Cybersecurity: how do you rise above the waves of a perfect storm?

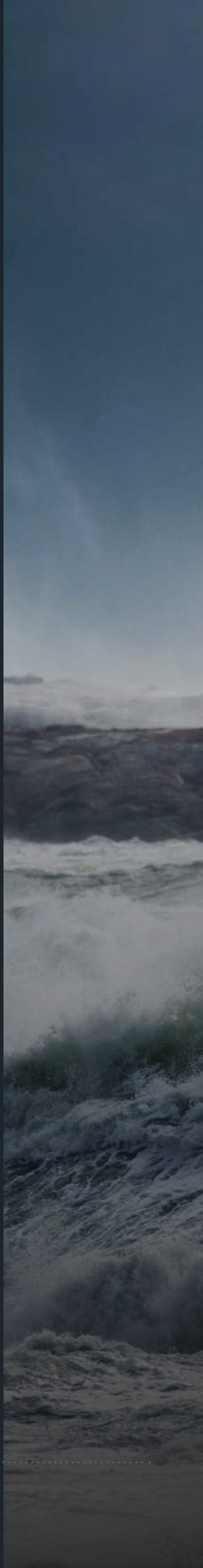
EY Global Information Security Survey 2021

The better the question.
The better the answer.
The better the world works.

Building a better working world

Welcome

Contents



Introduction

The EY Global Information Security Survey 2021 finds CISOs and security leaders battling against a new wave of threats unleashed by COVID-19.

The *EY Global Information Security Survey 2021* (GISS) illustrates the devastating and disproportionate impact that the crisis has had on a function that is striving to position itself as an enabler of growth and a strategic partner to the business.

Through a global survey of more than 1,000 senior cybersecurity leaders, we find CISOs grappling with inadequate budgets, struggling with regulatory fragmentation, and failing to find common ground with the functions that need them the most.

Indeed, the upheaval of the global pandemic has created a perfect storm of conditions in which threat agents can act. Since the 2020 GISS report, there has been a significant rise in the number of disruptive and sophisticated attacks, many of which could have been avoided had companies embedded security by design throughout the business.

The CISO's relationship with the business is also under more stress than before, and the fallout is greater exposure to cyber risk. On top of that, budget restrictions mean CISOs are struggling to bridge the gap between need and funding.

The situation is likely to get worse before it gets better. Organizations want to invest in technology and innovation for the post-COVID era, and they need to ensure resilience for the next major disruption, but many have yet to address the deferred risks and potential vulnerabilities that were introduced during their transformation efforts at the height of the pandemic.

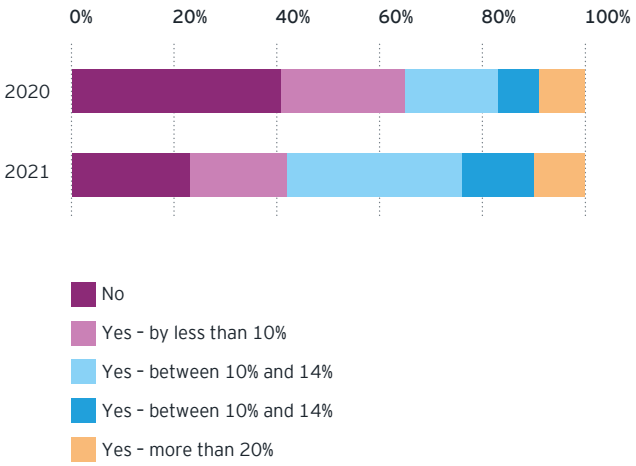
CISOs are at a crossroads. To contend with the complex and draining issues they face, they must act fast. Our report outlines what cybersecurity leaders need to know now about their current operating environment and what they need to do to transform it.

1 CISO at the crossroads

A time of stress, change and opportunity.

Figure 1: Respondents have seen a clear rise in attacks since 2020

Have you seen an increase in the number of disruptive attacks over the last 12 months?



Over the last year, every business has had to adapt to disruption in one form or another. Within timeframes that would have been thought impossible just a short time ago, progressive organizations rolled out new customer-facing technology and cloud-based tools that supported remote working and kept the channel to market open.

But the speed of change came with a heavy price. Many businesses did not involve cybersecurity in the decision-making process, whether through oversight or an urgency to move as quickly as possible. As a result, new vulnerabilities entered an already fast-moving environment and continue to threaten the business today.

Rapid transformation brings new risks

At the time of writing, CISOs and their teams may not have yet completed a full assessment of the long-term impact that their company's new technology will have on their defenses. In the meantime, their colleagues continue to use the technology regardless.

"The urgency of the crisis meant that security was overlooked even while organizations were opening up systems that had never been open before," reflects Richard Watson, EY Asia-Pacific Cybersecurity Risk Consulting Leader. "Not all organizations acknowledge they now need to go back and address those issues."

The risks of moving on without addressing the issues are, however, very real and increasingly urgent. More than three in four (77%) respondents to this year's GISS warn that they have seen an increase in the number of disruptive attacks, such as ransomware, over the last 12 months. By contrast, just 59% saw an increase in the prior 12 months (see figure 1).

> "I focus on understanding the implications of existing and unknown threats, and then add speed, security, and privacy by design into the product as it's built.
>
> **Roland Cloutier**
> Global CSO, TikTok

43% say they have never been as concerned as they are now about their ability to manage the cyber threat.

Yet CISOs are struggling to make themselves heard. Most respondents (56%) admit that cybersecurity teams are not consulted, or are consulted too late, when leadership makes urgent strategic decisions. While some maintain that this happens "not very often," it only needs to happen once for a flaw in the defenses to be exploited by threat actors (see figure 2).

The result is anxiety about what the future holds. "We strive for security as an enabler," says Richard Watson. "But there are still organizations that throw projects to security just before they go live."

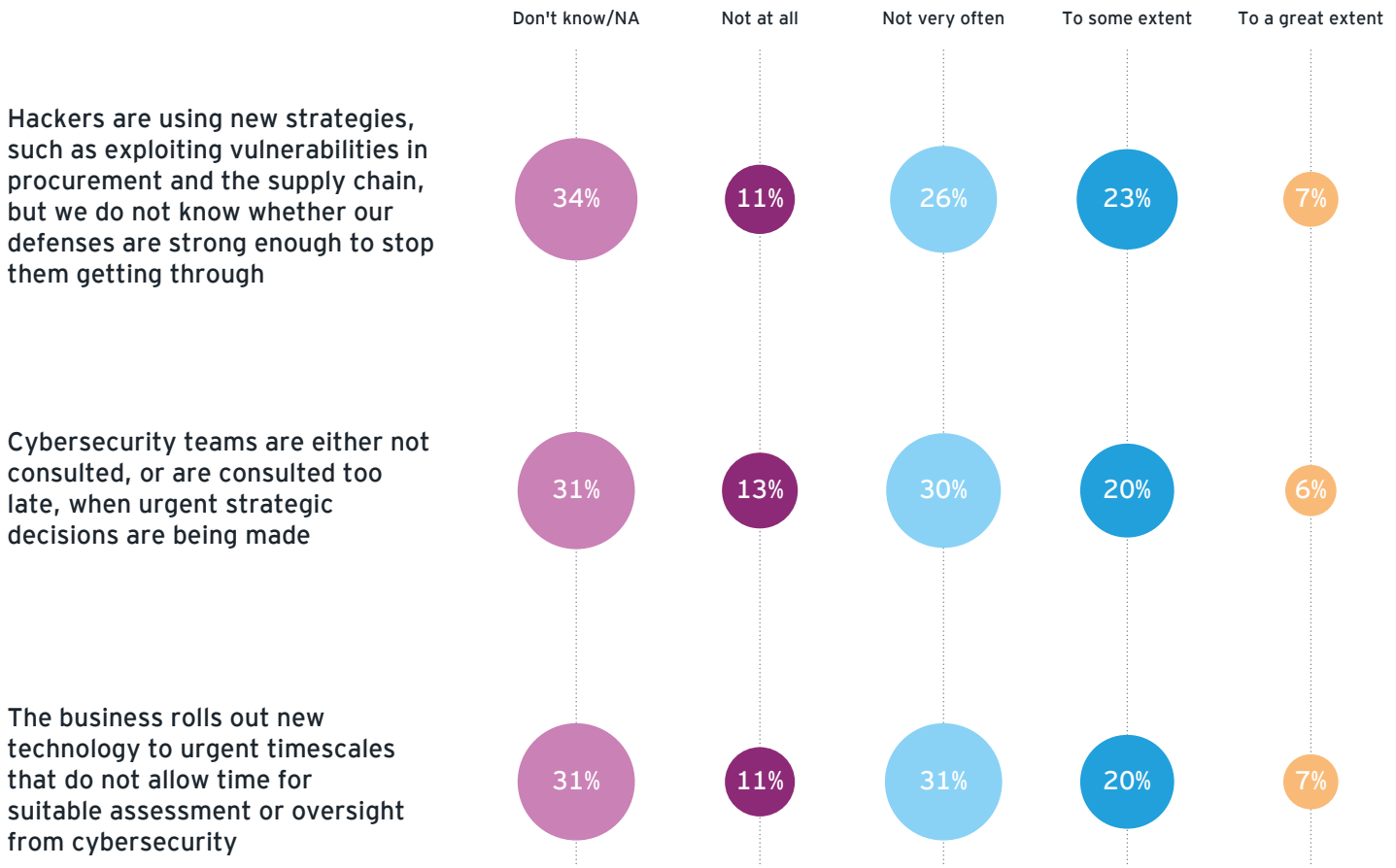
At worst, CISOs find their warnings are ignored. In this year's GISS, 43% say they have never been as concerned as they are now about their ability to manage the cyber threat. But it does not have to be this way.

TikTok – Security by design, at speed

Roland Cloutier, Global Chief Security Officer (CSO) at short-form video and entertainment platform TikTok, is deeply involved in strategic decision-making on an iterative, week-by-week basis. "It may range from a strategy for user growth to a new type of monetization or music product," he says. "All involve the construction and distribution of new technology. I focus on understanding the implications of existing and unknown threats, and then add speed, security, and privacy by design into the product as it's built. Then I prepare the organization for the new information coming through. How do we do that at both the speed of the internet and the speed of culture? That's what makes this job so much fun."

Figure 2: Cybersecurity teams are excluded from decision-making in businesses

To what extent do the following take place in your business?



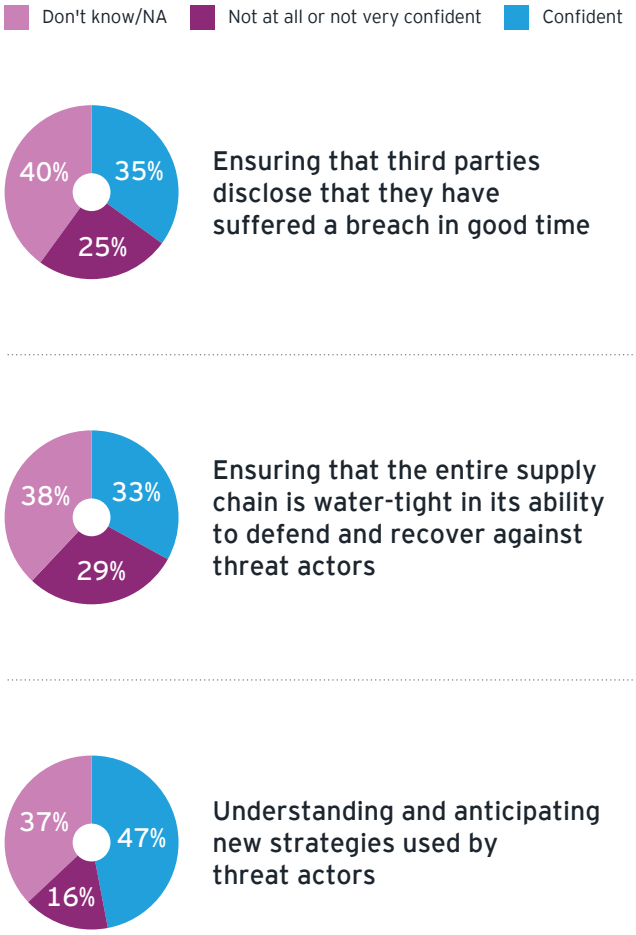
Less than half

47%

say they understand and can anticipate the strategies attackers use.

Figure 3: CISOs are lacking in confidence when faced with threat actors

How confident are you in your team's abilities across the following areas



Threat actors have hit a new level of maturity

Over the last year, threat actors have increasingly adopted new strategies, whether by targeting businesses with phishing campaigns containing malicious software that is forwarded by employees, or by embedding backdoor code that enables them to exploit commercial software after it has been procured by customers.

"The reality is there are more threats manifesting today than we've ever seen," says EY Americas Cybersecurity Leader Dave Burg. "It has been fueled by the ransomware business model, which is proving to be very effective."

The stakes could not be higher. The hackers who shut down the US Colonial Pipeline in May 2021 used ransomware-as-a-service that others can attain via the dark web, posing risks to critical organizations throughout the economy and society at large. At the same time, the individuals who infiltrated SolarWinds over several months in 2020 did so via a sophisticated supply chain attack that was largely unfamiliar to security teams.

Attackers are targeting a growing surface area and their tactics are increasingly unpredictable. Just one in three respondents is confident in their ability to make the supply chain suitably robust or water-tight (see figure 3), highlighting the importance of working closely with colleagues in procurement and operations. Less than half (47%) say they understand and can anticipate the strategies attackers use, an issue that has been illustrated by incidents in which threat actors infiltrate software that is later sold on to customers.

It is not as though the need for rapid transformation has passed. At the time of writing, significant progress has been made in containing COVID-19, but the crisis will pass through several stages before businesses return to "normal."

68% of CEOs are planning a major technology investment in the next 12 months.

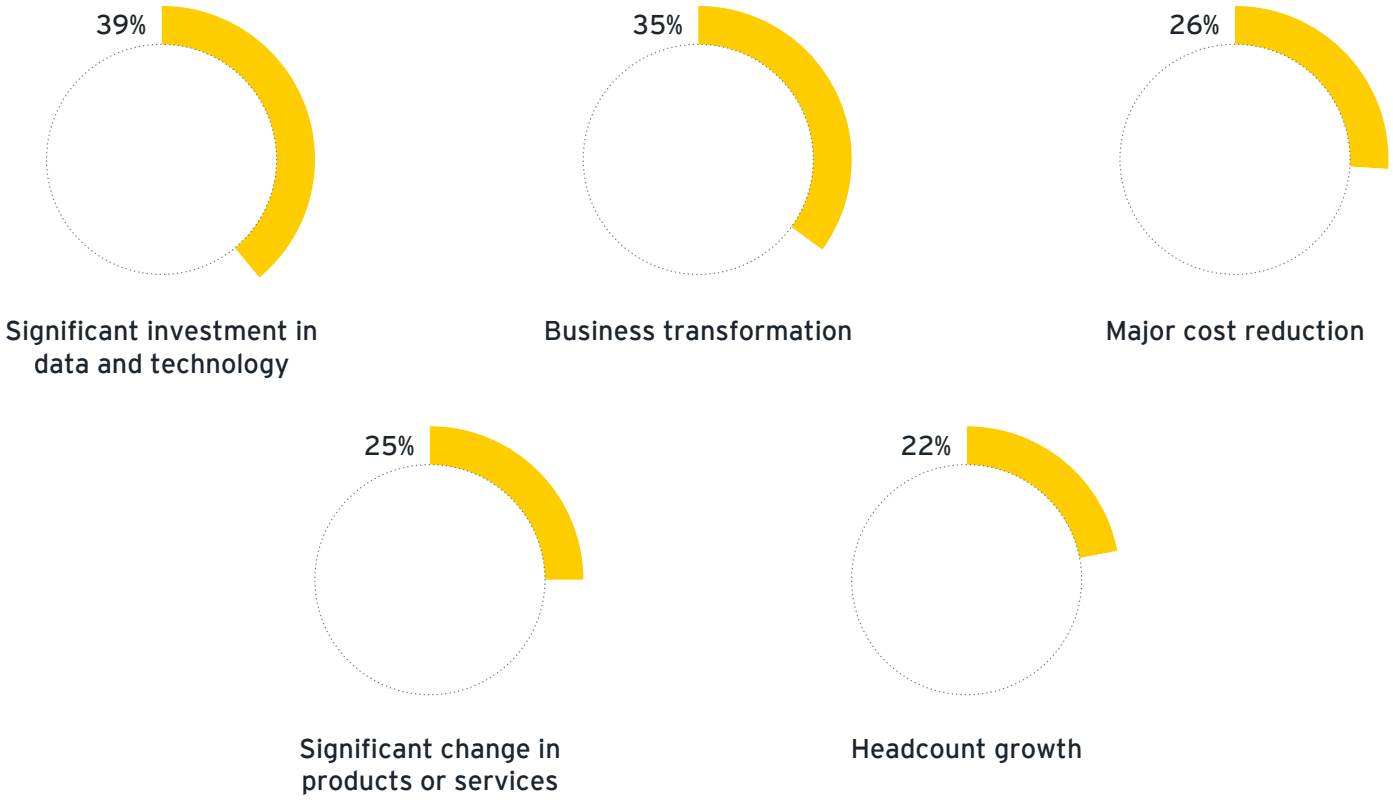
Employers are, for example, looking to support hybrid working models while unlocking growth in a recovering economy. A recent EY study, *Work Reimagined 2021,* found that 54% of respondents would consider resignation if their employers refused them the flexibility they were looking for. CISOs should also be aware that half of employees (48%) want investment in new home-office technology, which opens the possibility for yet more exposure if businesses cannot address security by design.

All eyes are on the CISO

CISOs face a critical moment. If they can support digital transformation from the planning stage – at a time when 68% of CEOs are planning a major data and technology investment in the next 12 months, according to the EY *CEO Imperative Study 2021* – they will truly become a strategic enabler of growth. If they can't play a more active role in transformation, the security threats will accelerate and their standing in the boardroom will decline.

Figure 4: Businesses' top 5 strategic priorities suggest an ongoing focus on transformation

Which of the following actions do you anticipate your organization will take in the next 12 months?



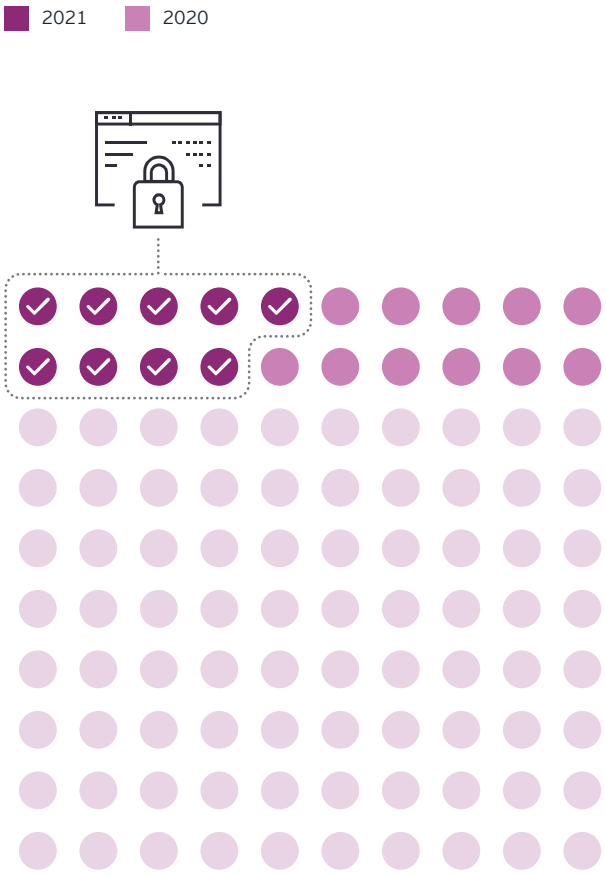
More than half

55%

of respondents say cybersecurity is coming under more scrutiny today than at any other point in their careers.

Figure 5: The erosion of trust

Just 9% of boards are extremely confident in their organization's cybersecurity risk and mitigation measures - a clear decline from last year



The senior leadership team is already concerned about the security function's ability to protect the organization. More than half (55%) of respondents say cybersecurity is coming under more scrutiny today than at any other point in their careers. Four in 10 (39%) organizations put cybersecurity on their board agendas quarterly, up from 29% in 2020.

And yet, in the EY *Global Board Risk Study 2021*, just 9% of boards declared themselves extremely confident that the cybersecurity risks and mitigation measures presented to them can protect the organization from major cyber-attacks – down from 20% last year.

An opportunity in crisis

The CISOs that can mitigate risk, while enabling their businesses' growth and technology ambitions, have a bright future. Most recognize this: 57% believe the crisis provides an opportunity for cybersecurity to raise its profile.

Dave Burg urges CISOs to capitalize on their increased visibility. "I know of many security officers who were viewed as superstars, and we want those superstars to be brought to the front of innovation," he says.

So, are CISOs ready to seize the opportunity of a new growth-enabling role? Can they embed resilience ahead of the next major business disruption? The answer is yes – but only if they can first address three critical and interrelated challenges that are standing in their way:

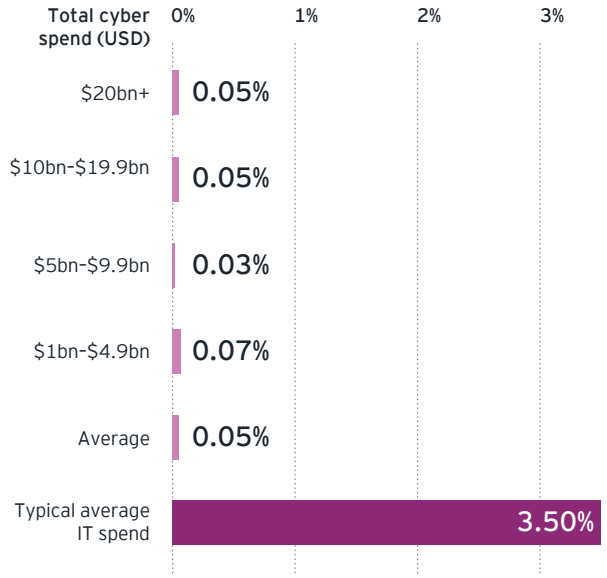
1. The cybersecurity organization is severely underfunded – at a time when it needs funding and flexible support more than ever before.
2. Regulatory fragmentation is a growing headache, creating additional work and new resourcing problems.
3. Cybersecurity's relationships with other functions are deteriorating – exactly when stronger connections are needed most.

2 Three challenges holding the CISO back

The perfect storm for cybersecurity.

Figure 6: Spending on IT and cybersecurity, with breakdown of company by size for cyber spend. Chart assumes IT spend is between 2 and 5%, in line with industry reports

What is your annual spend on cybersecurity, as a proportion of revenue?



1. Today's cybersecurity organization is severely underfunded

Despite the growing threat of cyber-attack, the cybersecurity budget is low relative to overall IT spend. The survey data also suggests that budget allocation processes are largely inflexible, despite the need for agility in response to pandemic-era volatility and the prospect of future disruption.

"Current funding models are simply inadequate for what is, in effect, an existential risk," says Kris Lovejoy, EY Global Consulting Cybersecurity Leader. "It is also symptomatic of the poor understanding that many businesses have of cyber issues and their failure to implement a culture of security by design."

Budgets are out of sync with need

In the creation of this report, EY carried out qualitative interviews with three heads of cybersecurity and surveyed 1,010 senior cybersecurity professionals. The survey respondents had average revenues of approximately $11b last year, while spending an average of just $5.28m, or 0.05% of the total, on cybersecurity per annum.

The picture varies from one sector to another. At one extreme, in the highly regulated financial services and technology, media and entertainment, and telecommunications (TMT) sectors, the average GISS respondent spent an average of $9.43m and $9.62m respectively on cybersecurity last year. At the other end of the spectrum, energy companies spent just $2.17m, on average. We also see differences by company size, with the smallest businesses spending a greater proportion.

One issue relates to how the budget is planned and allocated. Some six in 10 (61%) respondents say their security budget forms part of a larger corporate expense, such as IT, with 19% reporting that this is fixed and defined cyclically. More than a third (37%) say cybersecurity costs are shared across the organization, but only 15% do so dynamically, depending on how resources are used.

In other words, very few organizations define their security budgets as a variable and contingent cost of doing business. In effect, CISOs might struggle to scale their functions' efforts in the context of specific and fast-evolving business initiatives.

61% of respondents say their security budget forms part of a larger corporate expense, such as IT.

36% of respondents agree that it is only a matter of time before they suffer a breach that could have been avoided through investment.

Cost-cutting creates new weaknesses

CISOs are acutely aware of the vulnerabilities their organizations face because of inflexible and insufficient budgets.

Four in 10 respondents (39%) flag that cybersecurity expenses are not factored adequately into the cost of strategic investments, such as an IT supply chain transformation. More than a third (36%) say it is only a matter of time until they suffer a major breach that could have been avoided had there been more appropriate investment in cybersecurity defenses.

Given how organizations have rushed to transform their operations in the face of disruption, we could expect the problem to intensify as businesses invest to support growth. Four in 10 respondents (39%) warn their organization's budget is below what is required to manage the new challenges that have arisen in the last 12 months.

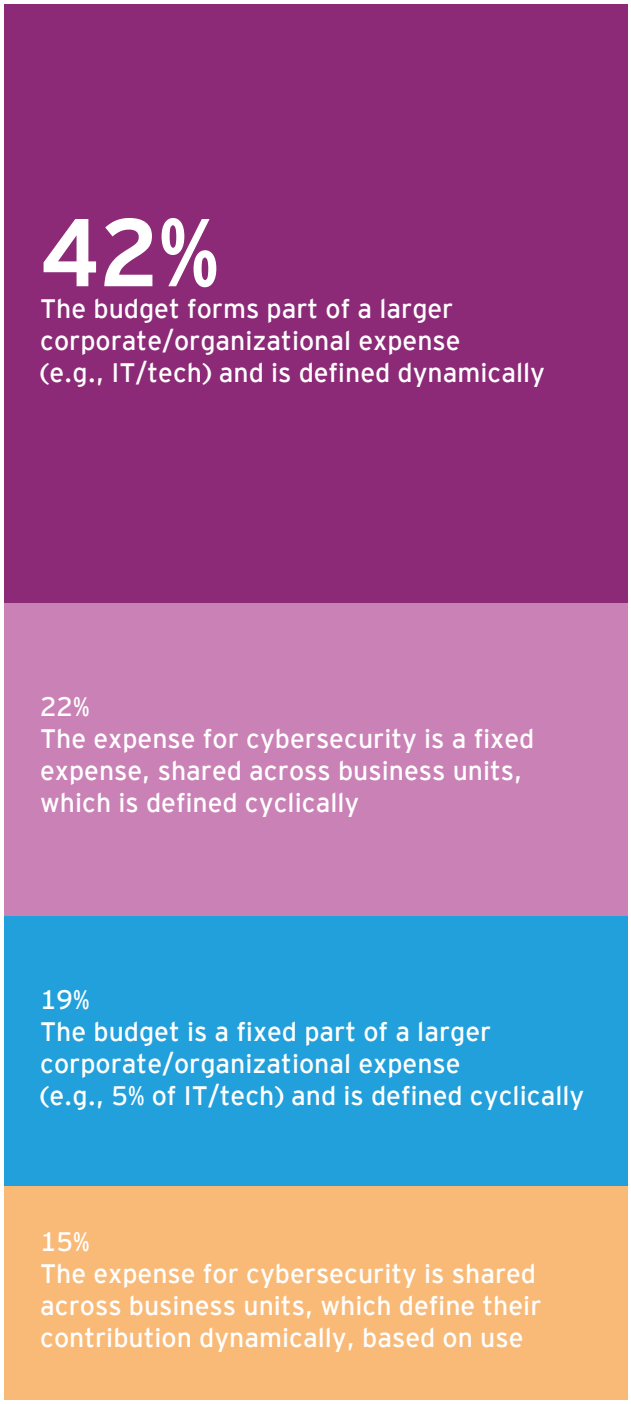
An inevitable outcome of budget restrictions is CISOs making difficult decisions and winding down some of the strategic activities that had been put into motion before the crisis began. More than half (56%) of those businesses with insufficient budgets tell us that they have had to realign their cybersecurity requirements. And 44% say they have been forced to cut costs by focusing on their legacy architecture and systems.

A minority of organizations do, however, take a more strategic approach to cybersecurity funding. At Assicurazioni Generali, one of the world's leading insurers, Group Chief Security Officer Remo Marini says the business takes a risk-based approach to cybersecurity funding. "We build a direct link between investments in security, business value and risk reduction," he says. "Our budget reflects sophisticated planning activity that starts from the definition of our strategy, typically with a horizon of three years, and collects inputs from all relevant internal and external stakeholders."

> "We build a direct link between investments in security, business value and risk reduction.
>
> **Remo Marini**
> Group Chief Security Officer at Assicurazioni Generali

Figure 7: CISOs are largely working with inflexible budgets

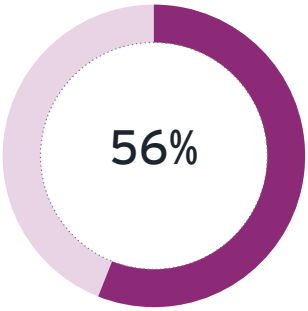
How do you define your cybersecurity budget?



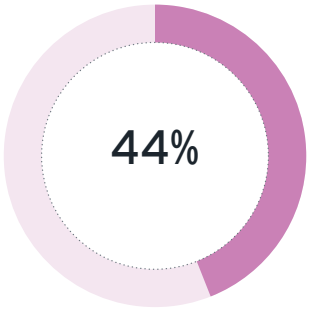
56% of respondents with insufficient budgets have had to realign their cybersecurity requirements.

Figure 8: CISOs with insufficient budgets have been forced to scale back essential security work

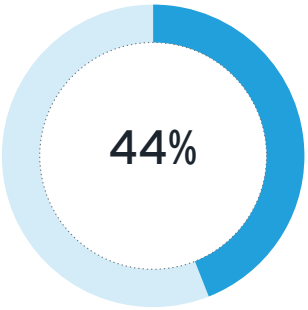
Which actions have you taken to manage insufficient budgets?



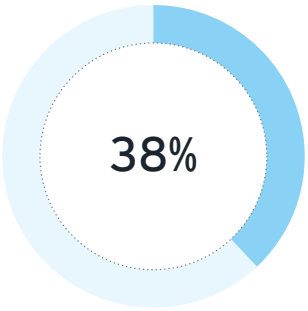
Realigned cybersecurity requirements to better meet changing business needs



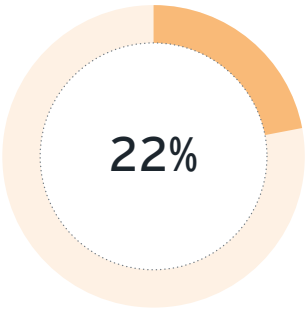
Reviewed our legacy architecture for cost-reduction opportunities



Increased reliance on third-party providers



Scaled back innovation activity to focus on core, non-strategic tasks



Reduced our headcount

2. Regulatory fragmentation is a growing headache for CISOs

The global compliance environment is becoming more complex, with regimes operating at regional and national levels worldwide. Organizations in certain sectors – notably financial services – must also manage industry-specific regulation.

Mike Maddison, EY EMEIA Cybersecurity Consulting Leader, believes regulation is a growing concern. "If you are an international organization, the way that you manage these overlapping – but sometimes conflicting – regulations is challenging, particularly as information becomes ubiquitous and travels internationally."

A drain on precious time and resources

Regulation is claiming time that CISOs do not have to give. One in two (49%) warns that ensuring compliance can be the most stressful part of their job. Six in 10 (57%) predict that regulation will become more heterogenous, time-consuming and – some might say – chaotic in the years to come. As CISOs struggle to secure the resources they need, an impact on their stress levels is understandable.

"The regulatory agenda is becoming more packed every day as local and international regulators intensify their focus," confirms Assicurazioni Generali's Marini. "We are seeing a proliferation of regulations posing difficulties, particularly for international groups. A standardized and common framework would be more efficient."

An additional concern, at least in the US, is that the Department of Justice has raised ransomware attacks to the same priority level as terrorism and is coordinating investigations through a task force in Washington. At the time of writing, it was unclear what resources would be made available to private sector organizations that fall victim to attacks.

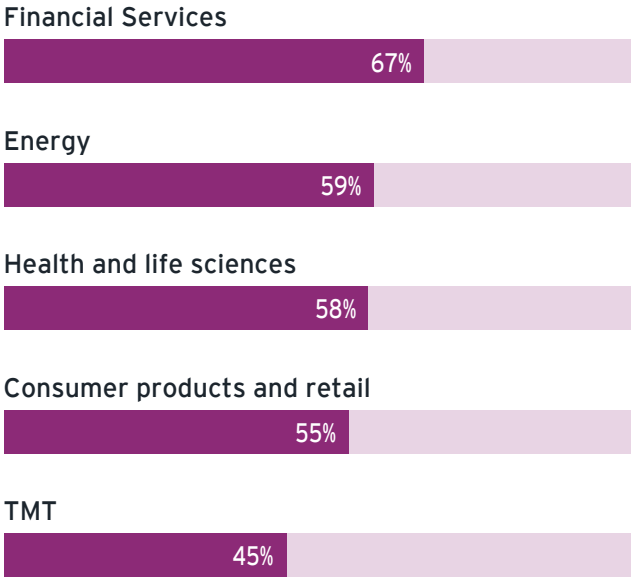
Compliance moves from budget friend to foe...

Kris Lovejoy believes there has been a fundamental shift in how CISOs regard compliance, which has worrying implications for their relationship with the regulator. "CISOs were still positive last year about the role of compliance," she says. "This year, they recognize that compliance has shifted. It has become so fragmented and so complex that it's now a distraction. Compliance is no longer the CISO's friend in that it no longer justifies budgets in the way that it did. Compliance has become their foe."

To Lovejoy's point, CISOs are less confident this year that regulation is supportive of improved cybersecurity standards in organizations. EY research also finds that compliance does not even provide the means to secure additional funding that it once

Figure 9: CISOs in financial services are most concerned about complex new regulation

Do you agree that regulation will become more fragmented and difficult to manage in the years to come?



49% say ensuring compliance can be the most stressful part of their job

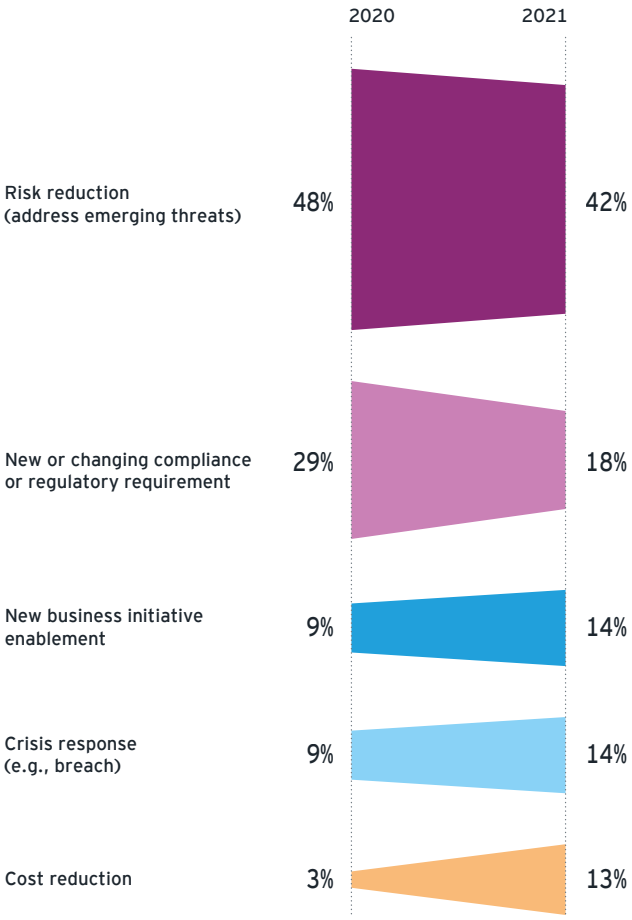
Just

35%

of respondents believe compliance drives the right behaviors.

Figure 10: Regulation scores relatively low as a budget justifier

What is the primary driver for new or increased cybersecurity spending in your business?



"In the dynamic environment we saw during COVID, there was such a need for speed and organizations questioned whether cybersecurity teams had the right skills.

Mike Maddison
EY EMEIA Cybersecurity Consulting Leader

did, which could – in the light of budget constraints – previously have been considered a silver lining.

In last year's GISS, 46% of respondents thought that compliance drives the right focus and behaviors within their business. In 2021, this figure has fallen to 35%. At the same time, less than one in five (18%) respondents describe regulation as an effective way for them to make the case to their boards for additional budget, down from 29% in 2020 (see figure 10).

While senior executives may have become more responsive to business cases that link increased cybersecurity spending with transformation, they appear less moved than they were by CISOs' warnings about the growing compliance burden.

Not all cybersecurity leaders are pessimistic about regulation. Roland Cloutier at TikTok says regulation is consuming "at least 50 or 60%" of his time, but he remains positive overall. "Our strategic security programs are based on the next generation requirement around regulatory considerations and consumer protection. That's a great thing. We're enabling our products to be ready for the future. It's helping us create the leading industry concept of how to operate as a business dedicated to protecting the safety, security, and privacy of our users worldwide."

3. Cybersecurity's relationships with other leaders are deteriorating

To manage the cyber risk attached to strategic transformation, CISOs need to provide counsel at the earliest stages of investment decision-making. But the relationships between cybersecurity and other functions in the business, which are essential for such consultations to take place, lack positivity and strength.

Business leaders exclude the CISO

Weak relationships have long been a concern for CISOs, but this year's GISS suggests the problem is becoming more pronounced. According to the survey, business leaders are cutting cybersecurity out of vital conversations. Around six in 10 (58%) say their organizations sometimes implement new technology with timescales that do not allow for suitable cybersecurity assessment or oversight.

Dan Higgins, EY Global Consulting Technology Leader, calls it concerning that CISOs are involved late in the process of deploying new technology and data solutions. "It is imperative that CISOs establish their seat at the table at the strategy and solution architecting phases of digital transformation, when these risks can be proactively addressed and avoided," he says.

It's a trend that may be driven from the top of the business. According to the EY *CEO Imperative Study 2021*, CEOs no longer describe cybersecurity as their top concern, as they did in 2020.

41% of respondents describe their relationship with the marketing function as negative.

Their focus in 2021 has turned instead to challenges around adopting new technology.

The pandemic is making matters worse: 81% of organizations sidestepped cyber processes and did not consult cybersecurity teams at the planning stage of new business initiatives.

"In the dynamic environment we saw during COVID, there was such a need for speed and organizations questioned whether cybersecurity teams had the right skills," says Mike Maddison. "Was the culture right: were they seen as blockers or as the people who offered effective solutions? Where the answers to those questions were in doubt, other parts of the organization went it alone without the cyber team."

Relationships are weakest where they need to be strong

The problem is most acute among functions that will be rolling out and scaling new cloud-based technology in the months ahead, and which therefore run a strong risk of being compromised by hackers deploying ransomware.

In this year's study, 41% of respondents describe their relationship with the marketing function as negative, up from 36% who said the same a year ago. At the same time, 28% say their relationship with business owners is poor, compared to 23% a year ago.

The result is that, while more than a third of respondents in 2020 (36%) were confident that cybersecurity teams were being consulted at the planning stage of new business initiatives, this figure has fallen to 19% in 2021.

"Cybersecurity's relationship with business lines, product development and marketing are negative – whereas their interactions with risk, legal and IT are positive," says Kris Lovejoy. "Essentially, the relationships become more positive the further away from the planning cycle you sit, which is a problem. Where cyber most needs to be involved, to support growth, it is not being invited to the party."

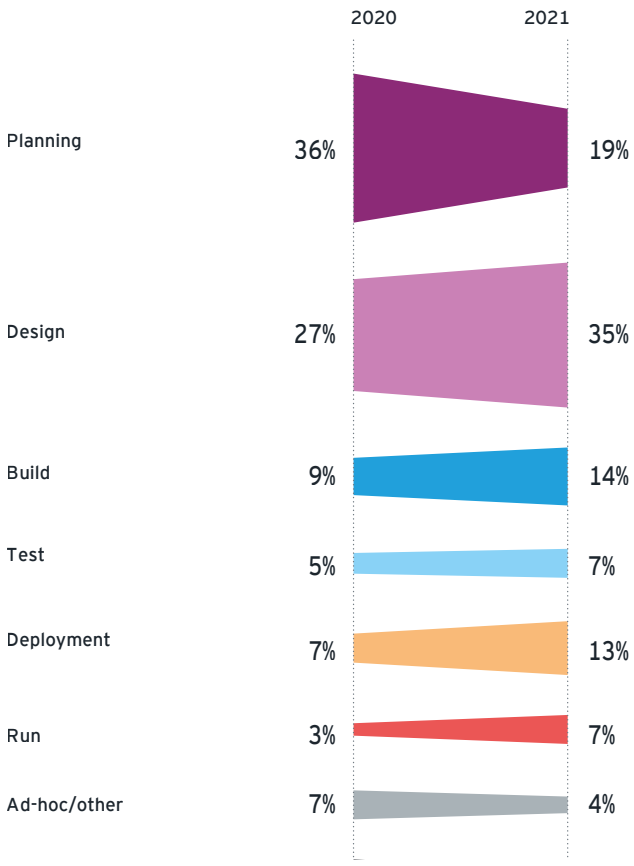
Communication breakdown

Poor communication between teams is a barrier to progress. CISOs tell us that they struggle to get their people to articulate the need for cyber consultation in commercial terms. Moreover, the business may recognize cybersecurity's traditional strengths, such as controlling risk, but it does not always perceive cybersecurity as a strategic partner.

"Across industry, I have seen a positive mindset shift with boards recognizing that cybersecurity is a risk," says Darren Kane, Chief Security Officer at NBN Co in Australia, who took part in a qualitative interview for this report but not in the survey. "But CISOs still have more work to do in breaking down the communication barriers by talking in less technical language for boards to better understand potential business risks."

Figure 11: Cybersecurity teams are less likely to be brought into the earliest stages of development

At what stage is cybersecurity brought into a new business initiative?



Less than half of respondents (44%) are confident in their team's ability to talk the same language as peers, and just 26% believe that senior leaders would use such terms to describe the function. Just one in four (25%) thinks senior business leaders would describe cybersecurity as commercially minded.

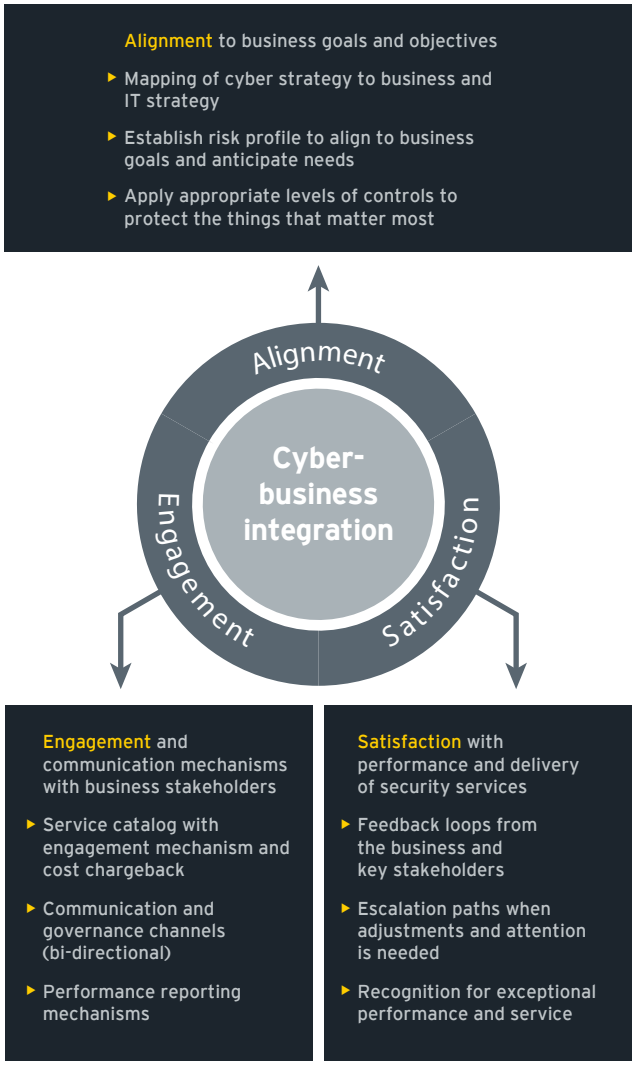
Respondents concede that the rest of the organization is much more likely to describe cybersecurity as protecting the business and responding quickly to crises. While these are admirable qualities in themselves, they need to be balanced with an ability to communicate, persuade, and build trust.

3 Conclusion and next steps

The CISO as enabler of value.

> CISOs are central to an organization's efforts to transform and deliver long-term value.
>
> **Errol Gardner**
> EY Global Vice Chair-Consulting

Figure 12: Three critical elements for cyber-business integration



How should CISOs respond to the core challenges outlined in this year's GISS? That they should play a more strategic and commercial role in their organizations – reinventing their teams as enablers of transformation – is not in doubt.

"CISOs are central to an organization's efforts to transform and deliver long-term value," says Errol Gardner, EY Global Vice-Chair – Consulting. Discussing how CISOs should position themselves as enablers of transformation, Gardner adds: "While CEOs are on a path to realize their vision and successfully transform their businesses through technology, they can't afford to turn a blind eye to the cyber risks this poses.

"At the same time, it falls on CISOs to ensure that CEOs have the right understanding of the value that investing in cybersecurity brings and that they recognize that as an integral part of the transformation journey. Investing in building a strategic relationship between CISOs, CEOs and the rest of the C-suite will help ensure that transformation programs are not only successful, but also implemented in a cyber-secure way for the organization and its people."

But the ability of cybersecurity executives to exert influence, and to ensure that the wider business is supportive of their growing role, is far from certain. Eight in ten boards believe improved risk management will be critical for protecting and building value, according to the EY *Global Board Risk Study 2021*, but we expect the CISO's contribution to be less widely recognized at the current time.

Our findings suggest that CISOs should consider three core actions to strengthen their position within the business:

- Reassess their alignment with the business
- Review the talent profile
- Focus on four key stakeholder groups

It is worth noting that these actions are consistent with the guidance we gave in our 2020 report, albeit with some evolution in the underlying thought process. The events of the crisis era have only emphasized their urgency and highlighted the importance of getting them right.

> There is no such thing as a "standard" cybersecurity profile

1

Get to "ground truth" – reassess your alignment with the business

Cybersecurity teams have traditionally been strongest when it comes to assessing their capabilities, identifying risk, and building roadmaps for the future.

CISOs should focus their attention on the elements of cybersecurity where many have been weaker in the past. Specifically, they should look to strengthen their engagement with stakeholders, ensure their alignment to core business goals and objectives, and assess their business partners' satisfaction with the performance and delivery of security services (see figure 12).

As their relationships with business partners have deteriorated in recent years, CISOs may now lack the visibility they need to operate in sync with other functions and pursue a strategy that aligns with the business.

2

Review your talent profile – but don't expect the impossible

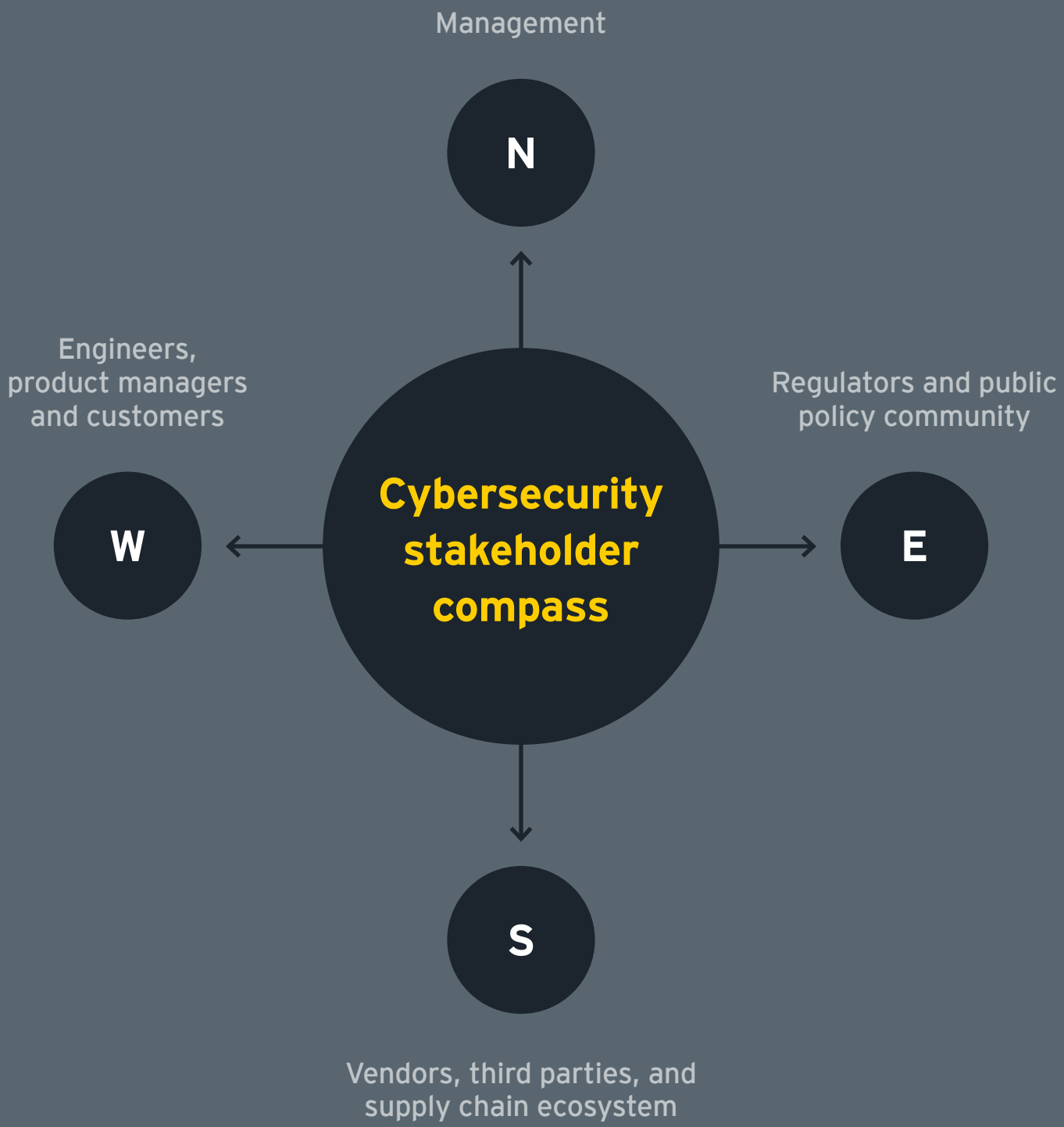
To respond to the organizational challenges highlighted by the survey, as well as the sophisticated nature of recent high-profile attacks, CISOs need the support of versatile, multi-skilled professionals.

A challenge is that the breadth of skills needed in today's function is expanding in several directions at once. There is no such thing as a "standard" cybersecurity profile. CISOs need individuals with advanced technical skills, as well as the ability to build interdepartmental relationships. They need people with a passion for innovation and growth – who can also detect emerging threats and find flaws in defenses.

Figure 13: Multiple profiles in today's cybersecurity function

Cybersecurity executive profile	Area of focus	Strengths	Weaknesses
Security expert	All things security	Deep subject matter expertise	Lack of business acumen
Tech advocate	Technology solutions and tools	Technology oriented	Siloed thinking
Risk and regulatory pros	Risk, controls and compliance	Good for highly regulated sectors	Lack of technology acumen
Business transplants	Business integration	Business connectivity	Lack of technology and security acumen
Part-timers and job-splitters	Split between cybersecurity and other primary roles	Cost saving	"Jack of all trades; master of none'

Figure 14: The CISO at the center of four stakeholder groups



In figure 13, we outline some of the many cybersecurity executive profiles that have emerged in recent years, despite the profession's relative newness. Each profile has its own area of focus, relies on its own range of soft skills and professional qualifications, and plays an important role in meeting the changing needs of the business.

Trying to find one individual who possesses all these talents is, however, like trying to recruit a unicorn. A better approach is to build a team that balances a combination of broad disciplines, with the understanding that each has its own strengths and weaknesses.

With respect to relationship-building, CISOs need to ensure their people have greater exposure to functions such as marketing, innovation and other relevant business units. "Cyber folks have had a reputation for occupying basement levels of an office building," says Darren Kane. "But with cyber risk now one of the top operational risks of any enterprise, cyber teams should be out more and getting greater exposure to other parts of the business."

CISOs are familiar with the principle of "shifting left," striving to involve cybersecurity earlier on in the transformation and product development lifecycle.

3

Shift everywhere – adopt a new stakeholder compass

CISOs are familiar with the principle of "shifting left," striving to involve cybersecurity earlier on in the transformation and product development lifecycle.

The challenges of COVID-19 indicate, however, that shifting left is no longer all that is required. Our suggestion to CISOs is that they shift north, east, south, and west. In practice, this means navigating four key stakeholder groups, as illustrated in figure 14.

Addressing the concerns of management, at "north," means focusing on reporting and accountability, as well as budgeting and resource allocation. Shifting the focus "east," to regulators, is a case of prioritizing certifications and attestations, along with regulatory mapping. Shifting south is about enhancing standards and testing. And shifting west involves focusing on security and privacy by design, along with certifications and continuous testing.

If CISOs can position themselves in the center of these four vital stakeholders, they will be in the right place to take their function to the next level of strategic influence.

Beyond the storm

The COVID-19 crisis has been a wake-up call for CISOs. The business has looked to the cybersecurity team to protect the organization from an evolving cyber threat, while enabling urgent technology transformation and new growth.

There is no doubt that many CISOs have risen to the challenge and can today demonstrate the growing strategic importance of their role. But it would also be fair to flag that the crisis has highlighted weaknesses in cybersecurity and areas where improvement is required. Specifically, CISOs need to accelerate their efforts to address security by design while building stronger, trust-based relationships with their C-suite peers.

It isn't a straightforward initiative, or an ambition that can be achieved within a year, but the business is watching. CISOs need to be involved when strategic investments are being planned. It's down to them to secure a seat at the table.

EY | Assurance | Tax | Transactions | Advisory

About EY
EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets. Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate. Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

EYG no. 006822-21Gbl

BMC Agency
GA 1014478

ED None

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

ey.com

About this report
The data in this year's GISS report is based on a survey of CISOs and other senior leaders at 1,010 organizations, carried out between March and May 2021. CISOs and other C-suite professionals comprised 50% of respondents; the others were C-1 cybersecurity professionals. Surveys were primarily conducted via telephone, with a minority completed online.

This was a global survey with Europe, Middle East, India & Africa (EMEIA) accounting for 43% of respondents, the Americas 36%, and the Asia-Pacific region 20%. Respondents included CISOs or their equivalents from the financial services, consumer products and retail, health and life sciences, energy, government, and technology, media and entertainment, and telecommunications (TMT) sectors. Each business included in the data for this report had annual revenues exceeding $1b.

Comparisons with 2020 represent a snapshot in time during 2020 and 2021, based on similar sample profiles year-on-year. Companies with annual revenues below $1b were included in 2020 but not 2021.

In addition to the quantitative research, EY carried out a series of in-depth discussions with cybersecurity thought leaders between April and June 2021.

Key contacts

Kris Lovejoy
EY Global Cybersecurity Leader
kristin.lovejoy@eyg.ey.com

Mike Maddison
EY EMEIA Cybersecurity Consulting Leader
mike.maddison@uk.ey.com

Dave Burg
EY Americas Cybersecurity Leader
dave.burg@ey.com

Richard Watson
EY Asia-Pacific Cybersecurity Leader
richard.watson@au.ey.com