Building a better working world

How does security evolve from bolted on to built-in?

Bridging the relationship gap to build a business aligned security program.

EY Global Information Security Survey 2020

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

Welcome

Contents

Kris Lovejoy

EY Global Advisory Cybersecurity Leader

Welcome to the 22nd annual *EY Global Information Security Survey* (GISS), which explores the most important cybersecurity issues facing organizations today.

More than two decades since EY started reporting on organizations' efforts to safeguard their cybersecurity, the threat continues to both increase and transform. We face more attacks than ever before, and from a wider range of increasingly creative bad actors — often with very different motivations.

The good news is that boards and senior management are engaging more intimately with cybersecurity and privacy matters. In this era of transformation, senior leaders are acutely conscious of their organizations' vulnerabilities and the potentially existential dangers posed by attackers.

But there is work to do. Not only is cybersecurity an evolving risk, it also has to be confronted in the context of innovation and change. **Security by Design** should be the aim of every organization.

This year's GISS explores these ideas in more detail. We're grateful to everyone who took time to participate in this research — almost 1,300 organizations. Pooling our knowledge and experience and working together will improve cybersecurity for all.

What is Security by Design?

Security by Design is a new approach that builds cybersecurity into any initiative from the onset, rather than as an afterthought, enabling innovation with confidence. It is a strategic and pragmatic approach that works across all parts of the organization. Security by Design remains in the initiative's lifecycle to help with the ongoing management and mitigation of security risks.

Executive summary

Against the backdrop of mounting threat in an era of disruption, the most forward-thinking cybersecurity functions can be critical agents of change. But this will require organizations to foster new relationships between CISOs, the board and C-suite, and every function of the business.

EY recommendations in brief

Based on the findings from this year's GISS, it is clear that there is now a real opportunity to position cybersecurity at the heart of business transformation and innovation. This will require boards, senior management teams, CISOs and leaders throughout the business to work together to:

1. Establish cybersecurity as a key value enabler in digital transformation – bring cybersecurity into the planning stage of every new initiative. Take advantage of a Security by Design approach to navigate risks in transformation, product or service design at the onset (instead of as an afterthought).

2. Build relationships of trust with every function of the organization – analyze key business processes with cybersecurity teams to understand how they may be impacted by cyber risks and how the cybersecurity team can help enhance the business function around them.

Certainly, cybersecurity teams pursuing and driving a culture of Security by Design can play a crucial role as enablers of transformation. However, making the shift to such a culture will be a shared responsibility. CISOs can — and must — engage more collaboratively with the rest of the business. But boards and C-suites must also commit to a closer working relationship with their cybersecurity colleagues. So too must other functions in the business.

By working together in this way, there is a golden opportunity for organizations to put enhanced cybersecurity and privacy at the heart of their strategies for competitive advantage and differentiation. CISOs must embrace the commercial realities facing their organizations in a disruptive marketplace. The rest of the business, from board level down, must ensure cybersecurity is welcomed to a seat at the leadership table.

3. Implement governance structures that are fit for purpose — develop a set of key performance indicators and key risk indicators that can be used to communicate a risk-centric view in executive and board reporting.

4. Focus on board engagement — communicate in a language the board can understand; consider a risk quantification program to more effectively communicate cyber risks.

5. Evaluate the effectiveness of the cybersecurity function to equip the CISO with new competencies — determine the strengths and weaknesses of the cybersecurity function to understand what the CISO should be equipped with and how.

This year's GISS focuses on this evolving role of the cybersecurity function and is divided into three sections:

1

A systemic failure in communication

The increase in activist attackers, who this report shows were the second-most common source of material or significant breaches, underlines how the cybersecurity function needs a much deeper understanding of its organization's business environment. CISOs who do not work collaboratively with colleagues across the business will inevitably be side-stepped by other functions and lines of business which could, for example, launch new products or services that expose the organization to new threats.

Early findings from the forthcoming *EY Global Board Risk Survey* identified "Technology Disruption" as the greatest strategic opportunity for organizations. The fact that many organizations are seizing on this opportunity by undergoing technological transformation also requires CISOs, the board and C-suite, and the business to work together even more closely. This is so that they can embed cybersecurity solutions at a much earlier stage of new business initiatives – a culture of Security by Design.

Only

36%

of organizations say cybersecurity is involved right from the planning stage of a new business initiative.

- The cyber and privacy threat is increasing and expanding. About 6 in 10 organizations (59%) have faced a material or significant incident in the past 12 months, and as our *EY Global Board Risk Survey* reveals, 48% of boards believe that cyber attacks and data breaches will more than moderately impact their business in the next 12 months. About one-fifth of these attacks (21%) came from "hacktivists" (that is, tech-enabled, political and social activists) – second only to organized crime groups (23%).
- Only 36% of organizations say cybersecurity is involved right from the planning stage of a new business initiative.
- Cybersecurity spending is driven by defensive priorities rather than innovation and transformation: 77% of new initiative spending focused on risk or compliance rather than opportunity.
- One in five respondents spend 5% or less of their cybersecurity budget on supporting new initiatives.

2

Increase trust with a relationships reboot

59%

of organizations say that the relationship between cybersecurity and the lines of business is at best neutral, to mistrustful or non-existent.

So, with Security by Design as the goal, CISOs and their colleagues across the organization – including functions such as marketing, R&D and sales – need to form much closer relationships in order to improve overall business understanding of cybersecurity and meet the mark of Security by Design.

Increased collaboration with other functions must be a priority, but cybersecurity also needs to form much more productive relationships with the board, the C-suite and senior leaders.

EY Global Board Risk Survey reveals that only

20%

of boards are extremely confident that the cybersecurity risks and mitigation measures presented to them can protect the organization from major cyber-attacks.

3

The CISO becomes the agent of transformation

- 74% of organizations say that the relationship between cybersecurity and marketing is at best neutral, to mistrustful or non-existent; 64% say the same of the research and development team; 59% for the lines of business. Cybersecurity teams even score poorly on their relationship with finance on whom they are dependent for budget authorization, where 57% of companies say they fall short.
- About half of respondents (48%) say that the board does not yet have a full understanding of cybersecurity risk; 43%, meanwhile, say that the board does not fully understand the value and needs of the cybersecurity team.
- The EY Global Board Risk Survey reveals that boards lack confidence in their organization's cybersecurity, with 50% – at best – stating they were only somewhat confident
- Just 54% of organizations regularly schedule cybersecurity as a board agenda item.
- Six in ten organizations say that they cannot quantify the effectiveness of their cybersecurity spending to their boards.

Only

7%

of organizations would describe cybersecurity as enabling innovation; most choose terms such as "compliance-driven" and "risk averse."

With stronger relationships at business and board level, a better understanding of the organization's commercial imperatives, and the ability to anticipate the evolving cyber threat, CISOs can become central to their organizations' transformation.

They will need a new mindset, as well as new skills in areas such as communication, negotiation, and collaboration. The CISOs that will become powerful agents of change will be the ones who instead of saying "No" to new initiatives say "Yes, but..."

- Just 7% of organizations would describe cybersecurity as enabling innovation; most choose terms such as "compliance-driven" and "risk averse."
- About half the organizations (48%) say that the primary driver for new spending is risk reduction, and 29% cite compliance requirements. Just 9% point to new business initiative enablement;
- Six in ten organizations do not have a head of cybersecurity who sits on the board or at executive management level.

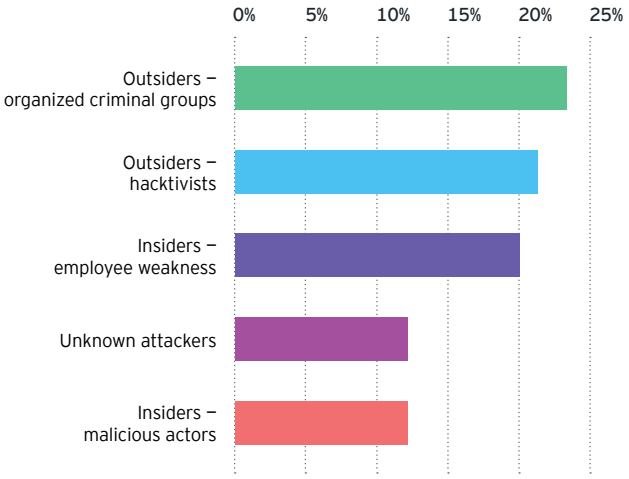
60%

organizations do not have a head of cybersecurity who sits on the board or at executive management level.

1 A systemic failure in communication

Figure 1: Attacks come from multiple sources, including hacktivists

Threat actors behind confirmed breaches



> “We have to think about cyber in a very different way, protecting ourselves against campaigns by actors with a point to make — and that requires a different level of business integration.

Kris Lovejoy
EY Global Advisory Cybersecurity Leader

The arrest of internet activist Julian Assange by the London Metropolitan Police in April 2019 prompted a furious response from his supporters. Within hours, cyber attackers had taken the Police.UK website offline and breached the sites of about 25 associated law-enforcement agencies.[1] This was not an isolated incident; around the world “hacktivists” are using cyber attack as a weapon against organizations, from businesses to government, to which they are opposed.

This year’s GISS underlines that trend. It is not just the significant increases in the number of destructive attacks respondents face (though this is serious enough – 59% say such attacks have become more frequent over the past 12 months, including 34% who report an increase of more than 10%); it is also the change in the types of perpetrators. According to respondents, hacktivists have launched more attacks than any group, other than organized criminal gangs.

The activist threat illustrates one of the challenges facing CISOs. After years spent combatting threats posed by traditional bad actors – data or intellectual property theft and fraud, for instance – and adapting to the techniques of those attackers – ransomware and business e-mail compromise, as prime examples – cybersecurity functions now have to protect the organization from attackers with much more diverse motivations. But, consider a CISO who does not realize that their organization’s investments in coal mining, for example, or its record on human rights, or revelations about one of its executives, put it in the sights of hacktivists. Unless they collaborate with their colleagues beyond the cybersecurity function, CISOs are likely to be blind to these weaknesses – and therefore to the threat.

“We are not necessarily ahead of the threat, because we’re not building cybersecurity inside,” says Kris Lovejoy, EY Global Advisory Cybersecurity Leader. “In cyber, we have focused on countering those threats who sought to steal data, access and IP for financial gain. Now, we have to think about cyber in a very different way, protecting ourselves against campaigns by actors with a point to make – and that requires a different level of business integration.”

Cybersecurity teams face a perfect storm. Amid a rise in destructive attacks, including attacks by angry and well-organized activists, CISOs who are not close to the businesses they serve, who lack the trust of colleagues across the organization, have less and less hope of providing the protection required. This is why, argues Richard Watson, EY Asia-Pacific Cybersecurity Leader, “Security and the CISO have to evolve from being introverted technologists to outgoing business partners.”

[1] Hacktivists attack UK police sites to protest arrest of Julian Assange, DataBreaches.net, April 2019. www.databreaches.net/hacktivists-attack-uk-police-sites-to-protest-arrest-of-julian-assange/

Only

36%

say that their cybersecurity team is involved right from the start of a new business initiative.

Cybersecurity is still an afterthought

The evidence of this year's GISS is that this evolution – from "introverted technologists to outgoing business partners" – has yet to take place at many organizations. Crucially, just 36% say that their cybersecurity team is involved right from the start of a new business initiative – taking part in the planning process for new projects rather than being brought in only as part of the design team, or even later.

In other words, many cybersecurity teams are working *for* the business, rather than *in* the business. The result is that instead of Security by Design, whereby cybersecurity is a central consideration right from the start of each new project, the function finds itself constantly retrofitting protection, which will often lead to imperfect and costly solutions or impractical workarounds.

In this era of digital transformation, where every organization is constantly revamping its products, services, operational processes and organizational structures, this is not good enough.

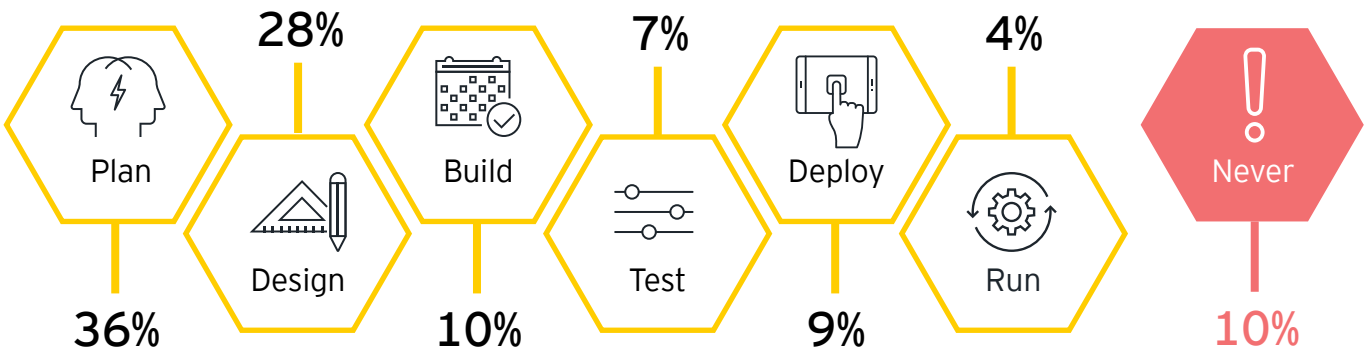
"You're in an environment where technology is evolving so quickly," warns Kris Lovejoy, EY Global Advisory Cybersecurity Leader. "Business initiatives are being rolled out with these new technology-enabling capabilities so that companies can maintain their competitiveness. If security continues as an afterthought, we will always be behind the threat."

Now that activists are using cyber attacks, and business transformation is driving the corporate agenda, cybersecurity teams have to move beyond the defensive, reactive role they might have played in the past. Only by embedding themselves within the organization will they be able to integrate the security agenda into digital transformation programs from the beginning, and anticipate the full range of bad actors that might target the business.

"Where we see companies winning, there has been a true, dedicated focus to drive programs that focus on integration, speed and consistency," says Dave Burg, EY Americas Cybersecurity Leader. "Where we see failure, there is a lack of integration, simplification and focus."

Figure 2

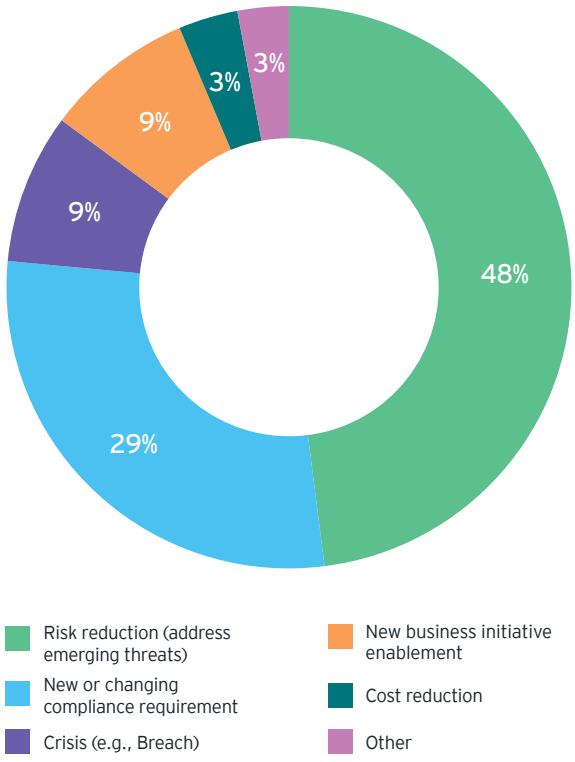
When are cybersecurity teams joining new business initiatives?



86% of organizations say that crisis prevention and compliance remain the top drivers of new or increased security spending.

Figure 3: New business initiatives miss out on extra spending

Justification for new or increased cybersecurity funds



Organizations are spending on business as usual, not on new initiatives

The spending priorities of many cybersecurity functions today show that there is significant work to do to embed a culture of Security by Design. Right now, the majority (60%) of organizations say that where there is additional focus and spending on cybersecurity, it is driven by concern about risk.

Asked to identify the new business or technology initiatives that are driving new spending, regulation and risk rank highest. Digital transformation might be on the radar for 14% of organizations, but few highlight emerging technologies as an area of focus. For example, despite highly publicized concerns in the media about the exposures that connected devices could bring, just 6% point to Internet of Things-related initiatives as driving new spending on cybersecurity. While artificial intelligence increasingly influences how organizations make decisions, run operations, and communicate with customers, only 5% cite increased focus on artificial intelligence.

Figure 3 suggests that the spending of many cybersecurity functions is heavily weighted toward business as usual instead of new initiatives. Some 17% of organizations spend 5% or less of their organization's cybersecurity budget on new initiatives; 44% spend less than 15%.

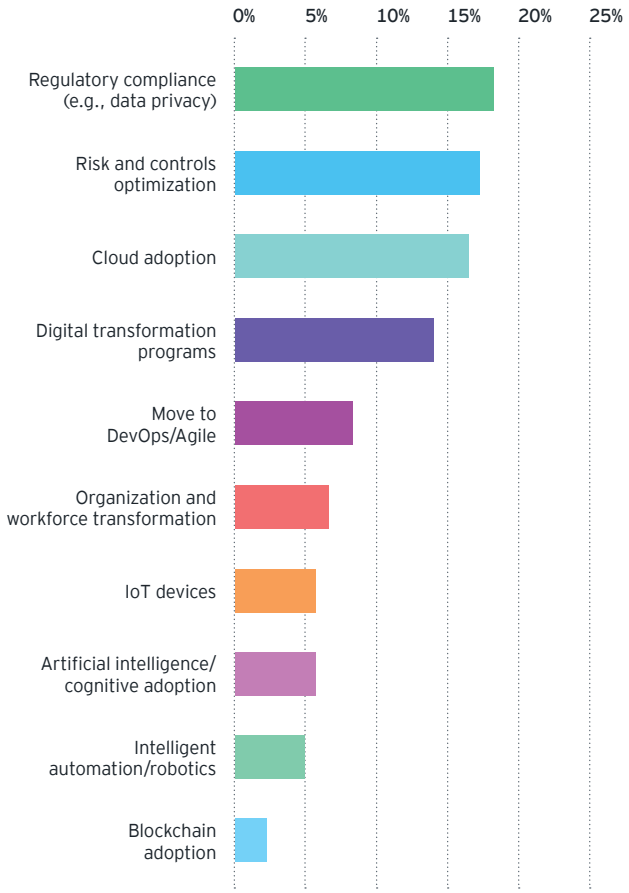
Nor are CISOs necessarily preparing and equipping their functions for future challenges. The majority of organizations (51%) in this report are spending more than half their cybersecurity budgets on operations; more than a third (43%) currently dedicate less than a quarter of their spend to capital projects and long-term investment. Meanwhile, in major sectors such as private equity, organizations anticipate increasing technological adoption to realize operational efficiencies, market insights and growth – in the *EY Global Private Equity Survey*, for instance, 75% of PE CFOs are pushing their teams to spend more time with and leverage more technology.

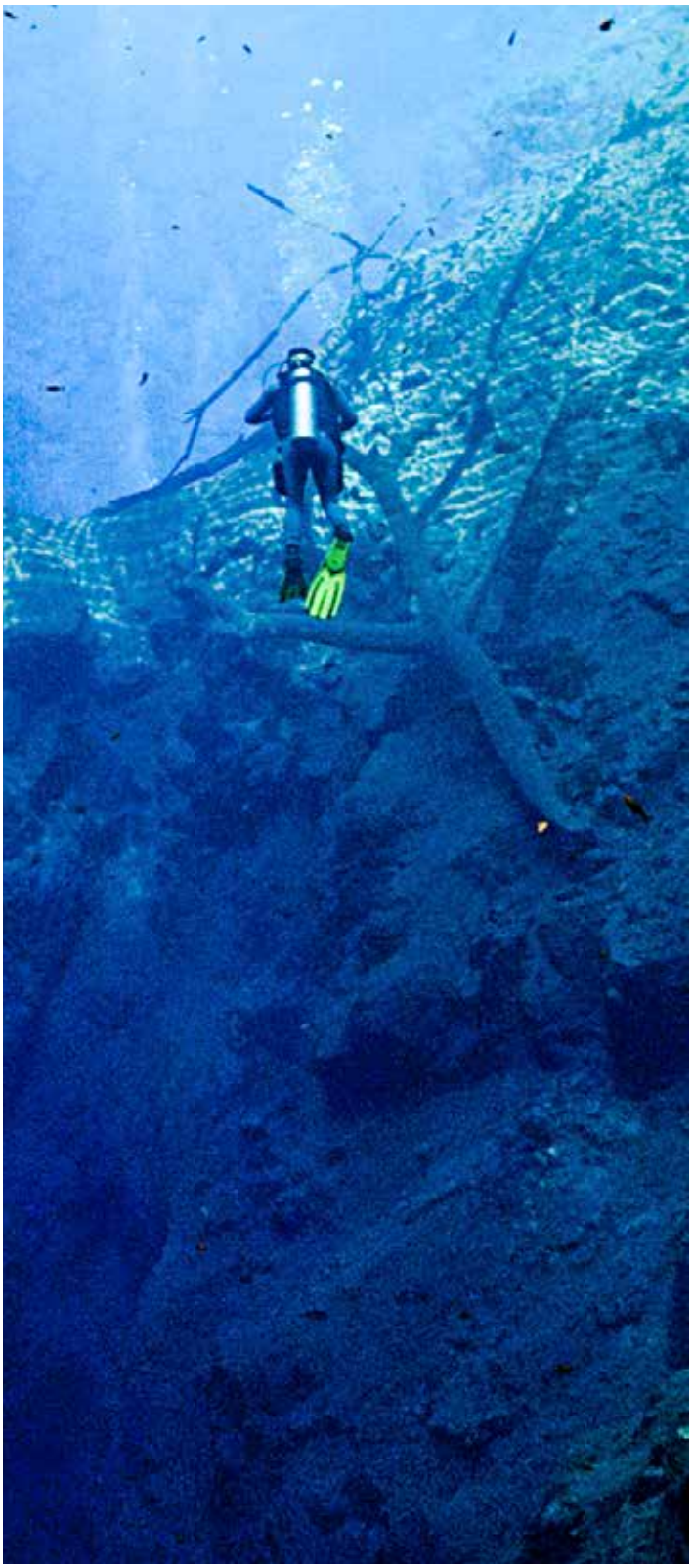
59% of organisations experienced a significant or material breach in the last 12 months.

"What strikes you about business today is that technology is no longer controlled by IT because every new product and service is tech enabled in some way," says Vinod Jayaprakash, EY GDS Cybersecurity Leader. "Unless you're working with those business partners, there will be all sorts of technologies being implemented across your business that are not even being considered from a security perspective."

Figure 4: How new or increased cybersecurity funds are spent

Use of net new funds for cybersecurity





Only

14%

of new or increased cybersecurity funds are used on digital transformation programs.

CISOs need to get ready for a new proactive role

A wholesale shift will not be easy. After all, cybersecurity functions continue to face significant workloads that require commitments to operations. And alongside the new need to confront a broader range of attackers and support innovation and transformation, the more familiar challenges have not gone away – attackers continue to target organizations' data – and particularly their customer data, which carries reputational and regulatory risks.

Many organizations are still struggling to detect and repel breaches. While 72% of survey respondents detected their most significant breach of the past 12 months within a month, 28% say the problem took longer to uncover. And they are more vulnerable in some areas than others – 39% of organizations say that they would be unlikely to detect a file-less malware attack, for instance.

CISOs will therefore be all too aware that they must not neglect business as usual; defending the organization will naturally remain their priority.

However, to perform this role effectively, the function will need to adapt. As their organizations transform around them and the external threat landscape evolves, CISOs must be ready for a more proactive role.

Defending the organization and enabling change are not mutually exclusive. Organizations that embrace the idea of Security by Design will be more resilient – and will therefore find themselves spending less time detecting, repelling or resolving breaches. Cybersecurity teams with a deep-rooted understanding of their businesses will be better placed to anticipate new threats and to recognize potential new aggressors, and to respond ahead of time.

So in taking on the role of business partner and change-enabler, CISOs will not only provide greater value to their organizations, but will also become more effective in their traditional areas of operation.

92% of boards are involved in cybersecurity direction and strategy but only 20% of boards are extremely confident in cyber attack mitigation measures.

Figure 5: Boards play a large role in approving the cybersecurity strategy, direction and budget

How CISOs perceive the level of board involvement in establishing and/or approving the strategy, direction, and budget of cybersecurity program measures.

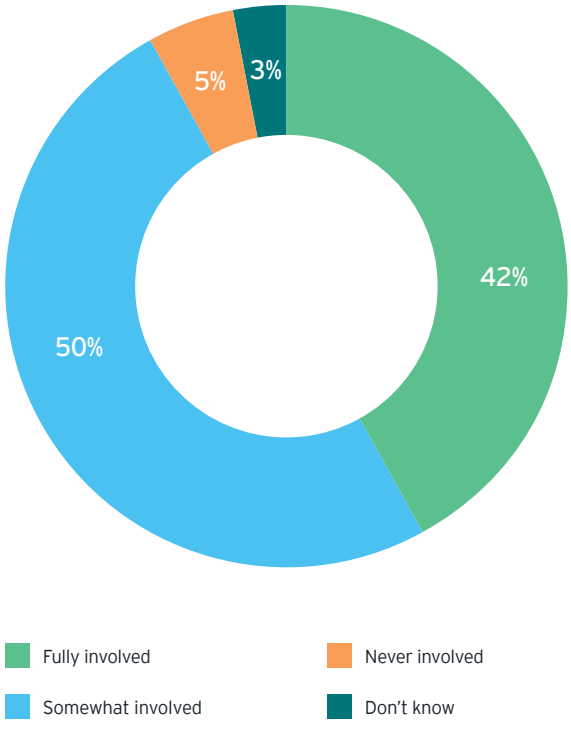
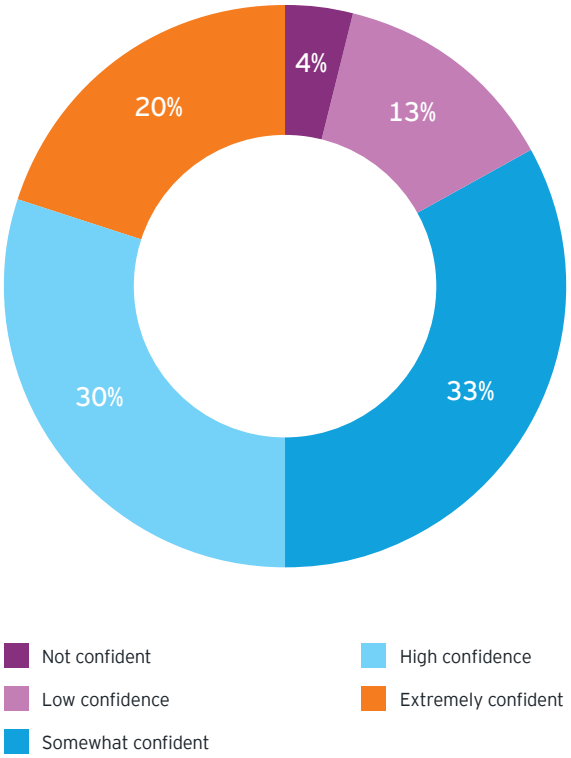


Figure 6: Boards lack confidence in their organizations' cyber attack mitigation measures

The Board's degree of confidence in their organization's ability to protect itself from major cyber attacks.

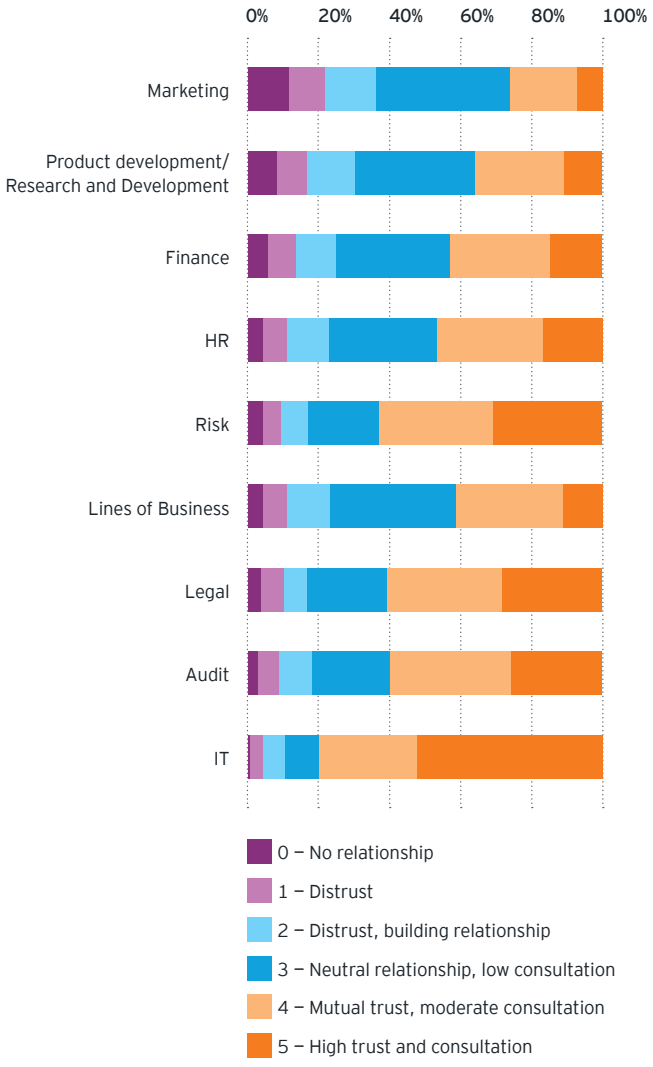


Source: Early findings from the forthcoming *EY Global Board Risk Survey 2019*.

2 Increase trust with a reboot of relationships

Figure 7: A trust deficit

Cybersecurity's business relationships



59% of organizations say that the relationship between cybersecurity and the lines of business are at best neutral, to mistrustful or non-existent.

As we have seen, many organizations feel that their cybersecurity functions are stuck in defensive mode – not yet ready to play a central role in enabling the business to transform. What is it that is preventing CISOs from making the leap?

The answer lies in the relationships between the cybersecurity function and other parts of the business – both at a functional level with other departments and with senior management and the board. Rebooting these relationships, establishing trust and proving cybersecurity's full value to the organization, is now essential.

Why is collaboration so crucial?

One imperative is to reach out to functions across the business in order to work more closely than ever before. As Figure 7 shows, the cybersecurity team at many organizations currently has little or no relationship with other key functions – and especially those involved in innovation, product development and customer-facing activities.

Almost three-quarters of organizations (74%) say that the relationship between cybersecurity and marketing is no better than neutral – and in many cases they describe it as mistrustful or non-existent. Some 64% say the same of the function's relationship with the product development and R&D teams. It is only when it comes to functions such as IT, risk and legal, where cybersecurity's traditionally defensive, compliance-driven role is a more comfortable fit, that significant numbers of businesses describe the relationship as trusting and cooperative (see Figure 7). In many organizations, even the relationship with finance is difficult, with more than a quarter of respondents describing it as non-existent or mistrustful.

The CISOs who find themselves on the lower end of these trust statistics will find it almost impossible to play the role their businesses increasingly expect of them. Without strong relationships of mutual trust with the rest of the organization, cybersecurity will struggle to get involved in the early stages of new business initiatives, which undermines the concept of security of design. Nor will the function pick up the market intelligence it needs to anticipate threats such as the danger posed by hacktivists.

So stronger relationships are vital. "The best CISOs have taken time to connect with the business deeply, in a trusted way," says Jeremy Pizzala, EY Global Financial Services Cybersecurity Leader. "What they're trying to do is to make sure that they're automatically brought into the business, into its strategy and planning and thinking. That's a really important frontier."

> The best CISOs have taken time to connect with the business deeply, in a trusted way.
>
> **Jeremy Pizzala**
> EY Global Financial Services Cybersecurity Leader

In part, it is a simple case of investing time and effort in relationships with other functions. But the nature of the interaction will be important, too. Today, cybersecurity is respected for its work in keeping the organization safe, but it is not seen as a key ally in the transformation process. While 29% of respondents say that they associate the function with the idea of protecting the enterprise, only 7% agree that the function "enables innovation with confidence."

Changing that perception will be key. If cybersecurity is seen as an obstacle to innovation and transformation — as a function that says no to new initiatives on security grounds — the rest of the organization will inevitably try to sidestep it. But if it can provide workable solutions to any problem, it will be more likely to become a trusted partner.

Build board engagement with better communication

These cross-functional relationships are not the only links for the cybersecurity team to work on: many organizations also report a disconnect between their boards and the cybersecurity function. This is a concern, because those disconnects will undermine the ability of cybersecurity to connect more fully with other departments: if the board does not afford the function status, nor will other parts of the business. They will also threaten the CISO's ability to secure the resources they need.

"One of the mantras of cybersecurity has always been 'The board doesn't get us,'" says Mike Maddison, EY EMEIA Advisory Cybersecurity Leader. "Actually, the senior people in most organizations do fundamentally recognize the threat. Where they find cybersecurity lacking is in its ability to articulate the issues and to execute."

> Senior people in most organizations do fundamentally recognize the threat. Where they find cybersecurity lacking is in its ability to articulate the issues and to execute.
>
> **Mike Maddison**
> EY EMEIA Advisory Cybersecurity Leader

54% of organizations regularly schedule cybersecurity as a board agenda item.

Figure 8: Cybersecurity is not a regular agenda item for the Board

How often is cybersecurity on the agenda of the full Board?

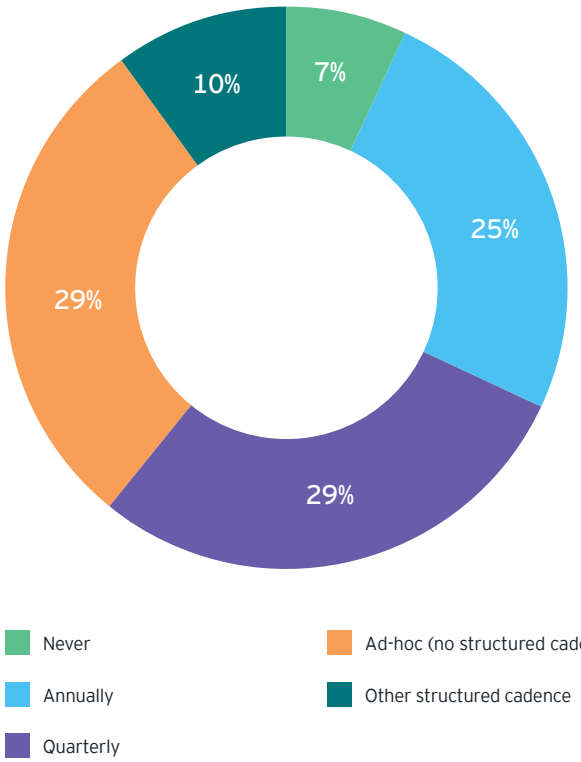
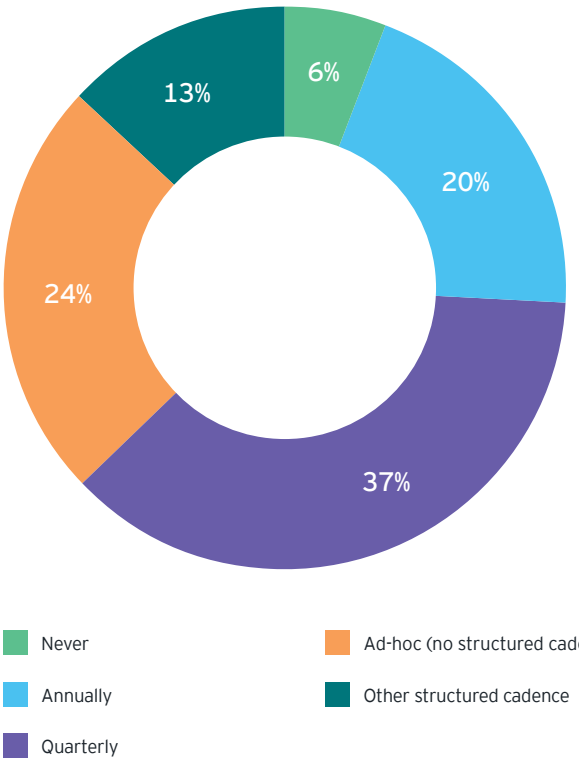


Figure 9: Subcommittees are not routinely briefed on cybersecurity developments.

How often is cybersecurity briefed to a subcommittee (e.g., Audit Committee) of the Board?



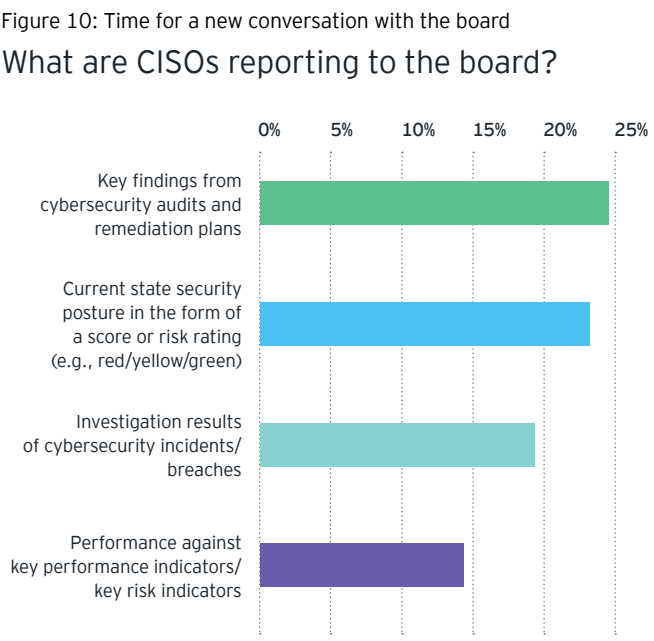
The problem is not that boards do not recognize the importance of committing to cybersecurity. In fact, EY research reveals that CEOs now believe that national and corporate cyber attack is the greatest threat facing the world economy over the next 10 years.[2] And in this year's GISS, 72% of organizations agree that the board sees cyber risk as 'significant'. From the board's point of view, they expect cyber risk to significantly impact their organization over the next 12 months: 50% of independent, non-executive board directors indicating so in early findings from the *EY Global Board Risk Survey*.

Instead, it is a question of the board's understanding of the issue. Only 48% of respondents say that their board and executive management team have the understanding they need to fully evaluate cyber risk and the measures it is taking to defend itself. Similarly, 42% complain that their boards do not fully understand the value of the cybersecurity team and its needs.

How can organizations improve this situation? One important job for CISOs is to think harder about how they communicate with their boards. For example, only 25% of respondents say they can quantify, in financial terms, the effectiveness of their cybersecurity spending in addressing the risks faced by the business. The *EY Global Board Risk Survey* suggests only 20% of board are highly confident that the cybersecurity team is effective. No wonder many CISOs are struggling to secure the resources they need.

Many CISOs are concerned that their boards do not have a structured way to review cyber risk. Just 54% of organizations regularly schedule cybersecurity as a board agenda item, and just 57% regularly put the issue on the agenda of a board sub-committee. This could be a symptom of the way the function chooses to communicate with the board — the emphasis is on current state security, audit results and so on, rather than performance or innovation (see Figure 10).

Figure 10: Time for a new conversation with the board



Only

32%

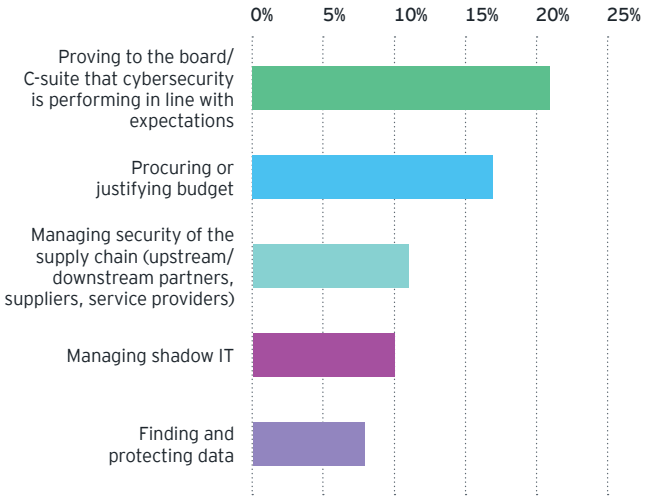
of security leaders use time with the board to discuss forward looking issues and drive change.

[2] How cybersecurity became the number one threat in the global economy for CEOs, EY, October 2019. www.ey.com/en_gl/advisory/how-cybersecurity-became-the-number-one-threat-in-the-global-eco

25% of organizations are able to quantify in financial terms the effectiveness of their cyber spend.

Figure 11: Fighting to be heard

Pressing challenges for cybersecurity



"

If resourcing is going to go up, establishing returns on investment will become increasingly important.

Dave Burg
EY Americas Cybersecurity Advisory Leader

In the absence of a richer conversation with boards and management teams about the value of cybersecurity to the business, greater engagement is likely to prove elusive. "We have to be able to quantify tangible impacts for boards – to quantify risk reduction, for example," says Richard Watson, EY Asia-Pacific Cybersecurity Leader. "Everything else is too abstract."

Many CISOs already say that the most challenging aspect of their role is proving the value of what they do and securing the budget they believe they require (see Figure 11). For many, this is more difficult than actually managing security – even when it comes to evolving technologies and new threats.

Kris Lovejoy, EY Global Advisory Cybersecurity Leader, believes that this is another reason to reset the mindset of the cybersecurity function. "Where are cybersecurity functions spending their money? They're spending it on risk and controls optimization. Where are they reporting? Often, into the audit committee. What are they giving to the audit committee? They're giving it benchmark results on their status on risk and controls optimization," she says.

"The way we've organized cybersecurity is as a backward-looking function, when it is capable of being a forward-looking, value-added function. When cybersecurity speaks the language of business, it takes that critical first step of both hearing and being understood. It starts to demonstrate value because it can directly tie business drivers to what cybersecurity is doing to enable them, justifying its spend and effectiveness. It gets closer to cementing positive relationships outside of traditional lines, and it changes the conversation from 'Why we can't' to 'How can we?' It moves the debate from risk reduction to innovation."

What is the role of third parties?

Can third-party vendors help CISOs improve the performance of cybersecurity and move it closer to the business? Right now, there is some scepticism about the value vendors in the industry genuinely add. Only 10% of respondents to this survey say they trust the marketing claims of cybersecurity vendors, though a further 69% say it depends on the vendor in question. Almost a quarter say vendors fall short on inconsistent delivery (24%) or their confusing products and services (20%).

However, with three-quarters of organizations using up to 20 cybersecurity products or tools (and some using even more), there is scope to drive performance through closer collaboration with a select group of the most trusted vendors. CISOs focus on industry experience and customer service as key qualities.

"CISOs are saying, 'how do I optimize and simplify?'," says Mike Maddison, EY EMEIA Cybersecurity Leader. "One option is to reduce the number of point solutions they have, or to bring in a particular flavor of software provider to reduce management overheads, moving towards broader enterprise agreements to get maximum consumption from one vendor."

Figure 12:

Industry experience and qualifications of the team is the number one factor cited to help increase levels of trust with a cybersecurity provider

#1 Industry experience, qualifications of the team

Great references

#2 Great customer experience

Easily understood terms and conditions

#3 Easily found product and service information

Easy to understand pricing

3 The CISO becomes the agent of transformation

Figure 13: Perceptions have a long way to go

How CISOs are perceived

Many CISOs now find themselves at crossroads. So far, they have focused on improving their organization's defenses and protecting it from cyber attackers. That challenge remains, but there is now an opportunity for CISOs to move on to the front foot – to become agents of change who are crucial figures in their organizations' efforts to transform their businesses.

These CISOs will build cybersecurity functions that operate as enablers of innovation. They will collaborate more closely with other functions than ever before. And they will leverage these relationships to anticipate emerging and changing disruptive threats from bad actors with a range of motivations.

Those who do not embrace the opportunity will find their function increasingly sidelined. "We have now been talking about cyber enablers for some time, and this idea will only become more important given the emphasis on optimization and growth," says Mike Maddison, EY EMEIA Advisory Cybersecurity Leader. "But many organizations are really struggling to get security leaders to step up to that."

The new opportunity will create a very different CISO and will require the cybersecurity function as a whole to adapt to new ways of working. But the upheaval will be worth it: this is a chance for cybersecurity to become a trusted business partner at the center of the organization's value chain, driving transformation and proving its worth.

The cybersecurity industry today is widely regarded as compliance-driven, set up to respond to crisis and focused on the tools it has at its disposal (see Figure 13). Just 13% of respondents describe the sector as constantly evolving and adaptive; even fewer use the word "innovative."

The future CISO: New skills, new structures, new status

One important question for CISOs is whether they currently have the right skills and experience to work in this new way, and to lead a function that is more proactive and forward-thinking. Their considerable technical skills, earned during careers moving up through cybersecurity functions, will not be enough. The new CISO role will require commercial expertise, strong communication skills and an ability to work collaboratively.

> "We have now been talking about cyber enablers for some time, and this idea will only become more important given the emphasis on optimisation and growth.
>
> **Mike Maddison**
> EY EMEIA Cybersecurity Leader

Only

7%

of security leaders have the ability to financially quantify the impact of breaches.

Recognizing this, some organizations are already hiring CISOs from beyond the cybersecurity function, says Richard Watson, EY Asia-Pacific Cybersecurity Leader. They are choosing executives who have served in other areas of the business — particularly the more commercial roles. "I don't think you need to be a technologist to be a CISO," he says. "At the end of the day, the job is about managing risk, so I think the best CISOs are the ones who understand the language of risk."

Other organizations will prefer to stick with CISOs who have more conventional backgrounds, while also trying to build the organizational processes that will enhance relationships between cybersecurity, the board/C-suite, and the rest of the business. "We've got to both mentor the function, as well as create more formal management and governance structures that enable cybersecurity to communicate within a business context," says Kris Lovejoy, EY Global Advisory Cybersecurity Leader. "Essentially, we need the language and mechanisms to interpret between that function and the board/C-suite and other functions."

The change can be summed up succinctly, continues Kris Lovejoy, "we need to go from a CISO who says 'no,' to one who says 'yes, but … '" In other words, CISOs cannot afford to be seen as blockers of innovation; they must be problem-solvers — enablers who promote Security by Design and allow their organizations to transform safely and securely.

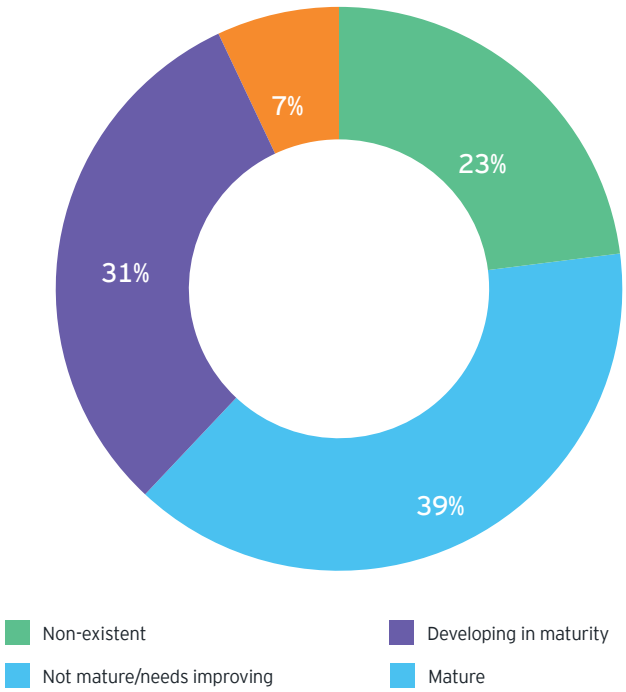
However, as CISOs contemplate this different type of role, are today's reporting structures fit for purpose? Currently, just 36% of CISOs sit on their organization's board or operate as a member of the executive management team. If the job of the CISO is going to broaden and closer relationships with senior leaders and other business functions become more vital, more organizations may need to elevate the role's status.

Take reporting structures: respondents tell us that CISOs are most likely to report into the organization's CIO. This could leave cybersecurity one step removed from the rest of the business, with the CIO required to act as a conduit.

That will have to change if cybersecurity is going to play an enabling role in business transformation, with these organizations following the example of the 18% whose CISO reports directly to the CEO. The small minority of organizations whose CISOs report into risk, finance or legal may find that these structures no longer work.

Figure 14: Shortfall in ability to quantify the financial impact of breaches

Security leaders' ability to quantify the financial impact of cybersecurity breaches



> "CISOs cannot afford to be seen as blockers of innovation; they must be problem-solvers — enablers who promote Security by Design and allow their organizations to transform safely and securely.
>
> **Kris Lovejoy**
> EY Global Advisory Cybersecurity Leader

Case study

AXA

Arnaud Tanguy
Group Chief Security Officer
AXA

Arnaud Tanguy became the Group Chief Security Officer of French insurance company AXA in October 2018, as part of a reorganization that brought previously separate teams responsible for cybersecurity, physical security and operational resilience together as one single security function. "This holistic approach of security globally reflects that threats are converging too".

The reorganization has not only put the security function in a stronger position to protect the business and its customers, but also enabled it to play at a strategic level. "We understand the business and we are close to it, but that's not enough," Arnaud says. "We are part of a company that is working to transform our customers' experience, we are here for them to demonstrate we are secure and resilient in a competitive world; the convergence of our function enables us to think about security holistically – to apply Security by Design in everything we do."

This enabling role is underpinned by a close relationship between AXA's security teams and the company's senior leaders, with the group chief security officer reporting directly to the group chief operating officer, who sits on the AXA's management committee. "this means that security is part of the strategic decisions of AXA, Arnaud adds. Really, we are here to support the strategy of the group, focusing on our customers in a tech-led company to protect our business."

#1 spending category in cybersecurity budgets is the SOC.

Encouraging signs but barriers still exist

Cybersecurity cannot fulfil its potential to add value if it is kept at arm's length from the rest of the organization. "Those organizations that really push for that proactive involvement of security are going to see very significant business benefits in both the near term and the long term," says Dave Burg, EY Americas Cybersecurity Leader.

There are some encouraging signs. For example, 50% of organizations say they are articulating cyber risk – and their tolerance of risk – in the context of business or operational risk. And two-thirds (67%) of organizations expect the security function to provide governance as new intellectual property is developed; only slightly fewer (61%) say the same of operational technologies.

This is promising, but organizations will encounter obstacles as they seek to integrate cybersecurity with other functions.

Budget allocation, in particular, may represent a challenge. In many organizations, the budget for cybersecurity is already derived from several sources, including monies from other lines of business and business functions. Almost a third of respondents (32%) say that their budget comes from more than one source, and this is likely to increase as collaboration rises. Who should be responsible for controlling those funds? Nearly three-quarters (68%) of organizations say that there is one centralized "owner" of sourcing and disbursement, but this will be an increasingly open question.

These are structural and operational issues to be weighed up rather than significant barriers to a new way of working. The benefits of greater integration to both the business and to cybersecurity outweigh these obstacles, and should persuade organizations to do all they can to resolve them.

"Those organizations that really push for that proactive involvement of security are going to see very significant business benefits in both the near term and the long term.

Dave Burg
EY Americas Cybersecurity Leader.

Are Security Operations Centers (SOCs) fit for purpose?

This year's GISS finds that the performance of many organizations' SOCs has been disappointing. Respondents report spending 28% of their cybersecurity budgets on their SOCs and allocating 27% of employee time to operating them; however, only 26% say that their SOC identified their most significant breach over the past 12 months.

This might be because many organizations continue to operate with first-generation SOCs that require significant amounts of manual intervention – particularly given the reluctance (or inability) to invest in future-proofing. Only 19% of budget is currently going towards architecture and engineering. Are SOCs holding cybersecurity functions back?

"SOCs operating with standardized technologies are reactive in their approach and highly manual, relying on the human eye to spot anomalies," says Richard Watson, EY Asia-Pacific Cybersecurity Leader. "The next generation of SOCs have common use cases, such as phishing remediation, automated. They are proactive in nature and use analytics to spot anomalies. They are cloud-based and designed specifically for the client they are serving."

That means that upgrading the SOC could now generate significant dividends. Not only will it improve the organization's ability to identify threats and breaches, but it will also free up resources through increased automation. Organizations that can reduce the amount of employee time required for operating SOCs can then redeploy cybersecurity staff into business-facing activities.

Only 26% of breaches in the last 12 months were detected by the SOC.

Conclusion and next steps

This year's *EY Global Information Security Survey* looks at the progress made by organizations as they attempt to position cybersecurity at the heart of business transformation, built on the foundation of Security by Design.

There is a significant opportunity here for CISOs, board and C-suites, and the rest of the business to work together to reposition the cybersecurity function. Organizations that succeed in this endeavor can ensure the cybersecurity function becomes a key agent of change, enabling the transformation their businesses must undergo to remain competitive. Organizations will also find that cybersecurity becomes more effective in its traditional defensive role, able to anticipate new threats as they evolve with a wider understanding of the potential risk posed by hactivists, for example. And with stronger relationships between boards and CISOs courtesy of a new style of reporting and communication, old battles over resources and value will fall away.

1

Establish cybersecurity as a key value enabler in digital transformation

Integrate cybersecurity into business processes using a Security by Design approach. Bringing cybersecurity into the planning stage of every new business initiative is the optimal model as it reduces the energy and expense of triaging issues after-the-fact and builds trust into a product or service from the start. It requires cybersecurity to become far more integrated and collaborative.

2

Build relationships of trust with every function of the organization

When cybersecurity is embedded in the business, CISOs will be in a strong position to help drive innovation and become better informed of threats faced by the organization. A key way of doing this is using existing data to model business processes and associated controls, and collaborating with CISOs to understand the true cybersecurity impacts to these business processes. As the evidence becomes clear to all, business functions gain real-time insight to the security of their processes and build trust; CISOs gain visibility on potential additional risks and threats, and how to help the business control or innovate around them.

3

Implement governance structures that are fit for purpose

When cybersecurity is embedded in the business, CISOs will be in a strong position to help drive innovation and become better informed of threats faced by the organization. A key way of doing this is using existing data to model business processes and associated controls, and collaborating with CISOs to understand the true cybersecurity impacts to these business processes. As the evidence becomes clear to all, business functions gain real-time insight to the security of their processes and build trust; CISOs gain visibility on potential additional risks and threats, and how to help the business control or innovate around them.

Making this transition is not straightforward, nor is it the same for everyone. What organizations do next – their CISOs, board and C-suites, and individual functions – will depend on the current state of their cybersecurity functions and the characteristics and objectives of their organizations. There are, however, five actions that every organization can prioritize to make the most of the opportunity:

4

Focus on board engagement

It is vital that organizations develop reporting structures and ways to quantify the value of cybersecurity that resonate with the board. A key step is to implement a cyber risk quantification program to more effectively communicate cyber risks in business terms and gain traction in board communications.

5

Evaluate the effectiveness of the cybersecurity function to equip the CISO with new competencies

Cybersecurity leaders must have commercial sense, an ability to communicate in language the business understands, and a willingness to find solutions to security problems rather than saying "No." This starts with understanding the strengths and weaknesses of the cybersecurity function to identify how much room a CISO has to maneuver. Determine if managed services are being used appropriately to deliver at scale, at competitive cost, and with effective results. Evaluate automation and orchestration capabilities to reduce manual effort by the cybersecurity function and free them to support the business in a value-added way.

Cybersecurity leaders must have commercial sense, an ability to communicate in language the business understands, and a willingness to find solutions to security problems rather than saying "No."

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

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. For more information about our organization, please visit ey.com.

EYG no. 000676-20Gbl

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
This year's *Global Information Security Survey* is based on a survey of senior leaders at almost 1,300 organizations carried out by EY between August and October 2019.

This was a global survey with Europe, Middle East, India & Africa (EMEIA) accounting for 47% of respondents, the Americas 29%, and the Asia-Pacific region 24%. Respondents included CISOs or their equivalents from across every industry sector.