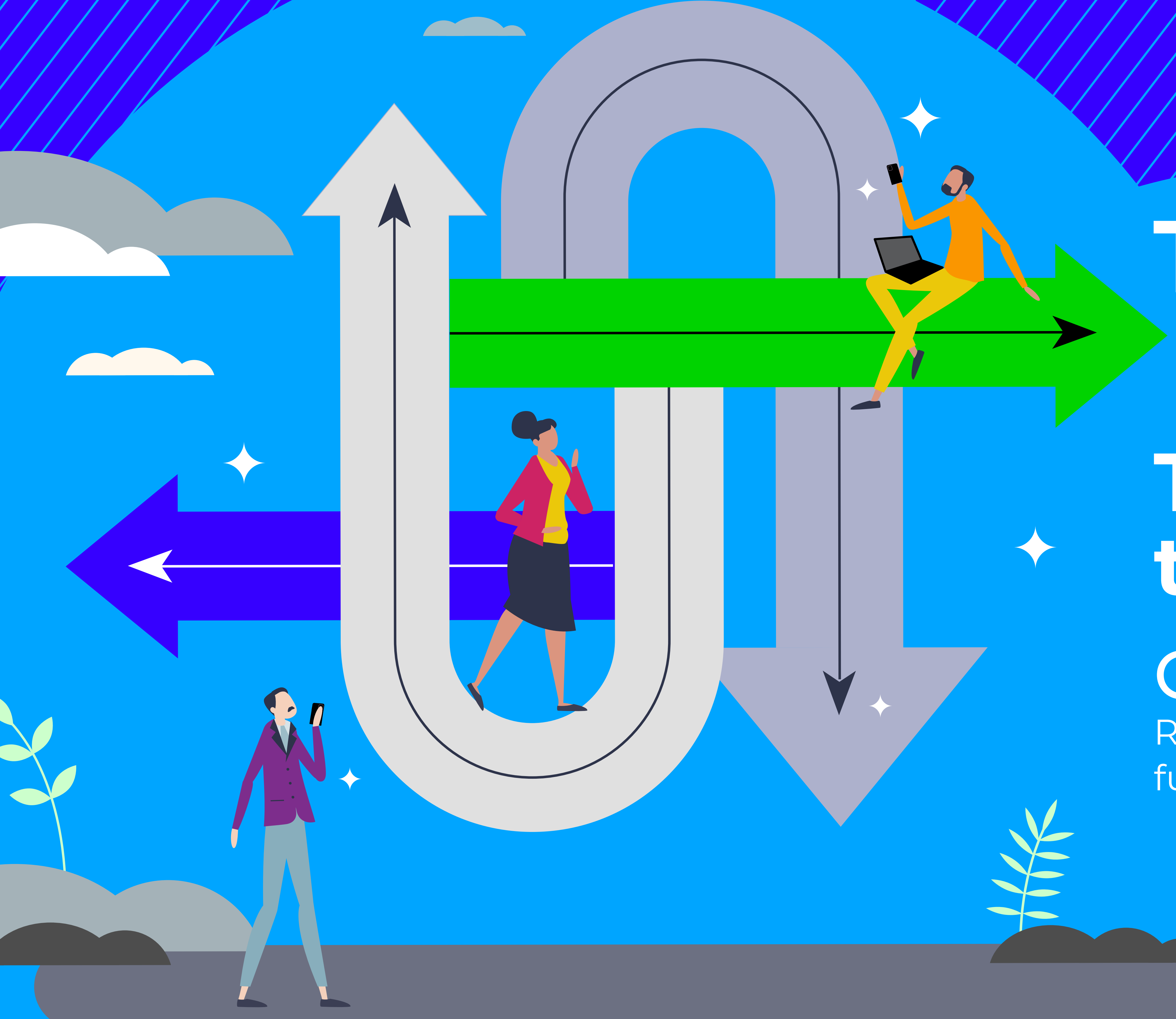


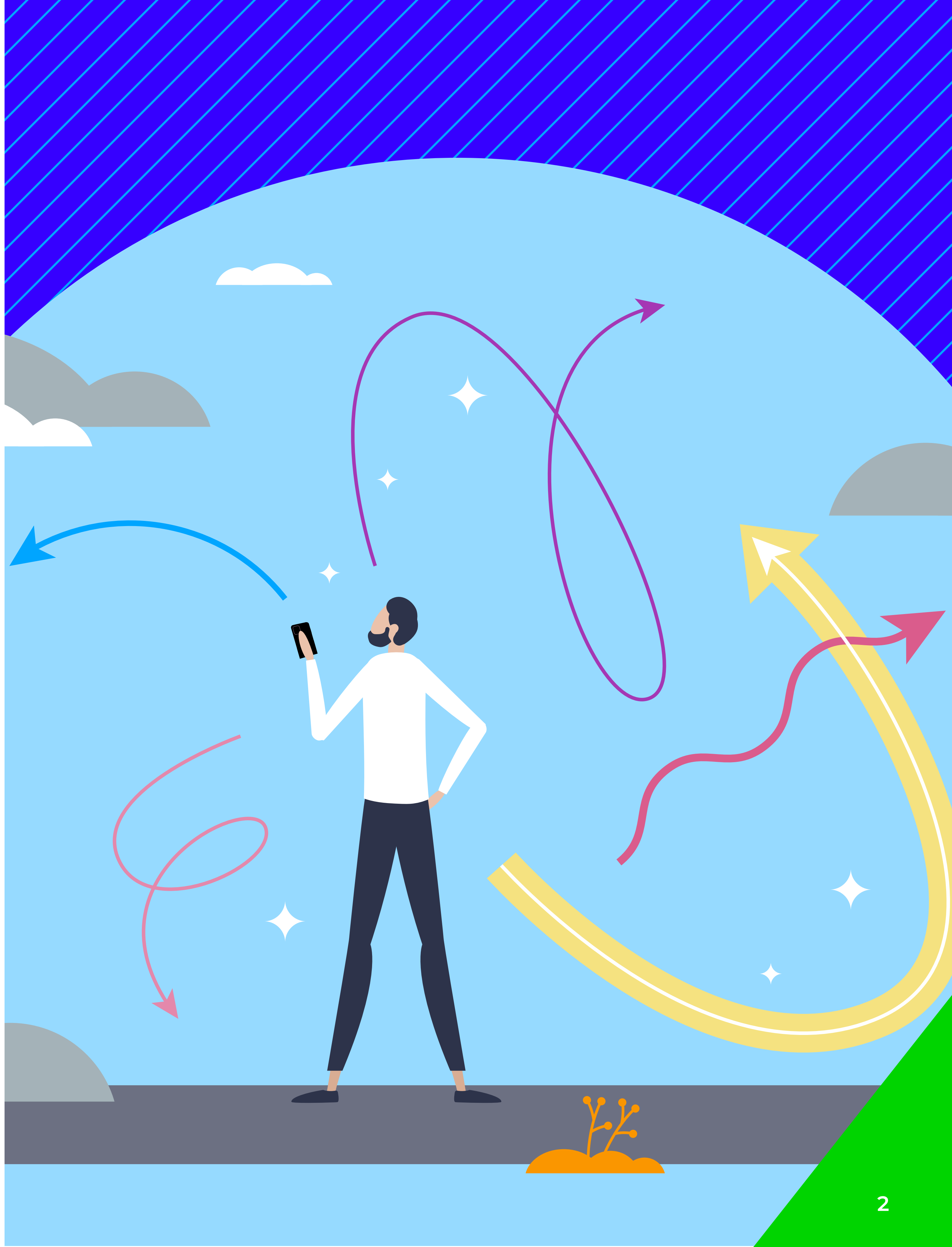
Trellix

The Mind of the CISO

CISO Crossroads:

Regulation, pressures, and the future of cybersecurity leadership

Contents



Introduction

The CISO's tipping point

From past reports exploring the Mind of the CISO (see page 18), the Chief Information Security Officer (CISO) role has been defined by security. How protected are they able to keep their organization? When a breach occurs, how swiftly do they resolve it, and what consequences do they face? How is AI impacting the cyber threat landscape, and how do they secure critical data in this new age? As the primary person in charge of their organization's security, their central challenge (and burden) has always been security.

However, in recent times, a new storm has been brewing, which is having a greater impact on the role of the CISO than most thought probable. Cybersecurity regulation emerged as digital systems became more integral to business operations, but over time, regulatory frameworks have expanded in response to the increasing frequency and sophistication of cyberattacks – and they are continually evolving as technology and cyber threats advance. The CISO, therefore, is facing a critical challenge to ensure compliance with regulations as they come into effect, but also to understand what will be regulated and when – and how they can ensure compliance within their organization's increasingly complex and intricate infrastructure.

Further to the challenge of regulatory compliance, the increasing awareness of security risks has provoked interest from organizations' boards. Many CISOs are now finding it a requirement to report to their board, whether on security, compliance, or other factors, requiring many CISOs to step out of their comfort zone and have a presence at the highest level within their organization.

This new duality to the role of the CISO is heightening pressure in an already pressure-loaded role. And because of this increased load, many organizations are at an extremely pivotal point. **At a time when CISOs are needed the most, many are thinking of leaving the role**, potentially leaving organizations headed into the regulatory storm without the knowledge and support of the CISO keeping them afloat so far.

Trellix commissioned independent market research agency Vanson Bourne to conduct a research survey of 508 CISOs across America, Europe, the Middle East, and the Asia Pacific region to understand their views on cybersecurity regulation, the CISO role, and their interactions and challenges when reporting to their organization's board. Respondents work across various industries, including finance, public sector, healthcare (public and private), manufacturing, energy, oil, gas, and utilities.

This report sheds light on the latest changes, responsibilities, and requirements for CISOs, the impacts of navigating them, and why **every organization needs to act now** to protect the future of the role of the CISO.

Key Findings

98%

of CISOs are concerned about the pace of regulatory change in cybersecurity

91%

state the changing regulatory landscape in cybersecurity is redefining what it means to be a CISO

79%

believe the time and effort it takes to keep pace with regulatory change is not sustainable

49%

report to the board at least on a weekly basis, with 15% reporting daily

84%

believe the role of the CISO should be split into technical and business-focused roles

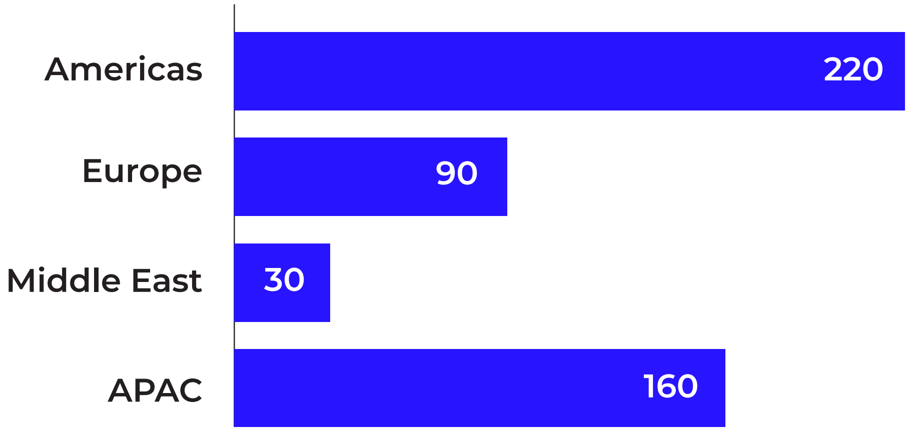
49%

do not see a future as a CISO due to the ever-expanding responsibilities

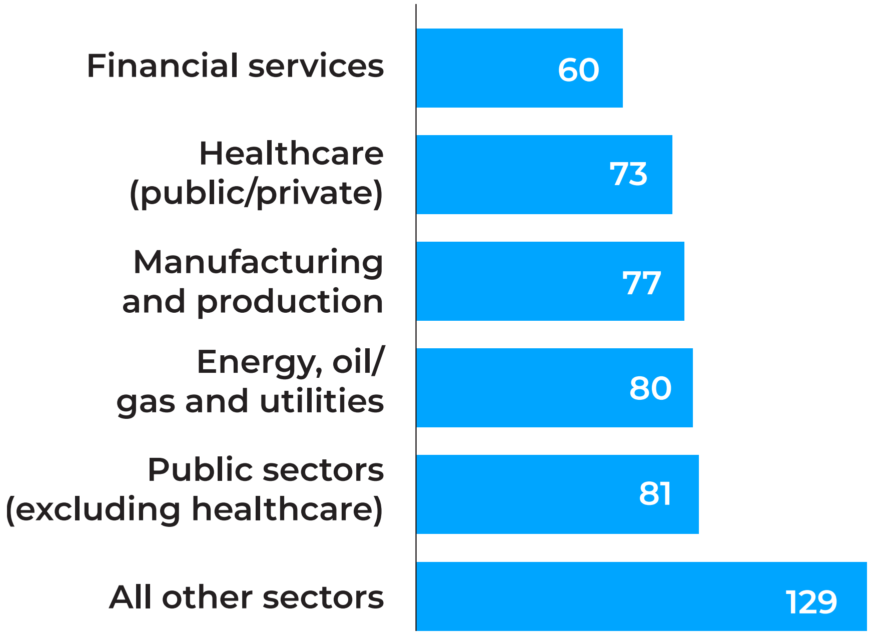
Quantitative Respondents

500 CISOs (or equivalent) were interviewed in August/September 2024, split in the following ways...

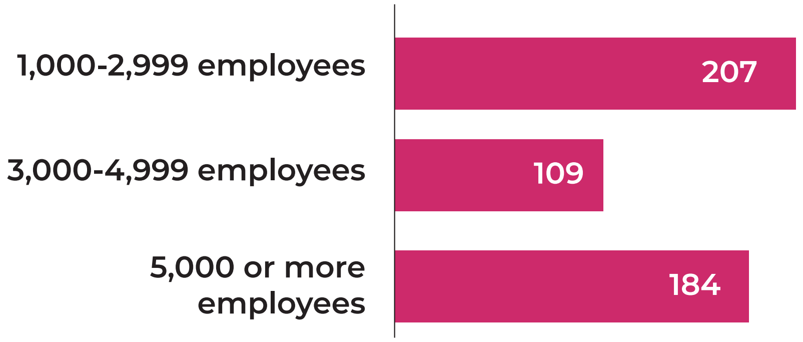
1. In four regions: America, Europe, Middle East, APAC



2. Across a number of sectors: including Finance, Healthcare, Public sector, Energy, Manufacturing etc.



3. Were from organizations with more than 1,000 employees



All interviews were conducted using a rigorous multi-level screening process to ensure only suitable candidates participated

Qualitative Respondents

… by region

In the UK, US
and Singapore…

🇺🇸	x 4
🇬🇧	x 2
🇸🇬	x 2

… by organizational sector

Public sector x 2

Healthcare x 2

Financial Services x 2

Energy x 1

Manufacturing x1

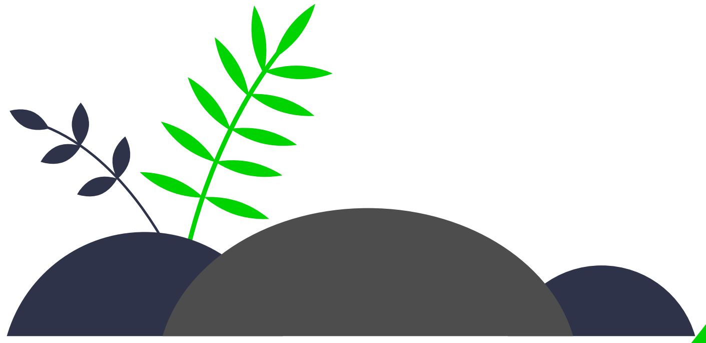
… by organizational size

1,000 – 2,999 employees x3

5,000 – 9,999 employees x2

10,000+ employees x3

All interviews were conducted using a rigorous multi-level screening
process to ensure only suitable candidates participated



Section 1

Regulation Overload: The New Threat to CISOs

Rising threats and the CISO's burden in 2024's shifting cyber landscape

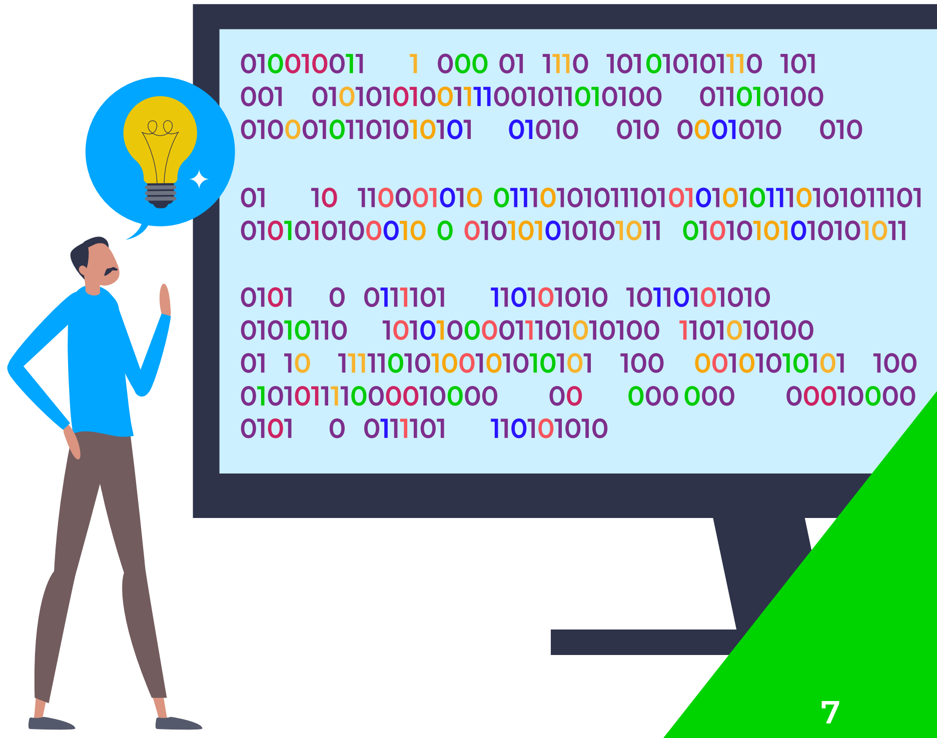
Of late, global events, technological advancements, and evolving threat actor tactics have created a dynamic environment where organizations are continuously at risk. For CISOs, this period arguably represents the most important and challenging era in their careers.

At present, challenges are advancing from all directions:

- **Election security** has emerged as a critical international concern. Almost half of the world's population is partaking in elections in their countries in 2024, and there are unprecedented challenges related to electoral integrity – ranging from misinformation campaigns to direct attempts to infiltrate voting systems.
- **Ransomware** continues to be one of the most pervasive cybersecurity threats, predicted to cost organizations $42 billion in 2024. The operational and financial implications from such an attack are staggering, from data loss, operational downtime, and reputational damage to the burden of paying ransoms to regain access to their systems.
- There is increased activity from **Chinese, Iranian, and Russian-backed threat groups**. These groups often target critical infrastructure to steal intellectual property, disrupt operations, or conduct espionage. There has been a marked uptick in both frequency and sophistication from these groups.
- **Artificial Intelligence (AI)** represents both a tremendous opportunity and significant risk in the cyber landscape (as we explored in our 'The Mind of the CISO: Decoding the GenAI Impact' report).
- **The global IT outage in July 2024** gave the cybersecurity community a stark reminder of how dependent organizations are on third-party solutions. Though temporary, the disruption to threat detection and response capabilities for the thousands of CrowdStrike customers running Microsoft operating systems led to extensive consequences:
  - 66% reported an increase in the number of cyberattacks experienced since the outage (20% reported a significant increase). To break this down further, over a quarter of financial services organizations experienced a significant increase in cyberattacks (27%), and not far behind were organizations in the energy, oil/gas and utilities sector (24%), and healthcare (23%).
  - Malware (38%), phishing (35%), and data theft attacks (35%) were the top reported attacks experienced in the aftermath. Healthcare reported state sponsored (41%), data theft attacks (35%), ransomware (35%), and business email compromise (35%) as the top attacks.

The global IT outage...

> **We were concerned a lot about the vendors and the third parties that directly support our business. Many of them [were] impacted and we were [...] concerned about the disruption in supply chains and delay in shipments of critical resource materials for our business.**
>
> – US, Energy, Oil / Gas and Utilities



Section 1

Regulation Overload: The New Threat to CISOs

It's apparent the workload of the CISO is vast. Ensuring the security of the democratic process (establishing public trust), prioritizing ransomware prevention and mitigation, defending against unpredictable and highly skilled state-sponsored attacks, and responding to global incidents are all top priorities. Not only these, but they must also navigate complex regulatory requirements, increasing stakeholder interest and expectation, and limited resources, all while being proactive in a rapidly shifting environment. We explore this shifting dynamic further in this eBook.

> **The industry broke, [...] because they think security is a response, security is a responsibility of a single team in the organization.**
>
> – US, Healthcare

> **Regulation can never foresee all possible software problems.**
>
> – UK, Public Sector

> **While I believe regulation can prevent many issues from happening, including a lot of software issues, with AI taking center stage I'm unsure we have the ability to properly regulate for what will come. Most regulations are so vague as to be unenforceable here in the US, possibly on purpose.**
>
> – US, Public Sector

Section 1

Regulation Overload: The New Threat to CISOs

Regulation as a catalyst for CISO recognition

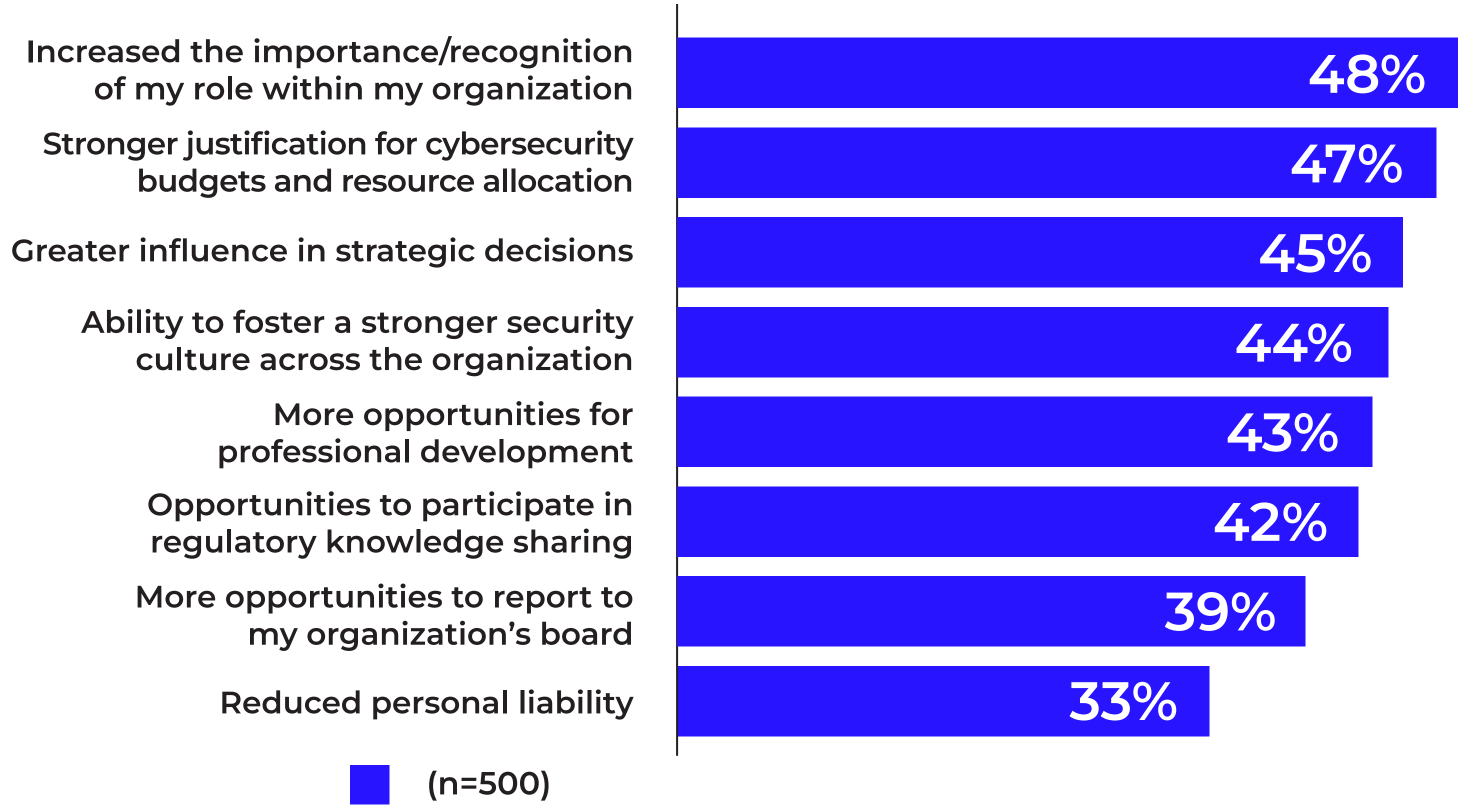
The growing burden on the CISO is not 'security' in its traditional sense. With increasing cyber threats and angles of attack, cybersecurity regulation is growing at a rapid rate, and organizations are left with no option but to demonstrate compliance.

The clear reality is regulations are necessary to enforce standardized practices and security measures, ensuring organizations are accountable and to prevent breaches and data theft. However, further to this, CISOs are also finding regulations have benefits for themselves – in their role, their organization, and their career.

In the past, we've seen CISOs have felt 'in the shadows,' where they only become known or come to the forefront of their organization when things go wrong. Almost half (48%) of the CISOs we spoke to feel there is greater acknowledgment and recognition of their role as part of their regulatory work, and **93% agreed cybersecurity regulation has helped their career as a CISO** – such as having greater influence in strategic decisions (45%) or elevation to board-level discussions (39%). In particular, this has been a great benefit from the increasing regulatory work CISOs are carrying out.

> **Yes, my job is getting harder and harder, but harder and harder means that I feel much safer that way because I can hold people accountable.**
>
> – US, Healthcare

Top benefits CISOs have experienced from cybersecurity regulations



> **The guardrails help me point out to them when they don't like the security that I'm implementing [...] I can point to something, and state [contract or regulations] requires that you do [that] [...] that ends the conversation. So, it makes that part of my life easier.**
>
> – US, Public Sector

> **I sit at that table [...] that helped me to have kind of insight and always lockstep with their directions from [their] perspective, so help to advise them at that level.**
>
> – US, Energy, Oil / Gas and Utilities

Section 1

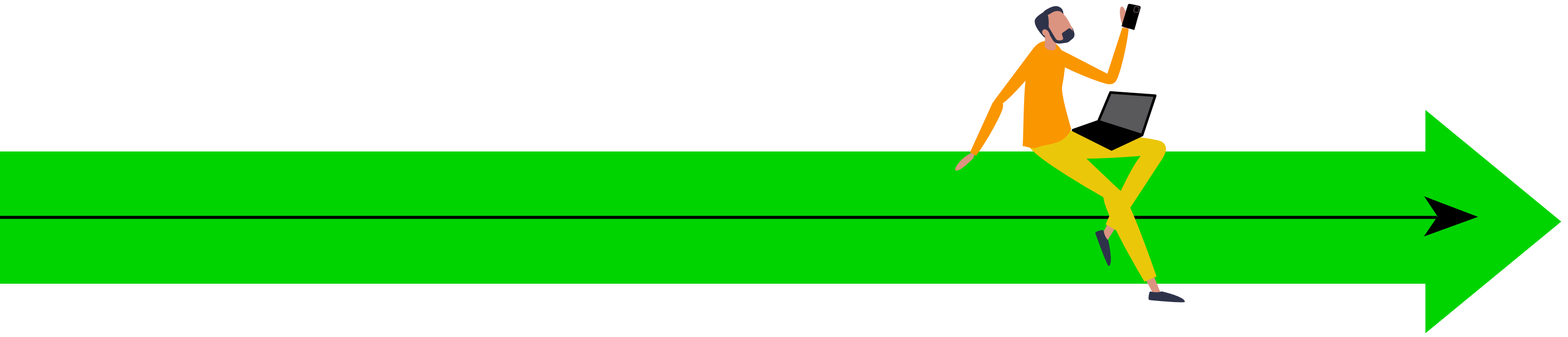
Regulation Overload: The New Threat to CISOs

The race to keep up with compliance

The complexities of the global regulatory landscape are fraught with intricacies for CISOs to manage. With regions, countries, and states implementing regulations at a different pace and with different priorities, CISOs have found they are dedicating more and more time to ensure they stay abreast of the latest regulations and can comply within their organization.

For many CISOs, it is a constant challenge and concern they must address. CISOs have to review their internal policies and infrastructure to align them to regulations, as well as dedicate their time and energy to identify regulatory changes or new additions and ensure they have the capability and resources to comply with these changes.

The frequency of regulatory change is a huge concern for over a third (37%) of CISOs, and keeping up with the pace of change is the top reported challenge they feel they face in compliance (42%). Where CISOs typically only face a cyberattack or security threat one at a time, cybersecurity regulation can hit like a ton of bricks. Several new regulations or changes can be released within a very short period, and it is catching CISOs off guard. The new 'normal' CISOs face is they need to plan for regulatory change as much as they plan for the next cyber threat. Anticipating the regulators and their intentions ensures CISOs can stay one step ahead of the game.



37%

Are extremely concerned about the pace of regulatory change in cybersecurity

34%

Strongly agree the agility of their organization to adapt to new cybersecurity regulations is concerning

35%

Are reviewing and updating their cybersecurity policies to remain compliant with new regulations multiple times per month

> **“You also need to […] understand what the regulator wants. And this requires a lot of networking […] to really understand what's going on in their minds and be able to anticipate that and build that into our security program […] But the traditional CISO will not do all these things.**
>
> – Singapore, Healthcare

> **“Because we put in the work upfront three, four, five years ago – if you do it right, the impact of those […] new regulatory requirements will be lessened […] so I guess where you are in your journeys definitely plays a role in how stressful these new requirements are to you.**
>
> US, Energy, Oil / Gas and Utilities

Section 1

Regulation Overload: The New Threat to CISOs

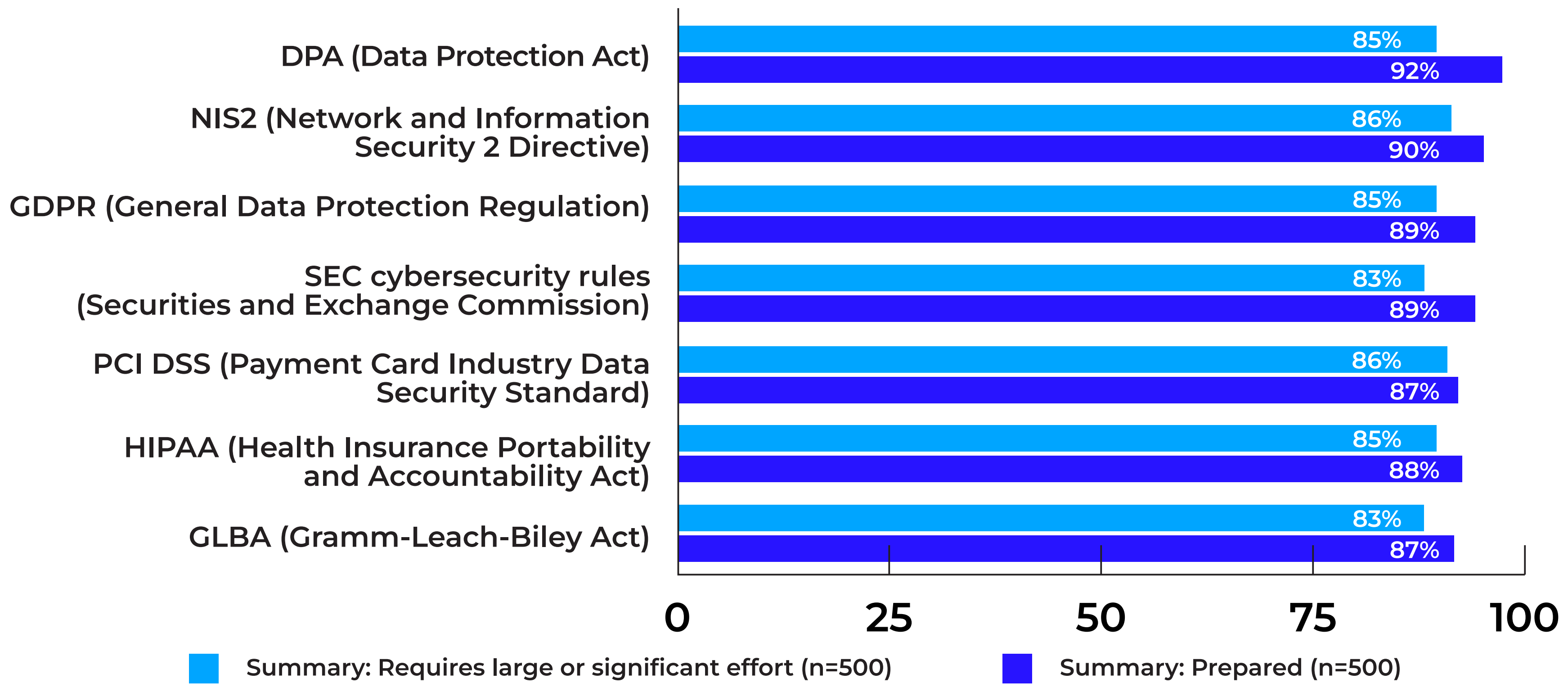
Confidence at a cost: balancing preparedness and effort

As the landscape of cybersecurity regulations becomes more complex, CISOs, for the most part, feel prepared and confident in the cyber regulations their organization must adhere to.

With governments and industry bodies rolling out new compliance requirements to counter cyber threats, CISOs spend an overwhelming amount of time ensuring their organizations meet these standards. While confidence is high in understanding the regulations (98% are confident), it's clear this is coming at a cost – **around 4 in 5 (79%) report the time and effort required to keep pace with regulatory change is not sustainable**. This growing burden diverts attention from other critical security functions as CISOs focus more on paperwork and audits than safeguarding digital assets.

This unsustainable dynamic could also be enabling a false sense of security. Complying with regulations does not ensure robust cybersecurity or prevent threats or attacks from success. Being overwhelmed by regulatory demands means CISOs may lack the time and resources needed to innovate or strengthen their defences, exposing organizations to risks compliance alone cannot mitigate.

Preparedness and effort to deal with regulatory changes



> It's become my entire job. As opposed to focusing on making sure we're more secure, I have been focused on ensuring that we are not running afoul of any of the regulatory mandates that we have.
>
> – US, Public sector

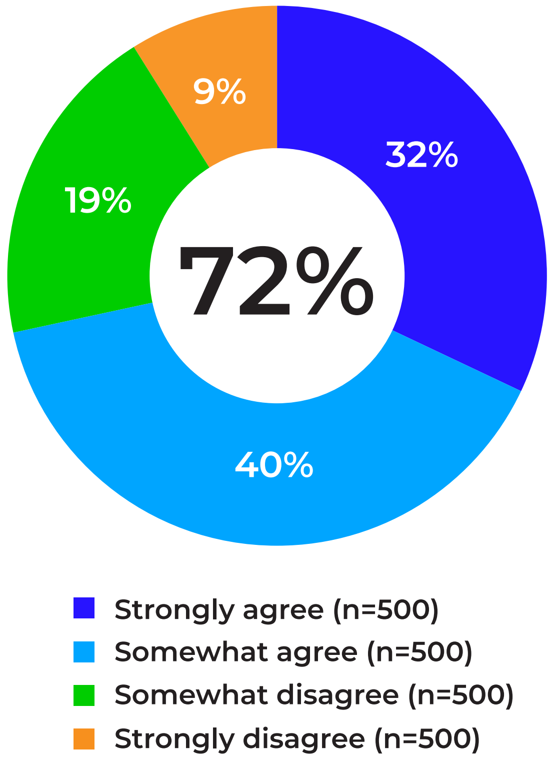
> So that is something which changed the way we look at cybersecurity solutions [...] most of the governments had introduced rules or regulations or guidelines around how they need to up their cybersecurity maturity, for an example [...] we had to achieve extra certifications on how we are implementing our cybersecurity solutions, how safe it is against the evolving threats, how are we going to detect the threats, etc., and what do we do about it.
>
> - UK, Manufacturing and production

Section 1

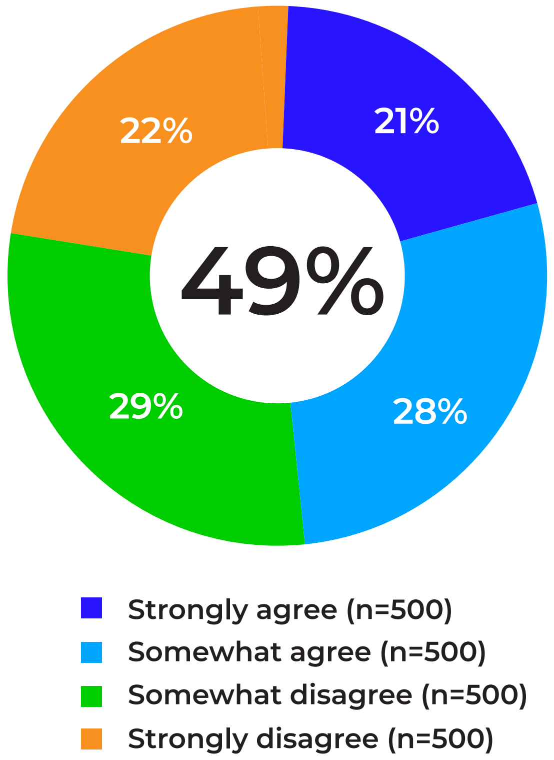
Regulation Overload: The New Threat to CISOs

Overload or longevity – why CISOs need support to remain

For CISOs themselves, the unsustainable workload of constantly juggling regulatory demands with day-to-day security operations is stretching them thin – and CISOs are crying out for help.



"I am concerned about my future in my CISO (or equivalent) role due to expanding responsibilities"



"I do not see a future in my CISO role due to the ever-expanding responsibilities"

The challenges faced and expanded responsibilities leave CISOs feeling drained, and the changing regulatory landscape is redefining what it means to be a CISO (strongly agreed by 41%). Many have reflected on these challenges and feel they have no option but to consider leaving the role – with almost half (49%) contemplating a change in their future. Therefore, organizations are at real risk of losing a highly skilled and talented workforce and putting the organization's security at risk without a CISO at the helm.

> **What we always wish [...] it would be wonderful if the regulators [...] come up with a regional or global regulation, [...] helping people from different countries or a business that's operating in multiple jurisdictions, then we'll just have to [...] comply with one regulation instead of multiple.**
>
> – Singapore, Healthcare

> **This is the business problem [...] security is a community. How you build a community from the ground up is required. The people [...] doing innovations, the people actually running the business as well as people defending it, and even all the way to the regulatory requirement, the government [etc.].**
>
> – US, Healthcare

Section 1

Regulation Overload: The New Threat to CISOs

There are key areas where responsibility can be taken to answer this cry for help from CISOs and to ensure longevity in the role:

Regulators

CISOs report a top challenge as having insufficient guidance from regulators (39%), and 59% agree current regulations do not provide clear guidance on CISO responsibilities. CISOs would vastly benefit from clearer, more streamlined regulatory frameworks reducing the complexity and any overlaps between regulations. Furthermore, including CISOs in the conversation around regulations and providing practical advance warning would enable CISOs to proactively ensure compliance, rather than retrospectively implementing changes when regulations are released.

Organizations

Support from within the organization is also critical for CISOs. 77% feel it is up to them, rather than their organization, to stay informed about regulatory changes, and notable proportions report impacts on their work-life balance (38%), and negative impacts on their mental wellbeing/ stress levels (26%). The non-stop cycle of documentation and review is overwhelming their workload, and therefore organizations could do more to share the load, by providing executive support, staff, or technology to offload some of this burden.

Peers and the Cybersecurity industry

Keeping up with the rapid pace of change can be daunting, and many CISOs feel isolated in their efforts to stay compliant. Over four in five CISOs (87%) agree discussing with peers regarding cybersecurity regulation is more valuable than doing their own research, and therefore is a notable area in which CISOs can seek further support. The security industry as a whole is notoriously private, with the overarching view sharing too much information increases your security risk (the less people know the better). However, with so many CISOs at risk of burnout and leaving the role, the call is for the industry to change – enabling opportunities to collaborate and share knowledge with peers, gain insights into best practices, and stay informed of new regulations. This sense of community can reduce the pressure of constantly having to reinvent the wheel and help CISOs feel less alone in their struggles.

> **“Talk to other companies in the field, talk to startups, they want to build something cool, help them out, build something even better, because at the end of the day you’re going to be using the product.**
>
> – US, Healthcare

> **“They’re retiring, it’s that time, or they’re early retiring, because they’re just done. I’m hoping to get a lot that we see more younger, fresh thinkers with new ideas in that role and that kind of changes how we view the entire role.**
>
> – US, Public Sector

Section 2

The Boardroom Battle: Elevating the CISO to Strategic Leadership

The new boardroom challenge for CISOs

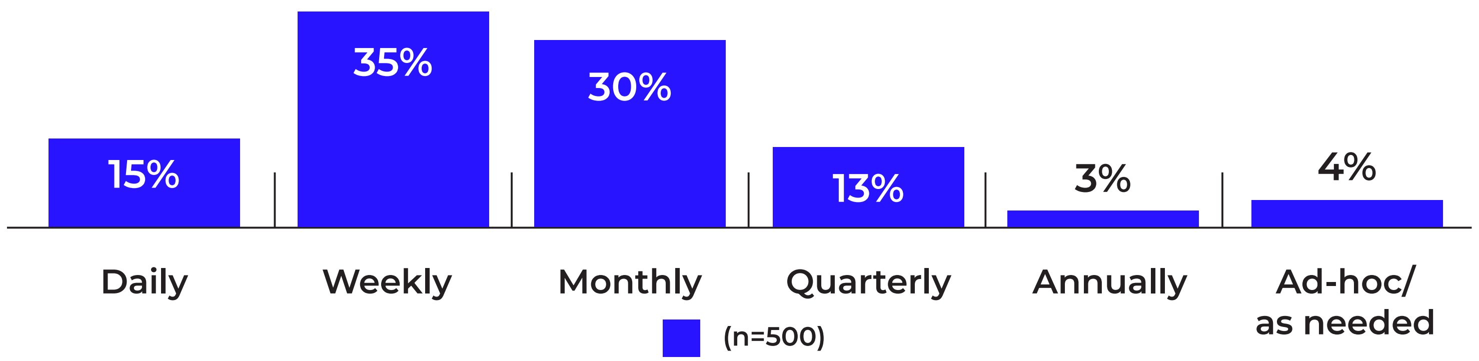
The increased visibility of cybersecurity within every organization and world media means the microscope is honed in on the decisions and actions of the CISO. As a result, organizations' boards are increasingly interested in understanding the security status of their organization and the security decisions being made. This has led to many CISOs directly reporting cybersecurity to their board, elevating their position and visibility within the business; a positive in many instances. However, this task is also becoming cumbersome, with reporting frequency and communication challenges presenting new hurdles CISOs must overcome.

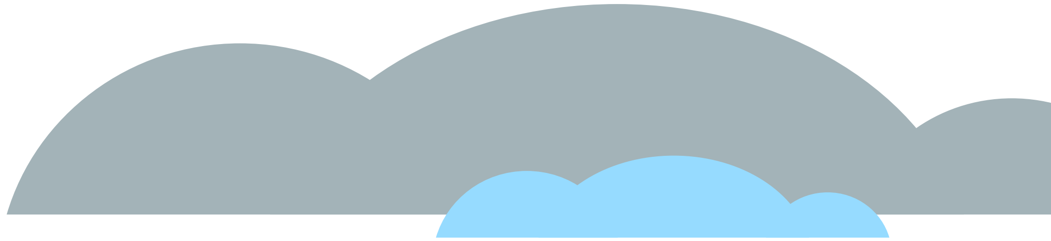
In 2024, board reporting is the norm for almost all CISOs (99.4%). However, the concern and challenge here is it's a new and critical demand on the CISO's already stretched time. Half (49%) of the CISOs we spoke with are reporting on at least a weekly basis with their board, with 15% reporting on a daily basis. In many cases, ensuring they have the right information and are sufficiently prepared can take significant preparation, therefore pulling CISOs away from their core security responsibilities – and adding to their burden.

CISOs report most on cybersecurity risk management, assessment, and mitigation plans (57%), high-level strategic overviews, planning and alignment (49%), and regulatory compliance and audit results (48%). This information helps organizations' boards remain abreast of the most critical information to ensure their organization is aligned and protected within the latest regulatory guidance, as well as planning for the future and ensuring alignment with the overall business strategy.

Many CISOs appreciate this opportunity to present and influence at the highest level, with 90% agreeing board engagement is helping to drive positive changes in cybersecurity strategies within their organization. Their work is paying off in many aspects, too – with a strong level of agreement their board is engaged with looking at cybersecurity regulation (40%), and their board understands the importance of cybersecurity risks (46%). However, the question is, how effective do the CISOs feel this new element to their role is, and how sustainable is it when considering the other priorities of the role?

Frequency report cybersecurity issues to the board





> In the past we would do a lot of tactical things, but because of the interaction with the board and the executive teams, we have higher-level conversations, we [...] have more insight to the business strategy so we can advise them on cyber risks with those business initiatives.
>
> – US, Energy

> This is where [...] the evolution of interaction has changed from reporting [...] one way and has become two way communication. And then we are deepening that two-way communication from just a conversation into a partnership.
>
> – US, Public Sector

Section 2

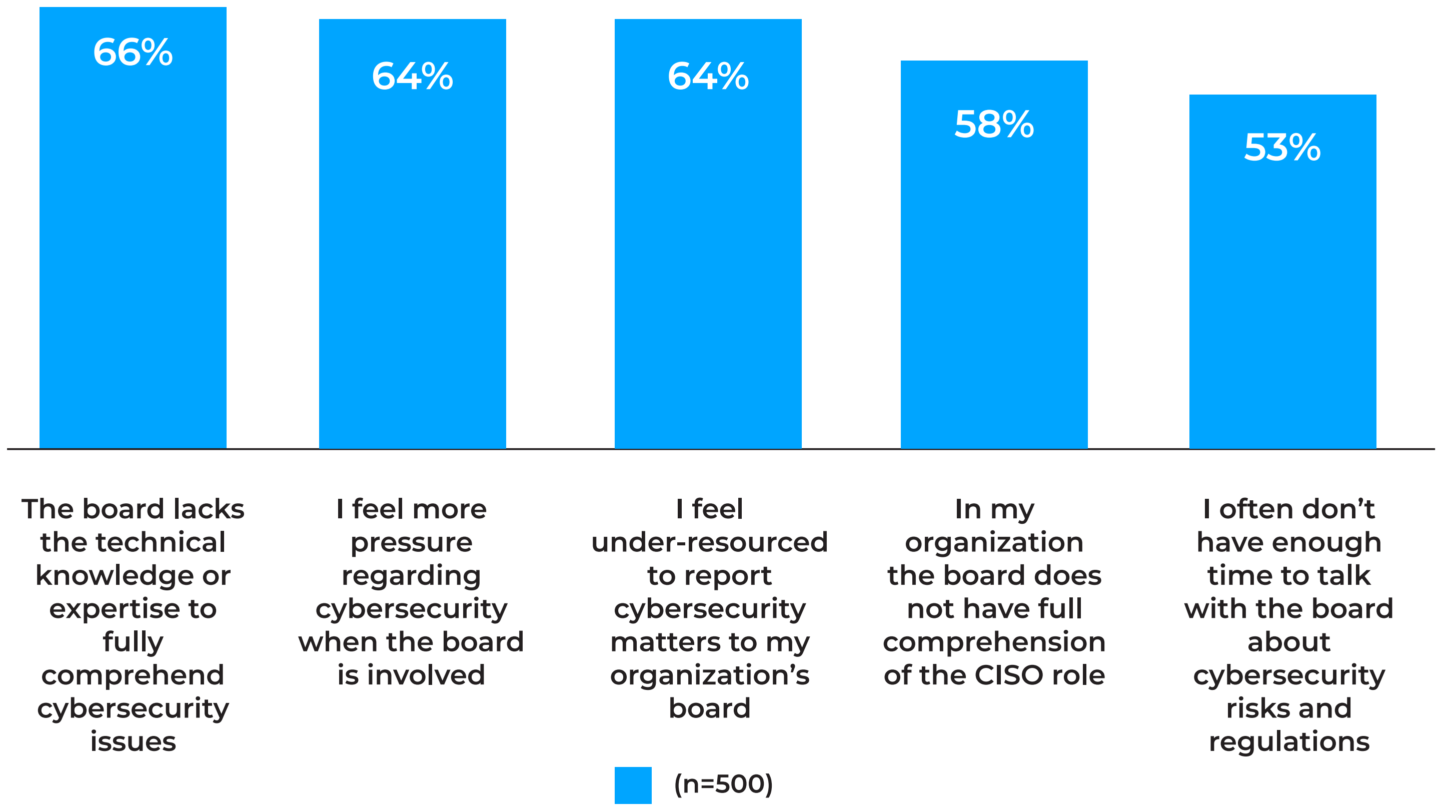
The Boardroom Battle: Elevating the CISO to Strategic Leadership

Learning the language of the board

Reporting to the board is not plain sailing for all CISOs. With the frequency of reports a daunting challenge, CISOs must learn new skills to ensure their interactions are succinct, productive, and valuable.

The boards' diverse and multi-role composition often means a wide range of knowledge, skills, and understanding – and not everyone has the technical expertise to comprehend many of the complexities and intricacies of cybersecurity and cyber threats (66%). This means CISOs are having to spend extra time simplifying information and learning to communicate in different ways without losing the nuances of cybersecurity risks. Despite their best efforts, over a third (35%) report communication barriers are a challenge with their board and, therefore, a real area of concern.

Challenges CISOs face when reporting to the board



> **Your board of directors, those folks, unless they are a technologist, often times talking, sharing technology related information might not be very effective. I think they understand the risk conversation very well. So refine and focus your conversations about managing risk for business. Risks for the organizations is, I think, how you can get the engagement from your board directors.**
>
> – US, Energy, Oil / Gas and Utilities

> **The role of the CISO will be more or less primarily about [being] a communicator, it is a major part of that person's role.**
>
> – US, Energy, Oil / Gas and Utilities

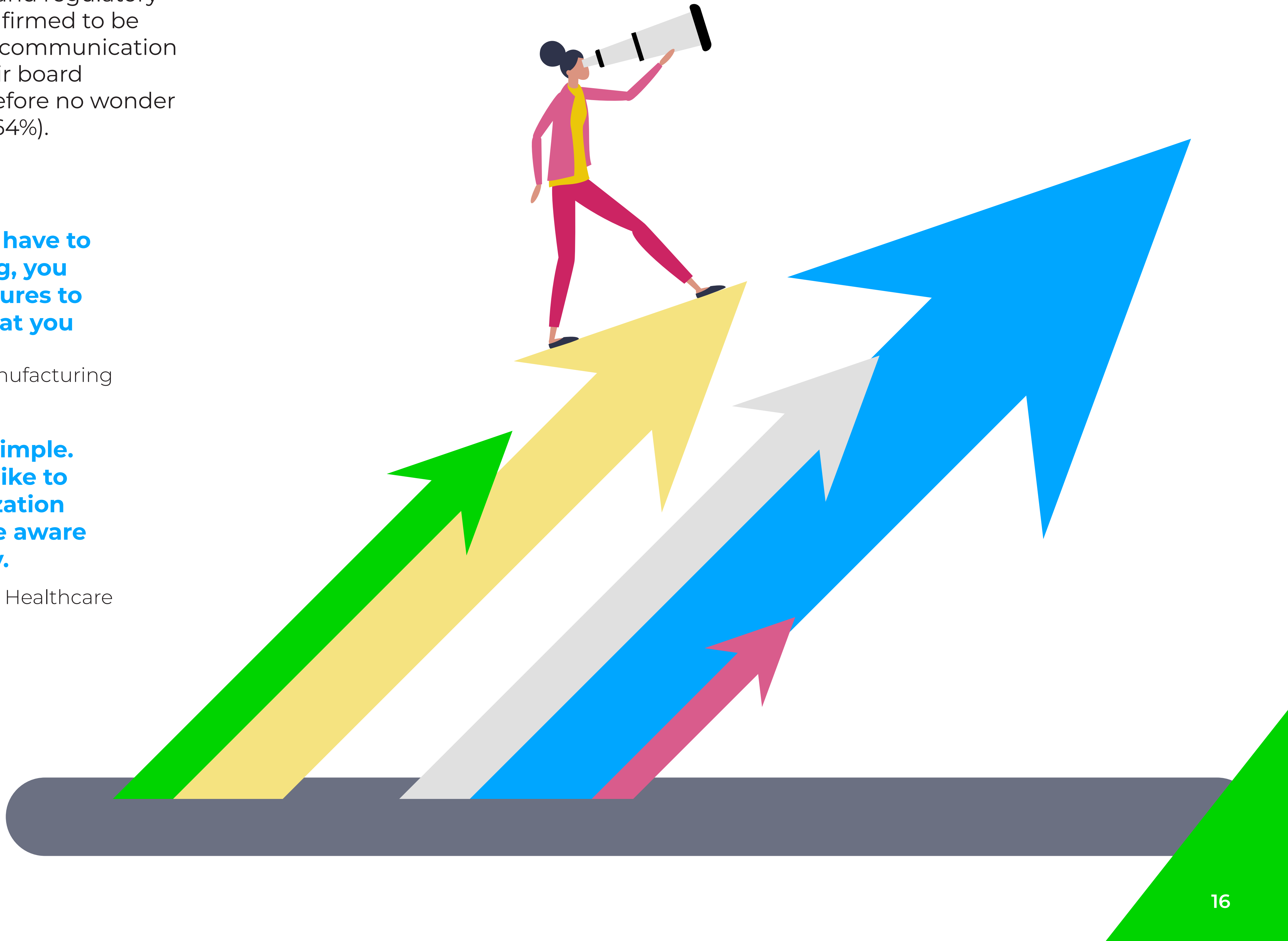
Section 2

The Boardroom Battle: Elevating the CISO to Strategic Leadership

As we've seen, CISOs are regularly reporting cybersecurity and regulatory compliance information, which are areas we've already confirmed to be vast causes of stress and pressure. If they are experiencing communication challenges and a lack of technical understanding from their board (alongside a lack of time to speak on these – 53%), it is therefore no wonder when the board is involved, the pressure felt is enhanced (64%).

> **"When you talk about board level engagement, you have to get your ducks in a row. If you know what you're doing, you can convince them for the right technology and measures to take around cybersecurity, but you have to deliver what you promised.**
>
> – UK, Manufacturing

> **"My slide deck for the board members is very, very simple. Two slides. You know, the good news, [...] and people like to know about or consider what is the risk to the organization and [...] tell them the bad thing. You know, let them be aware what we are working on [...] that's a much better story.**
>
> – US, Healthcare



Section 2

The Boardroom Battle: Elevating the CISO to Strategic Leadership

Navigating boardroom misalignment

The challenge for the CISO lies in being able to adequately and succinctly report on cybersecurity, as well as express their views and needs. Many struggle with apparent misalignment with their CIO and CEO, causing further tension, pressure, and challenge in the boardroom setting.

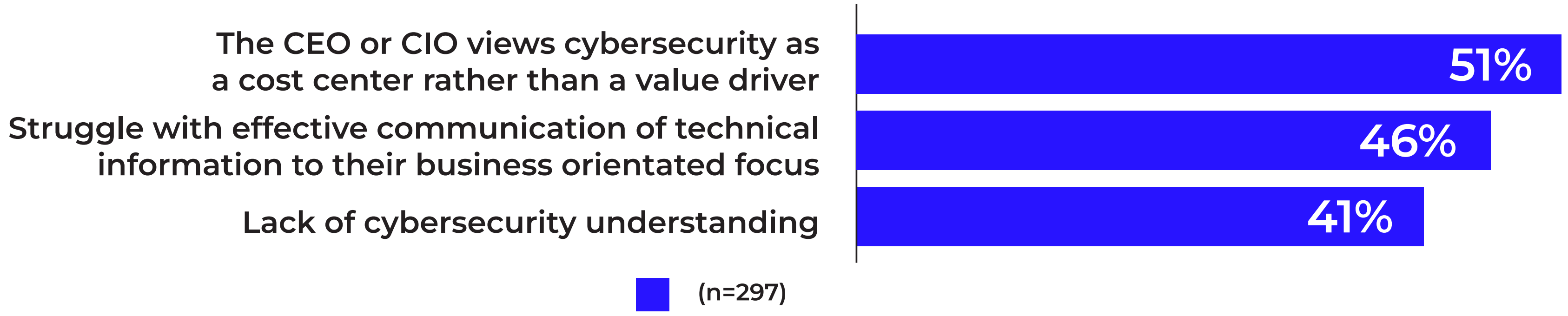
This misalignment stems from many different directions; however, key to this is the effectiveness of their communication. The difference in priorities of the CISO (technical-lens, security-focused) to the CEO and CIO (business-lens, outcome/value-oriented) come to the forefront in the top reported reason as to why views are misaligned. Cybersecurity initiatives are sometimes viewed as slowing down business processes or requiring significant investments which don't immediately contribute to the bottom line – leading to cybersecurity being seen as a 'cost center' rather than a 'value driver' (51%). This view can also lead to tensions in the boardroom, if there is not appreciation of the importance of cybersecurity beyond regulatory compliance, the CISOs recommendations may be seen as overly cautious or as an unnecessary expense.

CISOs are also cognizant of their communication challenges with the board, reported by 46% of CISOs. For instance, a CISO might emphasize technical vulnerabilities, while the CEO and board are more concerned with financial risks and business continuity. This disconnect can cause friction and make it difficult for CISOs to secure the funding or support they need to effectively protect the organization.

> **“Make sure you speak the business language, [...] understand the business, not just about technology [...] Because whenever you're talking to the board, ... they need to see that alignment, [...] so they will not be seen as a [cost] center. Make sure that everything you do aligns with the business.**
>
> – US, Financial Services

59% **feel their views are misaligned with those of their CIO/CEO**

Top 3 reasons why CISOs and CIO/CEO views are misaligned



The Boardroom Battle: Elevating the CISO to Strategic Leadership

To ease this pressure and succeed further in the boardroom, CISOs need to bridge the gap between their cybersecurity objectives and the broader business goals. Framing cybersecurity initiatives in terms of business value – highlighting how strong security practices can enable growth, protect brand reputation, and prevent financial losses. CISOs should also collaborate with CIOs to ensure security is integrated into IT strategies without stifling innovation. Communicating risks in financial terms and developing a more business-oriented approach will help CISOs remain visible and valuable at the most senior level within their organization. This will elevate their role within the organization, ensuring they reap the benefits for their organizations' security, as well as for their career.

> **“I think the CISO [...] really needs to understand the board very well [...] the board as a whole and each of the board members, because each [...] may have a different risk appetite, some will take more risk [...] Some are better in cyber, some are not in cyber. Some board members work in the regulated industry [...] a bit more [...] used to all the regulation. There are some board members that work with a nonprofit, which is not regulated.**
>
> – Singapore, Healthcare

> **“You ask them what they want to hear [...] what their level of information [...] and how important they think these things are. And then you fine tune your messages according [...] But [...] at the same time, you give them a very realistic view of where the organization is, where the risks are, and you always keep it linked to organizational strategy documents and organizational objectives.**
>
> – UK, Public Sector

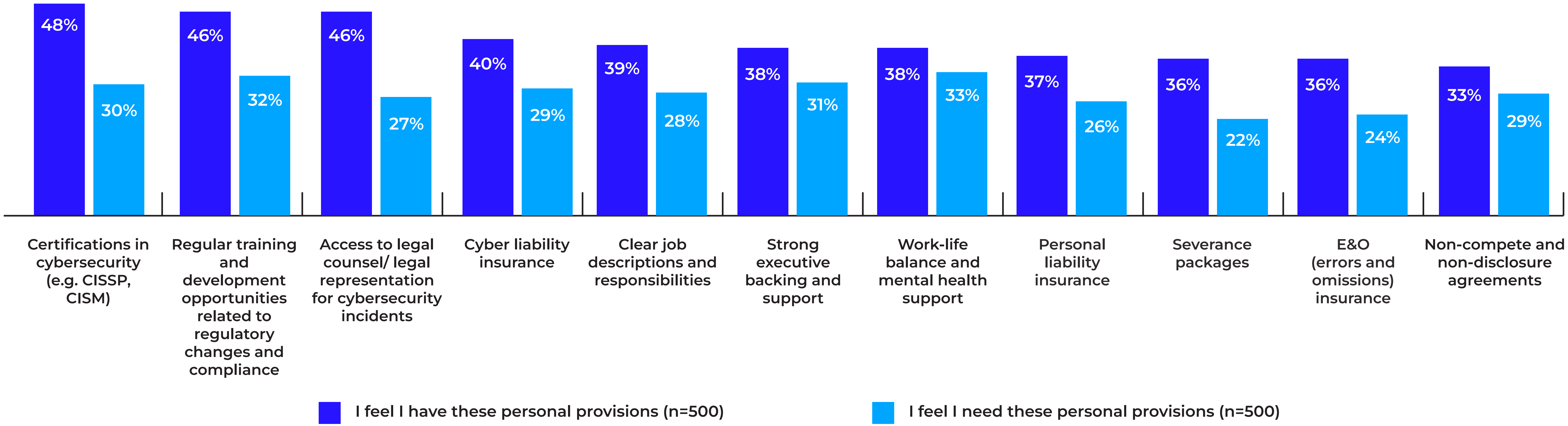
Beyond survival: How CISOs can Thrive Amid Regulatory and Leadership Challenges

Protecting the protector: what CISOs need to succeed

In the 2024 security landscape, CISOs are mindful they may need certain key provisions within their high-stakes role to ensure they remain protected. Ensuring protection is critical in a world where the CISO is at the forefront of responsibility for data breaches or compliance failures, and personal protection is therefore top of mind when considering a new CISO role.

> **“People often ask me what keeps me up at night and whether, you know, I worry about it. But where I am in my journey here with my organization, in the early days I felt a lot more stressed [...] where you are in your journey definitely plays a role in how stressful these new requirements [are] to you.**
>
> – US, Energy, Oil / Gas and Utilities

What CISOs feel they have in their role to ensure protection vs what they feel they need



Section 3

Beyond survival: How CISOs can Thrive Amid Regulatory and Leadership Challenges

The reality with CISO protection is most CISOs don't feel they have these provisions – under half of CISOs report they have certifications in cybersecurity (48%), access to legal counsel/ legal representation for cybersecurity incidents (46%), or regular training and development opportunities related to regulatory changes and compliance (46%). And even fewer report having the other personal provisions.

This is in contrast to almost all (99%) CISOs reporting they need at least one or more of these provisions, three being the average number selected. The most desired is for CISOs to have a greater work-life balance and mental health support, needed by a third (33%), which will be a critical change organizations need to recognize and provide to their CISOs to prevent burnout or CISOs leaving their role (as we explored on page 12). Almost a third (31%) also need strong executive backing and support to ensure their recommendations are given the weight they deserve in the decision-making process. It will also help secure the resources to implement and maintain the organization's robust cybersecurity.

The discrepancy between what CISOs want in their role and what they have creates a significant risk for CISOs and their organizations. Without proper protection, CISOs are at risk of becoming scapegoats for incidents occurring despite their best efforts, leading to high turnover rates and a reluctance to take on these roles in high-risk industries. 91% of CISOs agree the expanding responsibilities will lead to higher turnover in these positions in the future. The lack of sufficient resources and authority limits their ability to proactively address security issues, leaving organizations vulnerable to breaches and non-compliance penalties. For CISOs to thrive, organizations must recognize the need to align provisions with expectations and do better to provide the comprehensive personal protections CISOs need to manage cybersecurity effectively. Addressing these gaps is crucial for the well-being of CISOs and the organization's overall security posture and compliance readiness.

> **"Sometimes if we do not have the right support from management, we try to comply by doing the absolute minimum. And this is why I always said to my stakeholders, don't do the absolute minimum, but do what is the right thing for our organization, which means sometimes we need to even go higher than the regulation, because that's what is correct, what is right for us.**
>
> – Singapore, Healthcare

> **"And my boss is very big on work life balance. We know that's not always the case. I've been in other places where that's not even a remote consideration. And he's like, don't do that. You need to stop. Take a day, take a breather, take a vacation. Take vacation, please.**
>
> – US, Public Sector

> **"This spring, it was extremely stressful [...] I have to take that on, but I don't have to take on the emotional toil that it will take. I can't solve all these problems myself instead of trying to force myself to do it, which quite honestly, I think a lot of people in the field do. You know, you take on that responsibility and now you're like, I have to fix it [...] It took me a couple of weeks of fairly mild panic attacks to reach the conclusion that I can't and that he needs to [hire] another person [...] you got to stop working at a certain time of night.**
>
> – US, Public Sector

Section 3

Beyond survival: How CISOs can Thrive Amid Regulatory and Leadership Challenges

Is dividing the CISO role the answer to growing demands?

A debated solution to growing CISO pressures and demands is the potential to expand the CISO role into two separate responsibilities: one more focused on the technical aspects of the role and one more focused on the business success side.

This division acknowledges the dual nature of cybersecurity and the CISO role, requiring deep technical expertise and business acumen. The primary benefits of splitting the CISO role are the ability to better anticipate future security needs (40%) as well as having enhanced expertise and specialization (38%). The division allows each leader to dedicate themselves fully to their domain, without being stretched too thin and alleviates pressures and an overbearing workload. It would also reduce difficulties in communication with the board for CISOs who are more technical-leaning. This separation could enhance technical depth and strategic oversight for organizations, leading to more resilient security practices and a more integrated approach to risk management aligning with their business goals.

However, challenges would also be faced with this approach. Many (41%) feel it could end up increasing the workload and stress of the CISO, with a higher risk for burnout. This could come from ensuring compliance across multiple jurisdictions (40%) and difficulty balancing technical and strategic responsibilities due to confusion over role requirements (39%). Many also believe it could increase pressure on the role as the board and regulators would have higher expectations and place greater scrutiny (40%) if expanded. The risk of overlaps and gaps means organizations security efforts could be compromised, and there could be misalignment between the technical and business strategies, creating silos rather than bringing success to the role.

> **“Most of the people that I know in security have a very deep tech background. A lot of them speak only in acronyms. […] And I have to tell them […] people don’t understand what you’re saying.**
>
> – US, Public Sector

84%

agree the CISO role should be split into separate technical and business focused roles

42%

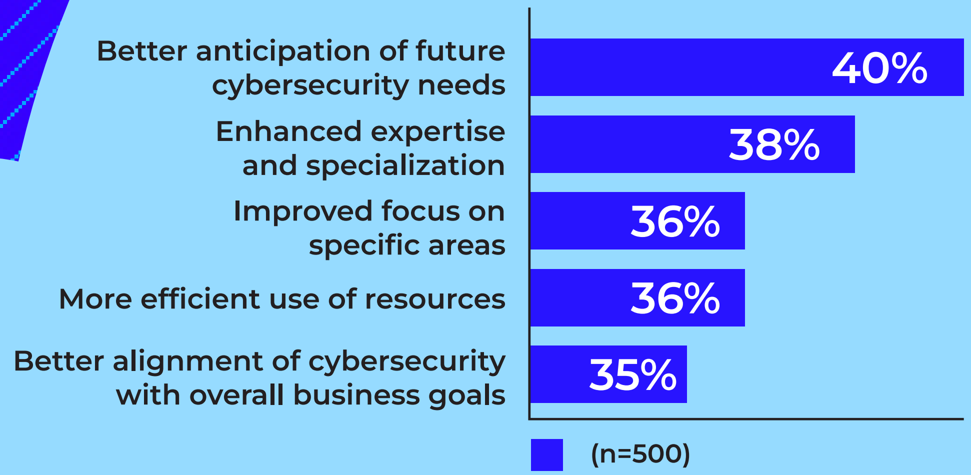
strongly agree expanding the responsibilities of the CISO role will lead to higher turnover in these positions

Section 3

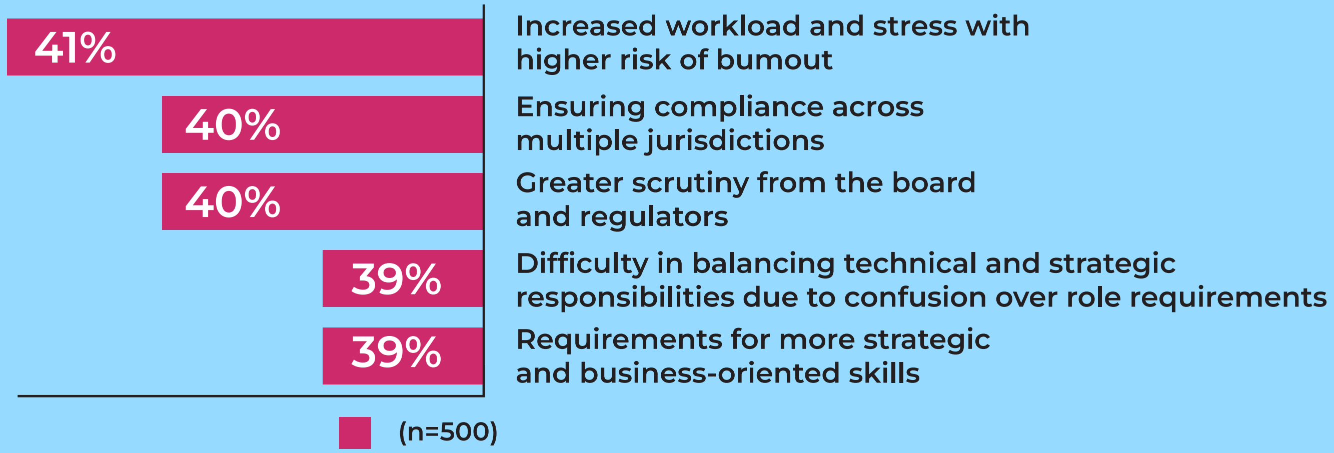
Beyond survival: How CISOs can Thrive Amid Regulatory and Leadership Challenges

Therefore, it is not a blanket solution solving CISOs problems overnight. It has the potential to elevate the role and alleviate many of the challenges, but the challenges will need to be addressed in the right way and with the right boundaries and clarity, to ensure it does not cause more problems.

Top 5 benefits to splitting the CISO role



Top 5 challenges to splitting the CISO role



> **“But you still need to have that one person that is a bit more holistic, being able to understand both the technical and the business work together.**
>
> Singapore, Healthcare

Recommendations

As the role of the CISO becomes increasingly complex and CISOs become increasingly time-poor, organizations must take proactive steps to ensure their security leaders remain engaged, supported, and able to focus on their core responsibilities. Regulatory compliance is the 'forgotten' requirement of the CISO role, existing in the shadows; however, it places a huge burden on the role, causing many to consider exiting the position.

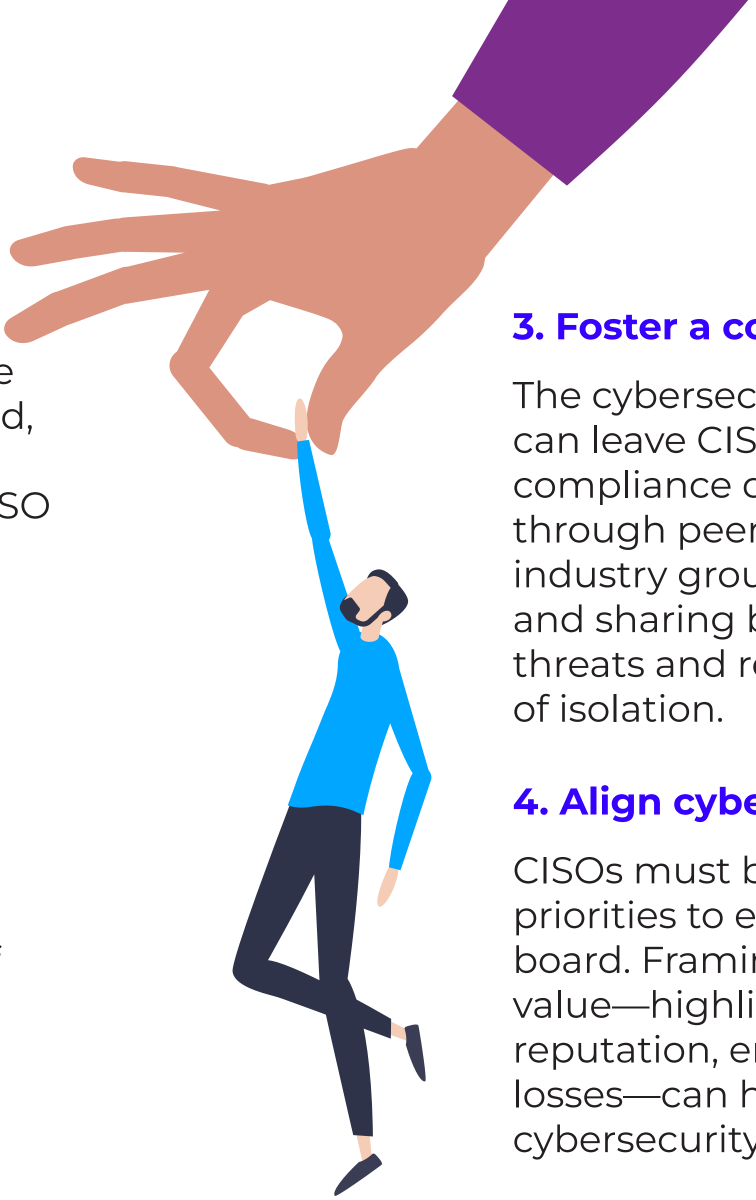
This report has helped highlight the forgotten burdens of the CISO, and here are the key recommendations for CISOs, their organizations, and the industry regulators:

1. Clear guidance and support from regulators

Regulatory bodies can do more to offer clearer, better-streamlined guidance to reduce the complexity and burden of compliance for CISOs. Including CISOs in discussions around new regulations and giving practical advance warnings will help them to stay proactive rather than reactive. This level of involvement would empower CISOs to manage compliance more effectively without it becoming overwhelming.

2. Empower CISOs with executive support and resources

Many CISOs feel their organization expects them to carry the entire burden of staying updated on regulatory changes. Organizations must share this responsibility by providing executive backing, additional staffing, or technological solutions to help reduce the CISO's workload. Stronger executive support ensures CISOs have the resources to focus on both compliance and core security tasks, preventing burnout and increasing overall effectiveness.



3. Foster a collaborative cybersecurity community

The cybersecurity industry is known for its secrecy, which can leave CISOs feeling isolated as they attempt to navigate compliance demands. Encouraging collaboration among CISOs through peer discussions, knowledge-sharing networks, and industry groups can offer valuable support. By learning from peers and sharing best practices, CISOs can stay informed on evolving threats and regulations, ultimately reducing stress and the feeling of isolation.

4. Align cybersecurity initiatives with business goals

CISOs must bridge the gap between technical and business priorities to ensure they gain support from their organization's board. Framing cybersecurity initiatives in terms of business value—highlighting how strong security protects brand reputation, ensures business continuity, and prevents financial losses—can help elevate the knowledge and importance of cybersecurity within the organization.

5. Clarify role responsibilities and expectations

The shift towards a separated CISO role (business and technical responsibilities) could redefine the career path for future CISOs. Allowing security professionals to choose between technical specialization and business leadership earlier in their careers could foster deeper expertise in both areas. However, it also risks limiting the pool of security leaders who possess the hybrid skills needed to bridge technical cybersecurity with organizational strategy. For this to succeed, careful planning is required to ensure clear roles, communication, and shared accountability across both positions. This could ensure the pressure eases for many CISOs amid a workload and regulatory storm, and they remain secure and committed to their role for many years to come.

Trellix

Trellix is a global company redefining the future of cybersecurity and soulful work. The company's comprehensive, open and native cybersecurity platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through artificial intelligence, automation, and analytics to empower over 50,000 business and government customers with responsibly architected security.

More at www.trellix.com

Follow Trellix on LinkedIn and X.

VansonBourne

Vanson Bourne is an independent specialist in market research for the technology sector. Our reputation for robust and credible research-based analysis is founded upon rigorous research principles and our ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and major markets.

More at www.vansonbourne.com