Delinea

The Impact of Business Alignment on Cybersecurity Effectiveness

Global Survey of Cybersecurity Leaders

WHITEPAPER

Executive Summary

There are obvious ways cybersecurity impacts business. For example, when a massive cyberattack happens, business can stop suddenly, like an emergency break derailing a train running at full speed.

Beyond this off-the-rails scenario, the work of the cybersecurity team also impacts day-to-day business efficiency, speed of service delivery, costs, employee productivity, user experience, and sales. While these impacts aren't as dramatic as the train accident analogy, they can slow down business and take it off course in ways that make it hard to recover.

The importance of alignment between cybersecurity and business enablement

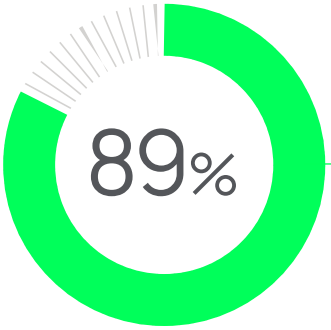
As organizations continue to navigate a complex IT landscape and uncertain economic climate, alignment between cybersecurity and business is essential for success. Cybersecurity teams are increasingly told they shouldn't be working in a silo, focused only on protecting technology. They hear they can't be the "department of no" and instead must become "business enablers."

However, many aren't sure how to make those buzzwords a reality. Most cybersecurity leaders have technical training and have come up through the ranks of technical departments. They may have worked in a silo for most of their career. Shifting mindset to enable a new way of working isn't accomplished overnight. Getting an accurate, shared understanding of where our industry is today is the first step.

Within this context, we surveyed over 2,000 cybersecurity decision-makers in 22 countries, working in enterprises with over 500 employees, to understand the current state of business enablement. More precisely, we wanted to identify, with data, the kinds of attributes that have a meaningful impact on business enablement, including alignment, skills, and organizational structures.

What we've learned is fascinating and troubling

The results indicate that the cybersecurity industry has a long way to go to become effective business enablers. The data reveals a lack of alignment among teams as well as within teams, which has the potential to negatively impact both security posture and achievement of business goals.



In fact, 89% of respondents say their business suffered at least one negative impact in the past year due to lack of cybersecurity and business alignment.

Much of the problem lies in an enterprise's inability to align goals and metrics effectively. And a very large part of that challenge lies squarely in organizations' struggle to achieve common agreement across a wide range of expectations.

In this report, you'll get a picture of the current situation and understand some of the drivers that determine not just cybersecurity posture but also business success.

Key Finding 1

When cyber leaders feel insecure, it's tough to focus on anything else

We begin here to understand the context in which cybersecurity leaders operate.

Only 40% of decision-makers surveyed say they're ready to take on the cybersecurity fight. In fact, most security leaders say they're simply running to keep up, treading water, or in the doldrums. These percentages are virtually unchanged from last year.

Figure 1 | Which of the following best describes your overall security strategy right now?

Interestingly, people within teams disagree about the current state of their company's security posture. Those in more senior roles are more positive about the current security posture than are those with day-to-day responsibility for IT and security management.

Figure 2 | Which of the following best describes your overall security strategy right now?

	CEO	CISO/CIO/CSO	IT or Security Director	IT or Security Manager
In the doldrums – we need to re-invigorate the importance of cybersecurity across the organization	**39%**	16%	16%	22%
Treading water – we're not implementing anything new, just keeping the lights on	6%	7%	12%	15%
Running to keep up – we have a great approach, but we're lacking the resources/budget to truly deliver on our strategy	17%	21%	28%	31%
The fight is on – we're adapting and evolving to keep pace with the threat landscape	38%	**56%**	**44%**	**32%**

Changing mindset

When you consider the question of "business enablement" in this context, you can see why it could be difficult for a cybersecurity leader to expand their remit beyond security fundamentals. Many are consumed with the day-to-day struggle of protecting the organization and reactively fighting fires as they occur. Unfortunately, this lack of security confidence means that many cybersecurity leaders may not have the capacity to focus on business goals as well.

The real devil with this situation is the opportunity cost. The pressure to get to a baseline level of security "crowds out" the energy and resources needed to pursue business goals that aren't traditionally the responsibility of the security team.

For a CISO stuck in the doldrums or running to keep up, the advice to focus on business goals may seem to run counter to their view of the world. But, as you'll see in this report, shifting focus to incorporate business goals can actually have a positive impact on security goals as well.

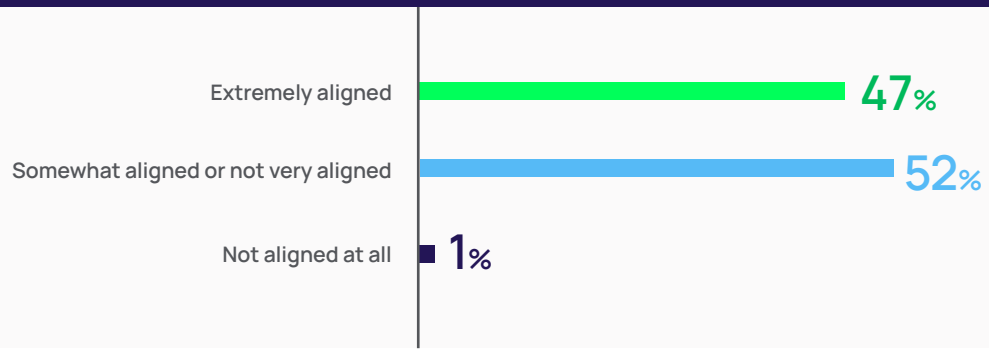
Key Finding 2

Cybersecurity decision-makers say business goals are important but admit they aren't achieving them

Cyber leaders admit to poor alignment between security and business goals

Overall, less than half (47%) of decision-makers feel their cybersecurity goals are extremely aligned with business goals.

Figure 3 | How well do you feel your cybersecurity goals align with the broader business goals?



Interestingly, virtually all organizations that are confident in their security posture – the ones that say, "the fight is on!" — ***also*** say they're either extremely or somewhat aligned with business goals. They're much more likely to be aligned than their counterparts who are simply treading water or running to keep up with security needs.

At the other end of the spectrum, those with the least confidence in their security posture also believe they're aligned with the business. This may be a case of companies overestimating their security/business alignment or underestimating their cybersecurity posture.

Figure 4 | How well do you feel your cybersecurity goals align with the broader business goals?

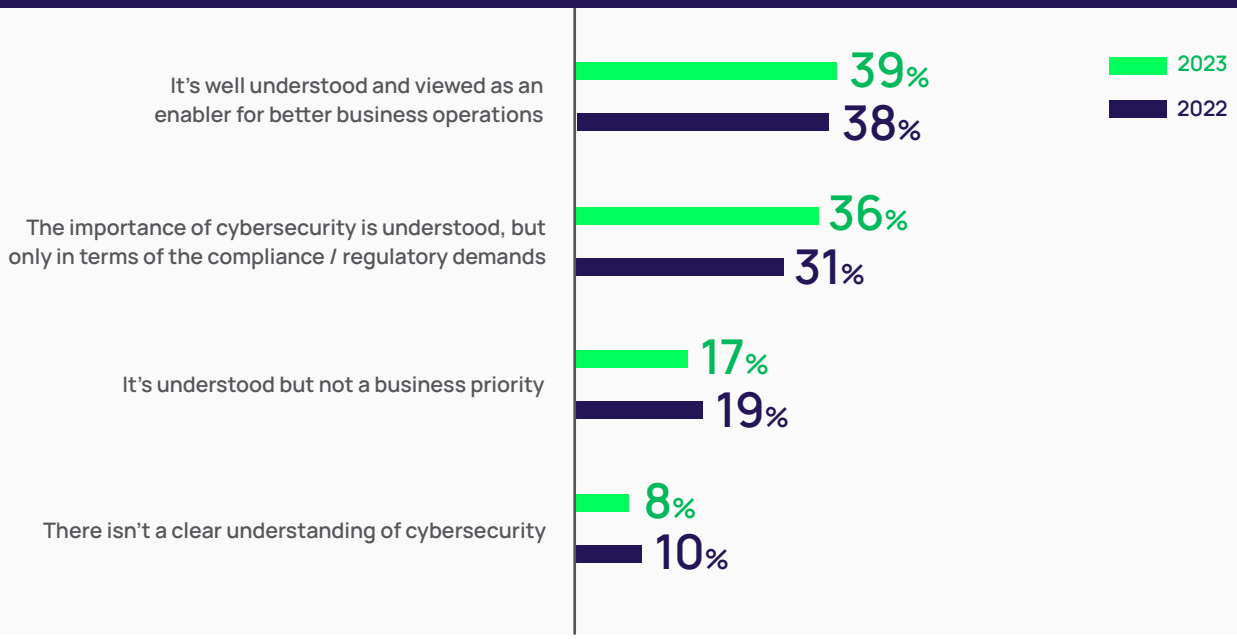
	Extremely aligned	Somewhat aligned	Not very aligned	Not aligned at all	Unsure
In the doldrums – we need to re-invigorate the importance of cybersecurity across the organization	59%	36%	4%	1%	1%
Treading water – we're not implementing anything new, just keeping the lights on	29%	56%	13%	2%	0%
Running to keep up – we have a great approach, but we're lacking the resources/budget to truly deliver on our strategy	31%	60%	7%	2%	0%
The fight is on – we're adapting and evolving to keep pace with the threat landscape	56%	43%	1%	0%	0%

The highest levels of an organization don't understand the business-security connection

The cybersecurity function isn't yet recognized as a business enabler by the highest levels of the organization. While half of respondents (53%) say cybersecurity is understood within their board and executive leadership, they believe these business leaders don't view the security function as a business enabler. This number hasn't budged much in the past year.

It's a painful story, but indicative of how misaligned cybersecurity and business goals are within the enterprise .

Figure 5 | Which of the following statements best describes the board / C-suite's understanding of cybersecurity across your organization?

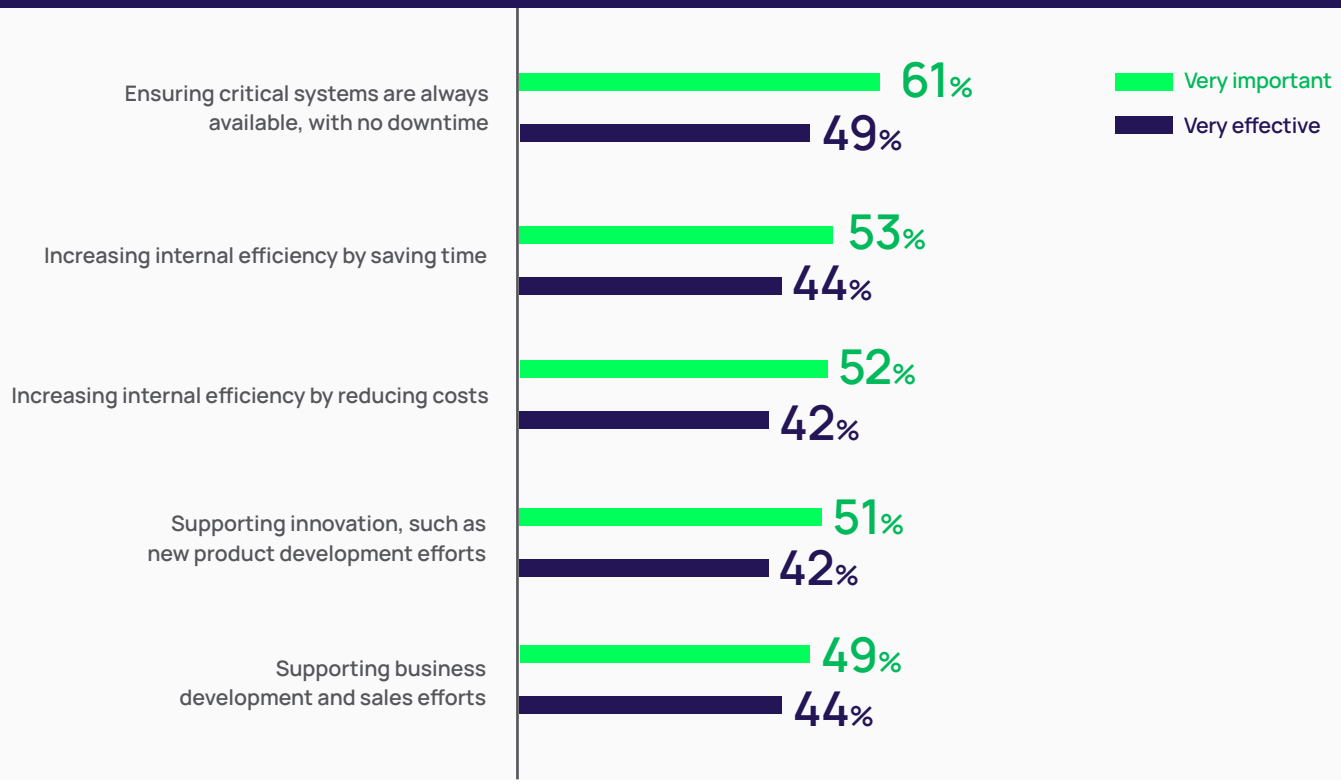


Cyber leaders don't think they're effective at achieving their highest priorities

It turns out that while the primary objective for most security decision-makers is a ***technical*** one — ensuring critical systems are protected and available — approximately half also believe that ***business*** objectives such as increasing efficiency, reducing costs, supporting innovation, and supporting sales are also important for their teams to achieve.

However, less than half believe they're very effective at achieving their priority objectives, including both technical objectives and business objectives.

Figure 6 | How important are the following objectives to your cybersecurity team? How effective do you think your cybersecurity team is at achieving those objectives?



Similarly, companies that are most confident in their security posture are more likely to be very ***effective*** at meeting business goals. Again, the least confident security teams say they're effective, as shown in the chart below.

Figure 7 | How effective do you think your cybersecurity team is at achieving those objectives?

	Ensuring critical systems are always available, with no downtime	Supporting business development and sales efforts	Increasing internal efficiency by saving time	Supporting innovation, such as new product development efforts	Increasing internal efficiency by reducing costs
In the doldrums – we need to re-invigorate the importance of cybersecurity across the organization	62%	60%	65%	58%	61%
Treading water – we're not implementing anything new, just keeping the lights on	51%	49%	44%	40%	43%
Running to keep up – we have a great approach, but we're lacking the resources/ budget to truly deliver on our strategy	53%	48%	42%	40%	48%
The fight is on – we're adapting and evolving to keep pace with the threat landscape	62%	53%	55%	55%	48%

Changing mindset

There could be several reasons for this lack of alignment. Some of the possible reasons are:

1. **Misalignment of security objectives with business goals:** Security leaders may focus too much on mitigating risks and protecting assets, without understanding the broader business objectives.

2. **Lack of communication and collaboration:** Security leaders may not effectively communicate their goals and objectives to other business units or stakeholders or may not collaborate with them to develop security strategies that support business objectives. This can result in security measures being seen as impediments to business objectives rather than as enablers.

3. **Insufficient resources:** Security leaders may not have adequate resources, such as budget, personnel, or technology, to implement security measures that meet business objectives. This can result in security measures that are inadequate or ineffective, or that impose undue burdens on other business units.

4. **Inadequate metrics:** Security leaders may not have the appropriate metrics to measure the effectiveness of their security measures in meeting business objectives. This can lead to a perception that security measures aren't effective, even if they are.

5. **Lack of understanding of business objectives:** Security leaders may not have a clear understanding of the business objectives, priorities, and challenges of the organization. This can result in security measures that don't account for the specific needs of the business.

We'll dig into each of these potential reasons throughout the remainder of the report.

Key Finding 3

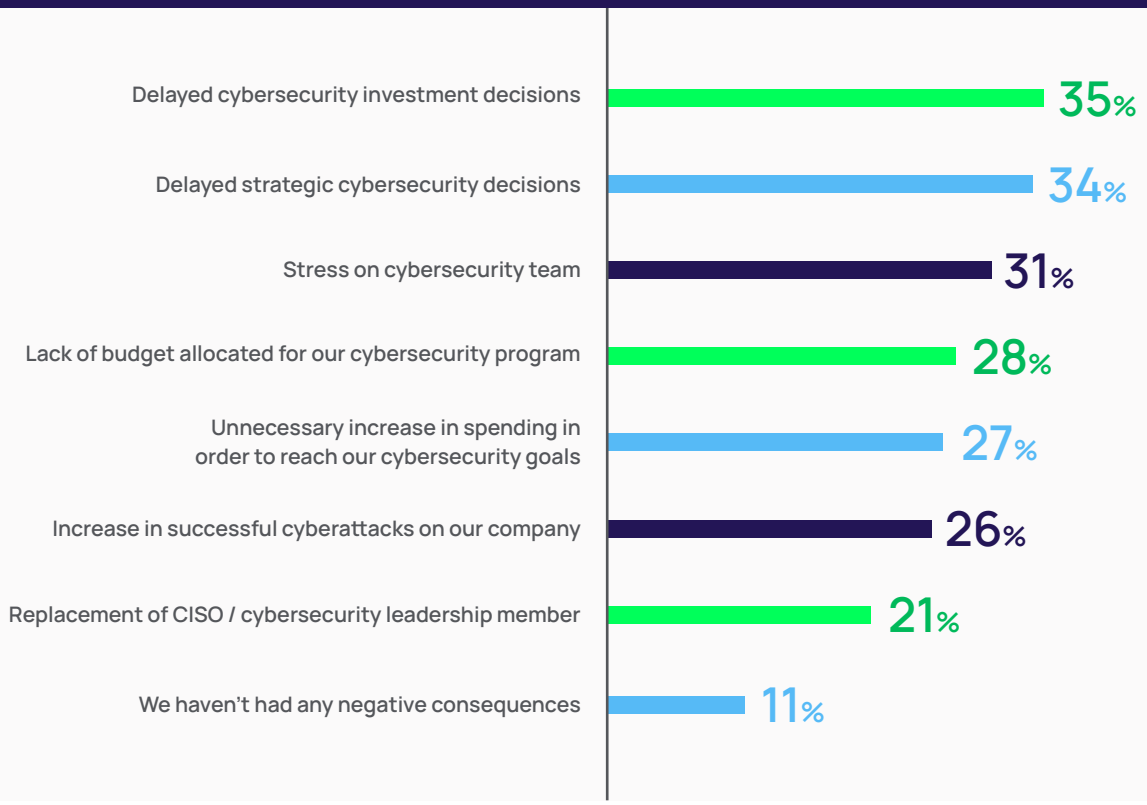
Misalignment has a negative impact on **both** business **and** security goals

A successful cyberattack can result in data breaches, system downtime, financial losses, and damage to a company's reputation, which can all undermine a company's business goals. The research findings back up this assertion.

Negative impacts run the gamut

Close to nine out of 10 organizations have suffered at least one negative impact in the past year due to the lack of cybersecurity and business alignment .

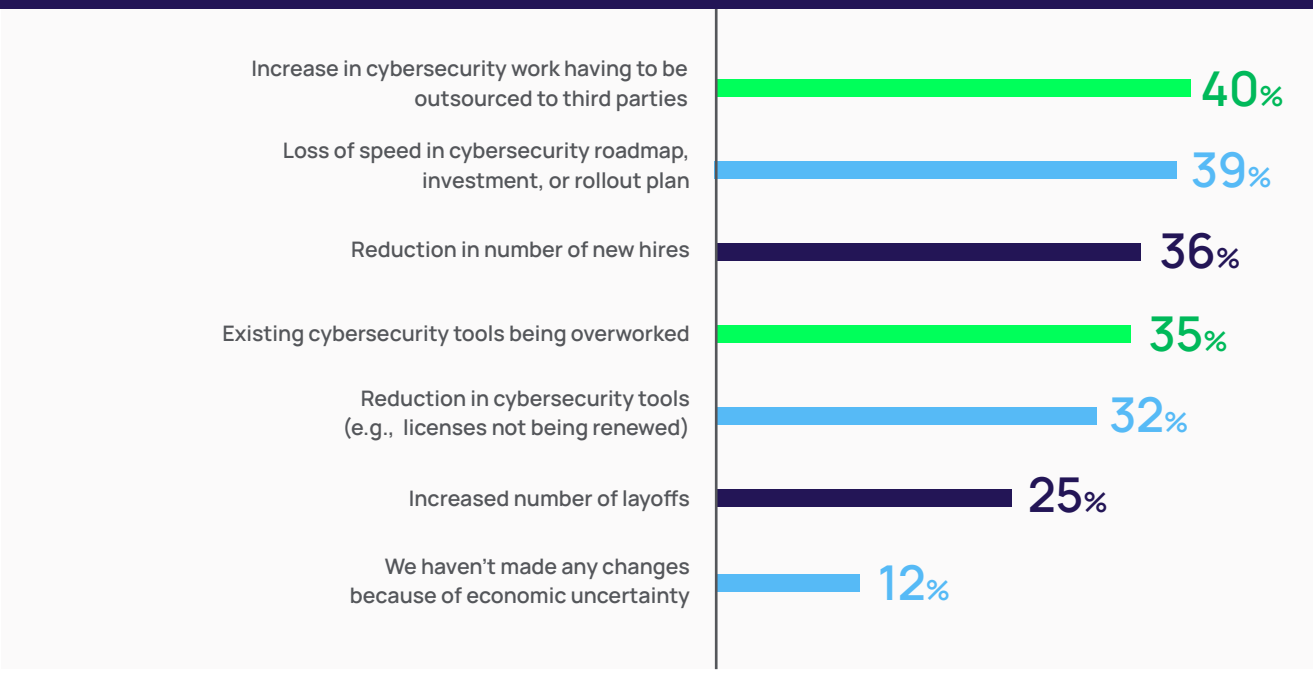
Figure 8 | What, if any, negative consequences have you experienced due to misalignment of cybersecurity and business goals? (Select up to three.)



Why now? The current economic climate is partly to blame

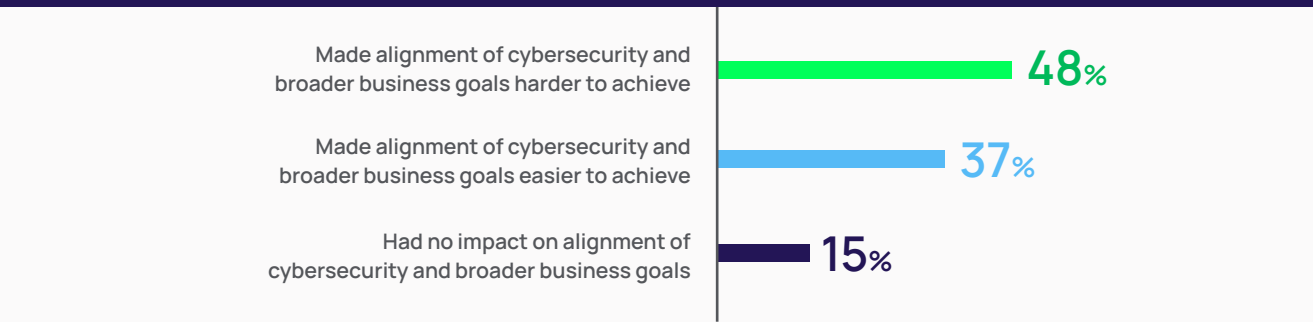
Eighty-eight percent have experienced change due to economic uncertainty. Many of these changes represent negative impacts on security, such as a slowdown in the roadmap and investment in technology, as well as lack of resources, as shown in the chart below.

Figure 9 | How has recent economic uncertainty impacted your cybersecurity team over the past 6 months?



In an environment of change, alignment can be challenging. Approximately half of the respondents agree that economic uncertainty has made cybersecurity and business alignment more difficult to achieve .

Figure 10 | How has recent economic uncertainty affected alignment of cybersecurity goals and broader business goals?



Changing mindset

With stakes like these, the real question about security and business alignment isn't "How can we afford to?" but "How can we afford not to?"

By incorporating cybersecurity as part of a company's overall business strategy, you can develop a proactive approach to security that can reduce the risk of cyberattacks and help safeguard critical business operations.

Key Resource:

Read the Global Survey of Cybersecurity Leaders: Benchmarking Security Gaps & Privileged Access.

Key Finding 4

Mismatched metrics reflect lack of cybersecurity and business alignment

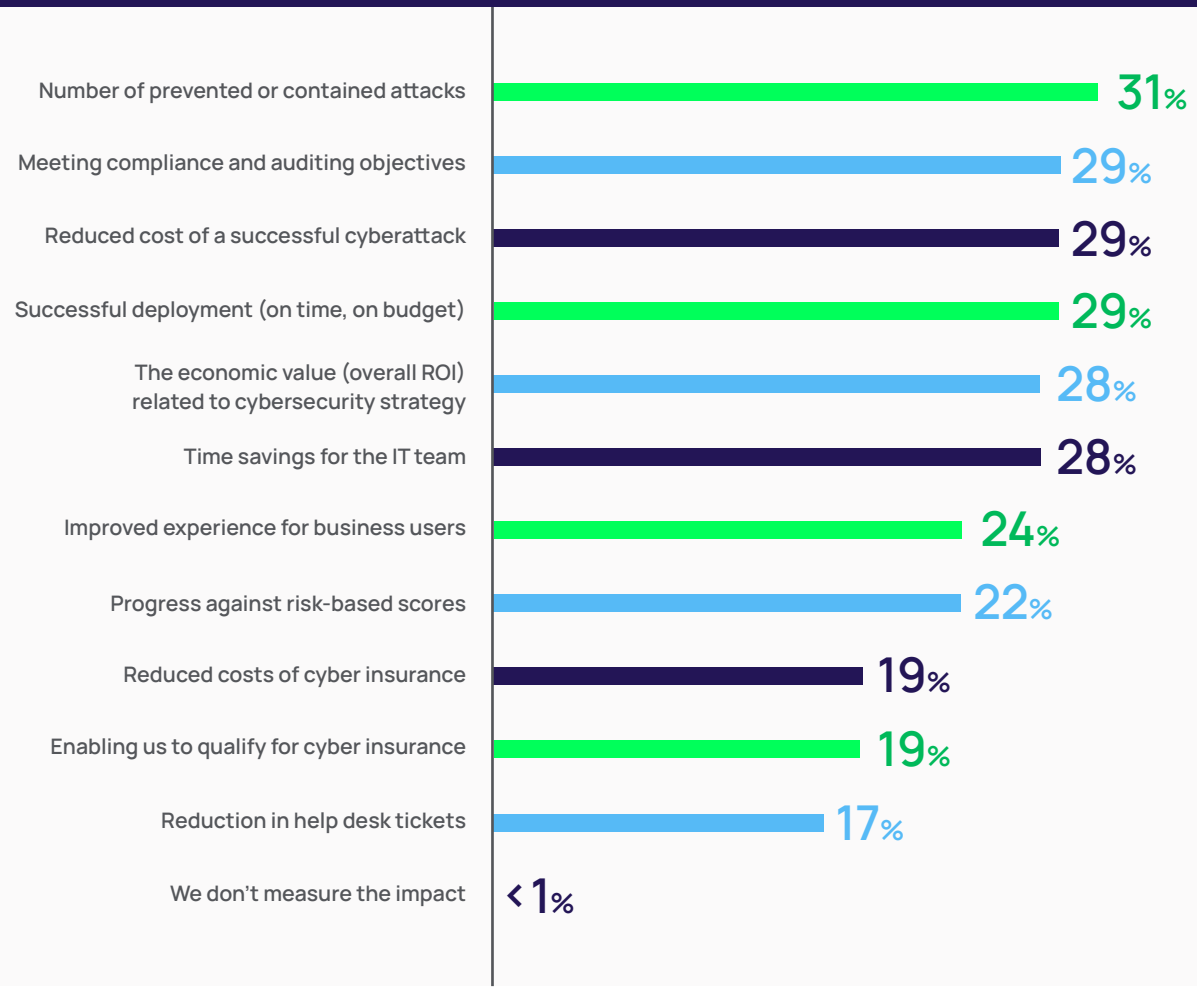
As the saying goes, if you want to manage something, you need to measure it. To attain business enablement goals, team objectives and individual MBOs (Management by Objectives) or OKRs (Objective and Key Results) must be tied together and tracked on an ongoing basis.

Unfortunately, with some exceptions, that doesn't appear to be the case. What leaders may want to be doing versus what they're actually measuring and reporting aren't the same thing.

The difference between technical and business metrics

The data shows that the performance of cybersecurity programs is still primarily judged based on technical or activity-based metrics, such as the number of prevented or contained attacks, rather than business-oriented metrics such as economic value, user experience, insurance costs, or impact on other teams.

Figure 11 | Which of the following are the most important when measuring the success of your cybersecurity programs? (Select up to three.)



That said, overall ROI/economic value is more important to smaller companies with fewer employees.

Figure 12 | Which of the following are the most important when measuring the success of your cybersecurity programs? (Select up to three.)

	1st	2nd	3rd
500-999 employees	The economic value (overall ROI, **29%**)	Number of prevented attacks / Reduced cost / Time savings (all **28%**)	
1000-4999 employees	Number of prevented / contained attacks (**32%**)	Successful deployment / Time savings for IT team (both **31%**)	
5000+ employees	Number of prevented, contained attacks / Meeting compliance & auditing objectives (both **31%**)		Reduced cost of successful cyberattacks (**30%**)

It's not surprising that leaders with broad organizational responsibility, such as CEOs/Owners, are more concerned with measuring user experience and reducing friction than CISOs are. It's interesting to note, however, that Director levels/ Departmental leaders also emphasize business metrics such as economic value/ROI.

Figure 13 | Which of the following are the most important when measuring the success of your cybersecurity programs? (Select up to three.)

	1st	2nd	3rd
CEO / Business Owner	Improved experience for business users (**31%**)	Successful deployment (on time, on budget, **30%**)	Meeting compliance and auditing objectives (**29%**)
CIO / CSO / CISO	Number of prevented / contained attacks (**32%**)	Successful deployment (on time, on budget, **31%**)	The economic value / Reduced cost / Meeting compliance objectives (all **28%**)
Head of IT Department	The economic value (overall ROI, **34%**)	Number of prevented / contained attacks (**32%**)	Reduced cost / Meeting compliance objectives (both **30%**)
IT Director	The economic value (overall ROI, **32%**)	Number of prevented / contained attacks / Time savings for IT teams (both **30%**)	
IT Manager	Number of prevented / contained attacks (**33%**)	Reduced cost / Meeting compliance objectives / Successful deployment (all **30%**)	
Security Manager	Reduced cost of successful cyberattacks (**36%**)	Successful deployment (on time, on budget, **29%**)	Meeting compliance and auditing objectives (**27%**)

Changing mindset

Cybersecurity teams often focus on technical metrics because they provide data that can be used to assess the security posture of an organization. Technical metrics such as the number of vulnerabilities detected and patched, the time taken to detect and respond to security incidents, and the percentage of systems with updated security software provide insight into the effectiveness of security controls and allow teams to identify areas for improvement.

However, while technical metrics are important, they're not the only factors that determine the success of a cybersecurity program. Cybersecurity is ultimately about serving business goals — strategic outcomes that are made possible by effective security.

Cybersecurity leaders can improve alignment by establishing clear and measurable business goals that are tied to their organization's strategic objectives. This could involve identifying the most critical assets for the business, the potential impact to the business if those assets were attacked, and how effective security controls improve the availability, confidentiality, and integrity of those assets. For example, when service is down, financial and operational cost is clear. Cybersecurity results can be measured by the cost of doing nothing versus the cost of doing something.

Cybersecurity teams could also work to improve their communication and collaboration with other parts of the organization, such as risk management, compliance, and business operations. By working closely with these stakeholders, cybersecurity teams can gain a better understanding of the business context and priorities and align their activities accordingly.

Finally, cybersecurity teams could consider adopting a more risk-based approach to security, where technical metrics are used in conjunction with business outcomes to inform decision-making. This would involve identifying the most significant risks to the business and then focusing resources on mitigating those risks rather than just pursuing technical metrics for their own sake.

To measure cybersecurity against business goals, consider the following:

1. **Risk management metrics:** To measure how effective a company is at identifying and mitigating cybersecurity risks, including the frequency of incidents and response times.

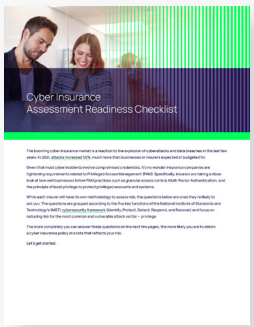
2. **Compliance metrics:** To track how well a company is meeting regulatory and industry compliance standards for cybersecurity.

3. **Business continuity metrics:** To measure the ability of a company to maintain business operations during a cybersecurity incident, including the duration of downtime and the recovery time.

4. **Cost metrics:** To track the cost of implementing and maintaining cybersecurity measures relative to the overall budget.

5. **Productivity metrics:** To measure how quickly a new employee or vendor can be onboarded, provided necessary resources and access to do their job.

By using these types of metrics, you can assess the effectiveness of your cybersecurity strategy in enabling the organization to achieve business goals and make informed decisions about investments in cybersecurity resources.



Key Resources:

- Cyber insurance checklist: answer the questions cyber insurance providers are sure to ask
- Align to regulatory frameworks and compliance requirements

Key Finding 5

Without structural changes, signs point to a difficult road ahead for cybersecurity and business alignment

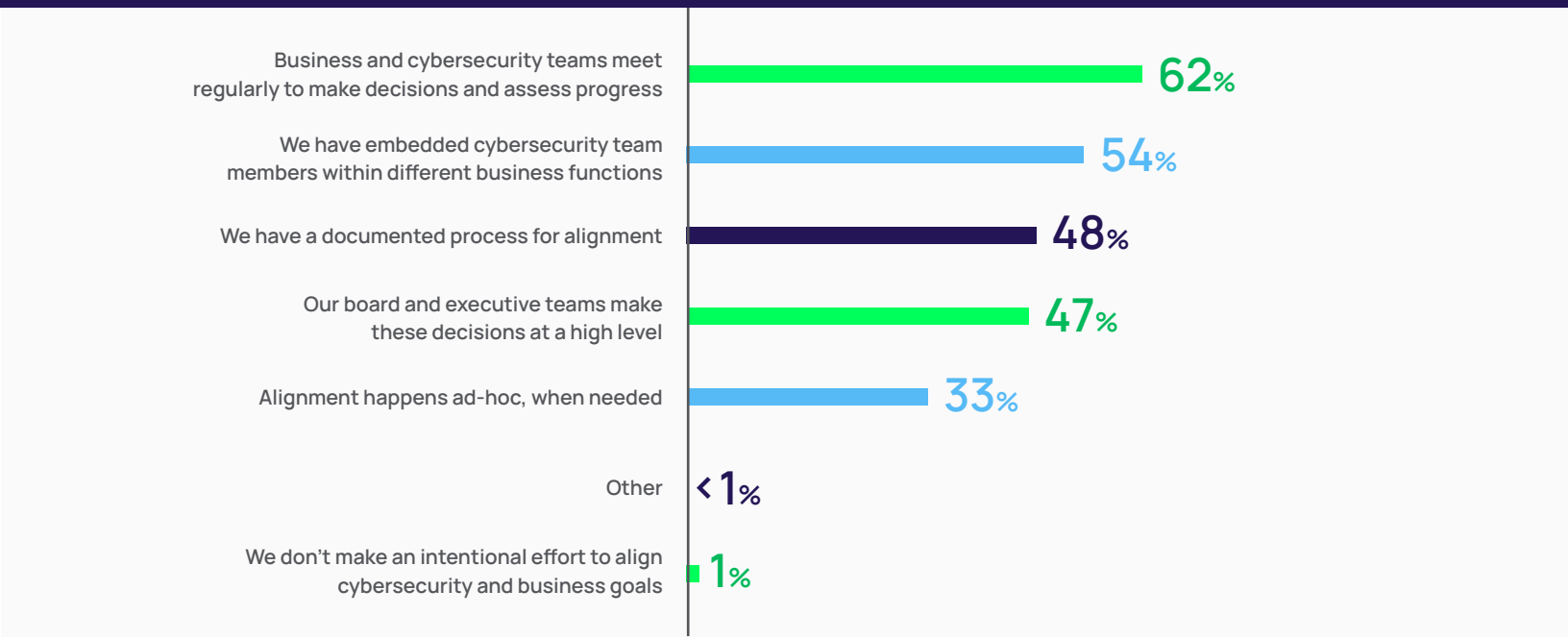
To make business and cybersecurity alignment happen, it's essential to consider organizational structure. So that's where we'll turn next.

Talking the talk vs. walking the walk

The good news is that cross-functional conversations are happening in the enterprise. Most cybersecurity teams meet regularly with their business counterparts at high levels or even have embedded security team members within business functions.

However, less than half of organizations are documenting policies and procedures to help them align.

Figure 14 | How is your organization ensuring cybersecurity goals are aligned with the broader business goals? (Select all that apply.)



Respondents that rate themselves as **"very aligned"** are most likely to say that:

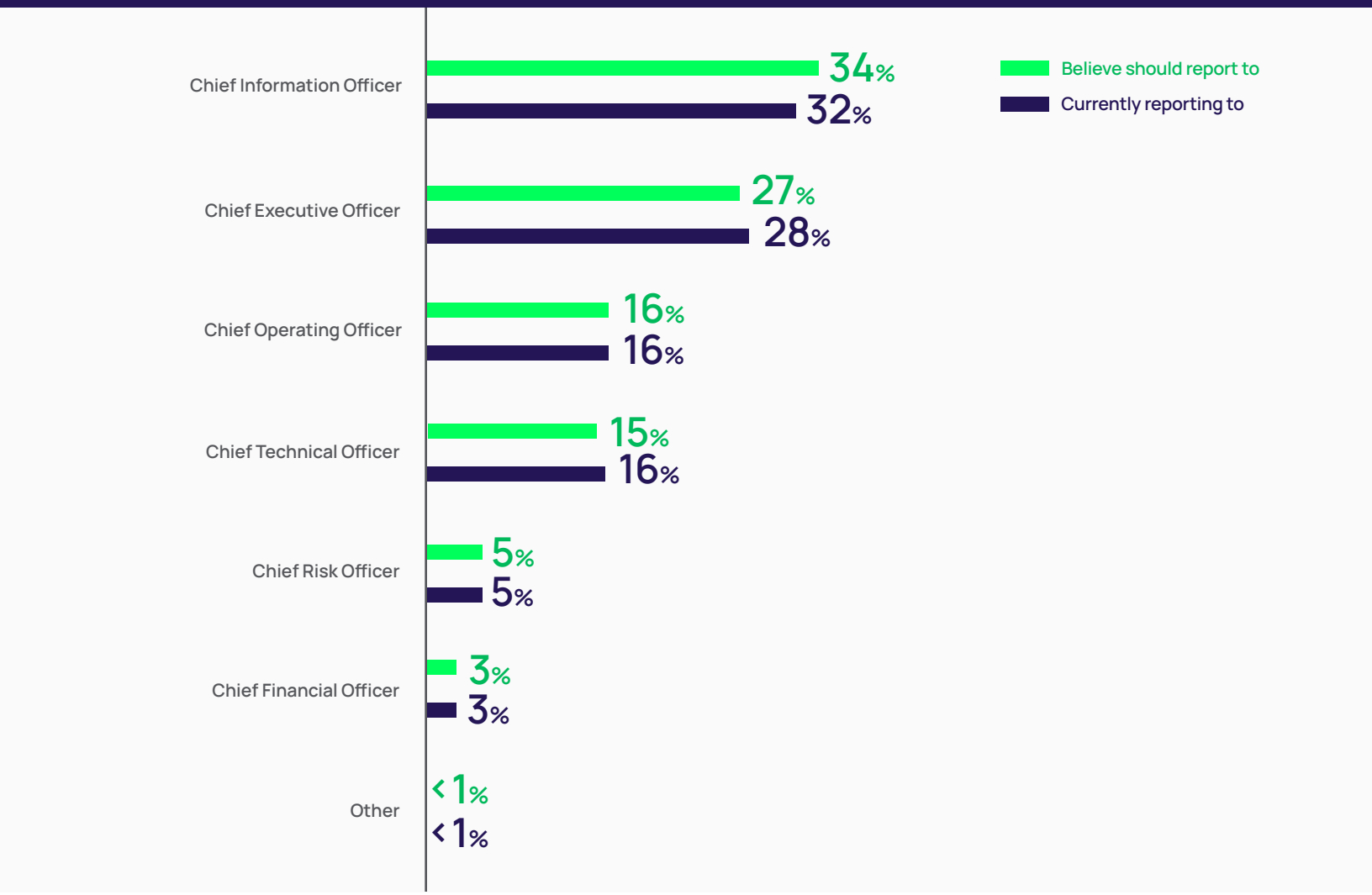
- Business and cybersecurity teams meet regularly to make decisions and assess progress (68%)
- We have embedded cybersecurity team members within different business functions (61%)
- Our board and executive teams make these decisions at a high level (56%)

Reporting structure may hurt rather than help business enablement

Over one-third (34%) of respondents believe the right person for a CISO to report to is the CIO. And in fact, in most organizations, that is who they are reporting to.

It's interesting to note that reporting preferences vary based on job title. For example, CEOs are more likely to prefer CISOs to report to them, while IT Directors are more likely to say CISOs should report to their boss – the CIO.

Figure 15 | Who do you believe the CISO or the most senior cybersecurity leader should report to, in order to best align cybersecurity with the overall goals of the business?
Currently, who does the CISO or the most senior cybersecurity leader report to in your organization?



Current skillsets reflect the need for more business focus among cybersecurity leaders

Overall, respondents believe that technical expertise is the most essential skill for a cybersecurity leader such as a CISO. They rank this skill much higher in importance than business-related skills such as communication, collaboration, making a business case, and business acumen.

Figure 16 | How important are each of these skills for a CISO / cybersecurity leader? Select one per row

As seen in the chart below, the skills respondents believe they most lack are the ability to manage or de-escalate stressful situations, followed by skills such as making a business case and communication. Without these skills, cybersecurity leaders will have a very difficult time aligning with their business counterparts.

Figure 17 | Where do you think your own skill gaps are? Select all that apply

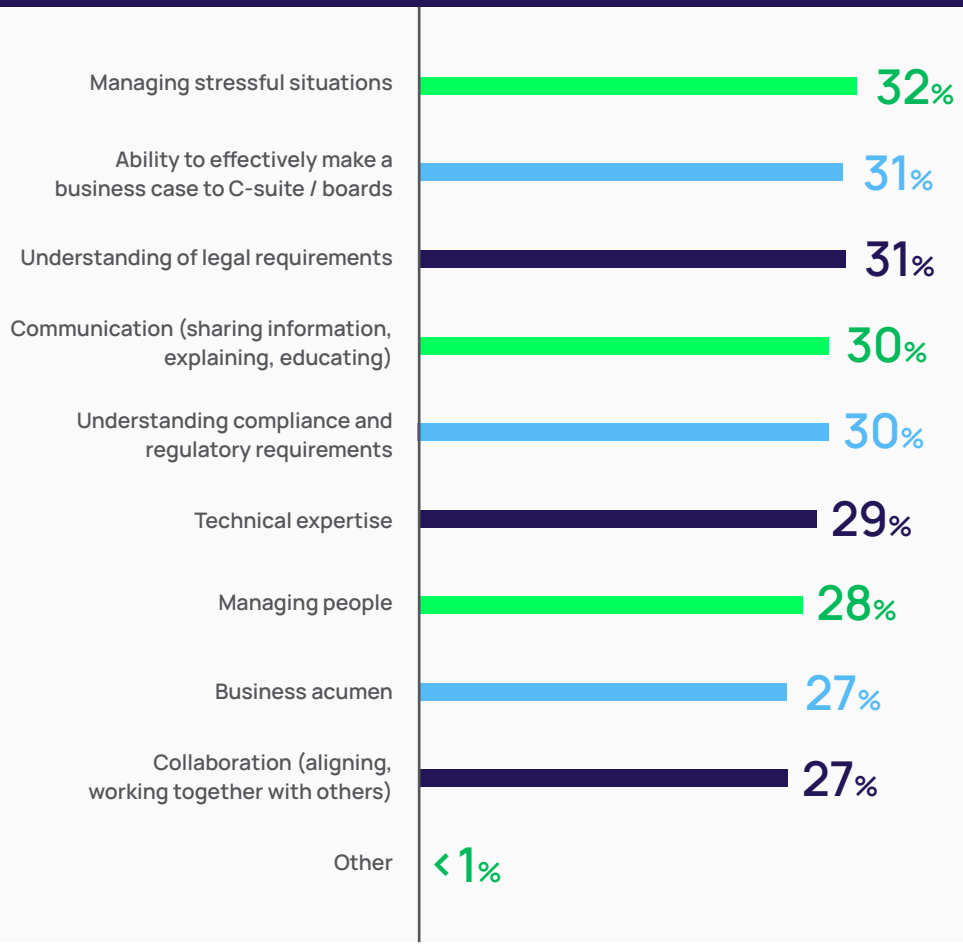


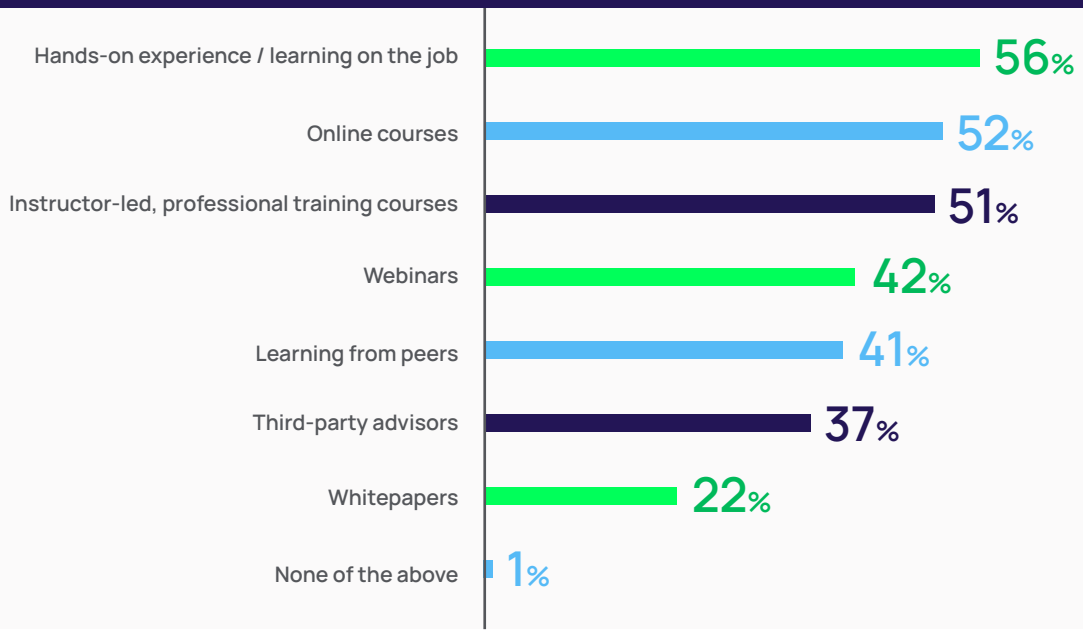
Figure 18 | Where do you think your own skill gaps are?

	1st	2nd	3rd
CEO / Business Owner	Managing stressful situations / Communication (sharing information, explaining, educating, both **38%**)		Ability to effectively make a business case to C-suite / boards (**36%**)
CIO / CSO / CISO	Understanding of legal requirements / technical expertise (**32%**)	Managing stressful situations / Ability to effectively make a business case to C-suite / Communication / Understanding compliance & regulatory requirements (all **31%**)	
Head of IT Department	Managing stressful situations (**31%**)	Understanding of legal requirements / Communication / Managing people (all **29%**)	
IT Director	Managing stressful situations (**32%**)	Understanding of legal; requirements (**31%**)	Understanding compliance and regulatory requirements (**30%**)
IT Manager	Ability to effectively make a business case to C-suite / boards (**34%**)	Reduced cost / Meeting compliance objectives / Successful deployment (all **30%**)	
Security Manager	Managing people (**37%**)	Business acumen (**29%**)	Ability to make a successful business case to C-suite, boards / Collaboration (both **28%**)

Reactive training isn't closing the skills gap

Hands-on experience and learning on the job are the most popular ways respondents improve their skills. It appears that people are saying, "we'll deal with that problem when we have to." That doesn't bode well for building skills necessary for proactive, intentional business enablement.

Figure 19 | How do you improve your own skills and educate yourself to align with business goals and improve overall business performance?



That said, as it should by now have become clear, business enablement isn't just a "skill" challenge. There may be a "will" challenge here as well.

Changing mindset

To better align and fulfill the goal of "business enablement," cybersecurity leaders should consider the following:

Running effective meetings

One might naturally think that the best way to drive alignment is to get everyone together in the first place. But meeting often doesn't guarantee alignment. In fact, that kind of gathering might not even be necessary at all. Alignment is about getting teams to interact with one another in a very specific way irrespective of whether they actually meet.

At the end of the day, alignment can be synchronous or asynchronous. Co-located or disbursed. In-person or over a Zoom call. As long as it is helping teams understand each other, share goals, and collectively measure success.

Developing skills

It's quite likely that organizations won't find the perfect blend of security and business skills in one person.
To find the right mix, cybersecurity leaders will have to look beyond technical experts and bring in people with non-traditional backgrounds to work with their teams.

Reconsidering reporting structure

While having the CISO report into the CIO can have its benefits, there are also potential issues.

Should the CISO report to the CIO?

PRO

- **Alignment with IT strategy:** The CISO and CIO work closely together to align the organization's IT security strategy with its overall business strategy. This approach ensures that security is integrated into all aspects of IT, including developing and implementing new technologies, applications, and infrastructure.
- **Clear accountability:** By reporting to the CIO, the CISO has clear accountability for the security of the organization's IT systems. This accountability helps ensure that security risks are identified, assessed and addressed promptly and effectively.
- **Resource allocation:** The CIO is responsible for allocating resources to IT projects, and by having the CISO report to the CIO, it ensures that security is considered in the allocation of resources. The CISO can help the CIO identify areas where additional resources are needed to strengthen the organization's security posture.
- **Better communication:** The CISO and CIO have a better understanding of the challenges facing each other and can work together to address them. By reporting to the CIO, the CISO has better access to IT decision-makers and can communicate more effectively with them.

CON

- **Conflict of interest:** The CIO is responsible for delivering IT services and projects on time and within budget. This focus on delivery can sometimes conflict with the CISO's responsibility for ensuring the security of IT systems. This conflict can lead to the CISO being pressured to prioritize the delivery of IT services over security.
- **Lack of autonomy:** It can limit the CISO's autonomy and ability to operate independently. If the CIO isn't supportive of the security function or doesn't provide sufficient resources, the CISO may struggle to implement security controls effectively.
- **Communication barriers:** It can limit their ability to communicate with the CEO and the board to understand the organization's security posture.
- **Limited focus on security:** It can reinforce the perception that security is a secondary concern, and may not receive the attention and resources it deserves.
- **Compliance vs. risk management:** The CIO's focus on delivering IT services can sometimes lead to a compliance-focused approach to security, where the emphasis is on meeting regulatory requirements rather than managing security risks.

Overall, while having the CISO report to the CIO can be beneficial, addressing these potential issues is important to ensure security is given the attention it deserves and that the CISO can operate independently and provide an objective assessment of the organization's security posture.

Where to go from here

It's crucial for cybersecurity to align with business goals because risks can directly impact a company's ability to achieve its strategic objectives. The better aligned cybersecurity is with the business, the more resilient the business becomes, AND the more the business can thrive.

Making the shift from "Me" to "We"

Building effective security and business alignment requires a mix of skills. It demands shared metrics. But most of all, it requires broad, consistent application across an organization. Cybersecurity leaders must work closely with other functions to allocate adequate resources and make decisions.

Furthermore, as organizations climb the "Me to We" mountain, they'll have to think very differently about how they view the purpose of cybersecurity. Rather than viewing the responsibility of the cybersecurity team purely in terms of protecting resources, they must expand their perspective to include strategic business goals. That perspective must come through in every assessment, every board report, and every communication the security team shares with the broader organization.

Only then can organizations ensure cyber resilience and achieve sustainable business growth.

Methodology

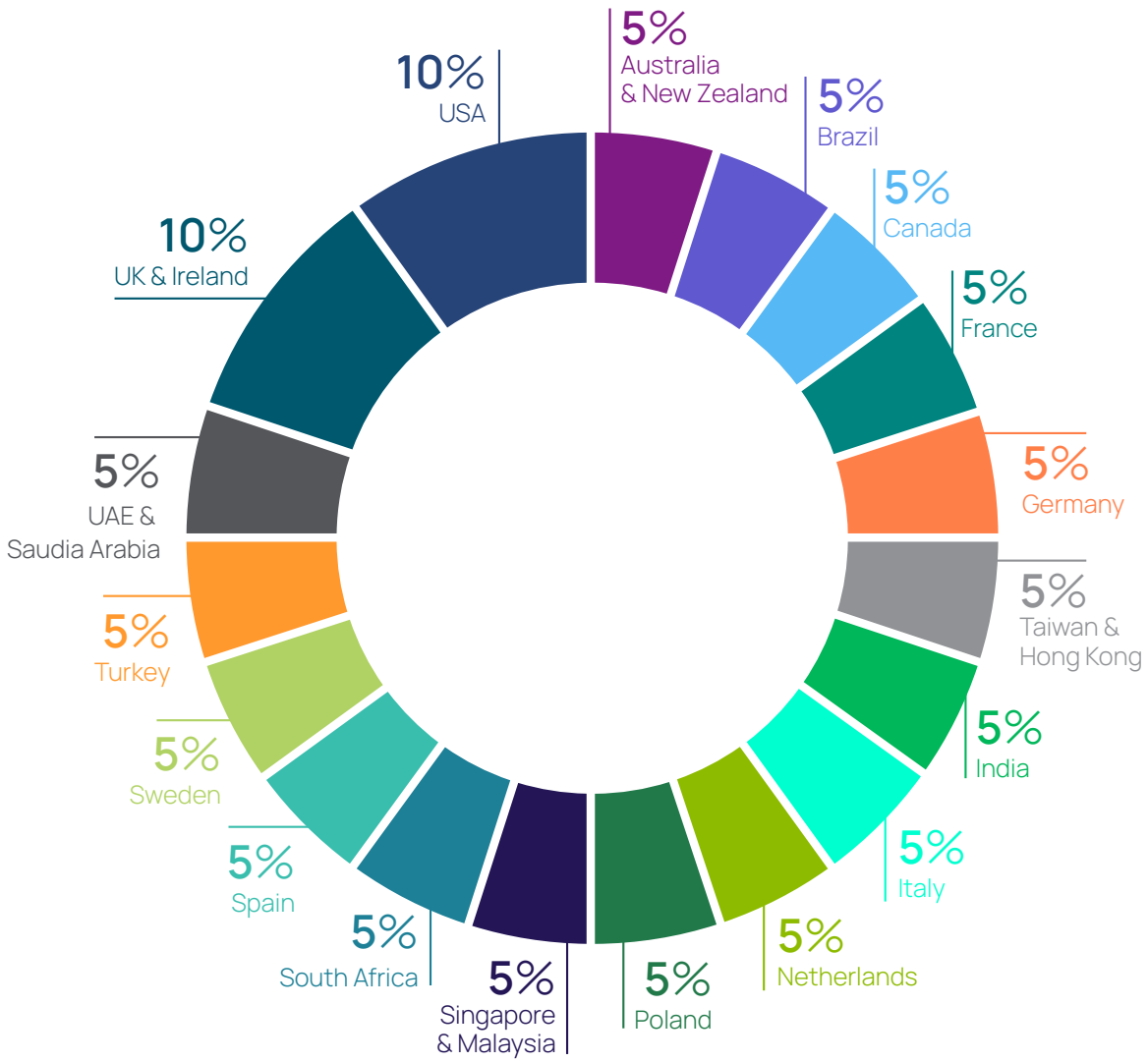
The survey gathered responses from 2007 people during March 2023.

It includes responses from the C-suite, departmental leadership, and management levels of organizations. Respondents came from 23 countries, across 22 industries, working at companies with 500 employees or more.

All participants said they took part in security decision-making as the ultimate decision-maker, part of a team, or as an influencer.

Results aren't weighted.

Country: In which country do you live?

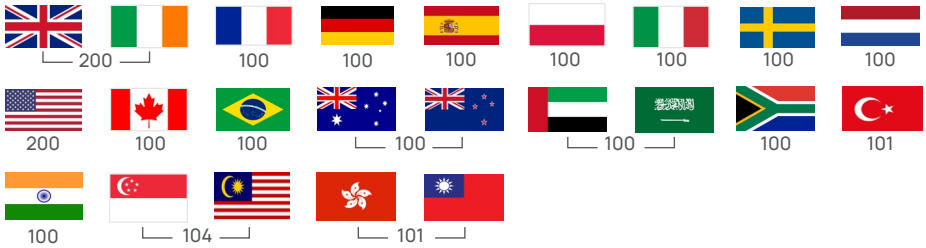


Respondent demographics summary

Demographics

Total respondents: **2007**

Country of residence



Role type

Size of company

# of employees	500-999	1000-4999	5000+
% of respondents	35%	40%	26%

Business sector

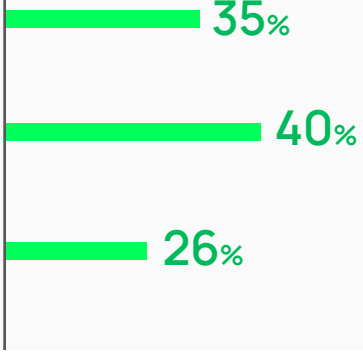
Gender & age

66% of responders were male and 34% female

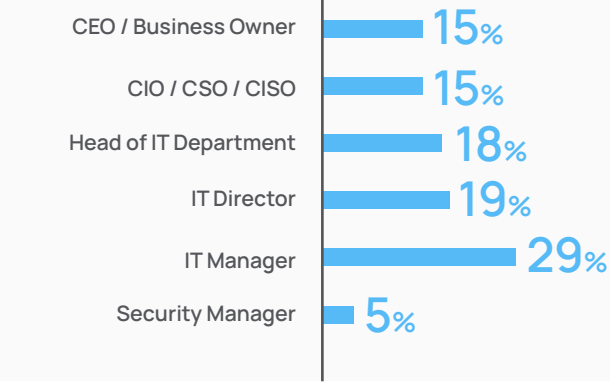
of respondents were aged between **25-44**

Organization Size & Job Role: How many people does the organization you work for employ? Which of the following best describes your job role?

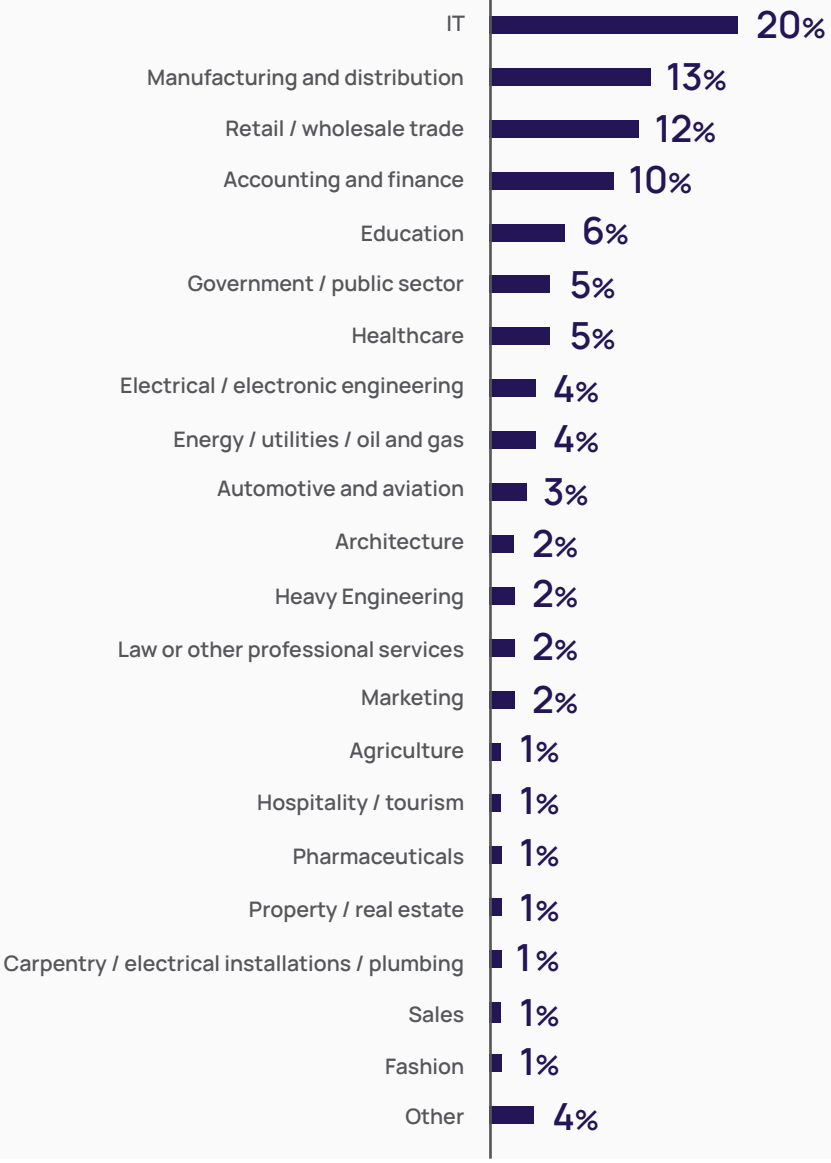
Organization size



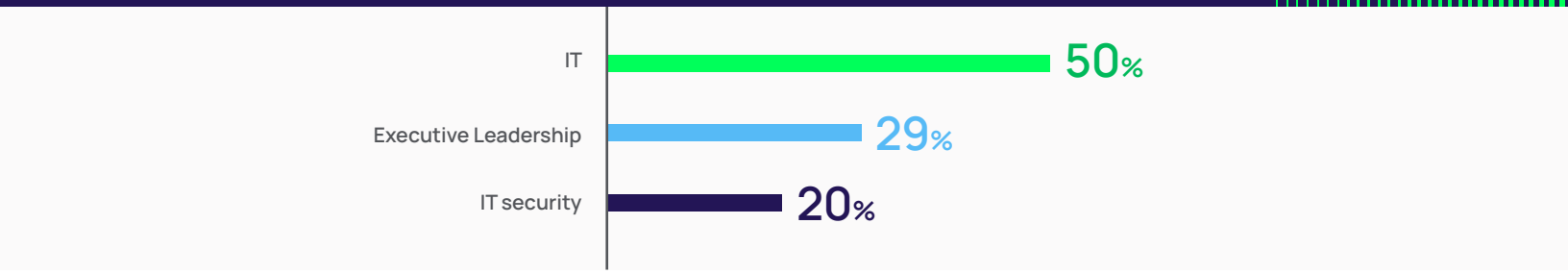
Job Role



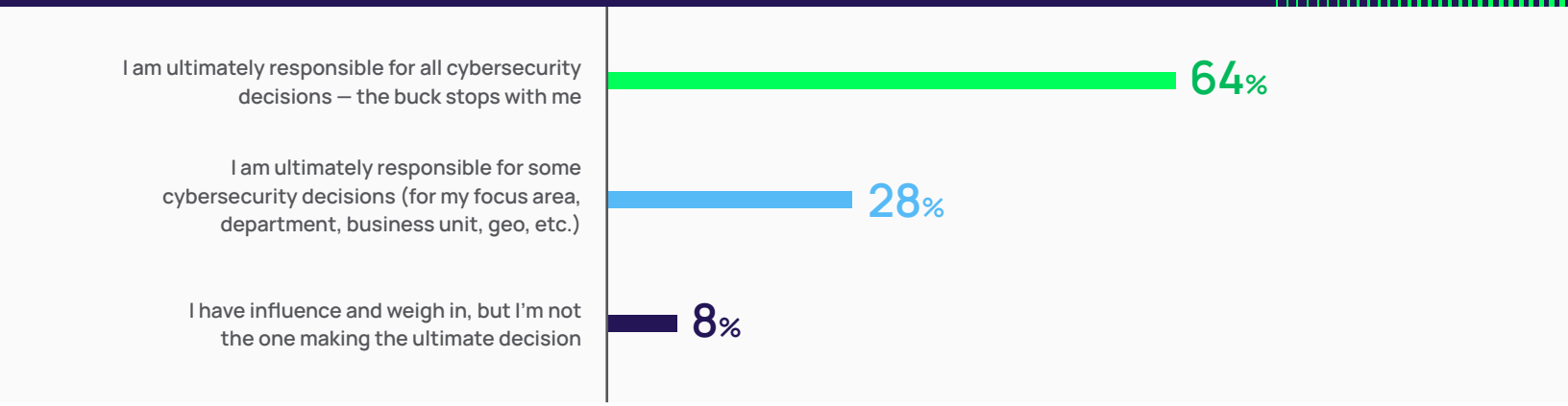
Industry: Which of these best describes your industry sector?



Departments: Which of the following departments do you work within?



Responsibility: To what extent are you responsible for making cybersecurity decisions at your organization?



Delinea

Defining the boundaries of access

Delinea is a leading provider of Privileged Access Management (PAM) solutions for the modern, hybrid enterprise. The Delinea Platform seamlessly extends PAM by providing authorization for all identities, controlling access to an organization's most critical hybrid cloud infrastructure and sensitive data to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide. Our customers range from small businesses to the world's largest financial institutions, intelligence agencies, and critical infrastructure companies. **delinea.com**