kyndryl. | aws

Cyber Gauge 2024: Navigating the complex cybersecurity landscape

About our survey

In partnership with AWS, Kyndryl conducted a survey of decision makers from 600+ organizations with more than 1,000 employees across the US, UK, Canada, Ireland, France, Germany, Spain, Portugal, Australia, New Zealand, India and Japan. The respondents represent seven industries, including banking, financial services and insurance (BFSI), retail, manufacturing, government, communications and media, healthcare and chemicals, and oil and gas.

Our goal was to better understand how prepared large organizations are for fast-changing cybersecurity threats across various industries and geographies.

In this document, we present the key global findings of our survey to address the current state of cyber threats large organizations face, how prepared they feel to mitigate these attacks, the challenges they are currently facing and the actions they can take to ready themselves for the future.

## How are large organizations holding up against cyberattacks?

Global organizations have recently been plagued by an onslaught of cyberattacks ranging from attacks on universities, hospitals, police agencies, banks and more. Over the last 12 months, more than half (54%) of large organizations reported experiencing a cyberattack that disrupted IT systems or data. Of those large organizations that have experienced a cyberattack in the past 12 months, 61% reported four or more attacks.

54% of large organizations reported experiencing a cyber attack that disrupted their IT systems and data in the last 12 months.

Percentage of large organizations that reported experiencing a cyberattack over the last 12 months

54%

Number of reported attacks experienced by large organizations
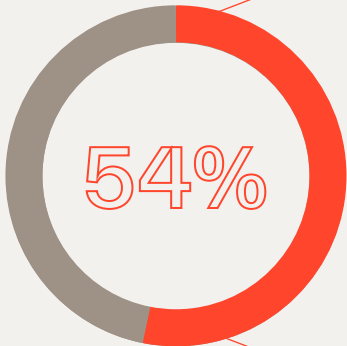
- 38% — 1–3 cyberattacks
- 35% — 4–6 cyberattacks
- 22% — 7–10 cyberattacks
- 4% — More than 10 cyberattacks
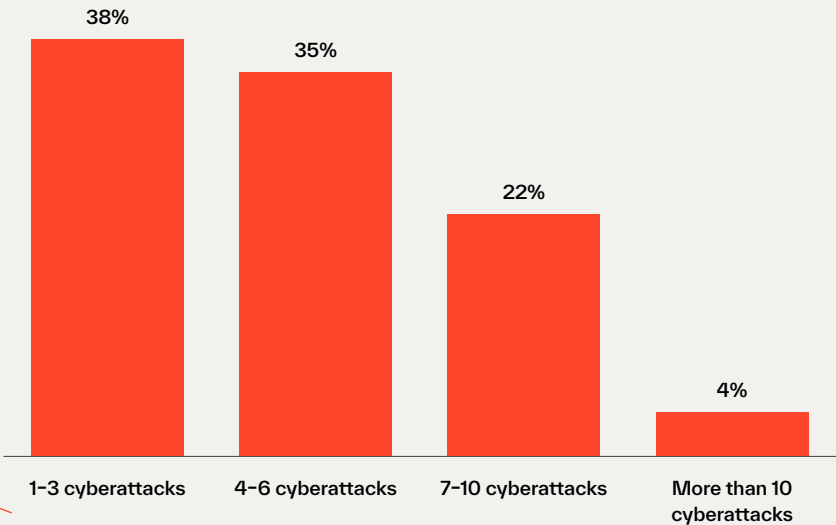
Q: In the past 12 months, has your organization experienced a cyberattack that disrupted your IT systems and or data?
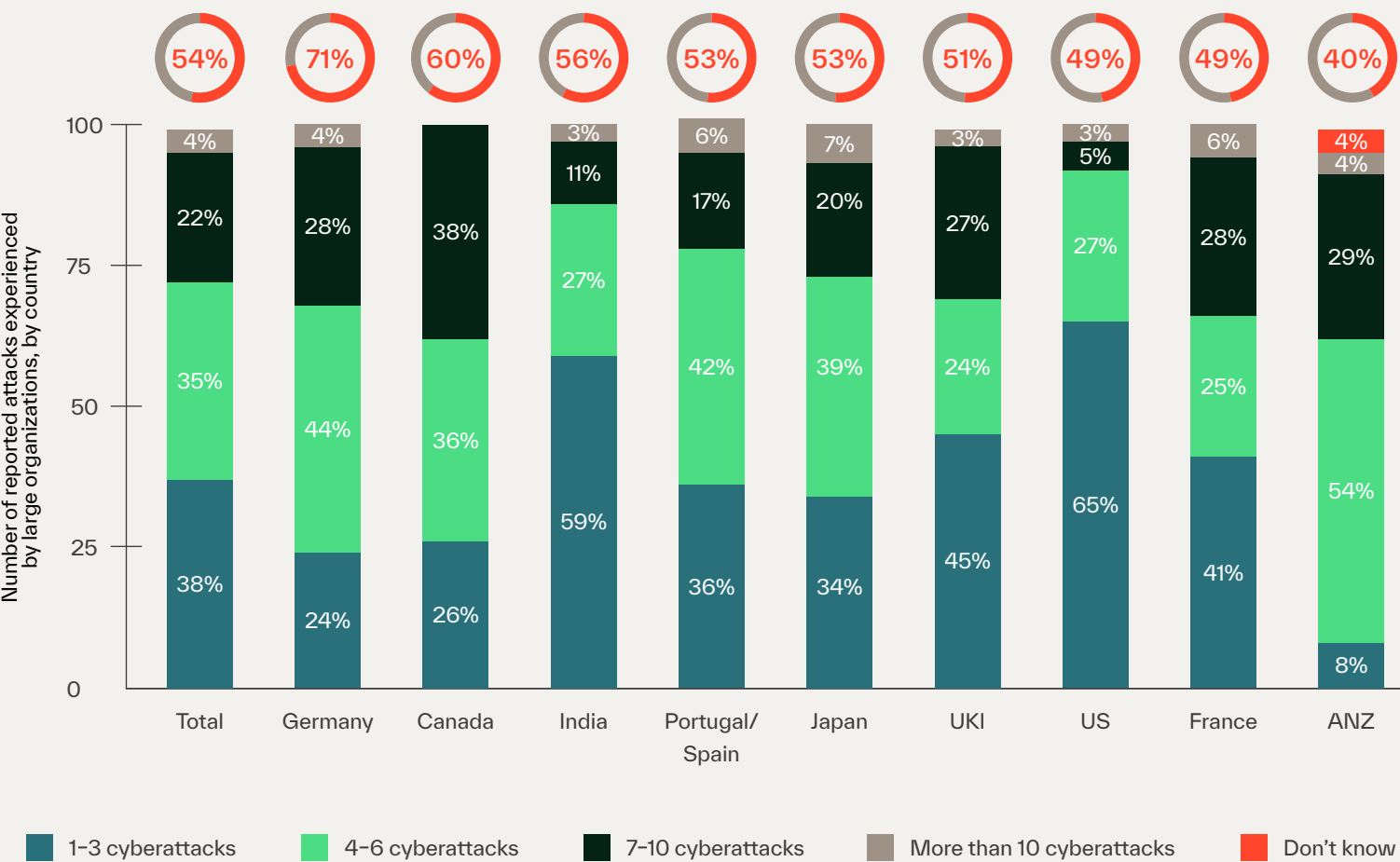
Q: Please estimate how many attacks you have experienced in the past 12 months that disrupted IT systems and data.

By country, 71% of large German organizations reported experiencing an attack in the past 12 months, making Germany the most affected of all the countries surveyed. Canada (60%) and India (56%) rounded out the top three countries affected. While respondents from Australia and New Zealand reported the lowest percentage of cyberattacks (40%), 92% of large organizations in Australia and New Zealand that experienced an attack reported four or more attacks. This finding represented the highest percentage of more than four attacks of all the countries we surveyed.

Germany was the most impacted, followed by Canada and India.

Percentage of large organizations that reported experiencing a cyberattack over the last 12 months, by country

Number of reported attacks experienced by large organizations, by country

Country	1–3 cyberattacks	4–6 cyberattacks	7–10 cyberattacks	More than 10 cyberattacks	Don't know	Overall %
Total	38%	35%	22%	4%		54%
Germany	24%	44%	28%	4%		71%
Canada	26%	36%	38%			60%
India	59%	27%	11%	3%		56%
Portugal/Spain	36%	42%	17%	6%		53%
Japan	34%	39%	20%	7%		53%
UKI	45%	24%	27%	3%		51%
US	65%	27%	5%	3%		49%
France	41%	25%	28%	6%		49%
ANZ	8%	54%	29%	4%	4%	40%

Legend: ■ 1–3 cyberattacks ■ 4–6 cyberattacks ■ 7–10 cyberattacks ■ More than 10 cyberattacks ■ Don't know
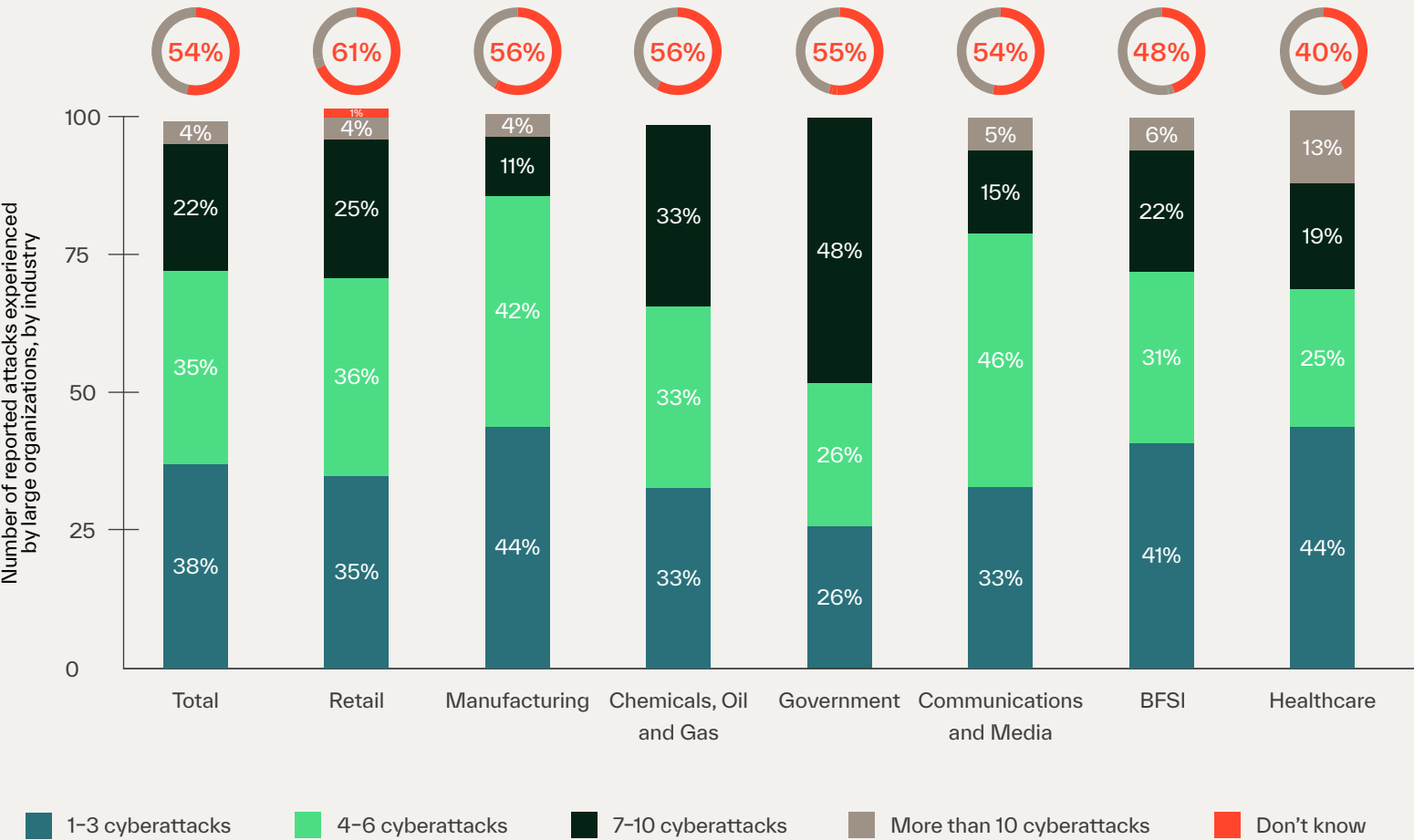
Q: In the past 12 months, has your organization experienced a cyberattack that disrupted your IT systems and or data?
Q: Please estimate how many attacks you have experienced in the past 12 months that disrupted IT systems and data.

3

By industry, large retail (61%), manufacturing (57%) and chemicals, oil and gas (56%) organizations represented the top three industries reporting a cyberattack.

Government organizations reported the highest frequency of cyberattacks with 74% experiencing an attack, reporting four or more attacks.

Retail was the most commonly hit, followed by manufacturing and chemicals, oil and gas.

Percentage of large organizations that reported experiencing a cyberattack over the last 12 months, by country

Number of reported attacks experienced by large organizations, by industry

	Total	Retail	Manufacturing	Chemicals, Oil and Gas	Government	Communications and Media	BFSI	Healthcare
Donut %	54%	61%	56%	56%	55%	54%	48%	40%
More than 10	4%	4%	4%			5%	6%	13%
7-10	22%	25%	11%	33%	48%	15%	22%	19%
4-6	35%	36%	42%	33%	26%	46%	31%	25%
1-3	38%	35%	44%	33%	26%	33%	41%	44%
Don't know		1%						

Legend:
- 1-3 cyberattacks
- 4-6 cyberattacks
- 7-10 cyberattacks
- More than 10 cyberattacks
- Don't know

Q: In the past 12 months, has your organization experienced a cyberattack that disrupted your IT systems and or data?
Q: Please estimate how many attacks you have experienced in the past 12 months that disrupted IT systems and data.
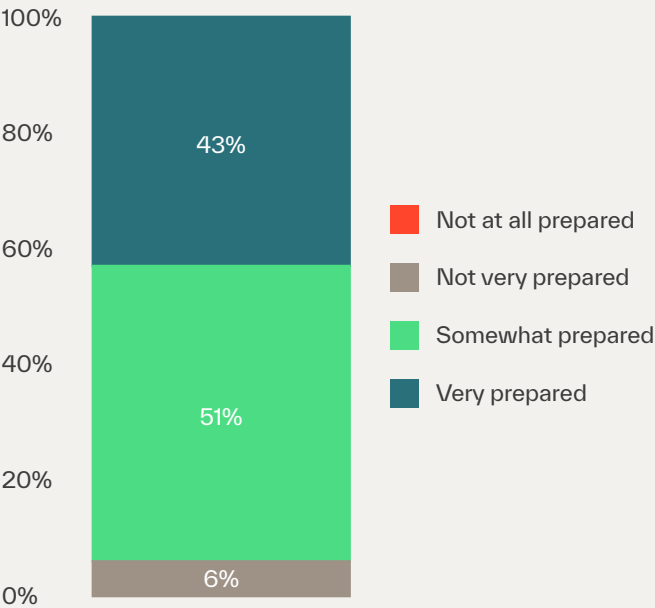
The mixed signals of preparing for cyberattacks

Nearly all (94%) respondents reported their organizations were somewhat (51%) or very (43%) prepared to mitigate potential cyberattacks. In contrast, 71% of those surveyed said their organizations were somewhat (46%) or very (25%) likely to experience a disruptive cyber incident in the next 12 months that will have a meaningful impact on financial performance. Diving deeper into the results, we found 69% of those who said their organizations are very prepared to mitigate an attack thought it was somewhat or very likely that an attack would occur.

The disconnect between perceived ability to mitigate attacks and likelihood of an attack impacting the organization can be explained in two ways. For one, it's common for security leaders to report higher perceived preparedness in surveys. Secondly, many security leaders realize that while they are doing everything in their power to mitigate a potential attack, the likelihood of an attack hitting their organization's expansive IT footprint is somewhat inevitable.
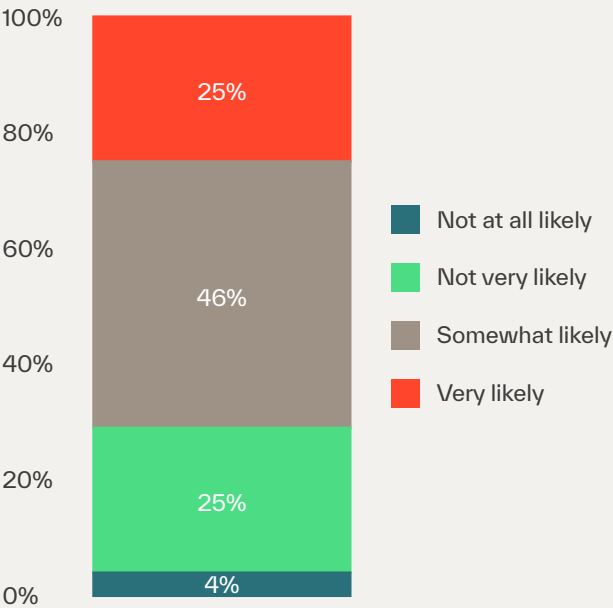
54% of large organizations reported experiencing a cyber attack that disrupted their IT systems and data in the last 12 months.

Self-identified level of preparedness to mitigate potential cyberattacks

Very prepared: 43%
Somewhat prepared: 51%
Not very prepared: 6%

Legend:
- Not at all prepared
- Not very prepared
- Somewhat prepared
- Very prepared

≠

Expected likelihood to experience a disruptive cyber incident in the next 12 months that will meaningfully impact financial performance

Very likely: 25%
Somewhat likely: 46%
Not very likely: 25%
Not at all likely: 4%

Legend:
- Not at all likely
- Not very likely
- Somewhat likely
- Very likely

Q. How prepared do you feel your organization is to mitigate potential cyberattacks?

Q: How likely do you think it is that your organization will experience a disruptive cyber incident in the next 12 months that will have a meaningful impact on your company's financial performance?

Current challenges inhibiting cybersecurity

We sought to better understand the top operational and organizational challenges that large organizations are currently facing to better understand roadblocks inhibiting their ability to mitigate attacks.
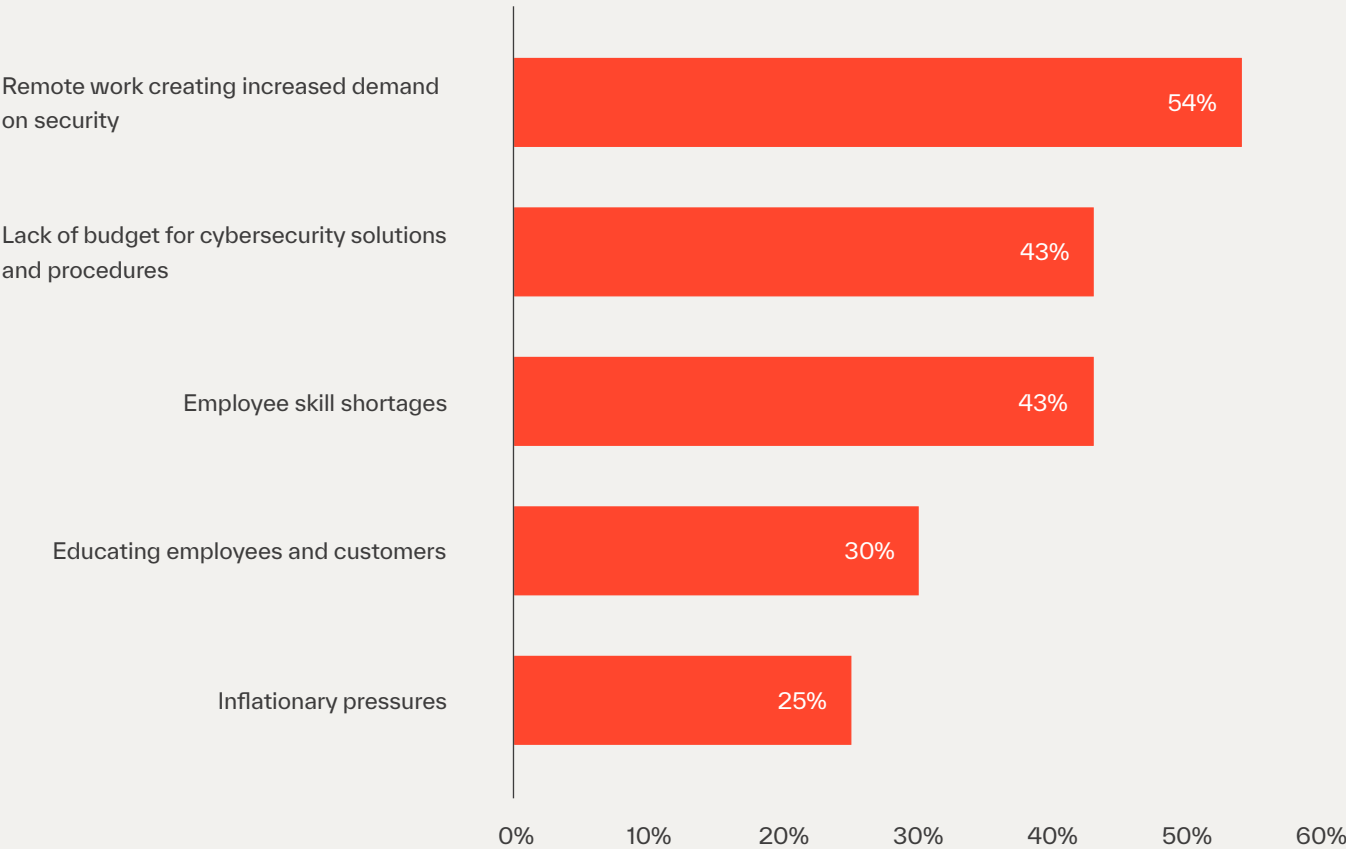
From an organizational perspective, the top challenge reported was remote work creating increased demand on security. This finding shows that although it's been more than four years since the 2020 pandemic drove a massive shift to remote work, security teams are still reeling from the aftereffects and are struggling to catch up.

Tied for second place as the most cited response were security skill shortages and lack of budget for cybersecurity solutions and procedures. Security skill shortages have been a major challenge for organizations for more than a decade. ISC2's 2023 Cybersecurity Workforce Study estimated that there are roughly four million cybersecurity professionals needed worldwide.1

A lack of cybersecurity budget has become increasingly common due to the global economic downturn. Security leaders are facing a higher quantity and complexity of new threats on a daily basis, but budgets to mitigate those risks are not keeping pace. This disconnect results in security leaders becoming shrewder with their investments to ensure they get the maximum return on investment to improve their security posture.

Remote work continues to strain security teams, while talent shortages and budget restrictions all aid to organizational challenges of mitigating security risk.

Top organizational challenges impacting cybersecurity capabilities

Challenge	Percentage
Remote work creating increased demand on security	54%
Lack of budget for cybersecurity solutions and procedures	43%
Employee skill shortages	43%
Educating employees and customers	30%
Inflationary pressures	25%

0%   10%   20%   30%   40%   50%   60%

What are the top organizational or regulatory challenges impacting your organization's cybersecurity capabilities?
Please select up to two.

Beyond organizational challenges, we sought to dive deeper into the operational challenges large organizations are currently facing.
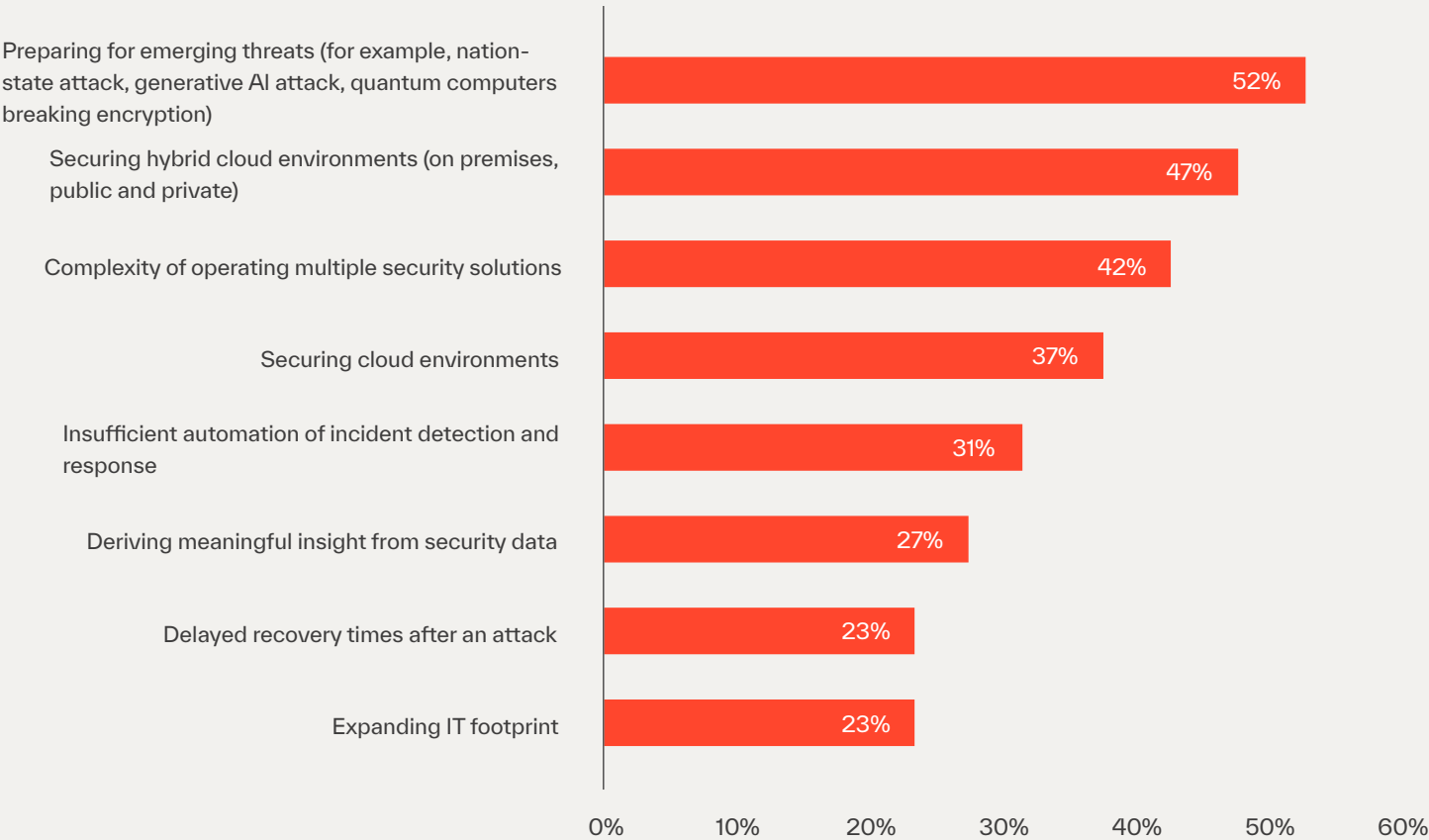
The most cited operational challenge among respondents was preparing for emerging threats (for example, nation-state attacks, generative AI attacks, quantum computers breaking encryption and more). Large organizations are often highly targeted by complex threat actors due to the inherent criticality of what these organizations do (for example, large banks power the world's financial systems and large manufacturers create the world's commodities).

Securing hybrid cloud environments was the second most cited operational challenge, while similarly securing cloud environments was the fourth most cited response. The organizational shift to cloud and building hybrid environments over the last 10+ years added a new vector in need of protection. Many large organizations use multiple cloud providers, each with their own security tools and integrations. Additionally, it can be difficult to maintain visibility and control over cloud data and assets across regions to ensure they remain secure.

The third most cited challenge was the complexity of operating multiple security solutions. As we will discuss in the next section, many large organizations are using dozens of security tools, which is creating fatigue for their security teams.

Emerging threats ranked as the top operational security challenge, followed by complexity of operating multiple security solutions.

Top operational cybersecurity challenges of organizations

Challenge	Percentage
Preparing for emerging threats (for example, nation-state attack, generative AI attack, quantum computers breaking encryption)	52%
Securing hybrid cloud environments (on premises, public and private)	47%
Complexity of operating multiple security solutions	42%
Securing cloud environments	37%
Insufficient automation of incident detection and response	31%
Deriving meaningful insight from security data	27%
Delayed recovery times after an attack	23%
Expanding IT footprint	23%

What are the top operational cybersecurity challenges your organization is currently facing? Please select up to three.

The complexity of today's security toolsets

We sought to dive deeper into the challenge of operating multiple security solutions by asking respondents to rate how challenging it was to manage their security toolset today. In total, 83% reported managing security toolsets was a challenge for their organization.

To get a baseline, we asked respondents how many security vendors and tools they were currently using. 63% of large organizations reported they were using six or more security vendors, while 42% reported using more than 20 security tools.
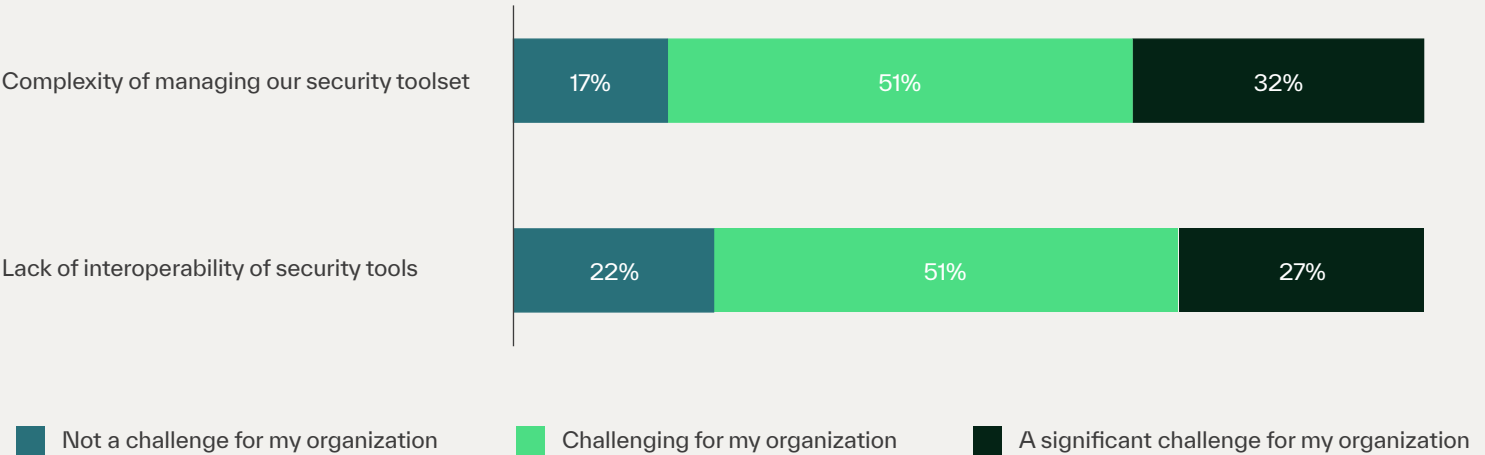
At face value, more security tools means more capabilities available to security teams. In fact, 52% of respondents indicated they plan to increase the number of tools they use over the next year. However, adding more tools will likely exacerbate the challenge of managing security toolsets.

Our survey found 78% of respondents indicated it was a challenge (51%) or significant challenge (27%) for security tools to be interoperable, meaning their security tools are often unable to share security data or insights. This lack of integration often creates a challenge that forces security teams to switch between tools and try to glean important insights on their own—leading to blind spots, inefficiencies and inconsistencies in security operations, which can strain already limited budgets and staffing resources.

Organizations find it challenging to mange their complex toolset that they report lacks interoperability.

Security toolset challenges

Category	Not a challenge	Challenging	Significant challenge
Complexity of managing our security toolset	17%	51%	32%
Lack of interoperability of security tools	22%	51%	27%

- Not a challenge for my organization
- Challenging for my organization
- A significant challenge for my organization

Q: Thinking about your organization's current cybersecurity capabilities, please rate the degree to which each of the following are a challenge for your organization.
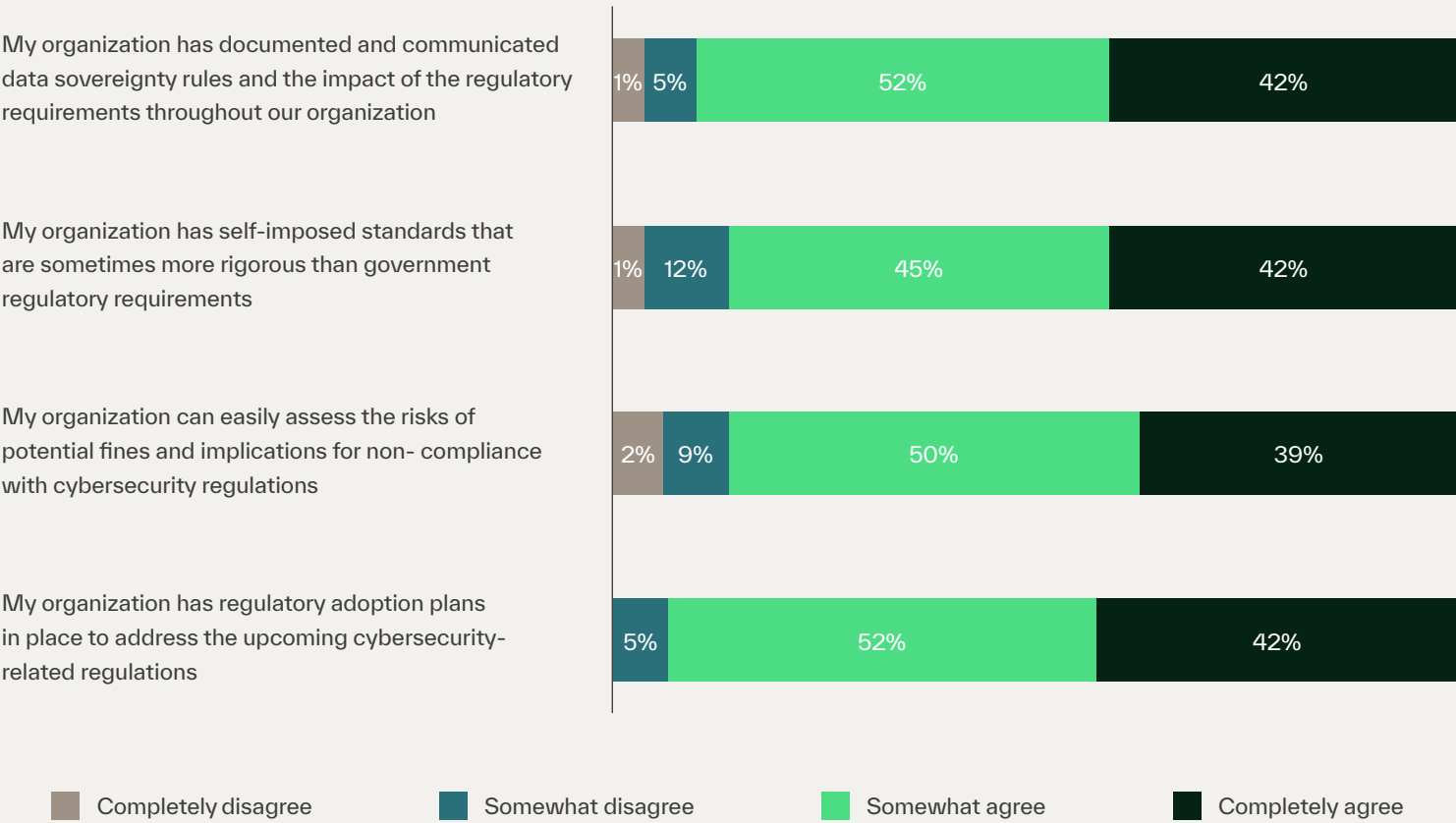
The lack of alignment and the role of regulations

In recent years, regulators have been increasing pressure on organizations to improve overall cyber resilience—the ability to anticipate, protect against, withstand and recover from a disruption. For example, in the US, the Securities and Exchange Commission (SEC) requires publicly traded organizations to disclose material cyberattacks, while in the EU, the Digital Operational Resilience Act (DORA) and NIS2 are focused on ensuring critical business processes are protected and can operate in the wake of IT disruption.

Overall, respondents reported confidence in their ability to handle changing regulatory dynamics. 94% of respondents either somewhat (52%) or completely (42%) agreed that their organization has regulatory adoption plans in place to address upcoming cybersecurity-related regulations. Furthermore, 87% agreed that their organization has self-imposed standards that are sometimes more rigorous than government regulatory requirements.

Large organizations report high confidence in their ability to prepare for the changing regulatory landscape.

Cyber regulatory preparedness

Statement	Completely disagree	Somewhat disagree	Somewhat agree	Completely agree
My organization has documented and communicated data sovereignty rules and the impact of the regulatory requirements throughout our organization	1%	5%	52%	42%
My organization has self-imposed standards that are sometimes more rigorous than government regulatory requirements	1%	12%	45%	42%
My organization can easily assess the risks of potential fines and implications for non- compliance with cybersecurity regulations	2%	9%	50%	39%
My organization has regulatory adoption plans in place to address the upcoming cybersecurity-related regulations		5%	52%	42%

■ Completely disagree ■ Somewhat disagree ■ Somewhat agree ■ Completely agree

Q: Many companies say they are experiencing increasingly rigorous cybersecurity-related regulations around the world (for example, SEC Cybersecurity Disclosure Mandate, DORA/NIS2, and more). Please rate how much you agree or disagree with the following statements.

Similar to the disconnect between perceived preparation and likelihood of attacks, we found an intriguing disconnect between perceived regulatory preparation and the ability to comply.
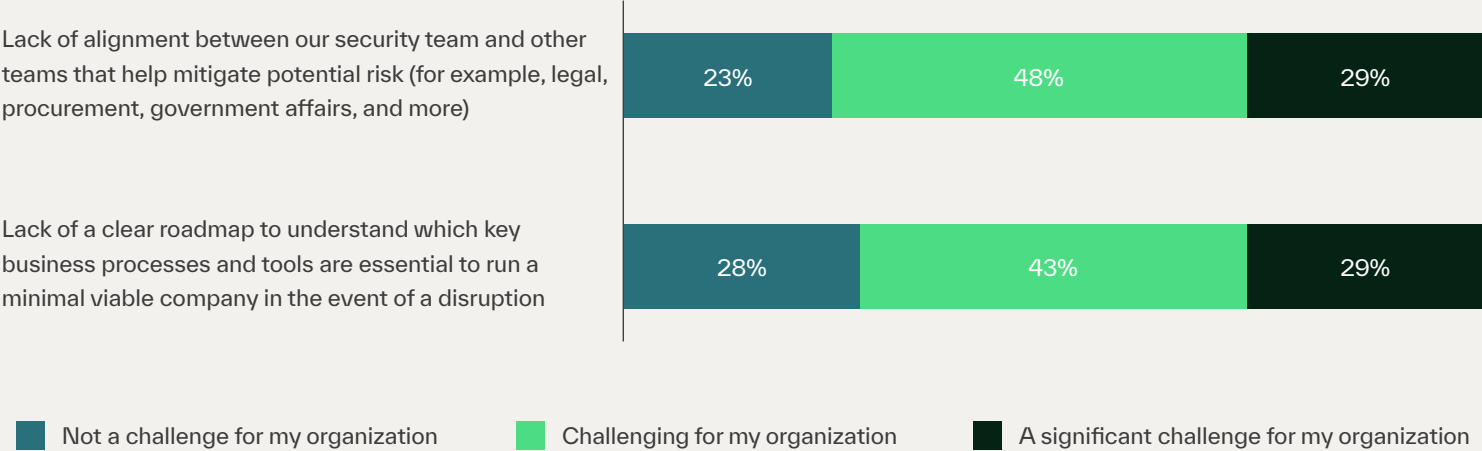
At their core, new cyber regulations require organizations to shift their teams' alignment across the different functions of their overall risk teams (for example, legal, procurement, operations and more) into a cohesive function. Simultaneously, they require a clear roadmap to understand which business processes and tools are essential in their operations. Enabling better alignment between teams and business processes helps reduce the potential for catastrophic fallout from an attack.

However, at present, many organizations are still struggling to align their risk teams and create a clear roadmap to understand which key business processes and tools are essential to run their minimum viable company in the event of a disruption. Our survey found 77% indicated alignment was either challenging (48%) or a significant challenge (29%), while 72% indicated a lack of a clear roadmap was either challenging (43%) or a significant challenge (29%).

Organizations report a lack of alignment between teams and a clear roadmap.

Alignment and roadmap

	Not a challenge	Challenging	Significant challenge
Lack of alignment between our security team and other teams that help mitigate potential risk (for example, legal, procurement, government affairs, and more)	23%	48%	29%
Lack of a clear roadmap to understand which key business processes and tools are essential to run a minimal viable company in the event of a disruption	28%	43%	29%

- Not a challenge for my organization
- Challenging for my organization
- A significant challenge for my organization

Q: Thinking about your organization's current cybersecurity capabilities, please rate the degree to which each of the following are a challenge for your organization.

Gaining the support of business leaders

The frequency and publicity of cyberattacks, coupled with the changing regulatory landscape, has resulted in business leaders becoming more cognizant of the cyber risk their organizations face. However, as mentioned earlier, the number two most cited organizational challenge was a lack of budget for security tools and solutions. Attaining this budget to ready and protect the organization requires support from business leaders.

Unfortunately, 69% of respondents reported a lack of support from business leaders for the security measures to protect their organization. Additionally, 73% of security leaders reported that their board of directors does not take an active interest in their organization's security readiness.

For many business leaders, dedicating funds to improve their organization's cybersecurity comes down to return on investment. One of the emerging ways security leaders can help gain buy-in from business leaders and the board is to quantify the cyber risk if their organization does not take action. This framing can help simplify cybersecurity projects in a tangible way that business leaders can easily understand. However, we found 80% of large organizations reported quantifying the potential impact of a cyberattack as another challenge.

Security leaders find it challenging to get the support from their business leaders and BoD to protect their organization.

Executive buy-in and ability to quantify risk

	Not a challenge	Challenging	Significant challenge
Lack of support from business leaders regarding the security measures necessary to protect my organization	32%	40%	29%
Our board of directors does not take an active interest in my organization's security readiness	37%	38%	25%
Lack of ability to quantify the impact a cyberattack could have	21%	51%	29%

- Not a challenge for my organization
- Challenging for my organization
- A significant challenge for my organization

Q: Thinking about your organization's current cybersecurity capabilities, please rate the degree to which each of the following are a challenge for your organization.

Action items and next steps

Based on the findings from our survey, here are key action items large organizations may find valuable to take:

1. **Align risk teams and strategize for risks and regulations ahead.** While our survey found large organizations felt prepared for attacks, they also felt that an attack impacting their organization's financials was highly likely. Diving deeper, a major challenge the survey highlighted was aligning the teams responsible for the organization's risk and having a clear strategy for risks ahead—such as emerging threats, which ranked as the top operational challenge. We recommend organizations take a step back and assess security risk through the broader lens of the business. For example, it's important to map IT assets to critical business processes to ensure that if that IT asset were disrupted by a cyber event, the organization understands the overall risk from a legal, regulatory and business perspective.

2. **Re-evaluate and centralize toolsets to optimize security spend.** Large organizations reported a high number of tools and vendors in use and said that managing these security tools is a complex challenge. An over-abundance of tools can fatigue security teams, causing these tools to lose their value to the organization. To better optimize security tool spending, security leaders can find value in assessing security tools currently in use and analyzing their capabilities. They will likely find overlapping capabilities, which can help drive better decisions for security spend. Additionally, security leaders may find value in consolidating tools into a centralized platform that enhances the overall productivity of the security team through a single-pane-of-glass view versus switching between various toolsets.

3. **Gain buy-in from executives through risk quantification.** Our survey found that gaining business leader and board-level support for security is a major challenge. To obtain this buy-in, security leaders are likely to find value in strong risk quantification tools and support that bridges the gap by translating the impact of a cyber event into real dollars. This quantification will help business leaders understand the potential impact and make strategic decisions to help security teams mitigate damage.

kyndryl. | **aws**

1 *How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce 2023*, ISC2, 2023