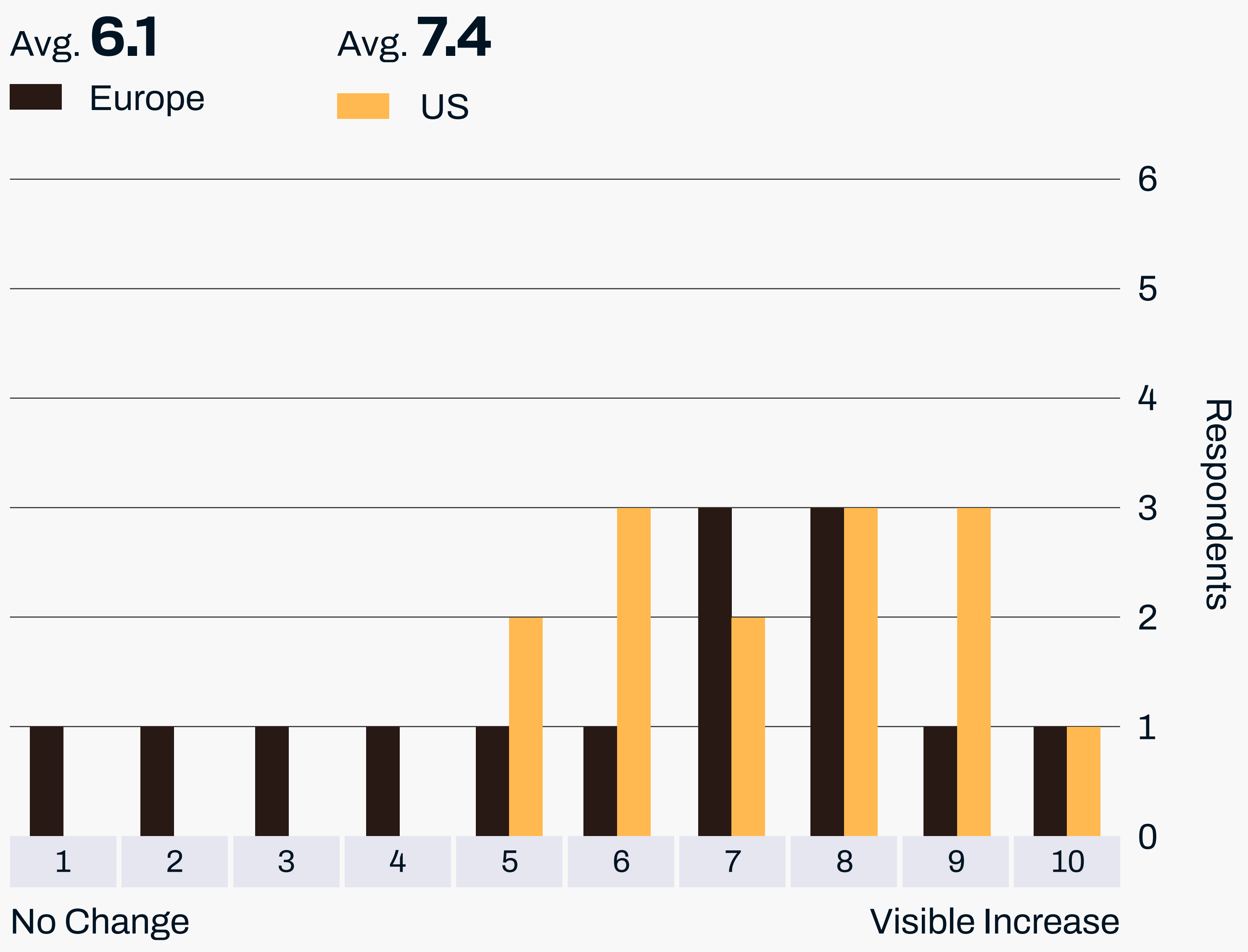
> **" With an increase in ecommerce and online financial transactions, coupled with the maturing of privacy laws around the world, the need to have a strong security role is becoming more critical to an organization's success."**

John Scrimsher, CISO, Kontoor Brands

Do you want to stay in your current role (move on or leave the profession)?



Do you believe that your role will become more critical to your business?



Question 5

Do you believe your role has increased in EQ as well as IQ?

Do you believe your role has increased in EQ as well as IQ?

For most people, emotional intelligence (EQ) is more important than one's intelligence (IQ) in attaining success in their lives and careers. As individuals, CISOs are largely seen as highly intelligent but somewhat unapproachable, one of a small number of techies at the boardroom table in many organizations. This stereotype may be just that, but it remains hard to shake off in some cultures. From frontline security and incident response teams all the way up to the CISO, the ability to empathize with users, managers and stakeholders and respond correctly is prized. It is also increasingly necessary, for more immediate reasons.

The success of CISOs and the success of the profession depends on their ability to demonstrate they embody the view that 'EQ is everything to the business.' And it isn't just management-speak; the prominence of EQ as a business skill is being included in some regulatory requirements for publicly listed companies in France.

Our interviewees recognized that a major aspect of their role is how they deliver through others and have them promote a security model. It has been clear from the interviews we conducted: 66% of CISOs clearly understand that each of them must develop the mature emotional intelligence skills required to better understand, empathize and negotiate with other people – particularly as globalization continues apace.

While 71% of US CISOs all scored heavily, from 7+, only 57% of European ones matched this level of enthusiasm, with the remaining 43% scoring in the 3-6 range.

Our interviewees recognize that they must converse across the diversity of their engagements, understanding that their issues and work/life balance is key, but more important is the ability for these communications to be conducted in a tone that the individual understands – and that is not always technical detail.

Far from being the unapproachable individual that the CISO persona may be associated with, many of the CISOs we spoke with recognize that they need to ask for help – and they believe that on the emotional side they need to be more forgiving of themselves to alleviate self-imposed pressures to get everything exact.

> **" The requirement for security is no longer just about technical understanding; you need a better understanding about people and how they interact and react."**

Scott Goodhart, CISO Emeritus, The AES Corporation

> **" When you go to remote services and distance learning, people call when panicking - become less tolerant to wait for the answers."**

Nathan Reisdorff, CIO, New England Law

> **" The majority of role is about how you deliver through others and get others to drive a security model."**

Dave Thomas, Director Security and Privacy Engineering, GoCardless

> **" Your EQ is the level of your ability to understand other people, what motivates them, and how to work cooperatively with them."**

Howard Gardner, Research Professor of Cognition and Education at the Harvard Graduate School of Education, Harvard University

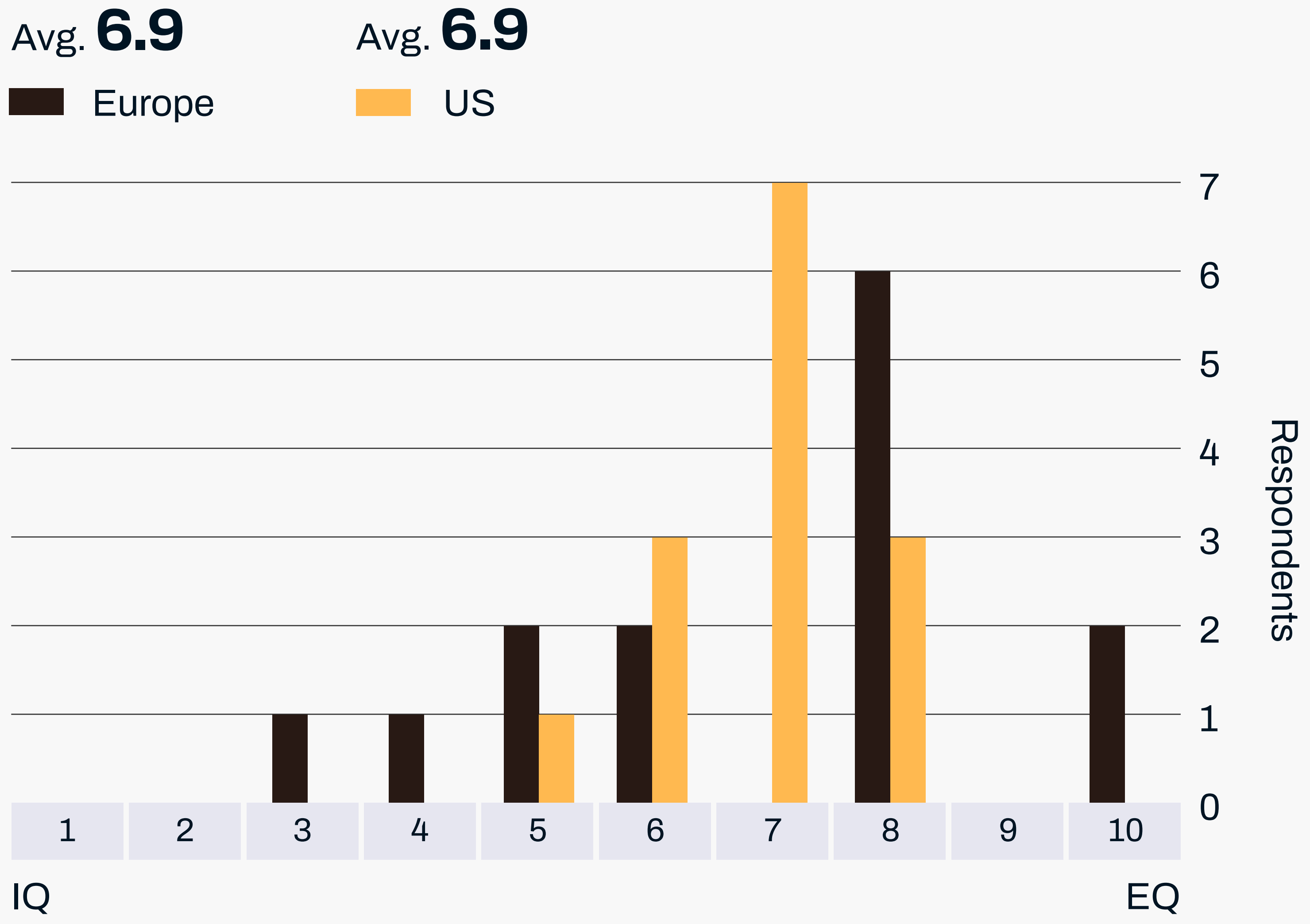
EQ has its place, especially in situations where the more dominant IQ traits of CISOs tend to emerge. Our panelists were generally prepared to accept they will be held to account for many things beyond their control, such as the shadow IT implemented without their knowledge, and the reluctance of other peers to accept their responsibility of understanding the impact of cyber security within their roles. They were adamant that this is something they are addressing to be a more conscientious EQ CISO using these new skills to engage wider across the business.

With the new working normal, CISOs must extend the notion of EQ to their security teams, to better support their employees. Distinct from a helpdesk function, CISOs understand that their teams need to know why someone is making the effort to engage with them or their team, rather than just focusing on the technical resolution.

As the volume and frequency of communications from security teams and CISOs to the rest of their organization increases, the need for plain-speaking, open communications that avoid jargon and 'IT-speak', become increasingly important. Clear and open communication in the other direction, so that employees can be heard and provide positive and critical feedback, is equally vital to success. The CISO and their security organization will not have all the answers – but they should be in a position to help find those answers.

> **“ EQ has driven the capability to engage with non-IT in metaphors to make it easier to understand. Proper communication will drive a positive environment.”**
>
> Todd Gordon, Director, Information Security, EisnerAmper LLP

Do you believe your role has increased in EQ as well as IQ?



Question 6

What do you believe you need to improve to excel in your role?

What do you believe you need to improve to excel in your role?

Across many of their responses, our CISOs have characterized their role, and that of their security specialists, as a responsibility to continuously learn. Although we know that good leaders will prioritize the skill sets of their teams, we specifically wanted to know what skills they are missing or need to improve in their capability that allows them to provide a first-class cyber security service across all their interactions and for personal satisfaction.

The CISO's job is traditionally a technical role, so ongoing development of these skills – especially around some of the newer emerging technologies – is seen as a priority. They also appreciate that having the latest knowledge of IT, the techniques of hackers and the associated tools being used should be maintained.

How CISOs can become better business enablers

As the role of the CISO now encompasses the need to understand more business-related competencies, they acknowledge that understanding industry and privacy regulations needs to be fully appreciated. They know that CxO management expects them to have an informed position for the company to remain compliant.

As a critical member of a company's operational team of excellence, CISOs need to continuously widen their internal and external engagements, primarily for two purposes. The first is obtaining business knowledge by interacting with areas such as COO, legal and M&A teams, allowing the CISO to appreciate how the company makes money and what risks (outside of security) could impact their objectives. Second, widening their external network with more 'peer group' interactions and regulatory, trade and government agencies partners will provide them with new insights and allow them to promote their role as a business enabler, and extend the operational excellence of their business.

> **“ The largest room in the world is the room for improvement. I always ask myself, 'How can I do better tomorrow?'**

John Scrimsher, CISO, Kontoor Brands

> **“ It may sound trivial, but to understand my own direct reports better. The biggest impact I could make is to ensure that every member of the team is successful.”**

Gene Zafrin, CISO, Renaissance Re

> **“ Like most CISOs, I'd like to strengthen my business relationships, so I can improve communication with the key managers in the company on how to enable their business lines beyond just risk reduction, and related to productivity resilience and cost avoidance.”**

Mike Davis, CISO, Alliantgroup

> **“ I need to be positive about the competition and how they are becoming more digital.”**

John Scrimsher, CISO, Kontoor Brands

> **“ How to ‘sleep in shifts’ and increase my understanding, patience and business judgement, and translate this into a language that a retail business will find compelling.”**

Simon Goldsmith, APAC Information Security Officer, Adidas

But many CISOs just don’t have enough time in the day. They can become overwhelmed running from cyber fire to cyber fire with too much smoke to clearly view the bigger picture. They do not always have the capability to stand back and put the overall problem space into context. Trying to find 25 hours in a day, the ability to survive on very little sleep, being less worried and paranoid, as well as remembering they have a home to go to, were not uncommon comments. The CISOs accept that, in many cases, they spend too much time in the depths of technical operations and need to learn to trust their teams more and let them do their jobs. By doing this they will have more time to look at their function in a more strategic manner.

Driving the right behaviors

There was appreciation that greater soft skills will encourage more effective interactions. In the past the tone of security discussions was less about value and more about highlighting the fear, uncertainty and doubt (FUD) – encouraging the suggestion that ‘maybe we need more incidents to be taken seriously.’ This is an approach with limited utility and long-term downsides.

Communicating more effectively in a language that allows every interaction to be accepted as a positive interchange and approaching security issues with example anecdotes would help the CISO to convey risks and threats in a less intimidating manner. This kind of approach would boost the likelihood that the security message is clearly received and understood.

Ensuring that their security teams are effective remains a priority to the CISO. Engaging more effectively with their teams requires the CISOs to push their ability to improve their EQ. They are striving to understand their teams more on an individual basis, how to simulate them, recognizing that each individual is different, understanding their personal insights, and adjusting their interactions to increase the opportunity for each individual to be successful.

The CISOs we spoke with want to explore new techniques to increase the value that each team member sees within themselves as a valued contributor. In realizing this, CISOs hope to create a more productive and rewarding environment that retains and seeds the individuals as part of the company’s long-term success. If the CISO approaches their talent acquisition with the same attitude, they will be able to employ and retain staff to whom they can delegate greater responsibilities.

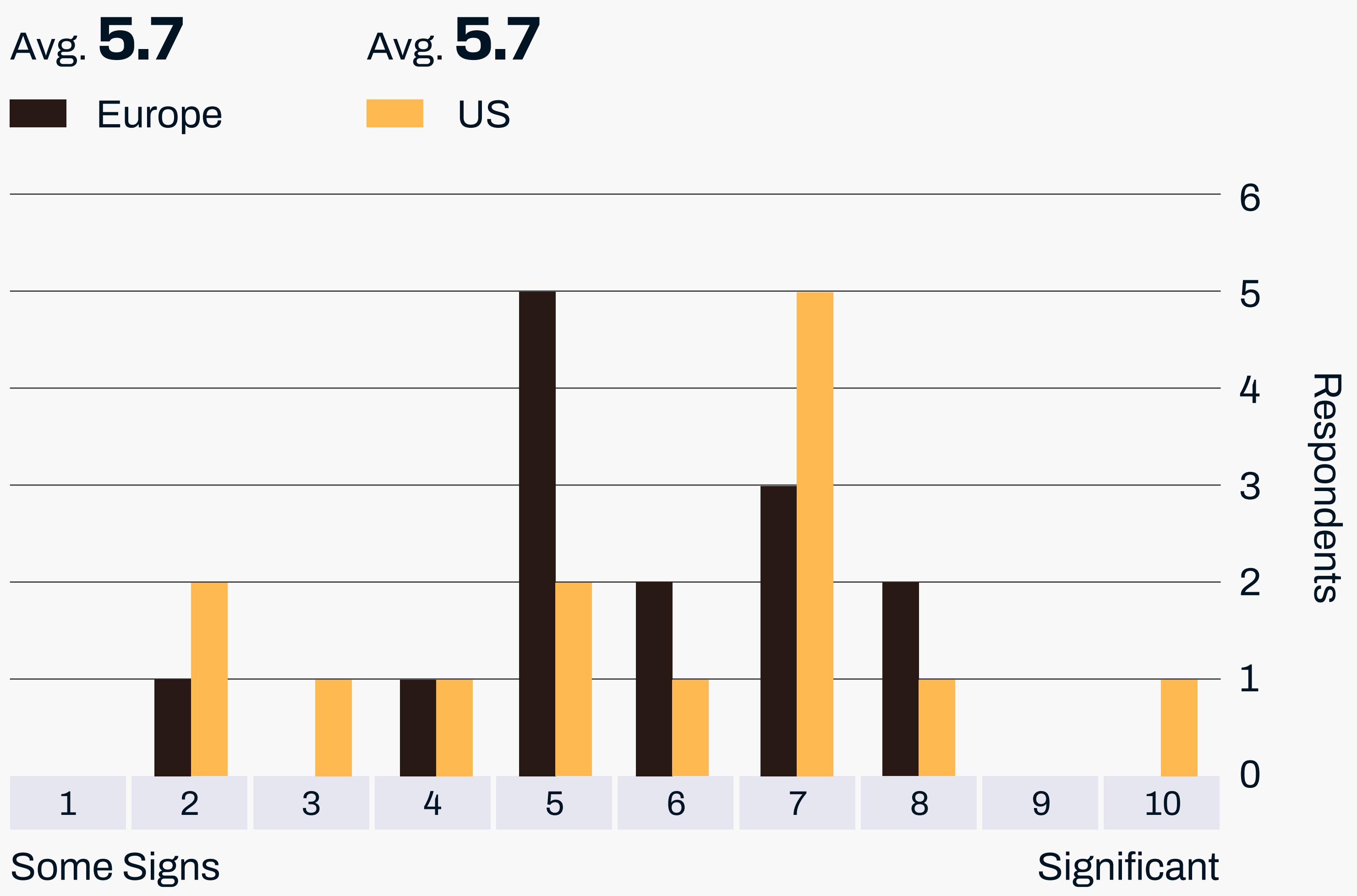
Secure in their role and the well-being of their team

Security in security: At the time of this research project (July to September 2020), 65% of the CISOs believed that, even with all the issues that the world has had to cope with in 2020, they feel more secure in their role. Only 37% of CISOs indicated that they are considering moving from the current position or leaving the industry.

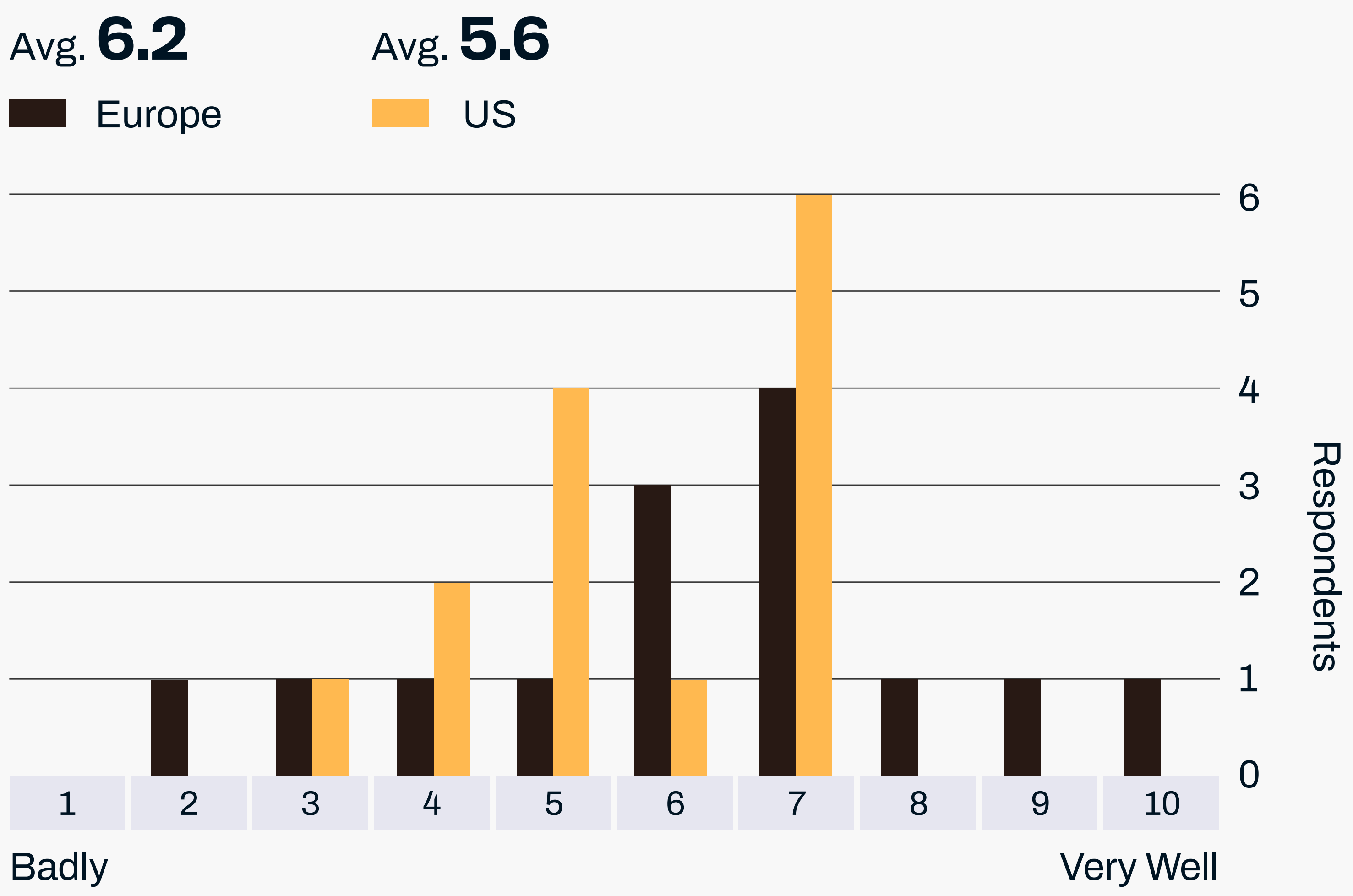
Stress levels across CISO teams are being managed, with 78% scoring consistently within the mid-range 4-7. Although when asked if the CISOs had recognized increasing levels of burnout in their teams, the same mid-range scored 71%, indicating that greater levels of engagement with the CISO, their security teams and the wider employee base needs to be undertaken in handling stress by the human resources and occupational health teams.

Budgets appear to remain consistent cross-industry, averaging 53%, with 39% of respondents seeing improvements in their budgetary spend. When asked about how CISOs allocate budgets between responsibility (company objectives) and accountability (delivering secure operations) of their role, 64% placed themselves directly in the middle (5). CISOs accept that as a member of the senior management team, they need to deliver on the business objectives, as well as ensure that their responsibilities to deliver a secure operating environment across the entire value and supply chains can be shared across their own and other teams.

Have you seen signs of burnout in your team?



How are you and your team handling stress?



Question 7

How could your peers and reporting line management help you succeed?

How could your peers and reporting line managementhelp you succeed?

The CISOs we heard from were adamant they should not be singled out for special treatment as corporate celebrities – far from it. Their belief was that, with other senior management, it was imperative to encourage regular dialog in an open culture, taking a personal responsibility to educate themselves in the essential deliverables of their peers and management's KPIs (key performance indicators). In contrast, respondents were clear that others should not be responsible for understanding their role and KPIs.

The CISOs know that it is down to them to learn how to communicate in a clear and unambiguous manner about what they see as possible risks to the business, employees and consumers, and align these concerns to the enterprise risk management framework.

Clear and aligned concerns can only be communicated if the CISOs are educated and informed about the business they work for. Understanding what the business does, how it makes money, what initiatives are underway, what relationships in the markets are important, as well as those with regulators and agencies, are all key insights for our CISOs.

But it should never be down to the CISO alone to seek to help support the business. Instead, it should be a team approach with other peers, each valuing insights and suggestions to increase the security and effectiveness of the business. They do not have a sixth sense.

Some CxOs must foster a more engaging culture, changing their attitudes, and end their belief that everything 'security' is the sole responsibility of the CISO, or only relevant when the next compliance audit is due. They need to take a level of accountability for security in their domain and ensure that the CISO and their teams are engaged to embed this in their processes. CISOs can help their peers identify how they should do this, thereby increasing the value across the entire management team. The bottom line for 360 support is as much about peers seeking support from the CISO, so that the CISO and their teams can have appropriate visibility to think about any issues.

> **“ Peers could use themselves as ambassadors to the company. Security is for all in the company, and so is reporting things that are suspicious.”**
>
> Royce Markose, CISO, rewardStyle

‘Not my job’ and shadow IT are friction points

Some of the CISOs acknowledged that they break up their teams to proactively support different business units to achieve that unit’s objectives. However, when levels of engagement are low, some IT departments become reactive and wait for the security team to advise. This risks piling the workload onto the security team, requiring them to be experts across all technology.

One of the largest challenges that the CISOs raised was around the growth of shadow IT. The owners of the various business functions may encourage the implementation of dedicated shadow IT for specific areas of business efficiencies, but they do not comprehend that the CISO’s team have no visibility or understanding of what programs and apps have been installed. This lack of visibility by the CISO, and negligence by peer groups, means that shadow IT does not get deployed with the appropriate levels of security hardening, increasing the attack surface and risk for the company.

Outfitting is better than retrofitting

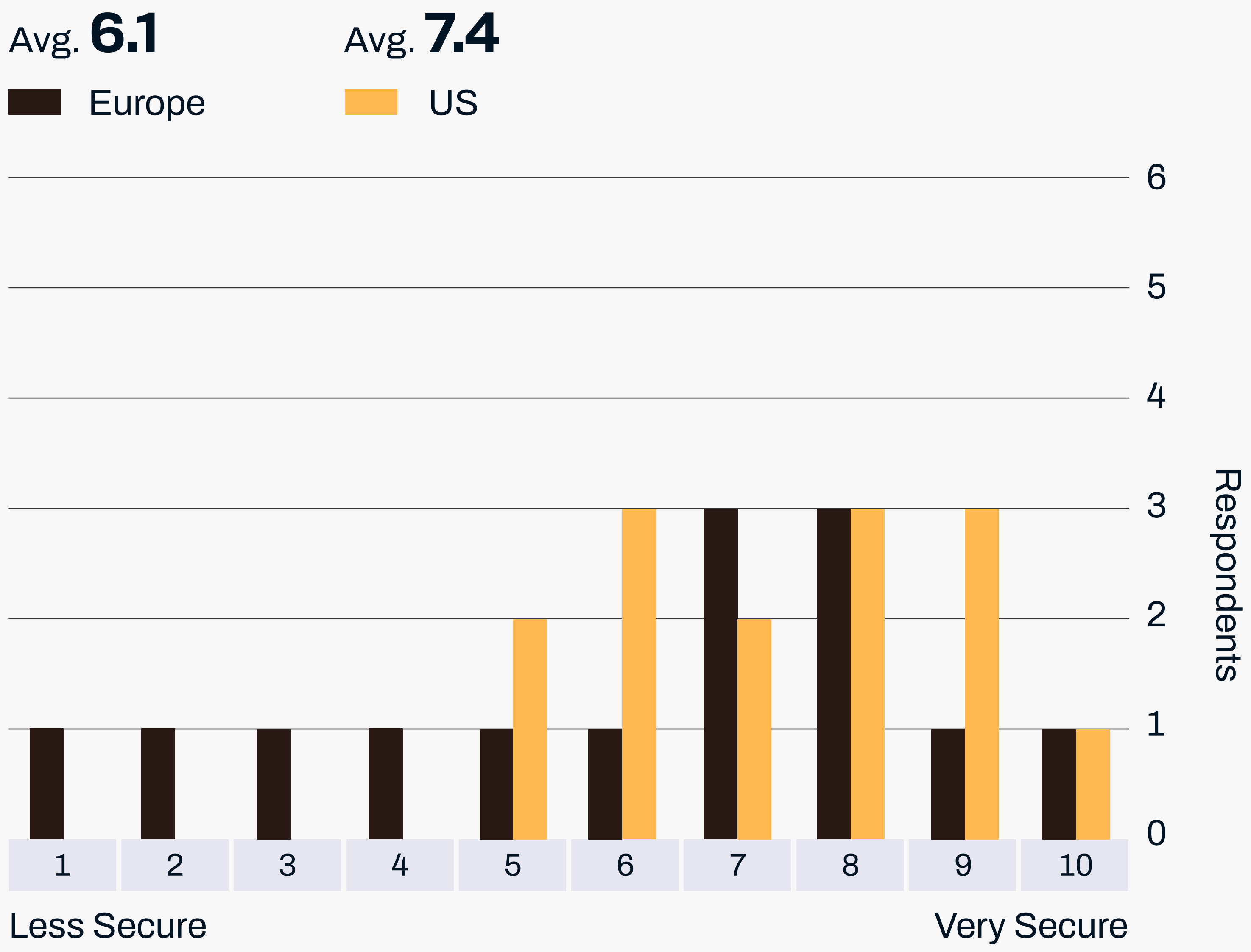
Reporting line management – primarily the CEO and CIO – need to establish and continually measure the effects of cyber security as an integral part of their business operations and a key area of enterprise risk. Think safe: think security.

Clear direction, communicated directly by the CEO or CIO, encourages a security culture within organizations. This would encourage everyone to provide feedback on suspicious activities, ensuring that all operations are undertaken with security by design.

Peer and line management’s understanding of how CISOs and their teams can help support and innovate business functions is not that difficult if you do it from the outset of a project, application introduction, change management adjustment, and even at the integration or creation of new business units. Retrofitting requires a change of attitude – and that can be more difficult.

> “ Clear communications, no blameculture, sharing knowledge and mentoring goes a long way.”
>
> Chani Simms, CISO, SHe CISO Exec

Do you feel more secure in your role as a result of the events of 2020?



The WithSecure™ Countercept perspective

What follows is a short commentary from WithSecure™ Countercept's perspective. This is informed by the constant engagement and dialog we have with CISOs. It is also combined with
a view of the breadth of attacks aimed at our customers.

CISOs are wise to devote time and effort to regulatory compliance, but it is not the only thing necessary to ensure success. Regulation, especially when it comes to privacy and cyber security, is often late to the party – although improvements have and are continuing to be made, our perspective is that effective cyber security risk mitigation has to go further than the minimum legal requirement. Successfully meeting regulatory requirements hardly ever results in a secure organization – just one less likely to fall foul of the law in the event of a breach that harms it and its customers.

We'd also want to sound a slight note of caution around two key technologies. SIEM and analytics are invaluable additions to any cyber security operation's toolkit. However, SIEM and analytics are not immune from the hype cycle and sometimes their capabilities are overstated. They aren't a magic bullet – as the panel rightly observed. The answer to the security challenges we face is rarely 'collect more data.' Rather, it's 'get the right data, interpreted the right way, at the right time.'

We have learned that collecting and processing the right data is the most effective way to address these use cases, particularly when it comes to threat detection. Understanding the role of the human in handling and interpreting data such as this is vital, and something we have spent time and effort working on, specifically around the work of our detection and response team.

Communicating well – with both one's own business and third parties including regulators and law enforcement – is a challenge we know well and devote significant time to getting right with our customers.

It is often a key requirement from the CISOs we deal with that we help them articulate the value of good MDR, often in the wider context of their team's role. This often requires that both the CISO and our team spend time with other parts of the business establishing lines of communication and setting expectations – on all sides.

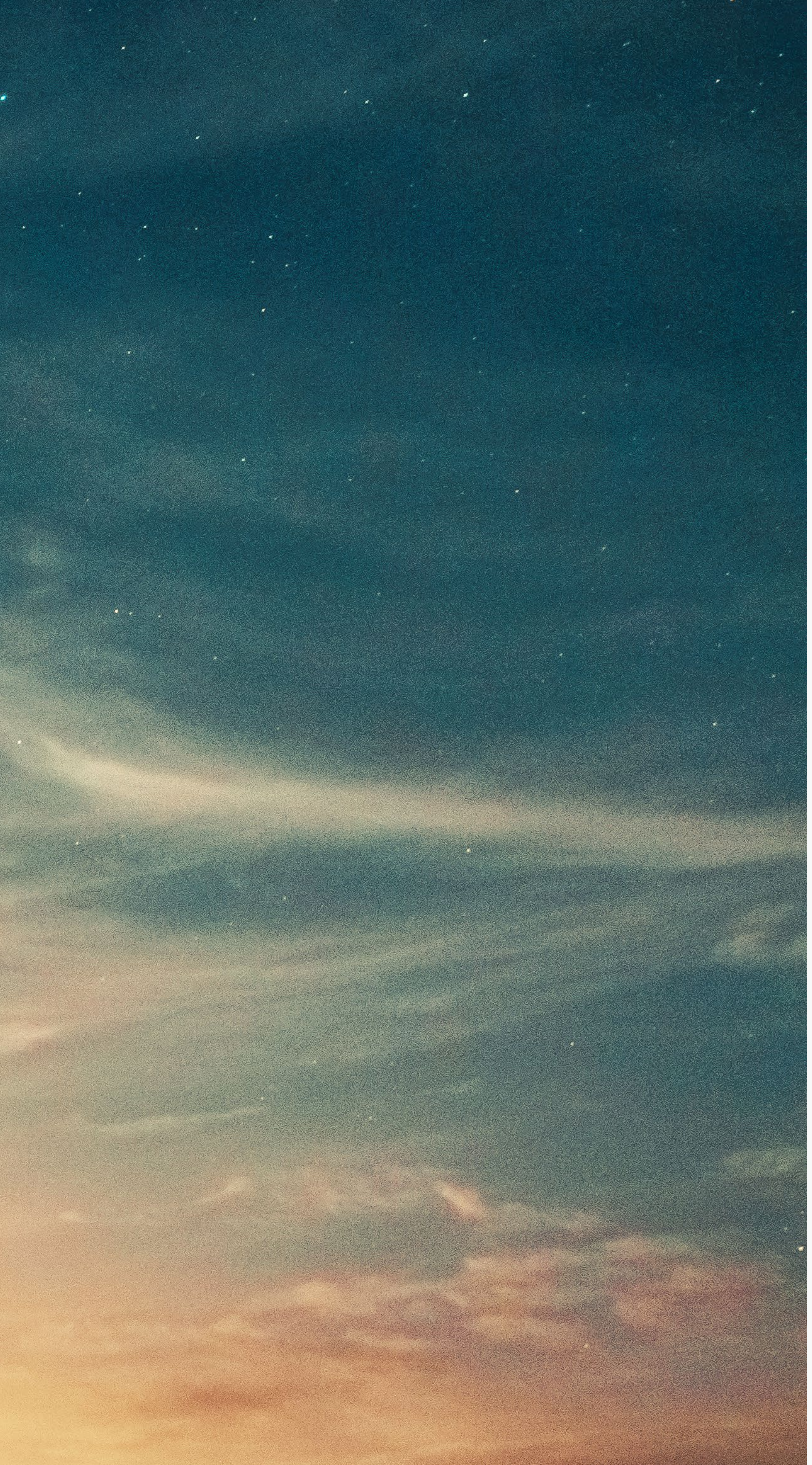
The WithSecure™ Countercept team continue to spend time with CISOs and their teams, advocating the role of security and the value of investments in different tools and capabilities to leaders.

At a very high level, the interpersonal communication challenge highlighted by CISOs comes down to the personal relationships and communication skills within organizations' hierarchies and with outsiders. But it can also boil down to reporting processes, choice of metrics and other tiny, significant factors.

During service delivery, this means working to communicate cyber security risk and the value of investments. It is also important to understand which metrics – and what about the metrics is valuable – are important to each organization and each team within it.

A key part of the WithSecure™ Countercept proposition is what we call Peacetime Value[3], which involves working with customers to get the visibility and evidence they need to both ensure and demonstrate to their organization and regulators that they are doing the right things – and doing them well.

Ensuring effective operations is a responsibility – and one that CISOs have had to work at even harder than usual over the past year. Sometimes the urgent can drown out the important, and strategic thinking, influencing how one's organization approaches new challenges from a cyber security perspective and other equally important tasks, have compounded the juggling act that CISOs have had to perfect recently.



Chapter 2 - A reality check

With great power comes great responsibility - and a to-do list.

While the events of the past year may have accelerated the rise of the CISO to a senior position, this pace of change has a price. Added recognition and responsibility is great, but it often comes with a laundry list of fresh challenges.

In this chapter, our panel consider accountability, culture, board engagement and the need to move from cyber as risk mitigation to a creator of business value.

All managers, not just security specialists, must take accountability for understanding the impact of cyber security on their departments. Allied to this is the need for open cultures and security charters. Ensuring the board is engaged with cyber security emerges as a pressing topic.

There's a big difference between being handed more responsibility and having the resources to do something about it. For that matter, responsibility is often a separate thing from recognition of the value of one's work.

Part of this issue is concerned with both how cyber security is viewed by different organizations, and about its position in many workplaces as a business function. Demonstrating a return on investment or risk avoidance value remains a challenge.

Compounding the problem is the nature of news coverage when it comes to cyber security: awareness of risks and threats is a good thing, but it can be a double-edged sword. Knowing of a problem at board level without any understanding of its relevance to an organization, or how to go about reducing risk, can make life hard for a CISO.

Question 1

Do you believe that cyber security has transitioned over the past 12-18 months in operational relevance?

Do you believe that cyber security has transitioned over the past 12-18 months in operational relevance?

Seventy-three per cent of the CISOs taking part in this report said they believe that cyber security continues to gain operational relevance, although it demands a ‘security first’ approach across the business. The challenge with maintaining the operational relevance of security is that, although a high average of the CISOs (6.6) indicated they believe cyber security had become more relevant to their organization, they didn’t think it would increase visibility: 28% of respondents scored 6.0 or below for the belief that cyber security will not become more prominent unless the growth in digital competence and new working from home practices increase the recognition of the role of security.

There was a higher level of optimism in the US, where 82% of respondents scored the regional average or higher (7.1), compared with 57% of European interviewees, who scored an average of 6.0 or higher.

Security teams in larger enterprise companies show relevance to the operation of the business: CISOs in these organizations have closer, broader and more diverse access to senior management, and this helps them deliver organization-specific reporting to track and respond to operational activities relating to cyber security. This is useful when it comes to reassuring regulators and clients.

Panelists hailing from small- and medium-sized organizations (SMBs) said operational relevance continues to be minimal. In contrast to bigger businesses, they see security classed as ‘just another’ IT function. Many cyber security officers for these smaller organizations refer to traditional risk measurements such as business impact analysis (BIA) and many of the data and system recovery point and recovery time objective measures. Because these organizations are using older risk measurements, they may not have an accurate picture of cyber risks to their business – or the data points to work out what to do about them.

The interviewees who made these observations are pushing their organizations for security to be taken more seriously so that [security] risk is effectively considered as part of business metrics.

Show a CISO a budget and there are plenty of things they’re happy to spend it on. But senior management rarely sees things that way: budget requests from the CISO are often seen as requests for technology spend, rather than for equally vital operational and resource priorities.

> **“ I want to be better than my competition. But as we become more digital, we have a wider threat surface.”**

Hitesh Patel, Head of Cybersecurity, Cloud Computing & Digital Infrastructure Audit & Risk, Fidelity Investments

> **“ Operational risk is the way forward, tied to business metrics and anchored in good models, methods and processes.”**

Simon Goldsmith, APAC Information Security Officer, Adidas

The approach required now for cyber security, like other functions in a business, needs consistent alignment to operational risk and to increase its relevance. Standalone organizational risk reports that align to operational relevance may exist but, unlike security posture frameworks from NIST and MITRE ATT&CK, all CISOs continually struggle with identifying and implementing a repeatable industry framework. The use of such a framework would increase cyber security return on investment and align more clearly with the varied types of business risks that executives understand.

CISOs are not without ideas, but they need to approach and communicate with clarity

The CISO's role is often viewed – from arm's length, at least – as complex and technical. But senior and operations management personnel need to recognize that the majority of the protection provided is to secure authorized access, sharing, and manipulation of 'data.'

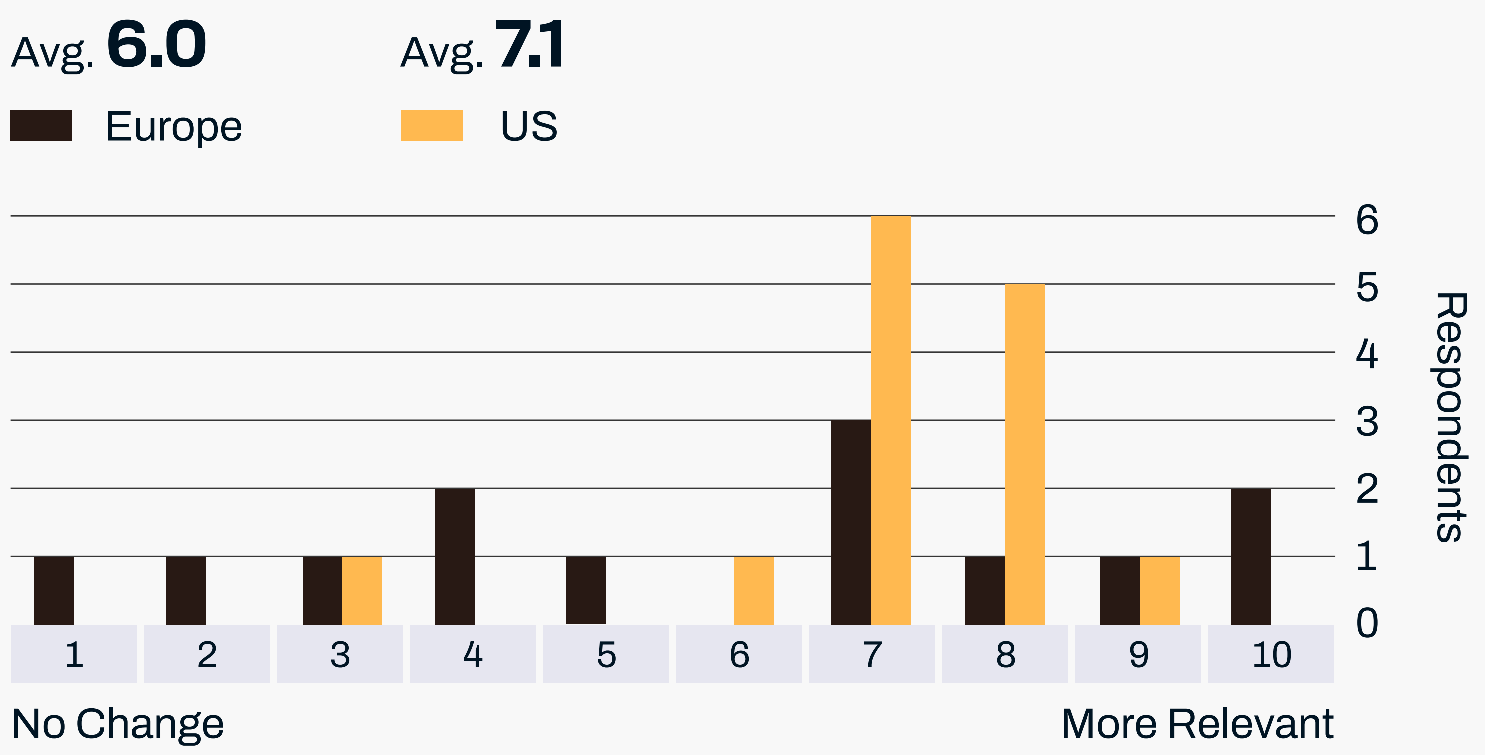
Using data regulation as an example to align cyber security to operational relevance can help to raise awareness and therefore garner support for understanding, interest, and profitability conversations at board level.

Business leaders are not failing to recognize cyber security as a key part of operational relevance. However, the CISOs in this study reported more direct questions from their CEOs about incidents, and if such incidents affect the operational availability of the business. Cyber risks can compromise the security of customer, employee and partner data – and that can lead to damaged reputations and threaten future success.

Efficacy of security products

One statement, reiterated many times by our interviewees, points the finger at the efficacy of cyber security vendors. Software and hardware security products are written with zero liability; any recourse of culpability invariably rests with the CISO instead. This response is confirmed by Debate Security's October 2020 Cybersecurity Technology Efficacy report[1.]

Do you believe that cyber security has transitioned over the past 12-18 months in operational relevance?



> " I believe people's awareness of security has increased, which has in turn brought security teams closer into the discussions around operations."

John Scrimsher, CISO, Kontoor Brands

> " Cyber crime has necessitated an increase in cyber resilience for organizations - more proactive than reactive. Having defense in layers, and the right people and processes over technology, is key."

Chani Simms, CISO, SHe CISO Exec

> " Cyber security can consume as much budget as you give it, but there is no ROI about the risk that it will manage."

Matt Stamper, CISO, Evotek

Question2

Are your leadership teams more, or less, engaged with IT security teams? relevance?

Are your leadership teams more, or less, engaged with it security teams?

The range of responses to this question highlighted varying degrees of engagement.

Leadership teams are keener to engage more with our CISOs and their security teams, according to our respondents. Almost two-thirds (65%) of the CISOs believe there has been a positive move to engage more with their teams. Both regions averaged 6.5-6.8, although more US CISOs (73%) scored at or above their average.

The heightened importance and coverage of security in the business and across the respondents' chosen industries has started to affect a changed engagement over the past 18 months. Commonly, when researching across different industries and sizes of organization, the more positive indicators come from those organizations with a flatter hierarchical structure.

CISOs suggested that it can be easy to assume that everything should be naturally aligned and that every employee from the top down takes an interest in cyber security across all roles, but this is never the case. Often, a positive outcome depends on CISOs applying pressure and communicating with convincing arguments before the engagement happens. Many of the CISOs believe that all leadership individuals could do better.

Those respondents that reported a positive engagement – for understanding the value of security teams and their concerns – believe that it is driven from the CEO down. These organizations have security councils with regular monthly and weekly meetings, engaging with other technical leaders, such as the CTO and CIO, providing valued input to board meetings.

> **“Especially as the customer agenda had changed, so they have had to change. The challenge is: was it security that increased the engagement, or was it the CISO?”**

Andrew Rose, CISO, Vocalink (A Mastercard Company)

> **“Yes, they are more engaged – because we have a very engaged CEO who wants to know about context.”**

Anonymous CISO

> **“Less engaged. Security is considered one step below relevance.”**

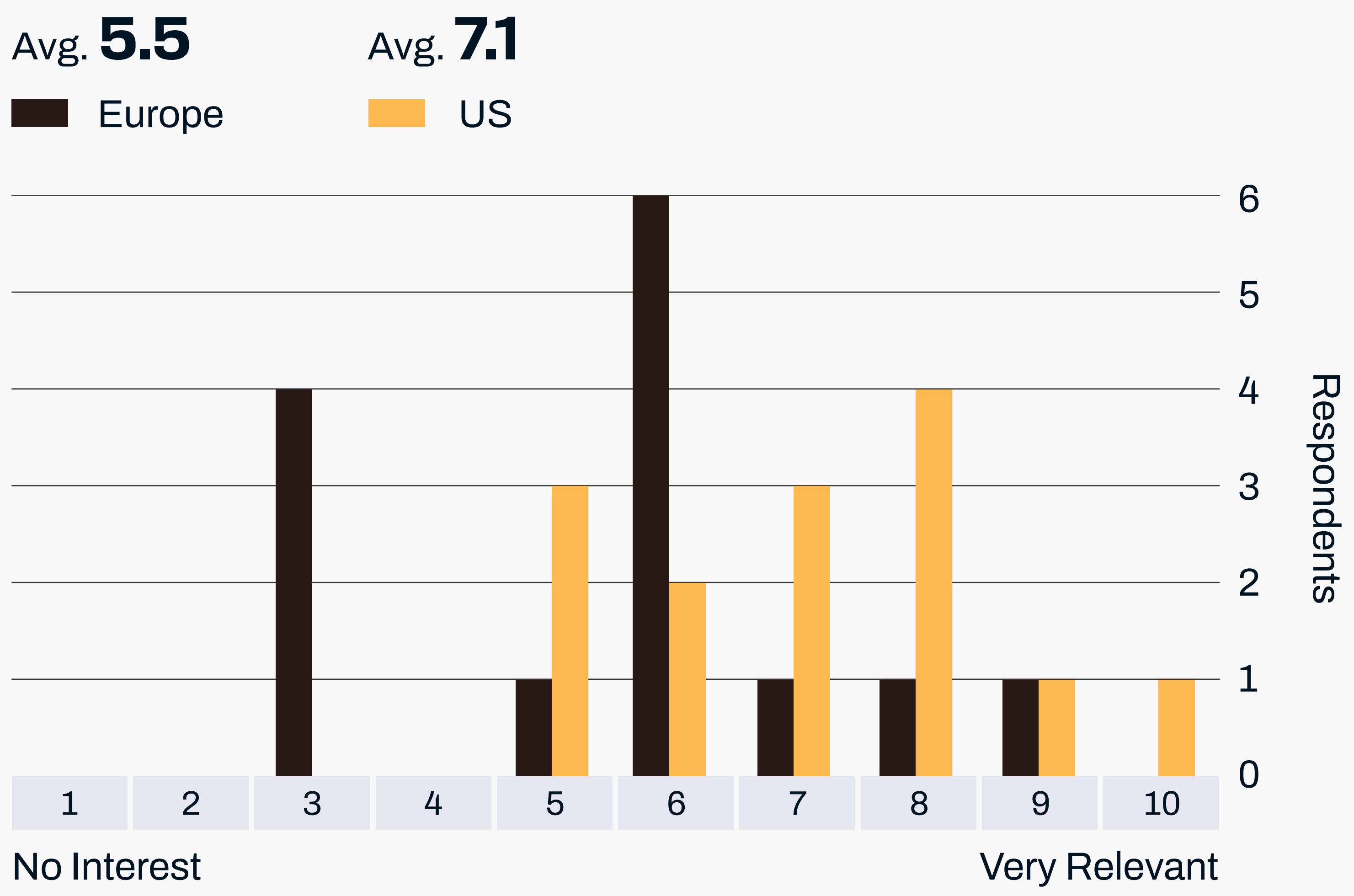
Nathan Reisdorff, CIO, New England Law

Lack of understanding is still a barrier

Some CISOs reported that security is still perceived purely as an IT function or a cost to the business, with no tangible ROI aligned to various business risks. Organizations where this perception was noted – and also where the CISO reports directly to the CIO – appear to suffer additional barriers primarily associated with lack of visibility and no direct access to senior management, which restricts accessibility to the security team.

Many CISOs noted that high-profile incidents such as ransomware infections raised awareness, but this often only created a short-term change or lip service. When CISOs ask senior management about their interactions with the security teams, they say they are more engaged, although many CISOs are not observing any evidence.

What priority do you place on responding to cyber security coverage in the news?



Question 3

Have board priorities and attitudes changed regarding the importance of cyber security protection?

Have board priorities and attitudes changed regarding the importance of cyber security protection?

CISOs must continuously deal with a variety of board perspectives regarding the importance of cyber security protection.

While 78% of the CISOs scored our question highly (between 6-10), only 10% believe that board priorities and attitudes have changed at the highest level (scoring 9 or 10), leaving much more work to be undertaken.

Many (69%) believe that boards, investors, and CEOs now understand that cyber incidents – and the reporting of them – could negatively affect them at any time. Stiffer regulatory enforcement and the threat of severe monetary penalties means that cyber security, when aligned to these requirements, has a greater top-down priority and needs to be taken more seriously.

Several of the CISOs we interviewed report that, when they first joined their employer, it did not have an appropriate security culture. Rectifying this required a persistent program of communication, metrics and education. CISOs have had to learn to convey the value of cyber security at the highest (spoken) level. In many cases, the conversation has needed to be constructively argued, or any appreciation is only recognized after the company has experienced a cyber incident.

In contrast, those CISOs working within organizations with more proactive boards believe executives at the top understand the relevance and detrimental effect of a cyber incident to their organization.

Proactive organizations have set a strategic direction for security via regular security board meetings (chaired by the CEO or COO) that informs how they should approach business operations and their cyber security priorities. They are also learning to understand their own liability and insist that CISOs build closer working relationships with the risk management teams, adopting both a qualitative and quantitative attitude, to ensure their company can mitigate or respond directly to negative stories about them or their industry in the headlines.

> **“ It used to be about qualitative risk in the past, but this has changed because of regulatory implications to the board.”**
>
> Todd Gordon, Director, Information Security, EisnerAmper LLC

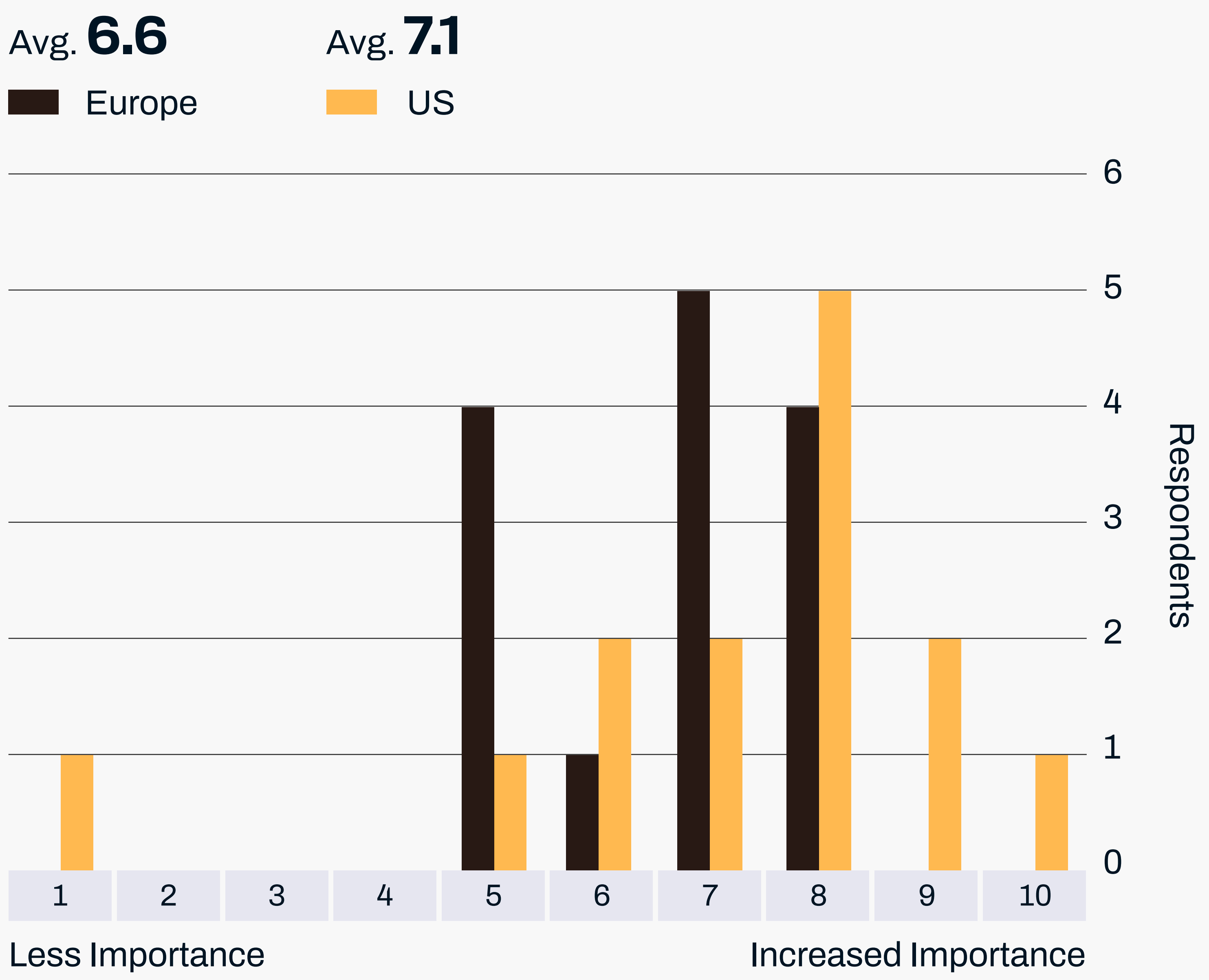
> **“ I do believe that [awareness of the impact of cyber attacks] is starting to change across organizations, as a breach could have far-reaching impact on brand reputation. Boards are starting to pay attention to Zero Trust and Defense in Depth strategies.”**
>
> Royce Markose, CISO, rewardStyle

The mid-range of acceptance covers those boards where attitudes have changed, but the CISOs are still unsure if it really is a priority. In many of these cases, CISOs who spoke with us believe that the reality of the security debt their organization has built up will hit home when a breach affects their organization's brand and reputation, triggering unprepared and reactive responses to previously ignored risk. This doesn't stop some organizations insisting that security teams are able to make do with the same resources. Many CISOs will not have the tools or skills to deal with incident response or minimize the impact on the business. With limited or no top-down direction, CISOs do not have the full picture that identifies what to protect (including unknown shadow IT) and what the impact of an attack may cause.

At the lower end (21% scoring 1-5), our CISOs report that some boards remain convinced they can solve any risk with traditional security management. A regular comment from our panel was that this type of board only wants to see security as a lower-priority cost to the business, and can be consequently unreceptive to the reporting of cyber security issues or risks. These boards may change their minds after an incident (if, indeed, they are still in their roles). However, the CISO also worries that any lessons learned following an incident may be forgotten, with no further recurrent investment or cultural changes applied, leaving the company open to further cyber incidents.

Our CISOs believe that for boards to prioritize and truly understand the significance of cyber security to their business, they must adopt the best practices from CISOs in the larger organizations and establish a cyber security board that is chaired by the CEO.

Have board priorities and attitudes changed regarding the importance of cyber security protection?



Question 4

What are your beliefs about cyber security as a board discussion?

What are your beliefs about cyber security as a board discussion?

The topic of cyber security and the board is probably one of the most evergreen. Although the CISOs scored predominately in the upper range (6-10) with an equal balance across the two regions believing that board-level conversations are a priority, surprisingly, the respondents had diametrically opposed contextual views on the subject.

In one corner, CISOs strongly believe that cyber security is one of multiple risks that all businesses have to contend with, and that these are owned by the top of the organization. As we've seen from earlier questions, some CISOs already had a seat on the board, or work with board committees that tackle cyber security, allowing them to relay security risk. This board-level inclusion has not come easily. The majority of CISOs have had to wrangle to establish high-level engagement around cyber security risk management, in the same way that their peers huddle to discuss legal, finance, and human capital risks with a collaborative objective to set expectations and agree KPIs.

In the opposing corner are the CISOs who continue to push cyber security as a board-level discussion but see a general inability for boards to recognize the criticality of cyber security in business operations, focusing instead on the 'other higher priorities in the business' directly associated with revenue generation. They believe that this shows senior management's lack of understanding of the risk exposure that comes with some of the higher priorities, such as increased digital adoption.

The CISOs acknowledge that maturity curves exist from both a governance perspective and numerous international standards for maturity and risk frameworks, but they do not have an accepted framework for board-level governance for cyber security. This lack of cyber security governance can provide more skeptical senior managers with an easier path to resist the need to change.

Our panelists made the point that cyber attacks can be near-constant. And in stark contrast, other risks in the ERM framework – e.g., property damage, currency risks, or product failure – are far less frequent.

> **“ Cyber security is one of the multiple risks to the business; we have a cyber security board committee chaired by the CEO.”**

Hitesh Patel, Head of Cybersecurity, Cloud Computing & Digital Infrastructure Audit & Risk, Fidelity Investments

> **“ It needs to be an integral part of business and security risk discussions. The board should be learning about risk as a possible impact to the business and shareholders.”**

Scott Goodhart, CISO Emeritus, The AES Corporation

> **“ It needs to be an integral part of business and security risk discussions. The board should be learning about risk as a possible impact to the business and shareholders.”**

Ian Dudley, IT Director, DriveTech

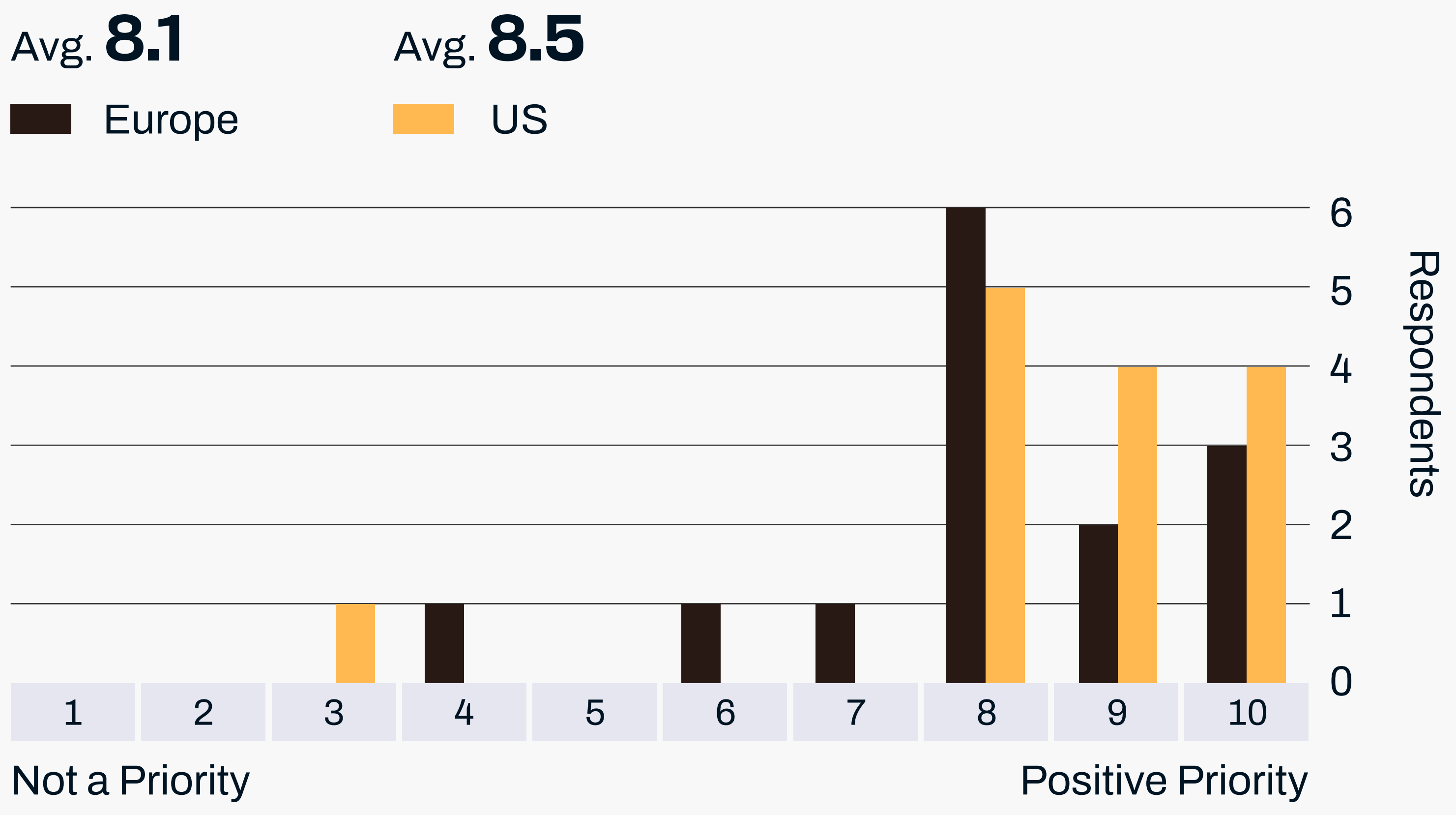
Another unhelpful factor to come up again is the media, and its high-level (but sometimes context-deficient) coverage, which can make matters complicated for the CISO. Those board members who do not understand the language of cyber security can be put off by perceived technical complexity. Further, the combination of reporting and an inability to 'direct down' to CISOs with the right questions can create a situation in which it is difficult to track the effectiveness of cyber security. Focusing on the latest news headline – without understanding how it corresponds to actual business risk – can make it difficult for non-technical executives to fully engage with cyber security. But at the same time, non-technical executives appreciate that high level of caution (Zero Trust) may help to protect consumers, employees and business partners. This latter insight suggests that half the battle is already won, but there is still some way to go to win over some non-technical parties on other areas of cyber security.

When a board member asks, 'how secure are our systems?' the CISOs believe that there is a desire to understand the complete answer with all risk factors and implications fully appreciated. But in truth, this would be a challenge for any non-security leader.

CISOs in both corners have to continually take ownership to educate the board and encourage engagement that will enable understanding, quantifiable measurements, and visibility for the operational risks that a cyber attack or incident can impact. And board members could be more appreciative of the digital competency required in modern business (and therefore the modern threats that they will be susceptible to).

Communication between the CISO and the board must not be a monologue, or a one-way trust request. Regular conversations are essential to set and maintain quantifiable measurements. These discussions need to be comprehensive and to the point, in a language and tone that can be clearly understood. Once this style of dialogue is established, it creates a conduit for continuous performance monitoring and higher overall gain. Better understanding can help other personnel to be more involved, and identify and raise potential cyber security issues. That could be an encouraging shift from 'siloed security' to more proactive 'business team players' across the business.

What are your beliefs about cyber security as a board discussion?



> " There should be a flow of information in both directions, rather than just from CISO to the board. The board should create the expectation and educate the company on what types of questions they would like answered."

Gene Zafrin, CISO, Renaissance Re

> " They think they want to know 'how secure is our system?' but any answer that's not 100% leaves them open. What they really want to know is, 'are we doing enough?' Trusting your opinion helps answer that."

Andrew Rose, CISO, Vocalink (A Mastercard Company)

Question 5

Do you believe cyber security is treated as a business enabler or a risk mitigation practice within your organization?

Do you believe cyber security is treated as a business enabler or a risk mitigation practice within your organization?

Every CISO would love to break down cyber security barriers and become a critical path for enabling business activities. It was clear during this study, however, that this is wishful thinking. A majority (72%) of the CISOs scored 7.9 on average and continue to see cyber security as a risk mitigation practice by the business. Around a fifth of CISOs say they are making progress towards shifting internal perception of cyber security towards it being a business enabler. That said, none believe they have completed this switch: not one respondent scored in the 1-4 range. The general perception is that identifying business enablement alignment is a pipe dream for the majority of organizations.

It seems that CISOs and their CEOs see cyber security predominately (79%) as a risk mitigation or compliance practice. Ideally, when invited to contribute, cyber security is considered within an enterprise risk management framework, the primary task being to reduce negatives rather than add positives. There are a very small number of industry-specific occurrences, such as legal firms and other types of service-based organizations, that can provide cyber-centric value-added services (SOC2) as a business enabler.

For some organizations, successful compliance is a minimum requirement

In this context, good security is a business enabler because it aids compliance. An example is SOC2, which applies to technology-based organizations storing customer data in the cloud, such as personally identifiable information (PII), health data (PHI), and credit card information (PCI). In these cases, SOC2 is one of the most common compliance requirements that technology-focused companies must meet today to operate legally. Other compliance requirements can vary depending on location.

> **“ At the moment [cyber security] is a risk mitigation. The business is starting to understand how it can be a business enabler, but it’s not in the innovation area at the moment.”**
>
> Mauro Israel, Corporate CISO, ORPEA Group

Respondents agreed that a level of internal misconception is being assumed, where individuals are interpreting cyber security as a business enabler, solely down to any increased security awareness and the involvement of the security team at the start of projects, which are still directed by the IT team. Peers of the CISO accept that a cyber incident could disable some or all of business operations, but they are not embracing a 'security-by-design' operation that could encourage consumers and business partners to engage with the organization. When you combine strong cyber measures to mitigate an attack, 'security-by-design' organizations will align correctly to business enablement.

The challenge of conveying the ROI of cyber security

Without the instance of a mitigated attack, cyber security offerings do not have an immediate demonstrable ROI for the top or bottom lines. The financial benefits of robust cyber security implementations come from not having to pay ransomware, regulatory fines, or suffering the loss of customer confidence after a breach.

It is all too easy to work on the assumption that cyber security is a cost of doing business, rather than a cost of business. Consequently, there is a requirement for better understanding and business application regarding cyber security.

We have already talked about how non-technical staff can be helped to realize the benefit of having a more secure system environment in which to work with email, web, and access and identity security tools.

But the other side of this is that no matter how experienced and knowledgeable CISOs are, very few of them truly understand how to use cyber security to increase the opportunity for their business. The good news is that many are open to understanding the correlation and how it can make budgeting easier and lower the perception that their role and its associated technologies are only a cost to the business.

What priority do you place on responding to cyber security coverage in the news?

CISOs view media coverage of cyber security incidents as a double-edged sword: beneficial but also distracting. If the coverage is relevant to their industry, they can prioritize the content and provide their own context. But many respondents saw most coverage as either too high level or part of a theme of cover, rinse, wash, repeat. This was reflected by half the CISOs we spoke with scoring between the mid-range (4-6) available. But numbers can be deceiving; 64% of US CISOs appear to acknowledge the relevance (scored 7-10) of cyber security coverage, three times more when compared with only 21% of their European peers.

> "Our SOC2 certification provides a good standard and testing, verifying to clients and selling to new clients. Although risk mitigation is still emphasized, and our exec board need to understand how we are dealing with it."

Todd Gordon, Director Information Security, EisnerAmper LLC

> "News can help – and distract. We leverage threat intelligence over news. If it's in my industry, we need to understand how it might affect us."

Hitesh Patel, Head of Cybersecurity, Cloud Computing & Digital Infrastructure, Audit & Risk, Fidelity Investments

> "It's important to stay advised of new threats but take everything with a grain of salt."

Todd Gordon, Director, Information Security, EisnerAmper LLC

How the right kind of coverage can help security firms to make money

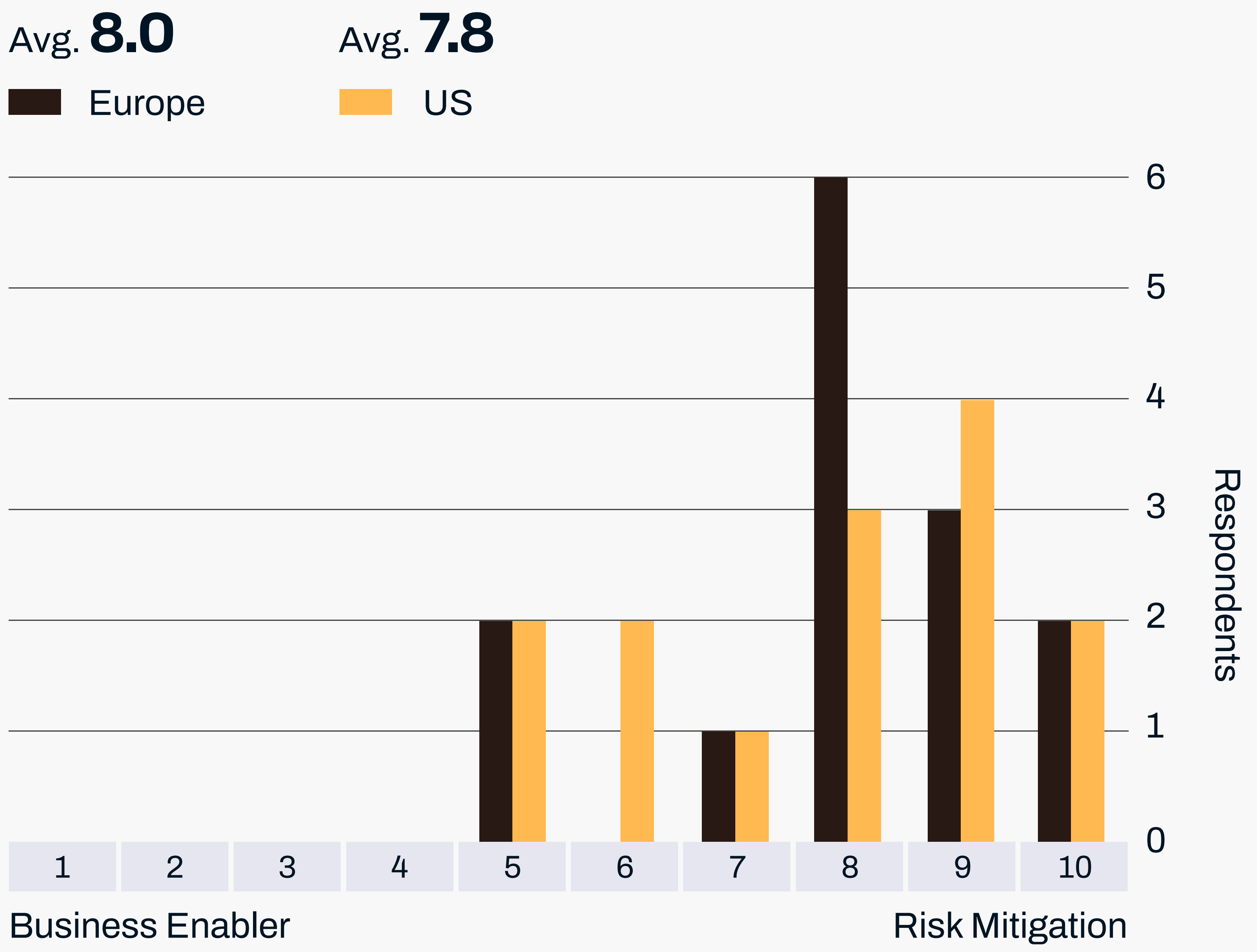
An exception to industry-focused coverage was WannaCry. Its cross-industry implications served as a blunt incentive to many CISOs to widen their focus and appraise the risk factors to their business. The majority of the CISOs expressed frustration at what they saw as sensationalism and wanted to see more factual content that informed the reader about the source of the attack, actual disruption to those affected, and what measures the target organizations and supporting agencies were undertaking.

Regardless of the writers' intent, media coverage is consumed and interpreted by CEOs who increasingly want to understand the relevance of these attacks to their own business. Sensational headlines from general reporting may be great for grabbing attention but they can often waste a CISO's time if the high-level soundbites aren't informative or lead to actionable, helpful insights. Often, such reporting can raise more questions than it answers. CISOs need solutions, ideas, and knowledge. They are not going to contact an alternative or additional security vendor without appropriate cause to do so.

So, where do security firms need to target to gain more interest in their offerings? CISOs use open-source newsfeeds from respected experts (rather than more generalist media) for an informative reality check that adequately describes attacker tools and procedures. They are not totally dismissive of the general media reporting but would ask the technical journalists to raise a tangible awareness around cyber security rather than just making headlines.

> **"Look for an opportunity to learn about the coverage and evaluate if it could improve the knowledge of cyber security in the company and respond internally as an educational exercise."**
>
> Scott Goodhart, CISO Emeritus, The AES Corporation

Do you believe that cyber security is treated as a business enabler or a risk mitigation practice within your organization?



Question 6

Do your (non-IT) peers in your organization understand how cyber security is a threat to their responsibilities?

Do your (non-it) peers in your organization understand how cyber security is a threat to their responsibilities?

There is still a cultural gap between the business of security and the business of the business, and this calls for difficult conversations and a lot of education. Some senior management believe that a cyber attack equates solely to phishing, and that if it is resolved by automated discovery or the suspicions of an employee, then all will be well.

In general, CISOs believe (73%) there is greater awareness of the impact of cyber security across their organizations, although no CISO scored this at the highest level (9 or 10). One of the largest chasms to cross regarding the value of security to business success is between technological and line of business discussions – with the CISO on one side and their peers on the other. CISOs in larger enterprises are integrating themselves into non-security-focused business meetings, planning, customer acquisition, and regulation discussions as a way to incorporate the business tone of voice into their discussions to elevate security as a critical element of business growth.

While security teams like to bang the drum about possible attack vectors and incidents that they have successfully mitigated, responses from non-tech staff can lack the same enthusiasm. Worse, this latter group sometimes pretend to understand, or pay lip service without fully realizing the benefit of security success stories that positively affect their own responsibilities in the organization. As one respondent put it: “Some do understand. Some pretend they understand. Some don’t care.”

The benefits of a security charter

The businesses with an ‘open culture’ are more likely to get buy-in from their peers about the relevance of security and its impact on their responsibilities. In many cases, they have implemented a security charter so that all functions in the business understand its relevance and importance to operational efficiency.

This has required many CISOs to build security awareness training to ensure everyone can appreciate the cause. It is never a single exercise but a continuous process with an objective to change cognitive actions and curtail the temptation of an employee to find a workaround if they feel security stipulations are restricting their workflows.

> **“ I do think they understand the threat to a certain level, but it’s a continuous learning exercise. They don’t always understand the possible impact(s), so it needs the CISO to explain this to them - an important education process. People need to take ownership in their areas.”**

Scott Goodhart, CISO Emeritus, The AES Corporationon

> **“ We have a security awareness program to address the weakest link. We can build a strong system, but no control over the humans (weakest link). They should understand their share of responsibilities.”**

Hitesh Patel, Head of Cybersecurity, Cloud Computing & Digital Infrastructure, Audit & Risk, Fidelity Investments

The WithSecure™ Countercept perspective

The CISO and their security team can set security policy all day long, but it takes everyone in an organization to make it work, and none more so than the members of the board. One of the most underrated yet valuable aspects of a CISO's role is the job of getting the rest of the business to understand the role cyber security plays.

The success – or otherwise – of communicating this often hinges on the way CISOs communicate with their board of directors about risk. There are two other challenges, however.

Owning risk

Persuading – or obliging – everyone is a job that's bigger than just the CISO and their team: it's a board-level issue, and they need to persuade everyone in the organization to be accountable for the security of their part.

The problem with this assertion is that it is utopian – but it is something to aspire to regardless. It can be improved by identifying and testing how best to communicate the importance of good security to employees and leaders. It's quite common for broader cyber security awareness to be limited to annual, compulsory training – and that needs to change. Delivering engaging, easily-understood training that nevertheless doesn't undermine the importance of what is being conveyed is a challenge – but one that can be overcome. This is something security vendors already do, but it is something few customers ask for help with as part of the service they pay for.

Communicating risk

The other side to this issue is identifying and communicating risk. There have been plenty of attempts over the years to work out how to establish how cyber security risk should be defined, assessed, and mitigated effectively, but none have been particularly successful due to the way that we, as a species, evaluate risk.

Yet all three of these things are important when working out whether a product, business or service will help solve a particular problem. Quite a lot of the tools and frameworks available for assessing what controls an organization has, and should have (two examples are NIST Cyber Defense Matrix[2] and MITRE ATT&CK[3]), are helpful, but they aren't a silver bullet solution to assess the risk an organization faces.

This leads us to another challenge: even if an organization can identify and quantify the risks it faces, it's not a given that it can accurately assess its own maturity when it comes to dealing with that risk; in part, this is down to vendors overstating the efficacy of their product or service. Regular red team exercises against your security providers (and involving them in the debrief) can address this, as can a discussion of purple teaming[4] and an overview of the results.

Buying risk offset

Understanding and communicating the risk and setting it against the context of maturity often leaves organizations with more than one hole in their defenses that they need to plug – and fast.

Going back to the board you've just educated with a big shopping list can be daunting, especially given how cyber security spending is often framed. Viewed as something akin to an insurance policy encourages buyers to think in terms of cost. That, however, omits cost avoidance, or even the potential value add of effective cyber security. Partly this is due to the way that humans look at risk when it comes to looking at losses and gains, and our judgement is sometimes skewed by the language used to describe the probabilities of risk, loss and gain. In short[5], investment in security is often framed as a definite loss – a cost – where the risk of not investing is 'only' a probable loss.

Chapter 3 – The cyber threat surface

Our Chief Information Security Officers (CISOs) reported that their teams fought off an increasing volume of attacks over the past 18 months. But they also said the number of incidents they faced remained pretty much the same. This revelation might lead to the conclusion that their teams are getting better at defending, criminals are more profligate and less effective, or a combination of the two.

Our respondents are fully aware they're up against a criminal industry, not just individuals or gangs. Using cast-offs and stolen tools from nation-state actors and other threat groups, some of the more sophisticated hackers are causing a real headache. Meanwhile, other threat groups are failing to move on from the tried-and-tested (and now more readily defeated) tactics, and are becoming background noise for many cyber security teams.

Employees remain the most popular and effective vector for attackers, and are therefore a continual area of concern for CISOs, especially as they've observed adversaries employing far more elaborate and sophisticated approaches of late.

Increasingly, ransom payments bring all kinds of risk, not least where organizations are having to weigh up the dilemma of making a ransom payment to restore their operations, while inadvertently breaching government sanctions by paying groups that are subject to international or national economic sanctions.

Rather than continuing their primary focus on endpoint security, CISOs gave the nod to a more holistic, architecture-wide security threat surface approach to match the criminal's attack vectors, expressing their willingness to assume greater responsibility in the event of breaches.

Question 1

Have you had to respond to a greater number of specific cyber incidents in the past 12-18 months? What are the top three threats?

Have you had to respond to a greater number of specific cyber incidents in the past 12-18 months? What are the top three threats?

A cyber attack is 'an attempt' by a skilled (or unskilled) adversary to breach a system's security policy to affect its integrity or availability, and/or the unauthorized access or attempted access to a system or systems.

A cyber incident is 'a breach' by a skilled (or unskilled) adversary of system's security policy to affect its integrity or availability, and/or the unauthorized access or attempted access to a system or systems.

The above definitions are clearly not one and the same. Additionally, the vast majority of CISOs we interviewed were exasperated with the continuous flow of inaccurate and poorly researched news stories about attacks and incidents, interspersing definitions to sensationalize their headlines, enthusiastically reused by security vendors.

The advancement of attack vectors being initiated by cyber criminals has sparked the need for CISOs to strive for a redefinition of cyber incidents that defines the difference between a 'major cyber incident' and a 'cyber incident.'

Forty-four per cent of the CISOs scored 1-5 and told us the number of cyber incidents they observed had not grown over the past 12 months. This does not mean that the number of cyber attacks and cyber incidents are at an equilibrium; the remaining 56% of CISOs in our study have seen the number of cyber incidents grow, including the diversity of attack vectors. One respondent had seen the number of attacks increase by 400%, but no discernible increase in incidents. In fact, some respondents have seen a downturn in specific cyber incident vectors.

Where the security teams have needed to respond to a cyber incident, it is never about the quantity of the initial attacks, except where quantity when related to volumetric attacks such as distributed denial of service (DDoS) is very much a problem. It's now about the quality of the attack, including the use of evasion techniques, machine learning (ML), and multiplicity of [simultaneous] attack vectors initiated by cyber criminals.

> **" Attacks are increasing; phishing, phishing and phishing. Seeing it all the time. But it's still the same method of attack vectors being used."**

Ian Dudley, IT Director, DriveTech

> **" We enforce our tools and look for more incidents, which means that we find more attacks."**

Hitesh Patel, Head of Cybersecurity, Cloud Computing & Digital Infrastructure Audit & Risk, Fidelity Investments

> **" The threats are higher, but the number of incidents has dropped."**

Marc Ashworth, SVP, CISO, First Bank

> **" We have seen a greater number of attacks as we moved off a managed SIEM/log management provider and insourced this function. We now see all of the incidents internally. Now seeing 500+ (attacks) a quarter, having better precision and identification using our internal tools and capabilities."**

Leo Cronin, CSO, Cincinnati Bell

The increased awareness and deployment of security tools, threat intelligence and MITRE ATT&CK frameworks has meant that many security teams are proactively looking for gaps and blind spots in their architecture and operating environment to identify the outlier attacks that could create a cyber incident; hence, an expected increase in the number of intelligence-led, reported cyber attacks.

Many of the CISOs said they are challenged with an increase in possible cyber incidents; the associated business risks, due to the increase in a more mobile and flexible office workforce, are identified:

1. A contaminated computer from outside comes inside the business network and acts like a trojan horse, infecting others on the network and creating the possibility of thousands of workers innocently exploiting the malware.
2. Hybrid – the continuous back and forth between business and social locations creates a major risk.
3. Contamination of computers used in the home that can be used for social engineering purposes, alongside its primary purpose of accessing communications and sensitive files, can impact the rest of the IT inventory, without entering the office.

The top three threats consistently encountered by the respo dents were:

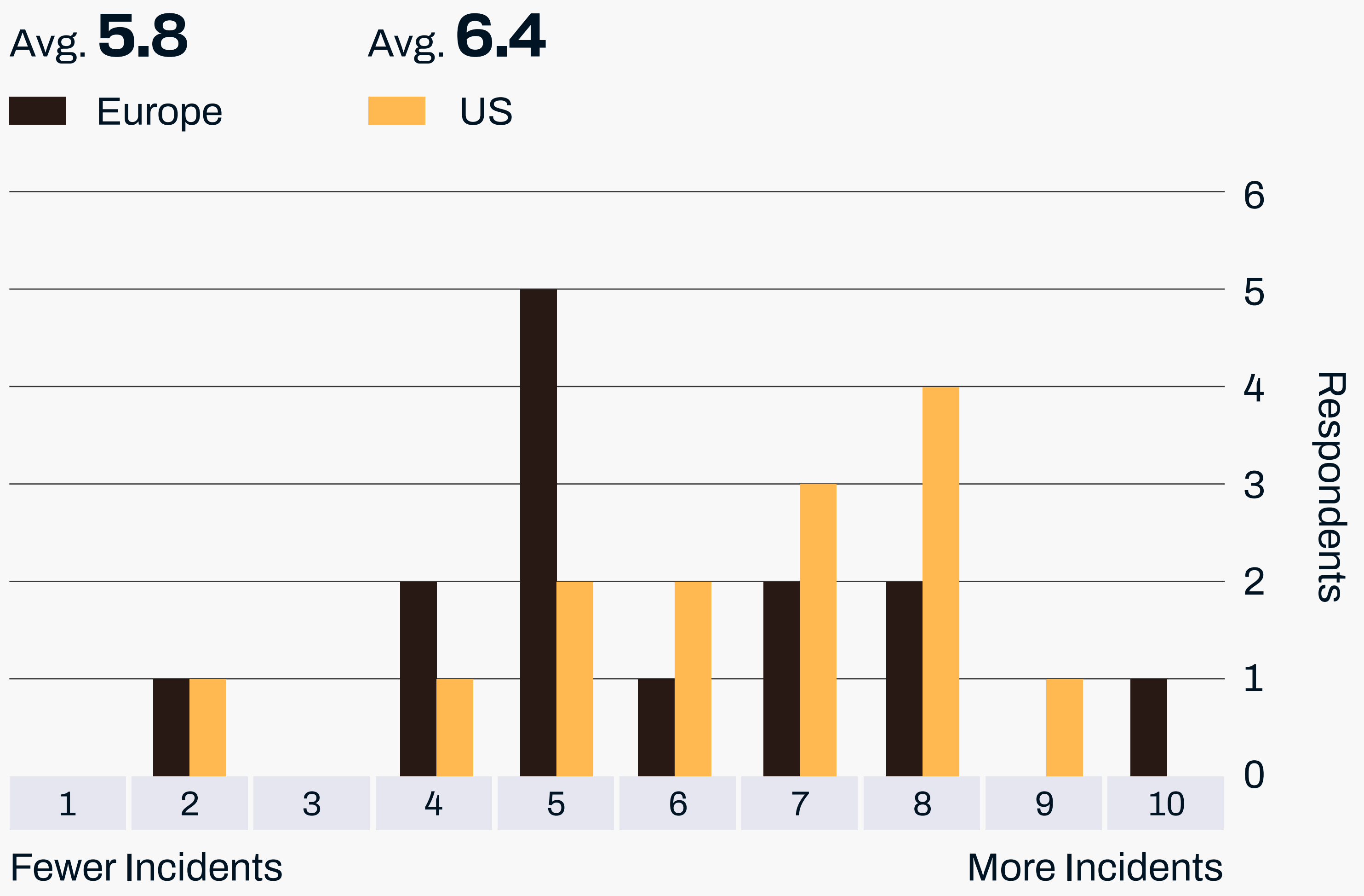
1. Phishing
2. Ransomware (wiper malware)
3. Business email compromise (BEC)

In addition, the following cyber attacks were cited as ongoing challenges for their security teams, showing the diversity of attack vectors employed by criminals: trojan horse (via exploitation of remote teleworkers); data leaks (predominately external and third-party led); DDoS (diversionary and application), MSS/cloud hacking (externally driven); identity/credential/account compromise (via social engineering/phishing); APT malware (organized groups).

The CISOs consistently mentioned that they are having to run their operations with a level of security debt, where new security tools, lack of early security integration across business projects, and internal security awareness had not been previously prioritized. CISOs appreciate that they are constrained with actioning these levels of debt due to budget constraints, resource workloads and priority of other business activities. They also recognize that many of the issues they read about can be overcome by enforcing basic security processes that would remove the problems with legacy technology, patching and inefficient security tools.

CISOs acknowledge that as their businesses increase their 'network-effect' (the value of a network is proportional to the square of the size of the network1) driven by greater digital platform integrations, they will need to be prepared for the introduction or increase of cyber attacks from nation-states that will be a threat to critical national infrastructure, defense, health, and financial industries all taking the opportunity to exploit innocent or rogue insiders.

Have you had to respond to a greater number of specific cyber incidents in the past 12-18 months?



Question 2

Who’s moving fastest – you or your adversaries (criminals)?

Who’s moving fastest – you or your adversaries (criminals)?

Seventy-two per cent of the CISOs are in no doubt that the cyber adversaries they face every day clearly move the fastest, having the capability to attack from a distance, with greater agility and increasing resources, delivering an impact at speed that could have a catastrophic effect on their organizations.

Compared with legitimate businesses that have regulatory constraints, fluctuating budgets and internal controls of security over operational efficiency to balance, adversaries have the unconstrained opportunity for financial gain or political interference.

Defensive security is always a harder challenge, as you need to get your game theory right every time. An oft-heard refrain was: “We have to win every day, for every attack, whereas the hacker only has to win once.” Trying to create a cyber security equilibrium with an adversary is overwhelming.

CISOs acknowledge that they have a critical dependency on security vendors, as they do not have the scale to develop their own security tools, so will continue to be reliant on the security vendors to deliver on their product intention. Whereas their adversaries write, update and can integrate their code with ease to deliver offensive attacks every time.

When CISOs raise concerns internally and insist that senior management fund or invest in ensuring the security basics are consistently in place and policies enforced, they’re often challenged with business priorities. These procedural actions can be viewed as boring and restrictive, and not approaching the issue with thought leadership.

> **“ The criminals always. I have a day job – they don’t!”**

Ian Dudley, IT Director, DriveTech

> **“ We have to win every day and every event, whereas the hacker only has to win once.”**

Mauro Israel, Corporate CISO, ORPEA Group

> **“ Adversaries. Constantly changing their attacks. Trying to stay up with them is overwhelming.”**

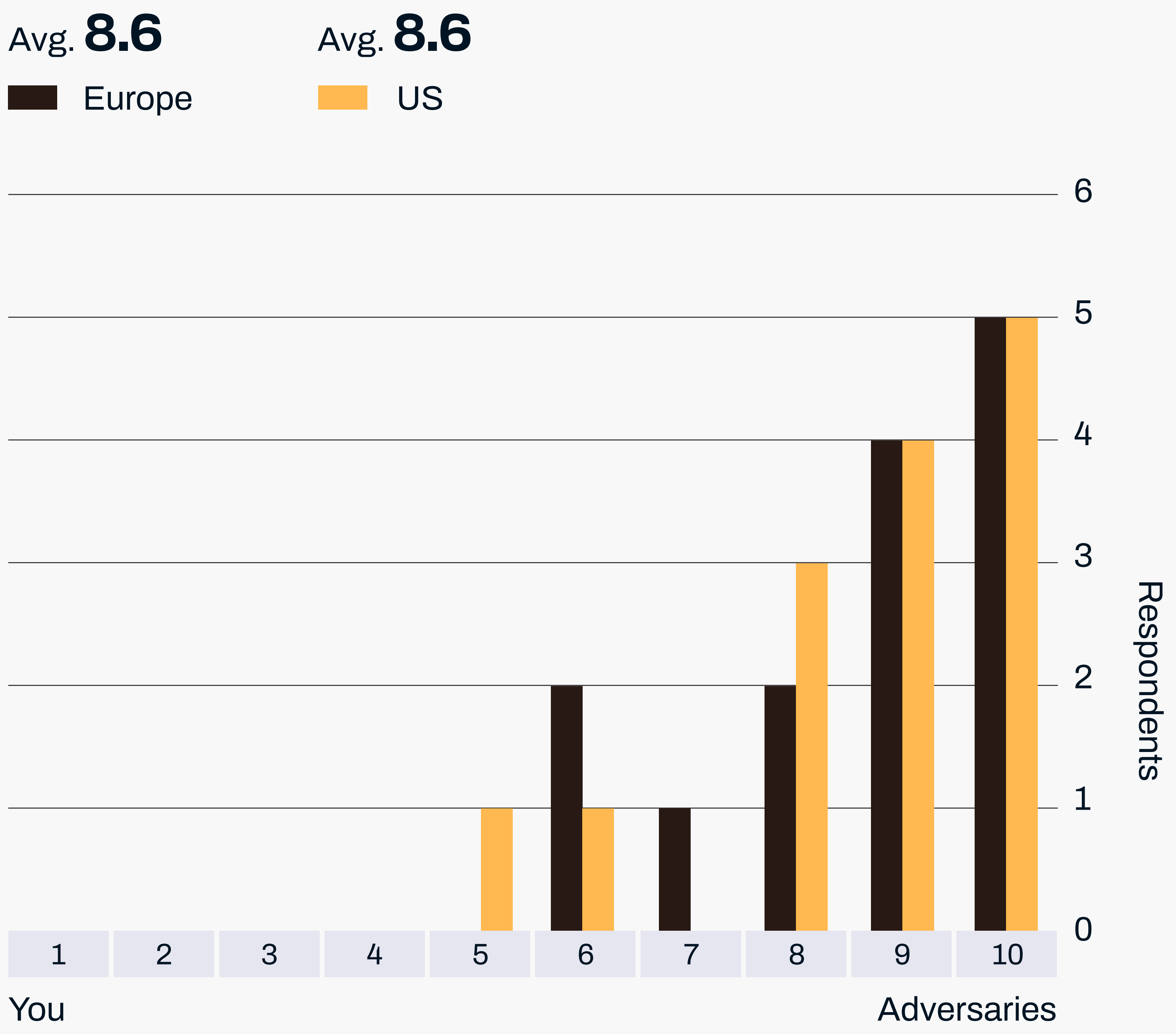
Marc Ashworth, SVP, CISO, First Bank

In general, the CISOs appreciate that the bright lights of cyber analytics, artificial intelligence (AI), ML, secure access service edge (SASE), and other emerging technologies and architectures may elicit an emotional level of cyber protection, but the CISOs all confirm that they will never be able to close the gap on the cyber adversaries unless the basics are in place.

Efficacy: challenged

Being the type to tell it straight, a major concern highlighted once again by a number of the CISOs was that something is definitely not working. They hear that the revenue opportunity for security products is in the trillions of dollars. So why, when businesses have security tools implemented, does the adversary continue to succeed in penetrating their defenses with cyber vectors that have been known about for more than a decade?

Who's moving fastest – you or your adversaries (criminals)?



> **"Definitely adversaries. Better funded and have more time on their hands to practice offensive security – defensive is always harder."**

Leo Cronin, CSO, Cincinnati Bell

Question 3

Do you believe there has been an increase in the threat capabilities of cyber criminals?

If so, what threats worry you the most?

Do you believe there has been an increase in the threat capabilities of cyber criminals? If so, what threats worry you the most?

As with every business, criminal cyber groups know they can improve performance by building partnerships with others. This opens up their market opportunities across more diverse industries, all the while maintaining a line of self-enforcement of their own ‘standards among thieves.’

Most of the CISOs we spoke with are under no illusion that cyber criminals have increased their threat capabilities. Nearly all (96%) of the respondents scored between 6-10 and recognize that the cyber underworld has evolved into a well-organized commercial industry.

In the same way that legitimate organizations build out skill sets to compete effectively in their market, cyber criminals, their teams and alliances exhibit multiple disciplines in a structure of owner-operated, small, mid-size and large group operations. These structures extend to geographically dispersed, organized criminal groups (OCGs). They’re also apparent in well-resourced, nation-state actors such as Lazarus Group and APT 29.

These days, cyber security groups are operating in a redefined arms race, or what one respondent called the “fifth wave of warfare.” US-based CISOs noted that the traditional hackers who have been around for a long time are still using low-grade attack packages. These attackers are becoming background noise.

The major concern for the future is around a small set of attack vectors that have ‘destroy-type capabilities.’ Thankfully, many CISOs have not yet experienced such an attack but recognize the need to prepare for a day when it could happen. One potential scenario could come from a nation-state attack that would normally be isolated and targeted at government and critical national infrastructure. CISOs see the probability of their organizations experiencing collateral damage from such an incident. A more discernible concern arises when OCGs and political activists are able to use nation-state tools gained from allies and enemies* for ‘zero-day’ – and other methods that no one else knows about – used against commercial operations.

> “ **Threat actors are more and more creative. They are now exfiltrating data when asking to pay the ransom.”**
>
> Leo Cronin, CSO, Cincinnati Bell

* These include: US National Security Agency (NSA); the UK’s General Communications Headquarters (GCHQ); France’s ASIS; China’s People’s Liberation Army (PLA); Israeli military intelligence (Mossad); and Russian military intelligence in the form of the GRU.

> “ Techniques have definitely developed and become more professional. My concerns remain on ransomware and wiper software, though; BEC for money is just money, but the other two can kill the business.”

Andrew Rose, CISO, VocaLink (A Mastercard Company)

FOR SALE: damage

Distribution of cyber attack products and services have their own marketplace, often on the ‘dark web.’ CISOs see the easy distribution of advanced cyber attack tooling as a major headache due to the availability of code for phishing, ransomware, APTs, etc, as well as groups that provide cyber criminality ‘as-a-service’ attacks built by teams funded by nation-states or major OCGs. Examples include EternalBlue, largely acknowledged to be a cyber attack tool stolen from the NSA, and elements of code developed by the groups behind the Stuxnet virus.

The free availability of these and other cyber weapons allow organized crime groups to use advanced capabilities against their targets that can be incorporated into the traditional attack vectors. As well as new tooling, the dark web is the centralized marketplace for stolen credentials, data, and intellectual property such as the designs for limited-edition clothing and high-end shoes, creating a one-stop experience that delivers malicious capability and stolen reward.

Wherever the global market looks to gain a foothold to offer services and products to citizens, the cyber criminal sees an opportunity to increase competitive differentiation, market presence, profitability and penetration. For example, CISOs appreciate that cloud infrastructure can be helpful for scaling business and obtaining wider efficiencies, thanks to flexible operating principles and lower costs. But our respondents also noted how cyber criminals have realized the benefits of ‘dark cloud’ operations. With mirrored benefits, the cloud can accelerate criminal user base and volume of attacks to deliver DDoS, malware and phishing, all as subscription services (damage-as-a-service).

It was clear from the feedback that CISOs believe cyber criminals are gunning for two things: financial gain and disruption, the latter via either data breach or infrastructure intrusion. The threats that align to these types of attacks and worry the CISOs most can be broken into two categories:

Ransomware, executed across information technology (IT) and operational technology (OT), is usually delivered directly via malware uploads, or by restricting access via DDoS. The objective of DDoS is to extract a ransom, or be used as a distraction tool, in combination with other downloaded malware for immediate or future exploitation (data theft, web redirects, command and control (C2) establishment).

Ransomware is a growth scourge. These attacks affect normal business operations, can damage services to existing clients/ consumers and hinder the on-boarding of new consumers. The advanced ransomware that CISOs fear the most deploys ‘wiper code,’ which brings unrecoverable damage.

There are also unknown risks to the CISO, such as whether the cyber criminal will go through with their threats if the ransom is not paid, if they will indeed stop flooding the networks or even provide the promised encryption keys after a ransom is paid, or if the threat actor has exfiltrated data that they will sell to the highest bidder, use to extort individual customers, or simply release to the outside world. The capacity for organizations to continue to operate after paying any ransom may be a lower concern for larger companies more able to swallow this loss of capital and services. But for smaller and micro-businesses, this kind of hit could take them out of business – fast.

The other category of threat is ‘impersonation.’ This category accelerates a cyber criminal’s focus on the human, the most fallible component in cyber security. CISOs are starting to experience the evolution of traditional forms of social engineering attacks blended with AI and ML technologies, underpinned with softer intelligence derived from psychology, neuro-linguistic programming (NLP), and human behavioral sciences. Once access and privileges are compromised, impersonation allows a wider variety of social engineering, phishing, BEC and whaling, among others, to evade learned human cognitive actions and take polymorphism functionality to a new level. The latter evasion techniques, combined with AI and ML, may, in the ‘near distant’ future, render many security tools as useless.

Technology capabilities are accelerating for everyone

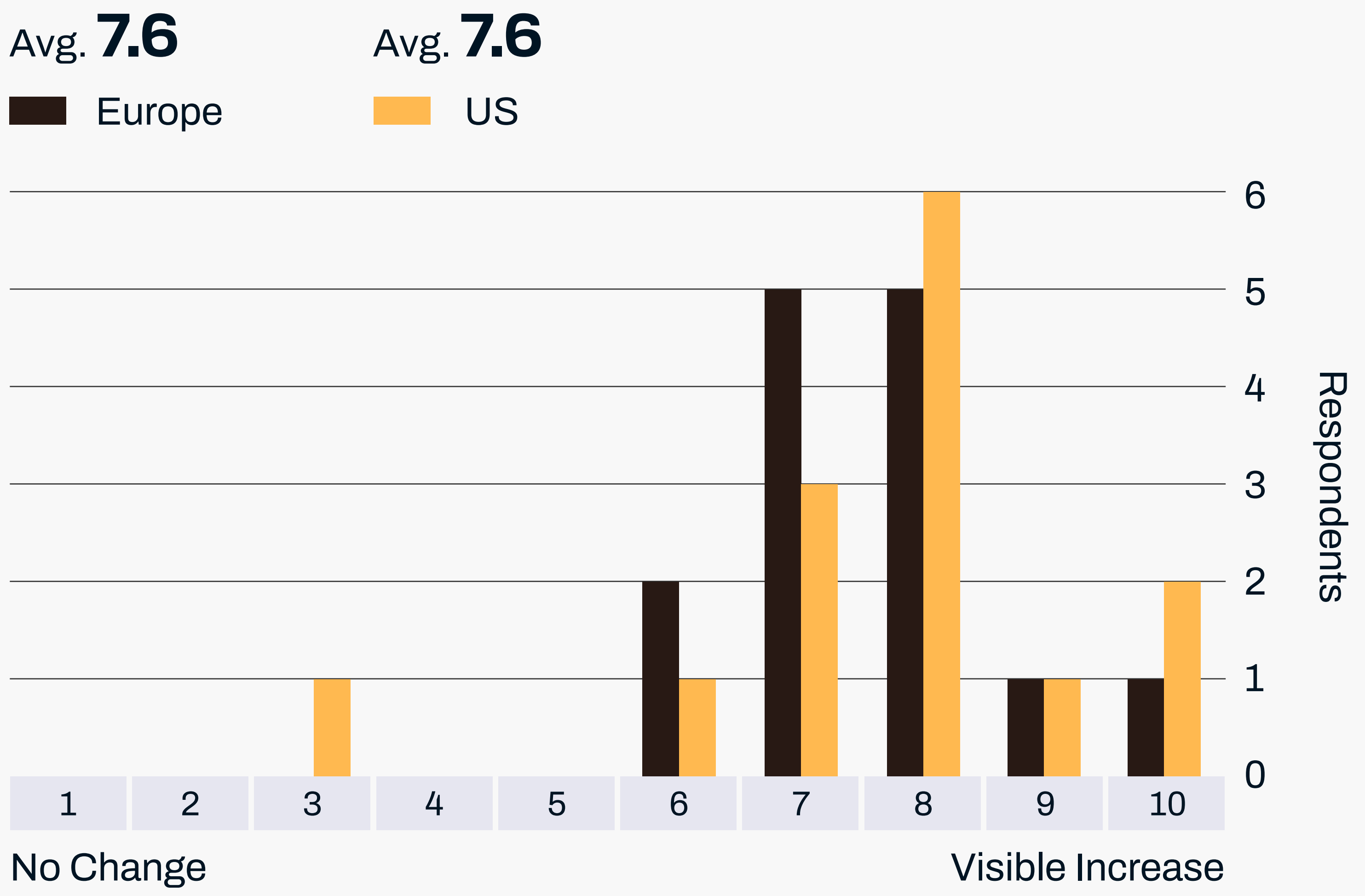
While our respondents’ organizations reap the benefits of technological change, so do attackers. Advances in automation and value exfiltration – for example, in the appropriation of infrastructure to mine cryptocurrency – make their crimes even more profitable. Our interviewees suspected that advanced threat actors are already observing how smart factories, homes and offices are all enabling IoT, mobile and next-generation devices. They worry that sophisticated OCGs have the capability to bias ML programs and adjust automated manufacturing operations, or build increased bots such as those capable with the Mirai botnet code from home and office networks, to impact corporate targets, nullifying the intended value of digitalization.

Finally, Quantum capability – where the ability to dramatically reduce the time required to solve the mathematical calculations that current cryptography (encryption) relies on – is seriously worrying a number of the CISOs. When this becomes available, CISOs believe it could nullify every organization, rendering cyber security – or any individual’s legitimate purpose – obsolete.

> **“ Techniques have definitely developed and become more professional. My concerns remain on ransomware and wiper software, though; BEC for money is just money, but the other two can kill the business.”**

Andrew Rose, CISO, VocaLink (A Mastercard Company)

Do you believe there has been an increase in the threat capabilities of cyber criminals?



Question 4

Are there more attacks targeted directly or indirectly at your employees?

Are there more attacks targeted directly or indirectly at your employees?

The employee is still seen as the primary attack vector for cyber actors

Almost three-quarters (71%) of the CISOs continue to recognize that the employee attack vector is still one of their most pressing concerns.

Our respondents acknowledge that cyber criminals are using a far larger attack surface to get to their intended target. They reported experiencing more sophisticated employee targeted attacks via social channels, where the employees' personal data is in the public domain. Our interviewees remain astonished that many individuals are blind to the fact that cyber criminals have the capability to understand the link between an employees' social/personal life on social media and their business role.

Social engineering and phishing attacks are used to connect directly or indirectly to the employee. Infiltration is often via a disguised but familiar-looking network link to trick a click to action the attack vector. And no one is immune to an attempt. Even CISOs in the financial industry reported a greater number of BEC attack attempts to convince employees to action false invoices or payment transactions apparently coming from the CFO or the head of procurement, for example. In interviews, CISOs continued to quash the belief that there have been more cyber incidents in the past 12 months as the majority of 'spray' type volumetric phishing (anything up to a 400% increase in employee-related attacks for one respondent) continue to be picked up by email and anti-phishing security products.

> **" Always being attacked; 95% of attacks come from phishing and tricking users."**

Ian Dudley, IT Director, DriveTech

> **" The attackers are finding out who works where in a company [by] using social media."**

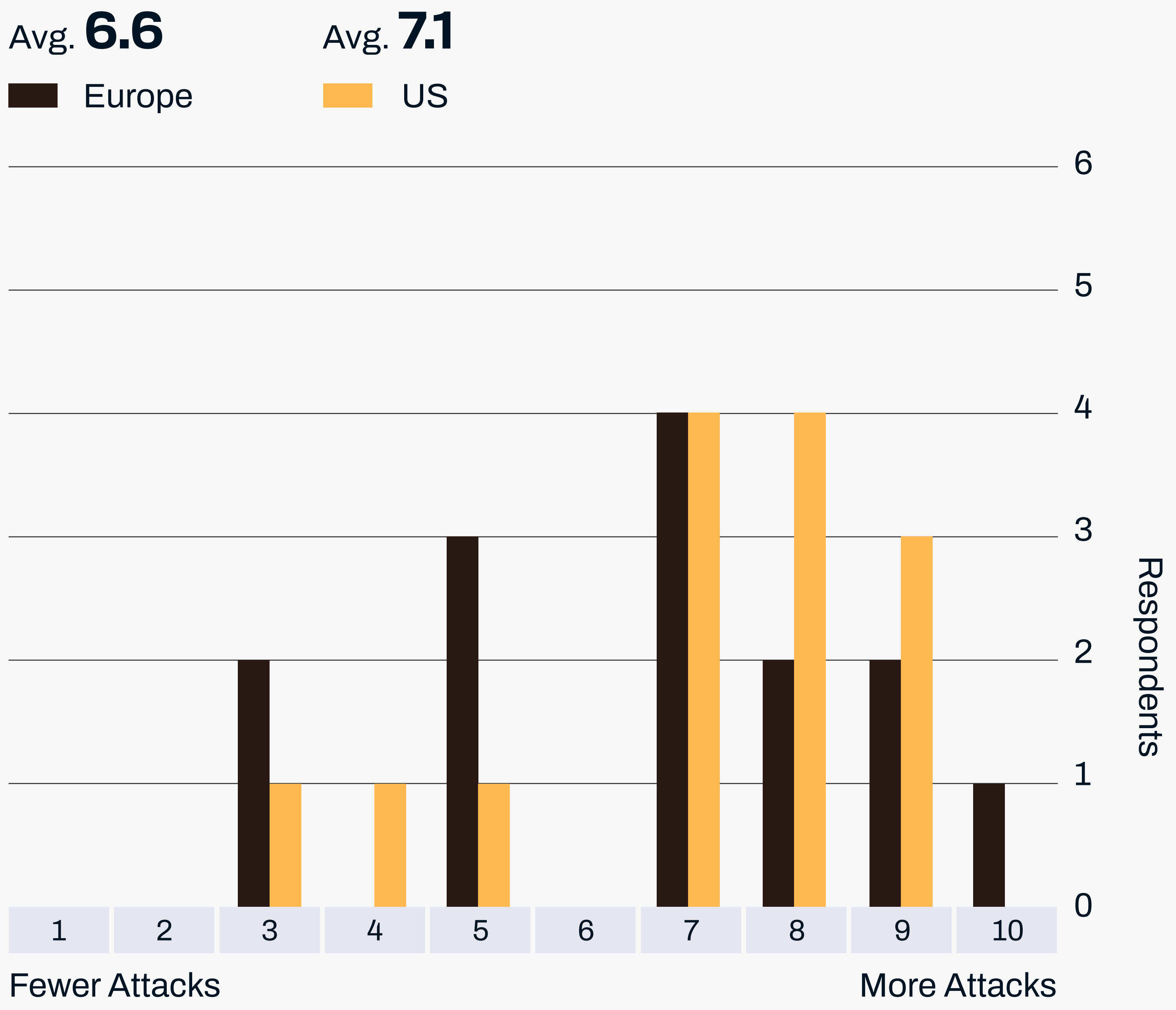
Leo Cronin, CSO, Cincinnati Bell

But it is not enough that all dubious emails are routed to the quarantine. CISOs need confidence that email security tools will immediately remove suspicious emails to a sandboxing environment, where anomalous links or executables – which have hidden malware – can be detected. If sandboxing is not used, businesses require better implementation of hard quarantine rules to remove potentially harmful links from user visibility, otherwise the risk remains. Any smart email attack that makes it through can compromise the security of a company

> “ 600% more attacks - could be higher. We have seen a 400% increase in employee-related attacks.”

Marc Ashworth, SVP, CISO, First Bank

Are there more attacks targeted directly or indirectly at your employees?



Question 5

Are there more attacks aimed at disrupting your business operations?

Are there more attacks aimed at disrupting your business operations?

One-third (32%) of the CISOs (scored 5-10) we spoke with have recognized an increase in the direct attacks on their business operations.

The most visible attacks are against internet-facing applications and the network itself. The growth in digital channels – to gain knowledge and buy goods – has also increased cyber criminal activity on internet-facing portals to target employees. CISOs are having to counter replicas of internet-facing portals that are being used to redirect the user and then scrape login details, personal information and financial data.

The implementation of more 'defense-in-depth' frameworks has increased the effectiveness of security infrastructure spanning all other areas of the business operations. This reinforces the point that, although there may be continuous attacks against their business, very few of these actually turn into incidents. This is a difference compared with attacks against individuals, which are seen as an easier route for the cyber criminal's intent.

All cyber attempts and those resulting in actual incidents are focused on an organization's internet-facing websites, portals or the networks that form the critical infrastructure for company communication and data flows. All other business-targeted attacks are primarily motivated by data theft or financial gain. These may disrupt the business but not its operations.

Those CISOs who have seen attacks and incidents against business operations have identified a diverse range of DDoS as the primary route attempt. Such an attack is intended to temporarily disrupt efficient engagement with internet-facing services and internal communication and data flows. CISOs reported the use of diversionary attacks, where DDoS is deployed to distract the security and network teams from mitigating other malware or ransomware infections.

> **"The distraction of a security incident cannot be overstated, especially as geopolitical tensions increase. We expect to see more attacks against business operations."**

Matt Stamper, CISO, Evotek

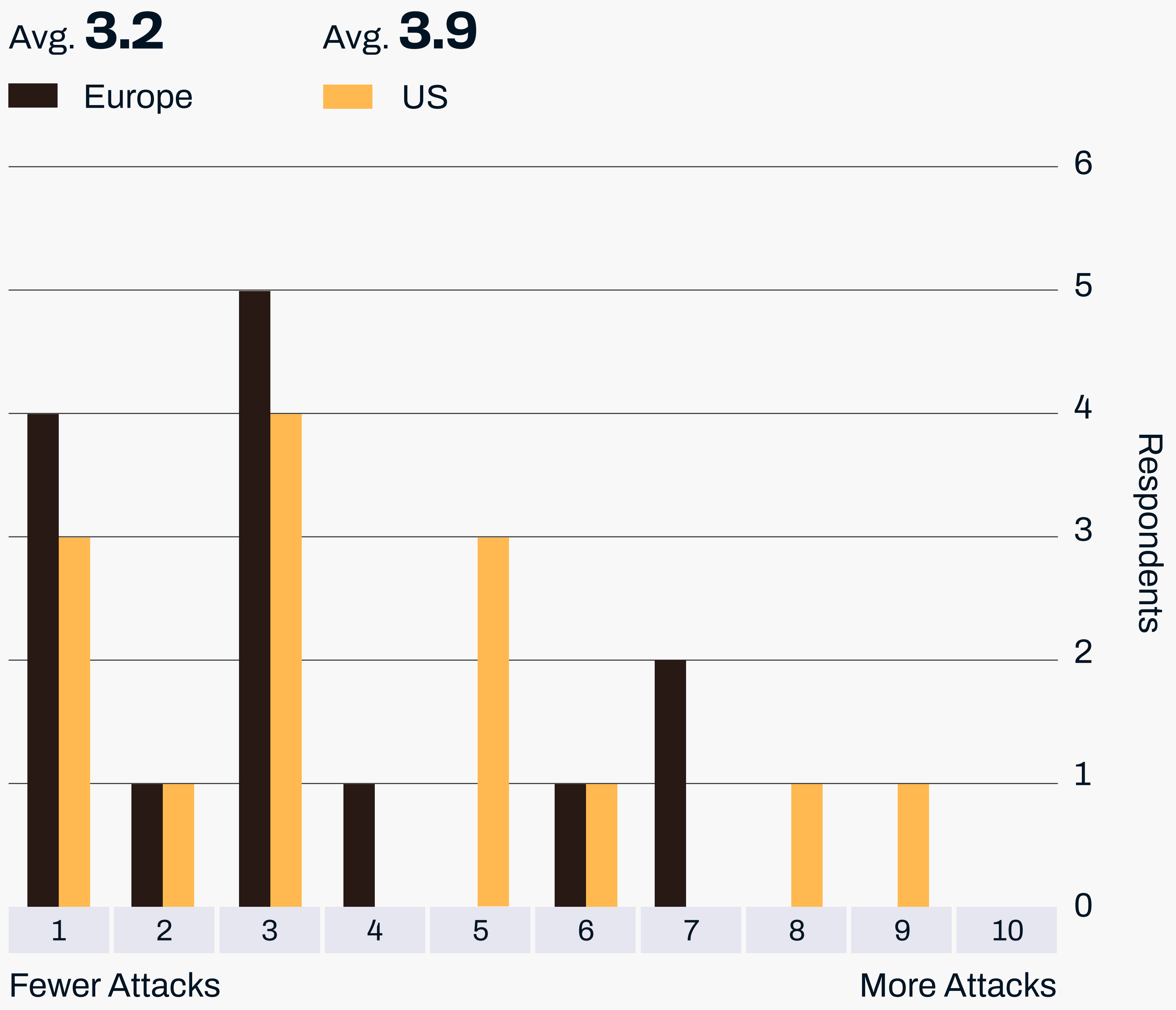
> **"Ransomware disrupts business operations alongside the growing issue of DDoS attacks, but we need a better understanding if it's a real attack or an IT issue (bug)."**

Mauro Israel, Corporate CISO, ORPEA Group

Many CISOs believe that if geopolitical tensions continue to increase, they will see more attacks directly focused on business operations intended to hamper their country's economic capability. CISOs emphasized that the intent of a security incident should never be understated. Many respondents believe that the efficiency of their security architecture ensures they can mitigate criminal intent to stop business operations. However, in many cases, CISOs never get to fully understand the 'end' motive of the cyber actor.

> " **DDoS and supplementary attacks are aimed at core destruction."**
>
> David Lello, CISO, Burning Tree

Are there more attacks aimed at disrupting your business operations?



Question 5

Have you been directly impacted by attacks coming indirectly from business partners?

Have you been directly impacted by attacks coming indirectly from business partners?

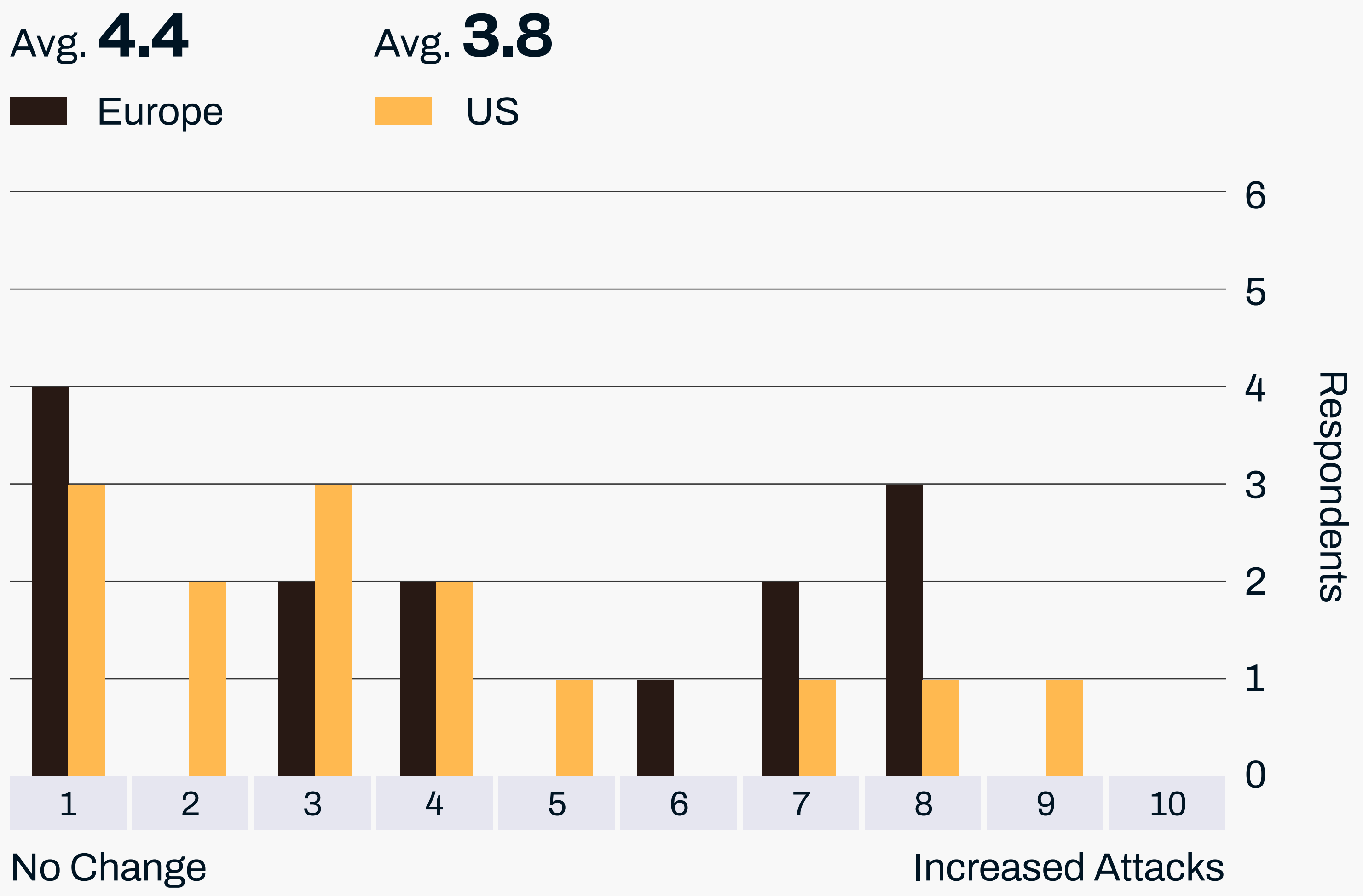
There is no definitive agreement from CISOs regarding attacks from business partners.

Only 28% of respondents who scored between 7-10 indicated any recognizable impact coming from external business partners, whereas 64% scored between 1-4, which suggests that while they may be experiencing sporadic attacks (where business partners have been found to be the source), very few are successful due to existing security tools.

Not surprisingly, the majority of attacks use business partner or customer emails as the transportation method of choice, executed via a compromised account of trust in an attempt to socially engineer with phishing or spoofing. A few CISOs have experienced business partners being exploited using BEC, where the partner has transitioned to cloud-based applications and has overlooked deploying all the necessary security controls, opening possible connections to their organization.

Increasing the number of network connections to partners places a significant burden of responsibility on the shoulders of the CISO. There needs to be more mutually agreeable due diligence in practice between the parties prior to engagement to ensure that the basics will be adhered to. That means agreement on security audits, penetration-testing, multi-factor authentication and real-time common vulnerabilities and exposures (CVE) testing are enforced. Regular two-way communications and even cross-party audit checks are essential to ensure that everyone is adequately security-hardened to the satisfaction of each CISO.

Have you been directly impacted by attacks coming indirectly from business partners?



> **“ We have strengthened down on social engineering and spoof emails, where an attacker is pretending to be someone of trust.”**

Nathan Reisdorff, CIO, New England Law

> **“ A big concern is that many business partners are not protected well enough. Mandate due diligence for anything they buy from IT companies and enforce security audits for all partners.”**

Mauro Israel, Corporate CISO, ORPEA Group

Question 7

Where would you place the motivation of cyber criminals against your company?

Where would you place the motivation of cyber criminals against your company?

Every CISO knows that a cyber criminal's primary goal is financial reward

Our CISOs also recognized that the initial attack may not appear to fit the model of financial motivation. While it is accepted that all organizations rely on data to run their business, each industry's data value is seen differently by cyber criminals. The split in opinion here is that 77% of CISOs saw the cyber criminals motivated by immediate financial reward. The remaining 23% of CISOs scored lower than the 7.4 average, suggesting that they view data as a greater motivating value for cyber criminals.

Today, cyber criminals want immediacy of payment using more direct attack vectors such as DDoS and ransomware that will result in the juxtaposition of operations, demanding instant financial payments. This has a more immediate effect on businesses compared with the more traditional methods of financial criminality, where the data was stolen or published on the dark web, and threats and consequences were issued unless a ransom was paid or the targeted organization performed another required action (take websites down, stop working with a government or commercial business, etc).

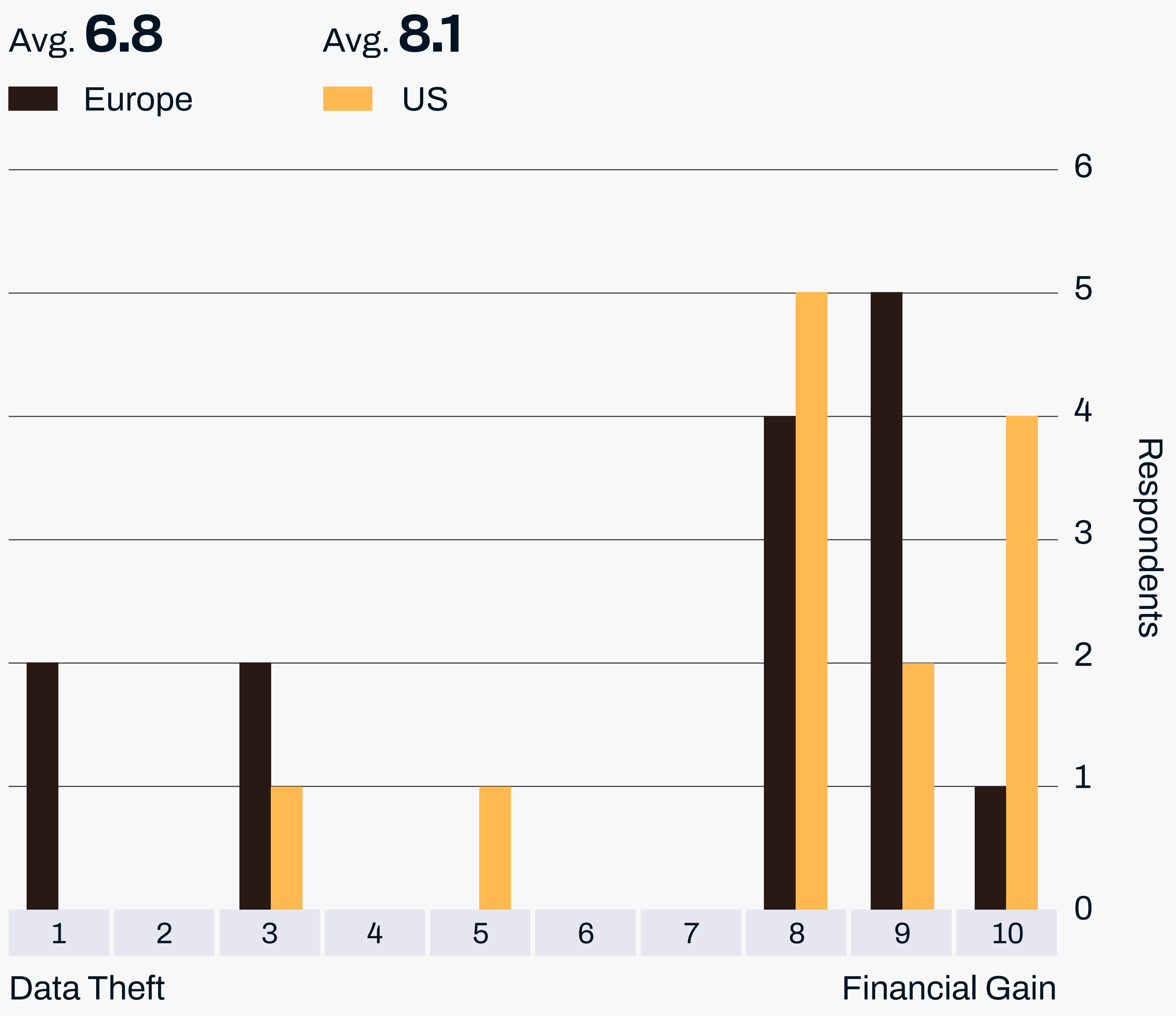
When systems and consumers are impacted, immediate and direct involvement of both security tools and security specialists is required to minimize damage and wider business exposure. But, as has been experienced in recent incidents, the cyber actors do not always release the networks or provide the necessary encryption keys after payment. An attack is criminal in the first place, but there is no guaranteed honor when it comes to unscrupulous commercial cyber criminal activity to deliver the antidote after they have achieved what they set out to do.

Payment consequences for financial damage

Continuing the theme around the immediacy of payments, BEC that initiates or redirects financial payments appears to be another growing attack vector. It is often executed under the category of socially engineered payment fraud. Additional use cases disclosed include instances where privileged knowledge is exploited as cyber actors nurture the media headlines by stealing data impacting company valuations during a known or intended merger or acquisition.

Paying a cyber criminal is causing the CISOs increased stress as they accept that their company, cyber insurance partners and intermediaries now have to tread a fine line. As more governments issue advisories regarding payment of ransomware to sanctioned persons or organizations, the company is at risk of suffering a triple-hit: revenue loss from the attack; payment to the cyber criminal; and being fined by the government for breaching sanctions. Ignorance of who is, or who is not, sanctioned is not a reasoned defense.

Where would you place the motivation of cyber criminals against your company?



> “ I see two motivations: #1 to get money – $100-$30,000; #2 set up botnets to attack other organizations.”

Nathan Reisdorff, CIO, New England Law

Question 8

Has your belief of what good security is changed over the past two years?

Has your belief of what good security is changed over the past two years?

Well-secured organizations are defined as companies that have alignment with risk-tolerance.

The 71% of CISOs that scored the average of 5.8 or above say that their belief of good security has changed, either in part or substantially. Although when all the CISOs contextualize their scoring, there are opposing corners.

In one corner, 29% believe that good security is still fundamentally the same as it has always been: focused on a risk-based discussion rather than just relying on security technology. They believe that if you continue to approach security with old-fashioned common sense and accept that the weakest link will always be the human, you always need to keep a healthy sense of awareness of your environment and enforce the application of strong security basics (hyper hygiene).

CISOs continually zoned in on the human element, appreciating the need that employees and consumers should be taking a greater level of personal responsibility for their actions.

In the opposing corner, others believe that good security has positively transitioned internally, with more peers and employees recognizing its importance. Much of this has been achieved with appropriate levels of training and awareness of various security incident possibilities.

Using a strong approach to people, process and technology, and a 'secure-by-design' approach, will produce the benefits. These CISOs believe they are in a good position to continually challenge the attacks and incidents and not be distracted into following fads.

> **" In the past, security tools, practices and initiatives were quite specific, but now it's more about fundamental practices that integrate and scale across business."**

Simon Goldsmith, APAC Information Security Officer, Adidas

> **" No real change, as I've always believed in the secure-by-design approach, which continues to be beneficial."**

Chani Simms, CISO, SHe CISO Exec

> **" My belief has substantially changed. It's now the endpoint that is key. In the past, it was the perimeter."**

Mauro Israel, Corporate CISO, ORPEA Group

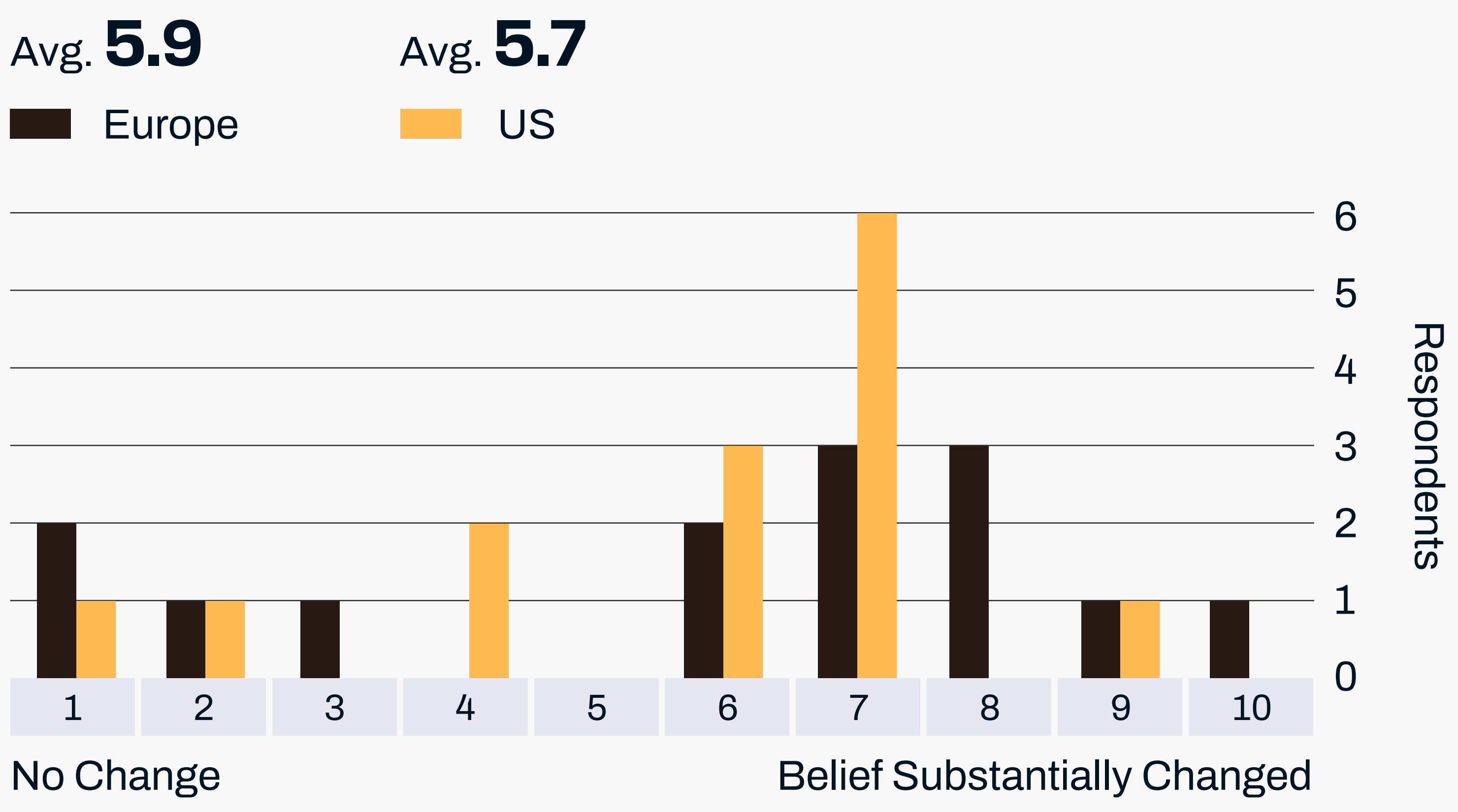
A strong message from all CISOs was the belief that they and their teams need to take more responsibility and ownership of any cyber incidents that affect the business and accept that fault may lie with the security team. Core to this is the acceptance that good security is about how you do things and less about what you do. The wider appreciation and influence of cyber security has meant that interactions with a wider diversity of business teams, partners and external parties (such as regulators) has increased and raised the stakes when providing security. In the past, there were minimal specialist teams that had a focus on security outside of the core team. But now we have many new disciplines that must be considered, including DevSecOps, app security, cloud security, and IoT security.

Information system boundaries have evolved and disappeared (perimeterless) due to the externalization of operations to the cloud, which has increased the threat 'inside' the new network. Cloud-based services, mobile working practices, and the increased adoption of digital projects has changed the scale that security is having to manage across the business.

CISOs singled out the greater emphasis on the endpoint as opposed to more traditional focus on the perimeter. These CISOs also look past the 'here and now' to envisage what good security needs to address for the future. They acknowledge that, due to the emergence of more advanced threats and nation-state actors/terrorists with the capability to destroy an organization, good security needs to be elevated. Additionally, greater accessibility of more advanced security tools such as threat analytics, isolation capabilities, biometrics, and many more that claim increased response times and proactive cyber attack mitigation are evolving the maturity of their security tools.

No longer just addressing cyber security from a technology perspective, the CISOs' changing attitudes toward security frameworks such as MITRE ATT&CK are bringing in more structure, providing visibility of gaps in their organization's security posture that cyber criminals exploit. This is encouraging security teams to approach cyber security effectiveness from a technology and collaborative best-practices perspective.

Has your belief of what good security is changed over the past two years?



> **" It's about good, old-fashioned common sense. If you keep a healthy sense of awareness of your environment, you won't need to respond to an email for banking information, etc."**

Todd Gordon, Director, Information Security, EisnerAmper LLC

> **" Information system boundaries have evolved due to externalization to the cloud, which have increased the threat 'inside' the network. We have to protect the 'core infrastructure' like Active Directory, hypervisors and backups."**

Florent Cottey, Operational CISO

The WithSecure™ Countercept perspective

If there is such a thing as a cyber crime ecosystem, then it is thriving. There has been much talk of a service industry for cyber crime – and plenty of evidence that it's taking place.

Affiliation models and services make threat groups new and old more operationally effective; they are now able to share mature tooling and offensive knowledge to conduct attacks. Another draw is financial reward: high-profile success of ransomware and extortion attacks have drawn more threat actors to focus their attention in this space, and are moving from other types of cyber crime as a result.

Engaging in some form of often expensive arms race may keep defenders current, but we'd argue that organizations working more closely together in the face of common threats represents the best value for money in the long term.

The state of the art

We expect phishing to remain a popular and fruitful avenue of exploitation for threat actors. Social engineering techniques rely on human nature, and phishing capitalizes on this. Malicious email content will always be interacted with, to some extent.

WithSecure™ suggests a number of approaches to mitigating risk:

Technological solutions can filter out the obviously 'malicious' email content before it reaches users, so they never have the opportunity to interact with it. Sandboxing, reputation-analysis and attack surface reduction through blocking esoteric file formats can all help.

- User training is an evergreen – a well-informed workforce will better understand the key role they play in security. But training shouldn't just focus on not clicking the link; it should also stress the importance of reporting links so security operations teams can find other users who received the link and contain any resulting compromise.
- SaaS/endpoint-detection capabilities reduce the impact (and therefore cost) of any intrusion that results from an interaction with malicious email content. The real cost to organizations is what happens after interacting with malicious content, not the interaction itself.
- The supply chain answer our interviewees gave may be different following last year's Solorigate/SolarWinds incident, since the interviews predated it. Supply chain attacks will continue to be relevant but will most likely only generate tangible risk for highly targeted organizations.
- Cloud and other technology adoption has changed, and will continue to change, the concept of 'good security' in the industry. One tenet of technology, and consequently how it is secured, is constant change and evolution. As a result it is important that CISOs and organizations keep up to date with the latest and best guidance in the industry, rather than relying on outdated viewpoints for strategy – something the interviewees stressed in their responses in Chapter 1. Those organizations that succeed in this environment are those that can be agile and respond to these changes. Their chances are better than those that struggle to communicate and act upon evolutions in the field.

Collaboration among hostile actors to improve attack capabilities set a rather dark example of how defenders should go about improving their own technology, tactics and procedures. Long gone are the days when having better safeguards in place than your neighbor worked as a defensive strategy; stragglers from the herd were only the prey when cyber security was an exercise in pace and resources. Survival of the fittest – or at least the ability to hide in the center of a herd while predators picked off those at the fringes – no longer applies when attacks are targeted and when active collaboration can make a massive, positive difference.

Defender collaboration is hardly ever a zero-sum game in this environment; it is also worth noting that attackers often share or trade information on targets, techniques and technologies. Information-sharing of this type has helped financial institutions[2] tackle organized cyber attackers, fraudsters and money launderers.

Chapter 4 – Cyber triggers influence chage

It’s a matter of conjecture within our group of CISOs as to whether cyber security should be a change agent for an organization’s operational posture. For a small number of respondents, cyber operations have affected the way their organization does business. But for plenty, it has yet to make a mark.

What is clear is that a concerted move to the cloud and to digital operations puts greater emphasis on involving cyber operations far earlier than with other business transformation projects. Regulatory compliance has helped move cyber up the agenda. For more progressive organizations, the early and proactive adoption of a ‘security-by-design’ mindset has gifted them a lead on competitors when picking up new digital platforms.

There’s clear recognition that the frequency and complexity of modern cyber attacks overwhelm many in-house security capabilities. Many CISOs desire their own security operations centers (SOCs), but this is often tempered by budgetary constraints and acquiring the necessary security skills rather than a lack of confidence in their team[s]. This drives a widespread willingness to incorporate more third-party security services, while acknowledging that making the best use of these requires a concerted effort in partnership with providers.

CISOs revealed their motivation to buying decisions: peer recommendations and tools aligned to a specific threat clearly stand out, rather than being induced by leadership reports, or buying something that looks interesting. Incumbent vendors cannot rest on their laurels either. They need to ensure that their tools deliver their original capability, as well as maintain pace with the diversity of specific attack vectors.

Staffing was another hot-button topic, with general agreement on changing skills requirements and a warning note about driving specialists away with a belief that technology alone can defend the attack surface, rather than realizing that technology is a toolkit that supports security specialists.

Attitudes towards ongoing training are positive. However, there are concerns for the provision of, and available time for, training. The capacity for full immersion in self-led training is being pushed out by more urgent demands on staff’s time.

Question 1

Have your cyber operations created the need for your organization to change the way it does business?

Have your cyber operations created the need for your organization to change the way it does business?

It is clear from the remarks provided by the CISOs that there are occasions – often sporadic, opportunistic and incidental – where they demonstrate how cyber operations have changed their organization's operational posture, primarily with supply chain and business partnerships. The average score of 5.3 highlights an almost equal 50/50 split of CISOs scoring above or below the mid-range (5).

The CISOs know that more digital and cloud offerings are approaching, or are already being integrated, and they need to involve security earlier on in such projects. These new offerings demand that organizations update the methods by which they provide access and interactions to enable growth and consistency for clients/consumers.

Many CISOs are pragmatic, taking the stance that cyber security is there to support the business rather than change the way it works; consequently, they will not proactively try to get in the way of the business.

Counter to this, the 74% of CISOs who scored an average of 8.3 (What are your beliefs about cyber security as a board discussion?) accept that cyber security should be a board priority, and believe that cyber security should be elevated and recognized as part of the business, not as an exception or a back-office function. Those who operate their own SOCs believe this type of capability does provide the opportunity to increase business confidence to execute their business differently.

> **"Where has it changed? Some of the requirements for projects have considered cyber security upfront. Now they don't think of cyber security as an afterthought – it's front and center."**

Scott Goodhart, CISO Emeritus, The AES Corporation

> **"I need to make sure my business does the business they want to do. I actively avoid trying to make them change the way they do business."**

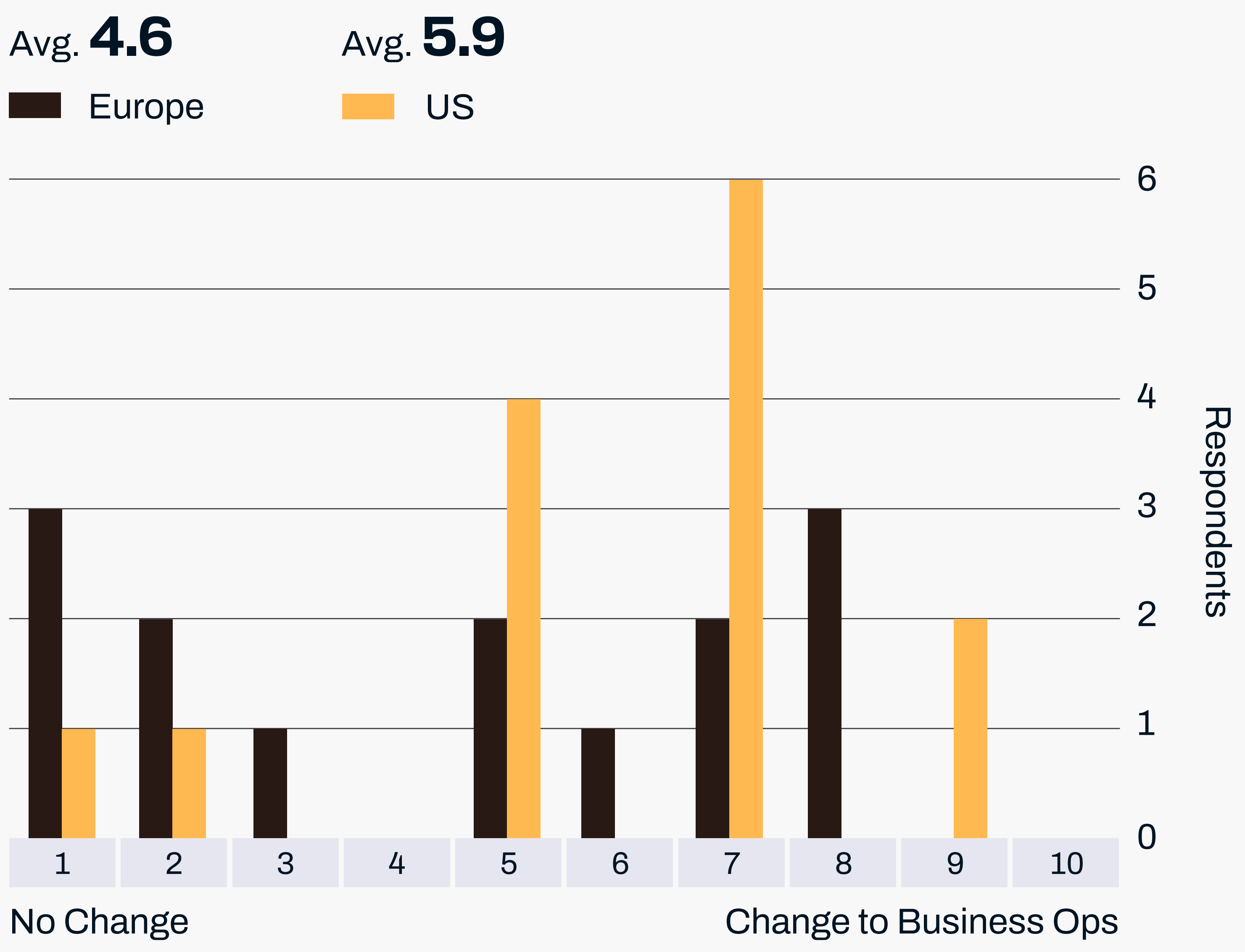
Ian Dudley, IT Director, DriveTech

With the growth in industry and privacy regulation, there is a recognized need to use cyber security access and process policies to allow the business to be compliant with the Gramm-Leach-Bliley Act (GLBA), General Data Protection Regulation (GDPR), the California Consumer Protection Act (CCPA), and other international regulations. This requires the business and its partners to be respectful in how it obtains personal data and moves that data around the business – something that could make leaders appreciate the value of cyber security as increased digital platforms change the way a business engages with its customers.

Organizations that have been proactive and introduced the security teams early on in projects, providing support to enable secure operations, have seen adjustments to the architecture aligning with the perceived risks they could face. This was clearly evident in larger organizations, as businesses look to utilize more cloudbased digital services. If the business approaches operations with a security-by-design mindset, then it will function in a way that is beneficial to the organization and secure for its consumers.

The optimistic CISOs believe that as business delivery changes and cyber attacks evolve, especially with growth in DevOps and cloud, the future looks more promising to really integrate security as a recognized enabler for business operations.

Have your cyber operations created the need for your organization to change the way it does business?



> **“ Definitely more increased scrutiny of third-party vendors (GDPR, CCPA) and general risk management and maturity.”**

Royce Markose, CISO, rewardStyle

Question 2

Do you believe that the rising and varied types of threats could mean that managing your own security operations team will not be proactive enough to ensure consistent business operations?

Do you believe that the rising and varied types of threats could mean that managing your own security operations team will not be proactive enough to ensure consistent business operations?

Most of the CISOs in this study (71%) recognize that they will need to integrate more third-party security services to help combat the advanced threats of cyber criminals across a growing digital-first attack surface.

Indeed, many continually look outside their employer's sector to reinforce their decisions. In a hospital, for example, dedicated crash rooms and intensive care units are run by trauma specialists who deal with critical care. Their mission is to make the most of the first 'golden hour' for a casualty that requires prompt medical and surgical treatment to improve the patient's chances of survival. Every second counts. The thought then follows: why should any organization not have similar action plans and approaches to survive distributed denial of service (DDoS), business email compromise (BEC), ransomware, or data breach incidents?

If CISOs could build their own security operations technology SOC, equipped with an army of 16 to 30 security specialists, then they would. But this luxury is not available to many CISOs. It is not that CISOs understate the capabilities of their teams – it's more about the most effective way they operationalize their available budget, either for an in-house team or partnering with a managed security service.

Security vendors need to increase their security tool capability to defend their customers

For a number of CISOs, partnering with security service providers will be unfamiliar territory. They are reaching out to their network contacts for recommendations. Approximately 30% of those interviewed already outsource varying elements of their Level 1 monitoring and threat-mitigation services from managed security service providers (MSSPs). They know that using these outsourcing partners frees up staff to focus on critical incidents that are disrupting the business, eradicating the need to wade through floods of alerts that, in many cases, are false positives and a waste of valuable resource time.

> "Specialists provide the best knowledge, and we use those with business knowledge and security for operational technology. Those that don't think this are kidding themselves."

Scott Goodhart, CISO Emeritus, The AES Corporation

> "Yes, especially given the increased use of AI/ML in malware/ ransomware and sophisticated attacker TTPs,
> I believe that everyone needs over-the-shoulder support that's 24/7 and provides effective SLAs, such as an MDR provides."

Mike Davis, CISO, Alliantgroup

Choosing the right service from an MSSP partner is critical to your business. One CISO confirmed that the numbers and types of threat alerts provided from their chosen MSSP partner did not constitute a constructive service. The CISO decided to revert back and in-source the service to achieve a greater level of intelligence of the cyber criminal activity and intent.

Interestingly, an organization's image can also be a major consideration when increasing resourcing levels. In a number of cases, CISOs believe that their company may not look as attractive, or be considered as one of the more progressive industries, for security specialists to consider joining them. Outsourcing can mitigate this issue, as security service providers can open the doors to specialist teams with wider knowledge sets across information technology (IT) and operational technology (OT).

Viewing this challenge from a technical aspect, many strongly believe the human is not the answer to current and more advanced automated attacks – or anticipated future threats – as organizations adopt new technologies and working practices. Their belief is that the security service providers have more readily available advanced skills and security technology that exploit varying levels of AI, ML and deep learning.

Assumptions vs cloud provision and control expectations

The scoring shows that not all CISOs share the same view. Around 25% saw outsourcing as an additional, unnecessary cost rather than increasing their security protection detail. The belief here is that if operations are approached from a 'cloud-first' mentality, then the cloud provider should alleviate any security concerns.

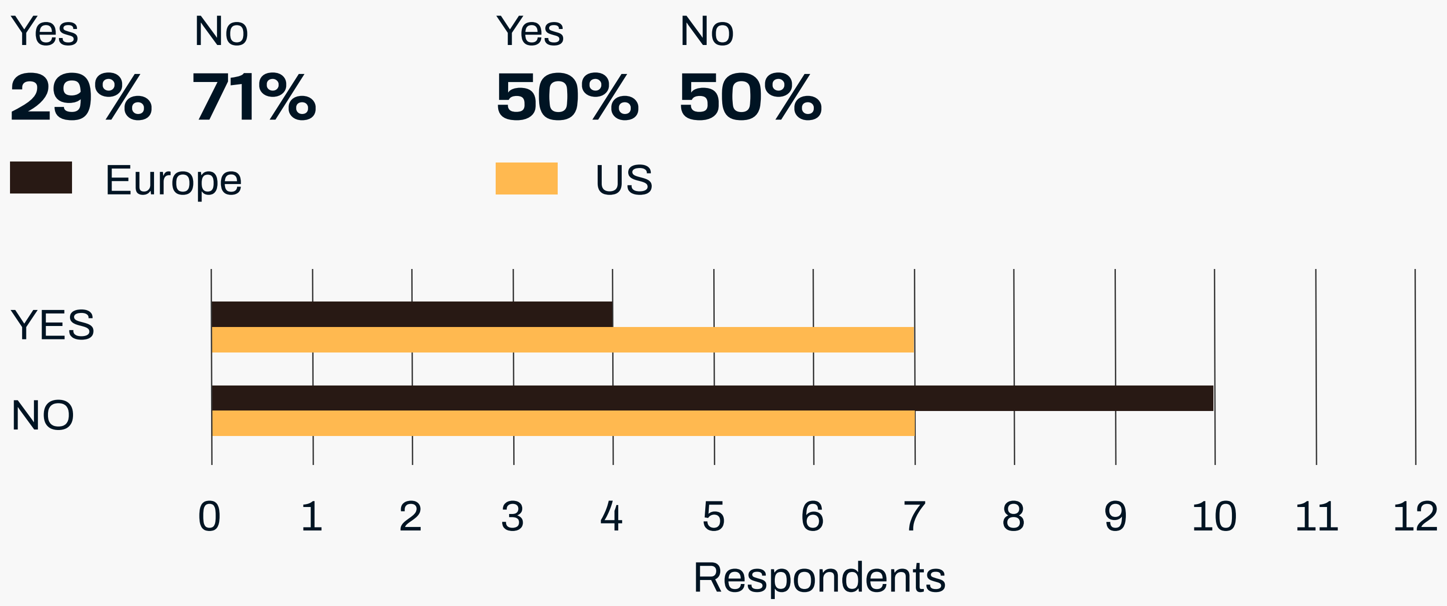
Also, if an organization already understands its capability, risks and threats should be transparent and appropriate employee training obvious. A good understanding also encourages strong controls in the first place. If not, then the problem is simply being moved around, not solved, and outsourcing could make the security posture weaker. In contrast, a mature capability would justify outsourcing for specialist areas of need.

It is clear that CISOs are very guarded in their views of new technology that looks interesting: 39% may look into the technology further, and 61% remain focused on tangible benefits while steering clear of 'interesting tech' until it has earned its stripes. Any interest is heavily biased in the US (50%) compared with Europe (29%). Interesting technology should clearly be left to the academics, researchers, and incubators before introducing it to the decision-makers.

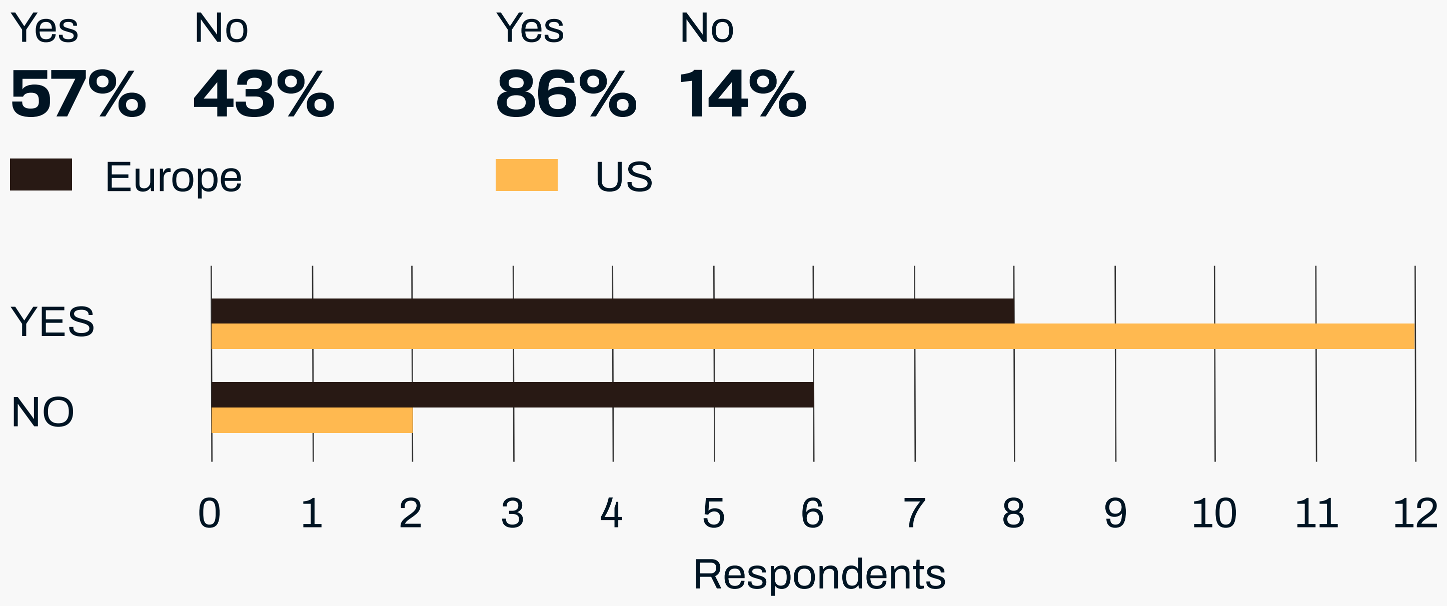
> “ We won't be proactive enough. If it's left to the team, then we will not be capable of supporting the business.”

Nathan Reisdorff, CIO, New England Law

Do you make at least 50% of your cyber technology decisions based on new technology that looks interesting?



Do you make at least 50% of your cyber technology decisions based on peer network contact recommendations?

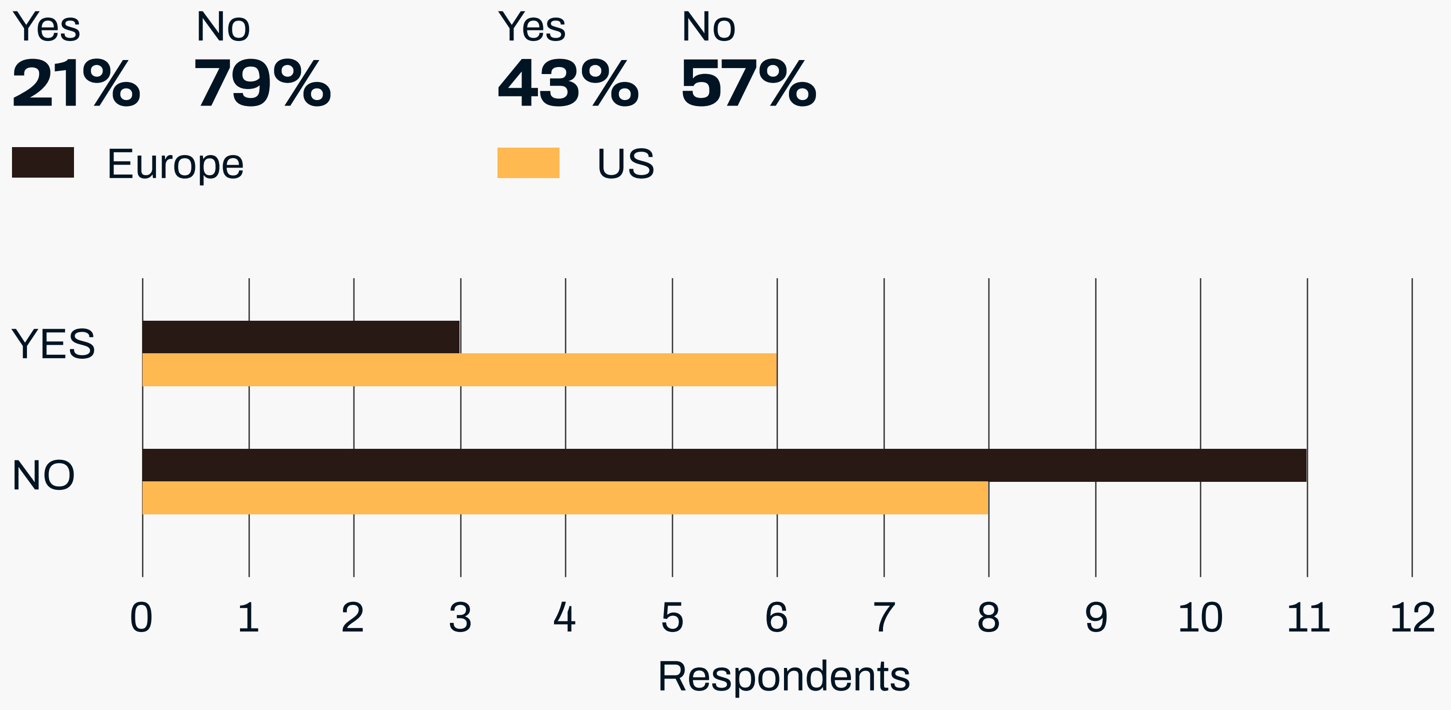


Echoing the previous discussion about CISO engagements across their peer networks, 71% would definitely consider spending greater time researching technology that a peer network contact has recommended. Once more, US CISOs appear to value their peer network (86%) more compared with the slightly more reserved European CISOs (57%). These results show how CISOs globally respect the power of their networks and, more importantly, the critical importance of delivering and supporting products for the solutions promised.

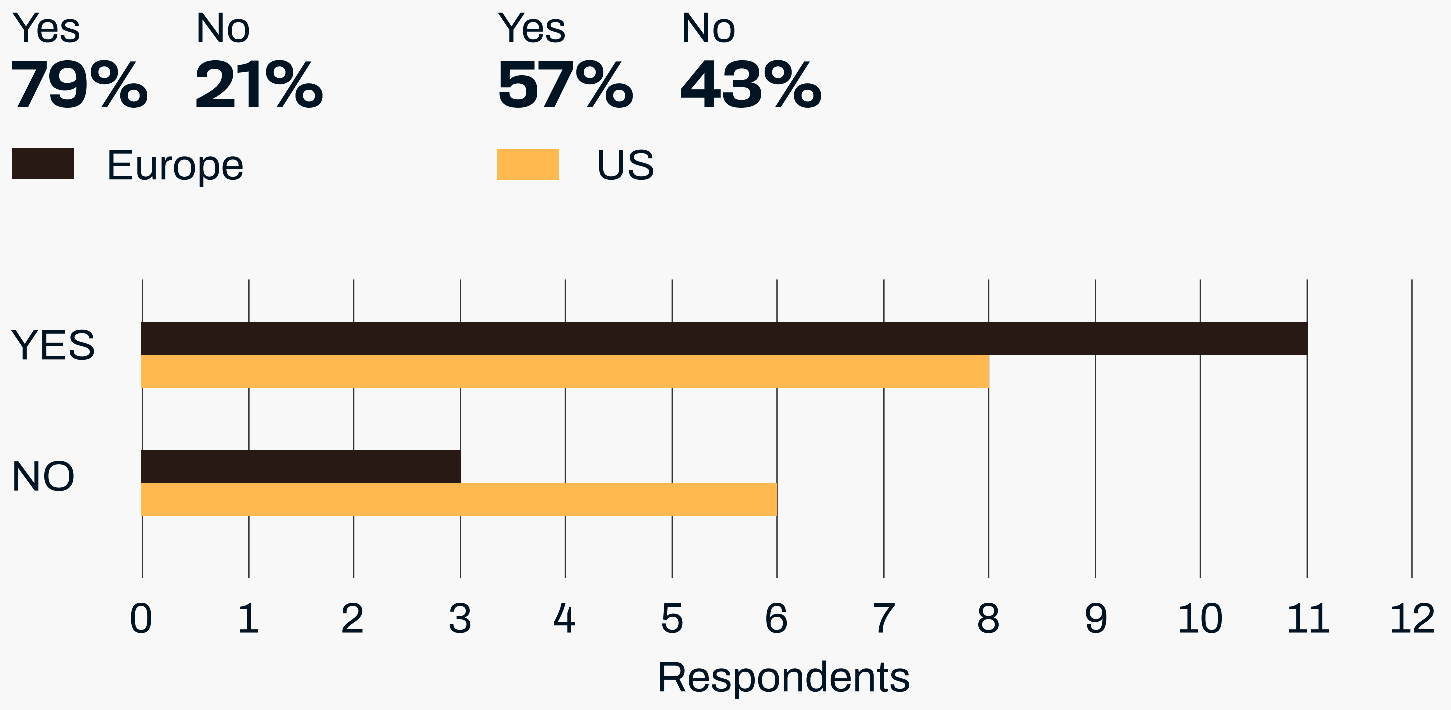
The adage that you never get fired for buying IBM is old-school. CISOs indicated (68%) that incumbents or leaders get no preferential treatment when they are making their technology decisions. European CISOs put a stake in the ground, with 79% indicating that their position is to remain clearly objective, stressing that vendors of all levels of maturity need to show continued value, innovation and commercial sensitivity to be invited to the field of play.

Risk is the priority of the CISO. If vendor technology aligns to a known, perceived, or future threat and can prove its capability, the opportunity to engage with CISOs (68%) increases. European CISOs expressed a willingness to be influenced (79%), more so than their US peers, but they advised security vendors to focus engagements on the realities of threat benefits and keep well away from hype and marketecture.

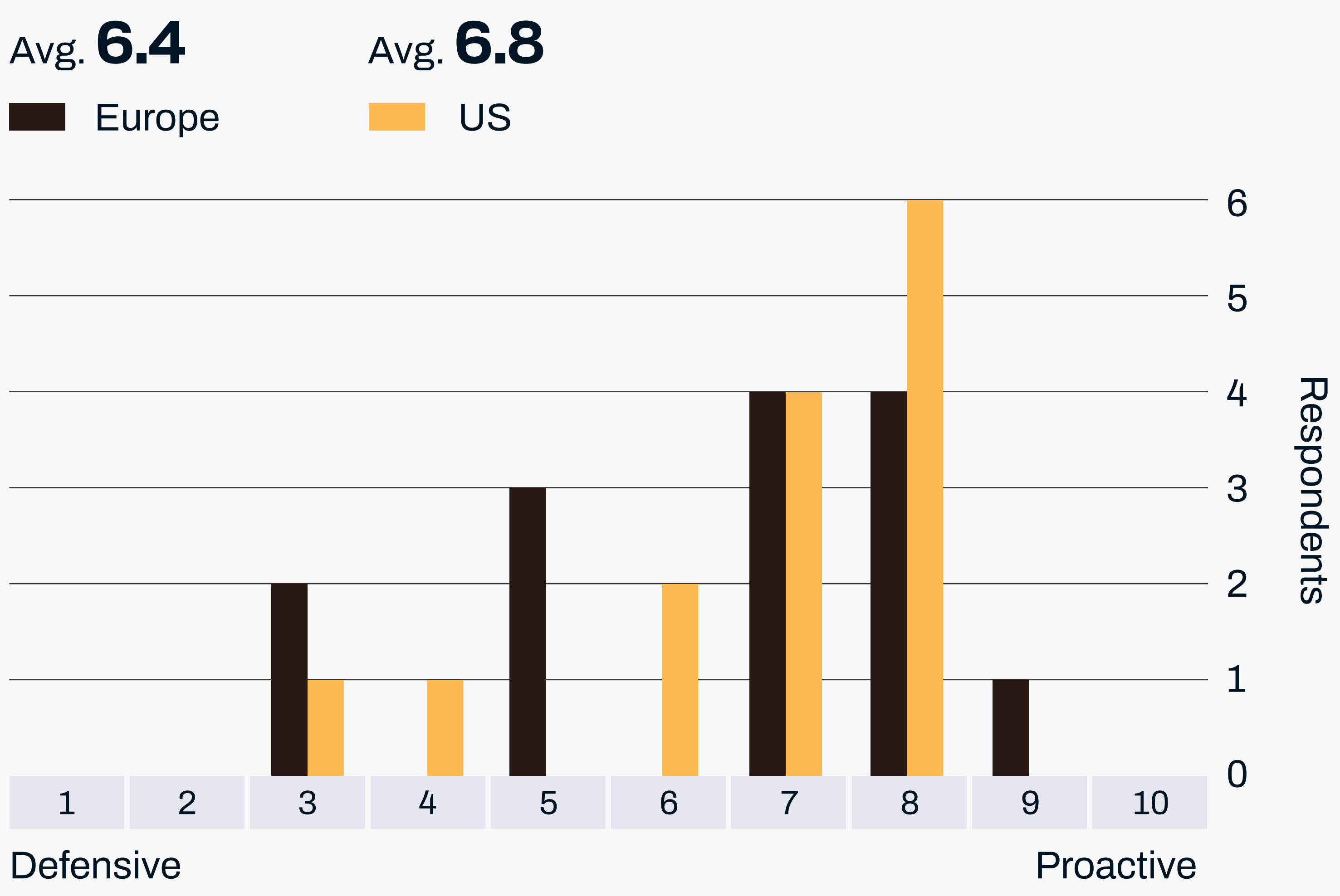
Do you make at least 50% of your cyber technology decisions based on the leader or incumbent vendor?



Do you make at least 50% of your cyber technology decisions based on whether they are aligned to a threat?



Do you believe that the rising and varied types of threats could mean that managing your own security operations team will not be proactive enough to ensure consistent business operations?



Question 3

Have the key disciplines that you look for in new (cyber specialist) employees changed in the past 12-18 months?

Have the key disciplines that you look for in new (cyber specialist) employees changed in the past 12-18 months?

In line with the widening reach and increasing influence of cyber security across businesses, the skills and disciplines for the security professional have had to maintain pace. With greater interaction across the business, CISOs are under pressure to recognize the value and advance their own – and their team's – security toolset in growth areas such as cyber analytics. While that might allow them to excel in the technical aspects of the role, there is also now a greater emphasis for all members of the security team to understand and use more soft skills (curiosity, adaptability, understanding the bigger risk picture, and an analytical mindset) to engage with other teams on a deeper level, as well as appreciating the diversity of the people they come across in their work.

Seventy-one per cent of CISOs clearly believe the role of the security specialist has evolved and become more critical to the business. Our interviewees' challenges come with the need to ensure that the security specialist learns new skills and specialisms – as new technology is introduced – while also ensuring that updates to legacy technology (>18 months) are optimized to gain the full capability of the product.

On the flipside, CISOs have a concern that although their teams' technical skills are good, they could become a commodity in the near future with the advance of AI/ML increasingly embedded within security tools. The validity of AI/ML language used within marketing vocabularies should be factual, so CISOs must understand the reality of intelligence-led tools or risk losing specialists who have become dispirited by the belief that technology will minimize the impact their role has in the future. It has always been the case that a well-rounded security specialist understands the relationship between business architecture and the integration of security tools that protect the operating environment.

> **"Yes, I look for people who understand the overall risk picture, on top of their security specialties."**

Mike Davis, CISO, Alliantgroup

> **"I have always looked for good humans with solid communication skills, and who are self-starters. Tech skills are nice to have, but it's a commodity, so what's changed in the past 12 months are the ability to manage themselves, and having the enthusiasm and the right attitude."**

Chani Simms, CISO, SHe CISO Exec

> **"Yes, shifting focus to new skills: cyber analytics focus, allow to make new response models."**

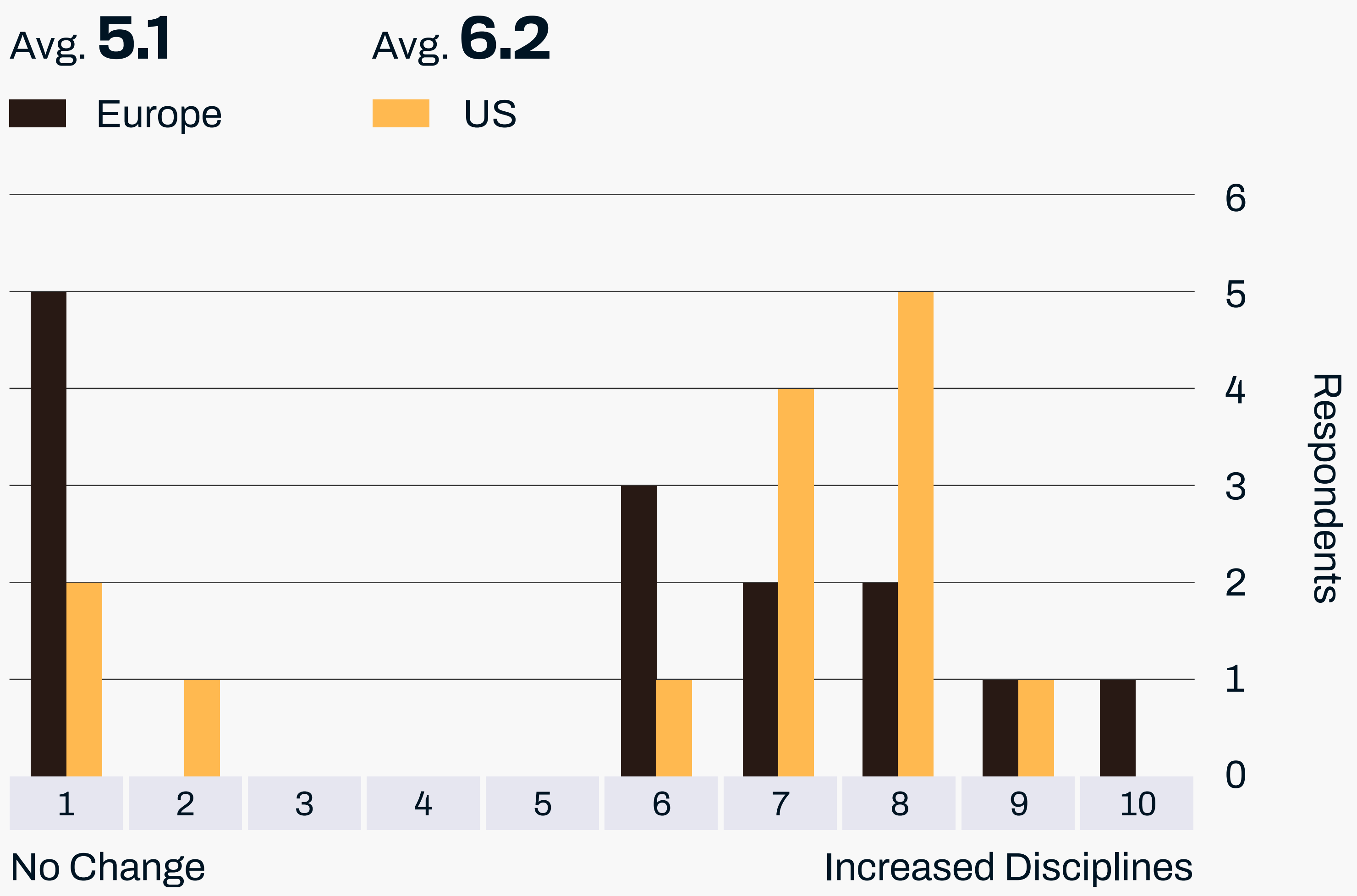
Scott Goodhart, CISO Emeritus, The AES Corporation

The plethora of new technology introduced almost daily has meant that a well-rounded and efficient security team skill set has spiraled to provide the full range of capabilities within DevSecOps, cloud, app develop, SOC analyst, UX designer, VR designer, Python, Ruby, 5G, software-defined networks, blockchain, 3D, among many others. Many of these requirements align to the increased use of digital applications, where there has been a focus to ensure that everyone has cloud, data and AI security capabilities alongside the IoT (Internet of Things) and OT devices used by the business.

Certifications such as CompTIA A+, S+ or Network+ are seen as more beneficial to the specialist than the organization. CISM and CISSP are viewed as a ‘nice to have,’ even though a majority of CISOs would assist security specialists gaining these certification awards once the base certifications are achieved.

As digital evolves across every aspect of the business, CISOs are concerned that the role of a security specialist will appear discouraging for any aspiring individual, limiting the growth in people resourcing and restricting the ability for individuals to learn new skills as they manage growing workloads.

Have the key disciplines that you look for in new (cyber specialist) employees changed in the past 12-18 months?



Question 4

How much time per month do your direct staff spend learning new skills?

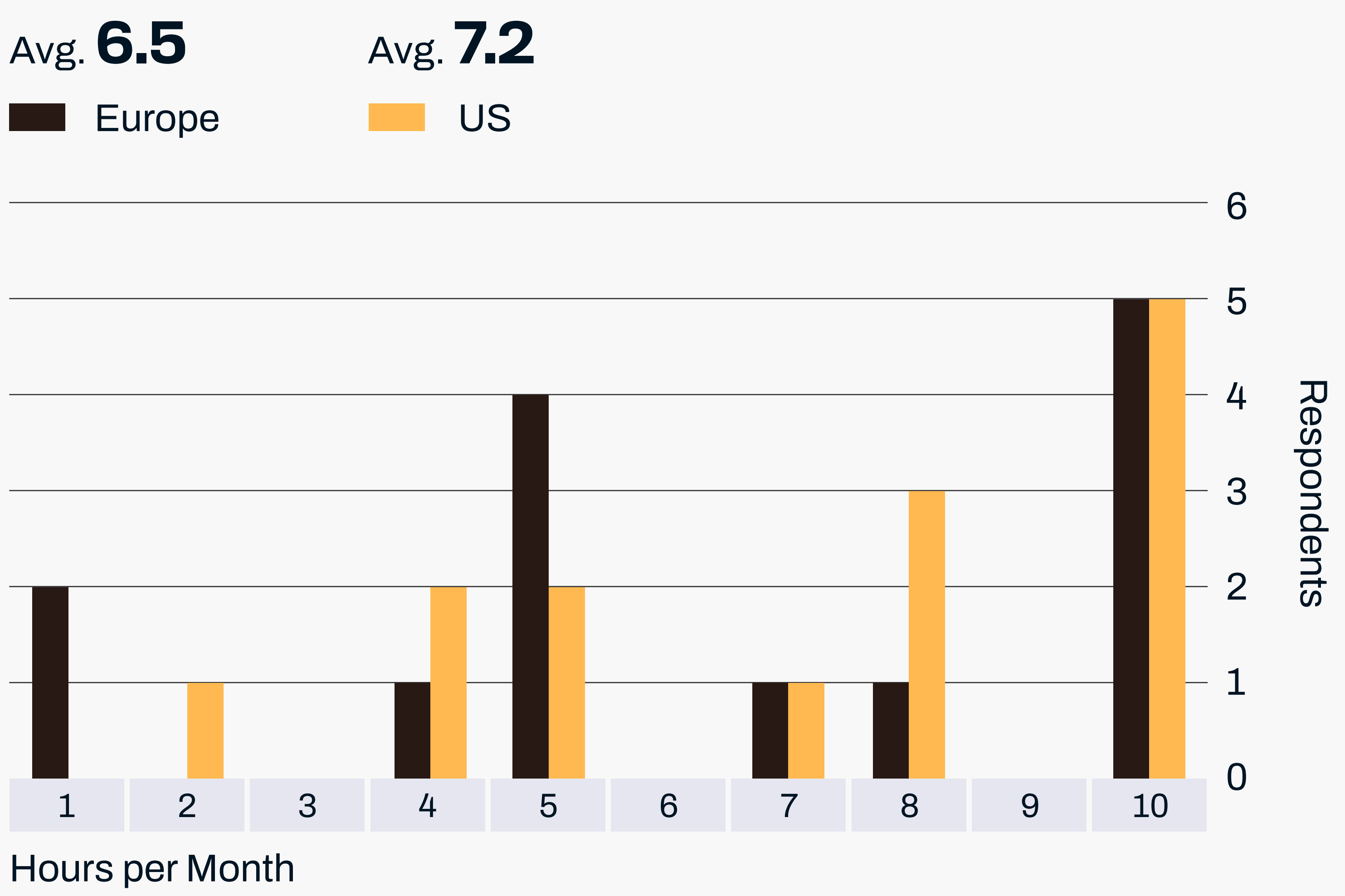
How much time per month do your direct staff spend learning new skills?

There are only 24 hours in a day; unfortunately (or fortunately), most cyber specialists are only officially active for eight or nine of those hours. Even so, the CISOs have a mindset that they and their teams are continuous learners who read, eat and drink cyber.

More work, less training

The increase in workloads created by the diversity of technology that require securing means that, in many cases, busy specialists often relegate training to an afterthought if CISOs and their management did not insist on regular business and cyber security-related training. Some of the respondents accepted things are not as good as they would like, due to the pressures of day-to-day operations, with the larger majority of training coming when new security tools are introduced. Even with these constraints, 57% of the respondents ensure that their teams are being provided with 7+ hours of training per month, and 36% ensure that more than 10 hours of training is achieved per month. Putting aside on-the-job training of new products, CISOs try to bolster their teams' technical capabilities around coding, cloud, analytics and business applications such as ERP (enterprise resource planning). Additionally, personal development of the individual ensures they are able to apply soft skills in their day-to-day activities. Certifications are not included within the monthly training statistics, nor are individual vendor certifications required to manage their products. These are seen as exceptions and not part of their specialist's standard development objectives. CISOs know that their teams find self-learn systems too difficult to undertake piecemeal, as many require full immersion – a rare luxury or many when it comes to setting aside a full day or more for training.

How much time per month do your direct staff spend learning new skills?



Question 4

Do you believe your security capability has improved and allows you to defend your organization?

Do you believe your security capability has improved and allows you to defend your organization?

The CISO's job is never done. It is a continuous and challenging environment. The majority (72%) believe there has been good progress in stemming the capability of cyber criminals, but they're ever-conscious that cyber criminals retain the element of surprise and therefore the ability to carry out unknown types of attacks. Increased awareness of cyber security by senior leadership and boards provides incremental increases in budgets, which is helpful for CISOs. But they recognize that money is only part of the solution and they have to be smart about where they invest. CISOs will not, and cannot, just throw money at the problem; instead, they ensure they align investment to the known and perceived [future] risk(s).

The many personas of a cyber adversary continue to grow, each introducing new tactics and tools. CISOs are no longer just dealing with individuals and disruptive techies. Their security teams are having to defend their business operations from organized criminal groups (OCGs) and nation-state actors. Both have more money, resources and technical capability than the CISOs of the biggest businesses.

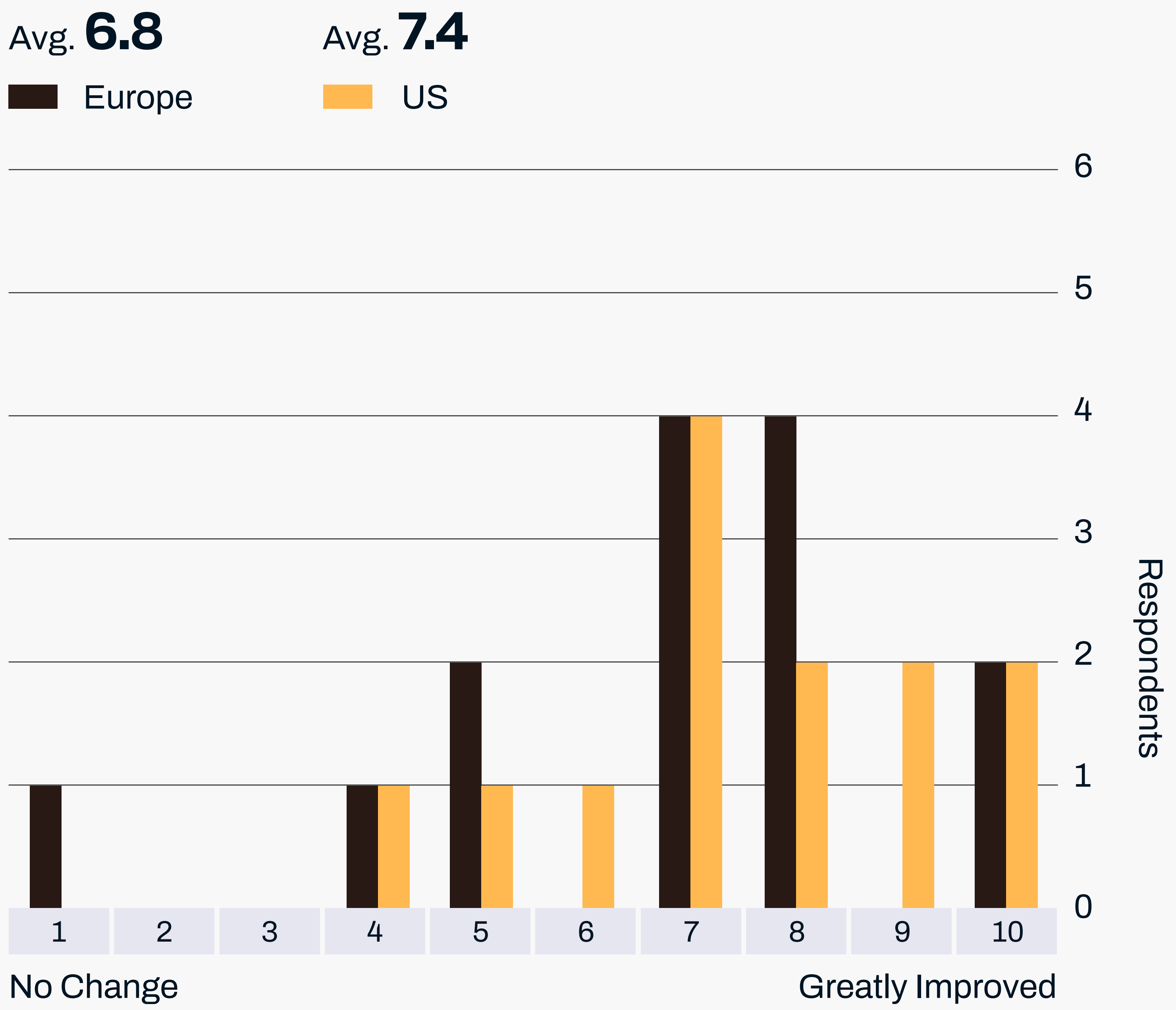
Some CISOs are concerned that the effects from the first half of 2020, where they have been asked to deliver amorphous strategies and deal with extremely disruptive changes to working practices with very little warning, are creating vast holes in their defense surface. Even with these unprecedented business needs, they are worried that financial investment in cyber security could be reduced, creating a regression in capability, back-foot firefighting, and stalling the momentum achieved.

> **"Maturity assessments show the improvement, but we need to be a continuous improvement process. The financial crisis could create a regression; cyber security needs to be kept front and center."**
>
> David Lello, CISO, Burning Tree

CISOs continue to implement a strategic approach to mitigating cyber attacks and reducing cyber incidents via the implementation of more threat-aligned security tools, standards and frameworks such as NIST and MITRE ATT&CK, as well as maturity assessments and a continuous improvement process.

The respondents all agreed that you can never be complacent with your security posture as your adversaries have the capability to move with agility and speed. While combatting general attacks such as phishing has advanced, there is still plenty of room for improvement in the technology and employee/user awareness via cognitive training. A number of CISOs continue to challenge security vendors' technology efficacy to execute and deliver on what the salesperson claims it will do.

Do you believe your security capability has improved and allows you to defend your organization?



> " Capabilities have improved over time as new solutions become available. I have found success with a greenfield approach that allows me to build a program for the future rather than adapting a program from the past."

John Scrimsher, CISO, Kontoor Brands

The WithSecure™ Countercept perspective

For perspective on this chapter and the wider report, we invited our own CISO, Erka Koivunen, and Jukka Seppänen, our Information Security Officer, to comment.

Reading this report, we could immediately relate to our fellow CISOs and senior infosecurity officers. I think there are some universal experiences for our profession: the issue of taking responsibility of security impacts of what others do and decide, the eternal struggle with shadow IT, and the virtual 180-degree change in perspective on cloud security during the past five to 10 years.

Influencing business [unit and function] owners to take security into consideration in their own operations is what brings sustainable results. We can't continue to go down the road of IT security being 'just' the job of the CISO and their team – the rest of the business can't absolve itself of responsibility for security. But equally, we have to give them the tools and skills. I see many respondents echo this and I am happy about what it implies: the security function should not be preoccupied with setting up 'security gates' and forcing the business processes to present their cases to the gatekeepers.

The security leaders of the 90s we grew up with were quite inflexible and spent far too much time building their own universes from which to keep the business hostage. I think they really gave security officers a bad name, something we younger ones are still being measured against.

The growth in maturity required to move a team from the eternal naysayer – the 'Department of No' – to become a communicator of risk appetite and the security implications of business choices is quite substantial. One must be truly enthusiastic about the opportunities to succeed nowadays – not just fixated on preventing risks.

Security leaders must appreciate the fact that the ultimate task of the board of directors is to handle strategic and business risks. CISOs can't just show up and present their gallery of horrors (risk registry, incident history, failures in execution and dark clouds in the threat horizon). As much as these are a daily reality for CISOs and mostly nothing more than a professional challenge, they shouldn't be presented to the board unfiltered. Instead, it's really important to identify and explain to the board the genuinely business-halting risks that threaten the core and indicate that the basics are not right.

Looking at the report overall, the commentary on emotional intelligence and EQ raises another issue. The coaching approach recognizes that while the CISO and their team may be an expert in security, they succeed best by humbly taking the time to understand what business and other support functions are trying to achieve. That means taking a reading on their underlying assumptions for the current cyber risk position and understanding the etymology of what controls have been put in place and why. The power of empathetically asking ‘why’ at the right moment can set things in motion with greater force than the CISO could ever wield by attempting to issue diktats.

We have also been preaching to anybody willing to listen that we (as in organizations and blue teamers) have never had better tools and access to smarter security pros than we have now. That contributes to security for those willing to invest in it.

That’s a good thing, because we’re also seeing the window for successful detection and response shortening to hours between initial compromise and incident. It’s still a huge ask for most organizations and most teams to meet this sort of threat without outside help.

We remain hungry for evidence of us investing in time, resources and controls in the right places and ways that bring effective security. There’s nothing more satisfying than our team seeing that, without X (or a combination of A, B and 3), we would have been exposed and impacted, but that we won the day for now.

The idea of ‘building security in’ could mean that systems are being designed and built with their defense in mind. That could be compartmentalization; containment strategies that reduce the blast radius of an incident and lessen the likelihood of losing the whole estate at once. It could mean the ability to track and monitor not only anomalies but also for compliance and normalcy.

And it definitely means the ability to respond in a meaningful way. That can be for investigatory purposes, for understanding the impact and the root causes. In cases where there is a proper threat actor, it can also mean understanding the adversary’s motivations.

It is not always evident what the defenders can do to frustrate and disrupt the attacker and to limit further damage. Without the necessary technical skills, without an intimate understanding of the system and its environment, and without a plan, the response is going to be improvised.

If the client is not a master of their own estate, they can hardly benefit from the help of outsourced services such as managed detection and response.

End Notes

Chapter 1

[1] https://cybersecurityventures.com/backstory-of-the-worlds-first-chief-information-security-officer/
[2] https://www.fca.org.uk/publication/research/cba-extension-senior-managers-certification-regime.pdf
[3] https://blog.WithSecure™.com/peacetime-value-dont-wait-for-a-security-incident-to-get-value-from-your-mdr/

Chapter 2

1 https://www.debatesecurity.com/downloads/Cybersecurity-Technology-Efficacy-Research-Report-V1.0.pdf
2 https://owasp.org/www-project-cyber-defense-matrix/
3 https://attack.mitre.org/
4 https://www.WithSecure™.com/en/consulting/our-thinking/purple-teaming/the-WithSecure™-guide-to-purple-teaming
5 https://www.linkedin.com/pulse/how-worlds-best-risk-decision-makers-decide-paul-brucciani/

Chapter 3

[1] https://link.springer.com/article/10.1007/s11390-015-1518-1
[2] https://www.ukfinance.org.uk/news-and-insight/blogs/collaboration-key-response-cyber-security-threats
https://blogs.imf.org/2020/01/13/cybersecurity-threats-call-for-a-global-response/
https://www.pwc.co.uk/financial-services/assets/pdf/operational-resilience-in-financial-services-time-to-act.pdf

Acknowledgments

The author would like to thank the interviewees for their input and time, without which this research would not have been possible. Special thanks also go to Georgina Elrington and Ben Tudor for their support in reviewing the interviewee responses and editing multiple drafts to create this final report.

The following interviewees have given permission to be named

Respondent	Title	Company	Country
Andrew Rose	CSO	Vocalink (A Mastercard Company)	UK
Bradely Schaufenbuel	CISO	PayChex	US
Chani Simms	CISO	SHe CISO Exec	US
Dave Thomas	Director of Security & Privacy Engineering	SHe CISO Exec	UK
David Lello	CISO	Burning Tree	UK
Ed Harrison	Director IM and Security	Metaswitch Networks	UK
Florent Cottey	Operational CISO	-	
Gene Zafrin	CISO	Renaissance Re	US
Hitesh Patel	Head of Cybersecurity, Cloud Computing & Digital Infrastructure, Audit & Risk	Fidelity Investments	US
Ian Dudley	IT Director	DriveTech	UK
John Scrimsher	CISO	Kontoor Brands	US
Leo Cronin	VP, CSO	Cincinnati Bell	US

Respondent	Title	Company	Country
Marc Ashworth	VP, CSO	First Bank	US
Matt Stamper	CISO	Evotek	US
Matthew Bowler	IT Security Manager	Commodity Trading Industry	UK
Mauro Israel	CISO	Orpea Group	France
Mike Davis	CISO	Alliantgroup	US
Nathan Reisdorf	CISO	New England Law	US
Royce Markose	CISO	rewardStyle	US
Scott Goodhart	Emeritus CISO	The AES Corporation	US
Simon Goldsmith	APAC Information Security Officer	Adidas	UK
Todd Gordon	Director, Information Security	EisnerAmper LLP	US
Anonymous	CISO	Finance Industry	UK
Anonymous	Head of Threat Intelligence	Finance Industry	UK
Anonymous	CISO	Health Industry	UK
Anonymous	Head of Security Intelligence	Public Sector Industry	Norway
Anonymous	CIO	Services	US
Anonymous	CIO	Food Industry	US

Appendix A: questions

The qualitative research study was segmented into the five topics of interest outlined below. To achieve maximum coverage of each topic, each question was related to a subtopic (people, business, technology, etc.). Following the discussion for each question, the qualitative responses were supported with targeted quantitative data points to achieve a grounded theory of the research objective.

- An Effective Security Leader: has your role changed and required you to learn new skills (technical, business and people)?
- Cyber Security Amplification: how have you seen cyber security transition from an obscure concern to a direct business threat (coverage, peers, CxO)?
- Cyber Triggers Influence Change: have any specific cyber incidents created a change in your business or technology decisions (business, technology, people, macro)?
- The Cyber Threat Surface Situation: what are your beliefs regarding the increased threat capabilities of cyber criminals (employees, business, partners, motive, macro)?
- A Security Leader's Vision: what are the necessities required to enable you to excel in your role (tech vendors, peers, yourself)?

Headline Question

Do you believe that events in 2020 could be a positive catalyst for cybe security? (global pandemic, scrutiny of online election balloting, the rise of technology dominance, reality of 5G implementations, cyber crime, fourth industrial revolution, etc.)

No Change — Positive Catalyst

1	2	3	4	5	6	7	8	9	10

An Effective Security Leader

Topic 1 Q1 **Have your role’s responsibilities changed in the past 12-18 months, and have you been equired to learn new skills**

Quant T1Q1 No Change Increased Responsibilities

1	2	3	4	5	6	7	8	9	10

Topic 1 Q2 **Technical: Have you needed to upskill around cloud security, device sprawl, RPA, AI, ML, analytics, threat intelligence, etc?**

Quant T1Q2 No Change GreaterTechnical Skills

1	2	3	4	5	6	7	8	9	10

Topic 1 Q3 **Business: Have you needed to increase your business skills and the impact you have on company achievements?**

Quant T1Q3 No Change GreaterTechnical Skills

1	2	3	4	5	6	7	8	9	10

Topic 1 Q4 **People: Has your role created a larger diversity of internal and external engagements?**

Quant T1Q4 No Change Greater Diversityof Engagements

1	2	3	4	5	6	7	8	9	10

Topic 1 Q5 **People: Do you believe your role has increased in EQ as well as IQ?**

Quant T1Q5 IQ EQ

1	2	3	4	5	6	7	8	9	10

Cyber Security Amplification

Topic 2 Q1 **Do you believe that cyber security has transitioned over the past 12-18 months in operational relevance?**

Quant T2Q1 No Change — More Relevant

1	2	3	4	5	6	7	8	9	10

Topic 2 Q2 **Coverage: What priority do you place on responding to cyber security coverage in the news?**

Quant T2Q2 No Interest — Very Relevant

1	2	3	4	5	6	7	8	9	10

Topic 2 Q3 **Peers: Do your (non-IT) peers in your organization understand how cyber security is a threat to their responsibilities?**

Quant T2Q3 Not a Threat — Increased Threat

1	2	3	4	5	6	7	8	9	10

Topic 2 Q4 **CxO: Do you believe cyber security is treated as a business enabler or a risk mitigation practice within your organization?**

Quant T2Q4 Business Enabler — Risk Mitigation

1	2	3	4	5	6	7	8	9	10

Topic 2 Q5 **CxO: What are your beliefs about cyber security as a board discussion?**

Quant T2Q5 Not a Priority — Positive Priority

1	2	3	4	5	6	7	8	9	10

Cyber Triggers Influence Change

Topic 3 Q1 **Have you had to respond to a greater number of specific cyber incidents in the past 12-18 months? What are the top three threats?**

Quant T3Q1 Fewer Incidents — More Incidents

1	2	3	4	5	6	7	8	9	10

Topic 3 Q2 **Business: Have your cyber operations created the need for your organization to change the way it does business?**

Quant T3Q2 No Change — Change to Business Ops

1	2	3	4	5	6	7	8	9	10

Topic 3 Q3a **Technology: Do you make at least 50% of your cyber technology decisions based on new technology that looks interesting?**

Quant T3Q3a Yes □ No □

Topic 3 Q3b **Technology: Do you make at least 50% of your cyber technology decisions based on peer network contact recommendations?**

Quant T3Q3b Yes □ No □

Topic 3 Q3c **Technology: Do you make at least 50% of your cyber technology decisions based on the leader or incumbent vendor?**

Quant T3Q3c Yes □ No □

Topic 3 Q3d **Technology: Do you make at least 50% of your cyber technology decisions based on whether they are aligned to a threat?**

Quant T3Q3d Yes □ No □

Topic 3 Q4 **People: Have the key disciplines that you look for in new (cyber specialist) employees changed in the past 12-18 months?**

Quant T3Q4 No Change — Increased Disciplines

1	2	3	4	5	6	7	8	9	10

Topic 3 Q5 **People: How much time per month do your direct staff spend learning new skills?**

Quant T3Q5 Hours per Month

1	2	3	4	5	6	7	8	9	10+

Topic 3 Q6 **Macro: Do you believe your security capability has improved and allows you to defend your organization?**

Quant T3Q6 No Change — Greatly Improved

1	2	3	4	5	6	7	8	9	10

Topic 3 Q7 **Macro: Who’s moving fastest – you or your adversaries (criminals)?**

Quant T3Q7 You — Adversaries

1	2	3	4	5	6	7	8	9	10

The Cyber Threat Surface Situation

Topic 4 Q1 **Do you believe there has been an increase in threat capabilities of cyber wcriminals? If so, what threats worry you the most?**

Quant T4Q1 No Change — Visible Increase

1	2	3	4	5	6	7	8	9	10

Topic 4 Q2 **Employees: Are there more attacks targeted directly or indirectly at your employees??**

Quant T4Q2 Fewer Attacks — More Attacks

1	2	3	4	5	6	7	8	9	10

Topic 4 Q3 **Business: Are there more attacks aimed at disrupting your business operations?**

Quant T4Q3 Fewer Attacks — More Attacks

1	2	3	4	5	6	7	8	9	10

Topic 4 Q4 **Partners: Have you been directly impacted by attacks coming indirectly from business partners?**

Quant T4Q4 No Change — Increased Attacks

1	2	3	4	5	6	7	8	9	10

Topic 4 Q5 **Motive: Where would you place the motivation of cyber criminals against your company?**

Quant T4Q5 Data Theft — Financial Gain

1	2	3	4	5	6	7	8	9	10

Topic 4 Q6 **Macro: Has your belief of what good security is changed over the past two years?**

Quant T4Q6 No Change — Belief Substantially Changed

1	2	3	4	5	6	7	8	9	10

A Security Leader’s Vision

Topic 5 Q1 **Do you believe your role will become more critical to your business??**

Quant T5Q1 No Change — More Critical

1	2	3	4	5	6	7	8	9	10

Topic 5 Q2 **Tech Vendors: What should tech vendors be doing to help you succeed?**

Topic 5 Q3 **Direct Staff: Do you believe that the rising and varied types of threats could mean that managing your own security operations team will not be proactive enough to ensure consistent business operations?**

Quant T5Q3 Defensive — Proactive

1	2	3	4	5	6	7	8	9	10

Topic 5 Q4 **Peers: How could your peers and reporting line management help you succeed?**

Topic 5 Q5 **Peers: Are your leadership teams more, or less, engaged with IT security teams?**

Quant T5Q5 Less Engaged — More Engaged

1	2	3	4	5	6	7	8	9	10

Topic 5 Q6 **Peers: Have board priorities and attitudes changed regarding the impor tance of cyber security protection?**

Quant T5Q6 Less Importanceft — Increased Importance

1	2	3	4	5	6	7	8	9	10

Topic 5 Q7 **Yourself: What do you believe you need to improve to excel in your role?**

Topic 5 Qa **Do you feel more secure in your role as a result of the events of 2020?**

Quant T5Qa Less Secure — Very Secure

1	2	3	4	5	6	7	8	9	10

Topic 5 Qb **Do you want to stay in your current role (move on or leave the profession)?**

Quant T5Qb Stay — Move

1	2	3	4	5	6	7	8	9	10

Topic 5 Qc **How are you and your team handling stress?**

Quant T5Qc Badly — Very Well

1	2	3	4	5	6	7	8	9	10

Topic 5 Qd **Have you seen signs of burnout in your team?**

Quant T5Qd Some Signs — Significant

1	2	3	4	5	6	7	8	9	10

Topic 5 Qe **Do you have more funding available?**

Quant T5Qe Less — Increased

1	2	3	4	5	6	7	8	9	10

Topic 5 Qf **How do you balance your budget between responsibility and accountability?**

Quant T5Qc Responsibility — Accountability

1	2	3	4	5	6	7	8	9	10

Who We Are

WithSecure™ is cyber security's reliable partner. IT service providers, MSSPs and businesses along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection & response is powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ is part of WithSecure™ Corporation, founded in 1988, and listed on the NASDAQ OMX Helsinki Ltd.

withsecure.com/business | twitter.com/withsecure | linkedin.com/withsecure

WITH secure