REPORT

proofpoint.

2021 VOICE OF THE CISO REPORT

TABLE OF CONTENTS

2021: THE AFTERMATH OF A YEAR LIKE NO OTHER

There's no question that 2020 was a challenging year – for organizations and individuals alike. The pandemic placed an enormous strain on the global economy, and cybercriminals took advantage of this disruption to accelerate their nefarious activities.

We were inundated with cyberattacks, both new and familiar, from pandemic-themed phishing scams to the unwavering march of ransomware. The conclusion of 2020 dealt a final blow with the SolarWinds hack, which highlighted supply chain and ecosystem vulnerabilities. With thousands of organizations impacted, what has been dubbed "the most sophisticated attack the world has ever seen" has reignited the "assume compromise" philosophy among CISOs.

Compounding our challenge, all of this occurred while we transitioned to working from home on a grand scale, literally overnight. Cybersecurity teams around the world were challenged to shore-up their security posture in this new and changing environment, attempting to pull off a balancing act between supporting remote work and avoiding business interruption, while keeping businesses secure.

With work becoming increasingly flexible, this challenge now extends into the future. In addition to securing many more points of attack and educating users on long-term remote and hybrid work, CISOs must instill confidence among customers, internal stakeholders, and the market that such setups are workable indefinitely.

In order to gauge the mood of the industry during this pivotal time, Proofpoint surveyed 1,400 CISOs from around the world and invited them to share their first-hand experiences during the past 12 months and offer their insights for the next two years.

This report contains a summary of our findings. We explore how CISOs face a constant barrage of attacks from all angles and how they are preparing for the challenges of a hybrid workforce. We look at why human error continues to be a key vulnerability and what role cybersecurity awareness training needs to play.

We also examine the changing role and growing expectations of the CISO. Are they equipped to handle these new demands? And, what more can organizations do to help users and the cybersecurity teams tasked with their protection?

This report would not have been possible without the participation of cybersecurity and information security practitioners across the globe. Thank you for your insights and feedback.

Lucia Milică,
Global Resident Chief Information Security Officer at Proofpoint

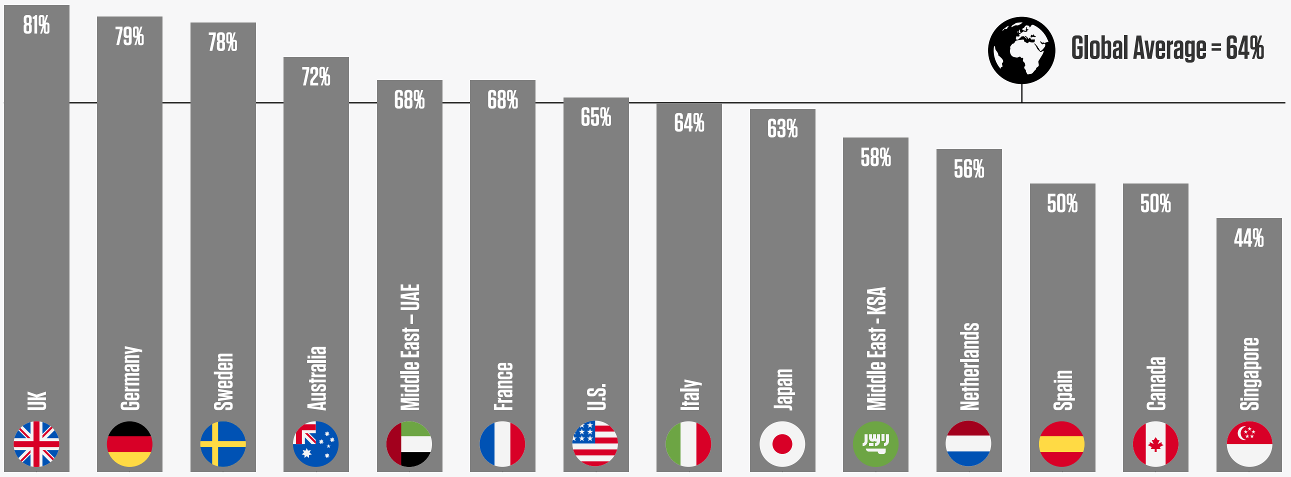
CHAPTER 1: FACING A DYNAMIC THREAT LANDSCAPE

Organizations around the world feel vulnerable in the aftermath of 2020. Almost two-thirds of surveyed CISOs believe they are at risk of suffering a material cyberattack within the next 12 months. Of these, one in five believes this risk to be very high.

That CISOs consider the risk of cyberattack to be high may be unsurprising. Cybercriminals are relentless, and CISOs know better than to be complacent, especially in the aftermath of the most disruptive year in recent memory.

64% of surveyed CISOs feel their organization is at risk of suffering a material cyberattack in the next 12 months. 20% rate the risk as very high.

Percentage of CISOs in agreement that their organization is at risk of a material cyber attack in the next 12 months



UK (**81%**) and German (**79%**) CISOs are most worried about experiencing a material cyberattack.

Fifty percent of Canadian CISOs fear that their company is very or somewhat likely to experience an attack.

Only **44%** of CISOs from Singapore agree with the statement, making them the most optimistic of all regions surveyed.

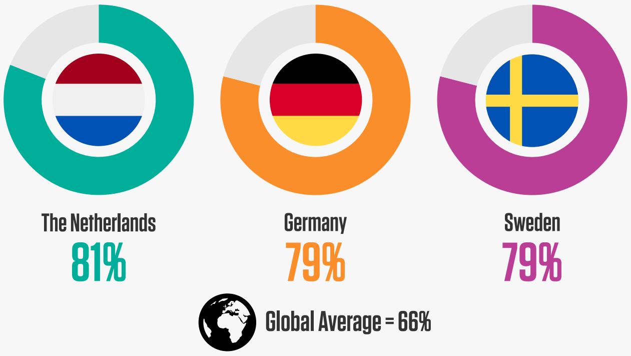
83% of CISOs from retail companies rate the cyberattack risks on their organizations as likely, the highest amongst all surveyed verticals.

The public sector is most optimistic amongst all surveyed verticals: **24%** of respondents feel it is unlikely that attacks on their organizations will cause material damage - **10 percentage points** higher than the average at **14%**.

What should concern all business leaders is the finding that **66%** of CISOs do not believe that their organization is prepared to cope with an attack. CISOs from the Netherlands (**81%**) feel least prepared for a cyberattack, followed by Germany and Sweden (**79%**).

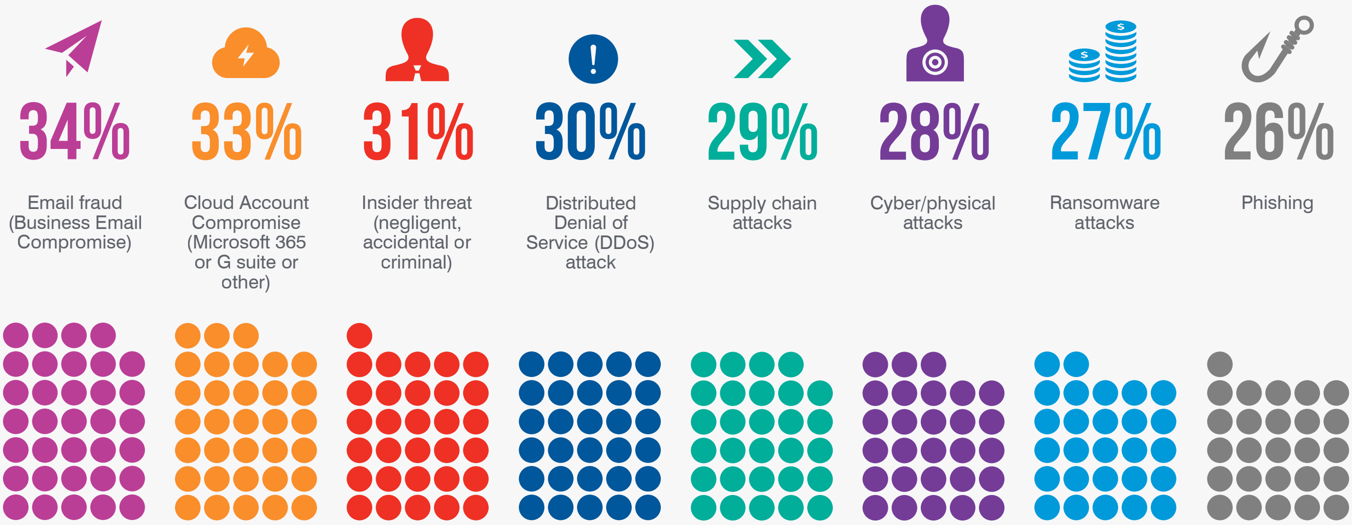
This disconnect between perceived risk levels and preparedness is the most pressing concern keeping cybersecurity teams up at night. At the heart of the issue is a struggle to pinpoint which of the many common threats is most likely to strike first.

My organization is unprepared to cope with a targeted cyberattack in 2021 – Top 3 countries



The attacks most causing concern are Business Email Compromise (BEC) (**34%**) and Cloud Account Compromise (**33%**), followed by insider threats (**31%**).

Perceived Biggest Cybersecurity Threats in the Next Year



Business Email Compromise

12 out of 14 surveyed countries consider BEC a **top 3 risk**.

BEC is considered the **number 1** risk in Canada, Sweden, Spain, and Japan.

Cloud Account Compromise

10 out of 14 surveyed countries consider Cloud Account Compromise a **top 3 risk**.

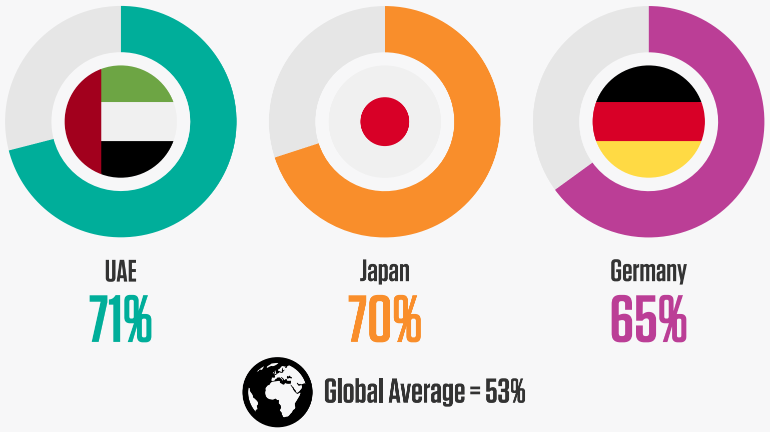
Cloud Account Compromise is the **number 1** risk in the U.S., France, Italy, and Saudi Arabia (KSA).

In the U.S., the greatest concerns are cloud account compromise (**39%**), followed by supply chain attacks (**38%**), and insider threats and cyber/physical attacks (both **37%**).

When on high alert for a range of threats, CISOs are in a constant state of flux, tasked with implementing comprehensive defenses against varying methods of attack. This makes it increasingly difficult to prioritize an adequate response.

While technical controls may offer broad protection against common threats, user security training must be targeted to avoid information overload. However, this isn't possible when CISOs are unsure exactly where the next attack is coming from.

I am more concerned about the repercussions of a cyberattack in 2021 than I was in 2020 – Top 3 countries



This level of uncertainty is an understandable response to the past 12 months. A year of constant disruption made it near impossible for any organization to identify and rank threats and implement adequate defenses.

Hastily deployed remote environments, users distracted by home working and the malaise of a global pandemic, and a network of cybercriminals exploiting the situation ensured that, for most, coherent strategy made way for ad hoc firefighting.

This is best encapsulated in most CISOs' belief that, despite strengthening defenses in 2020, they have gone backwards in terms of security and peace of mind.

Over half of CISOs are more concerned about the repercussions of a cyberattack in 2021 than they were in 2020 – with one in four strongly in agreement.

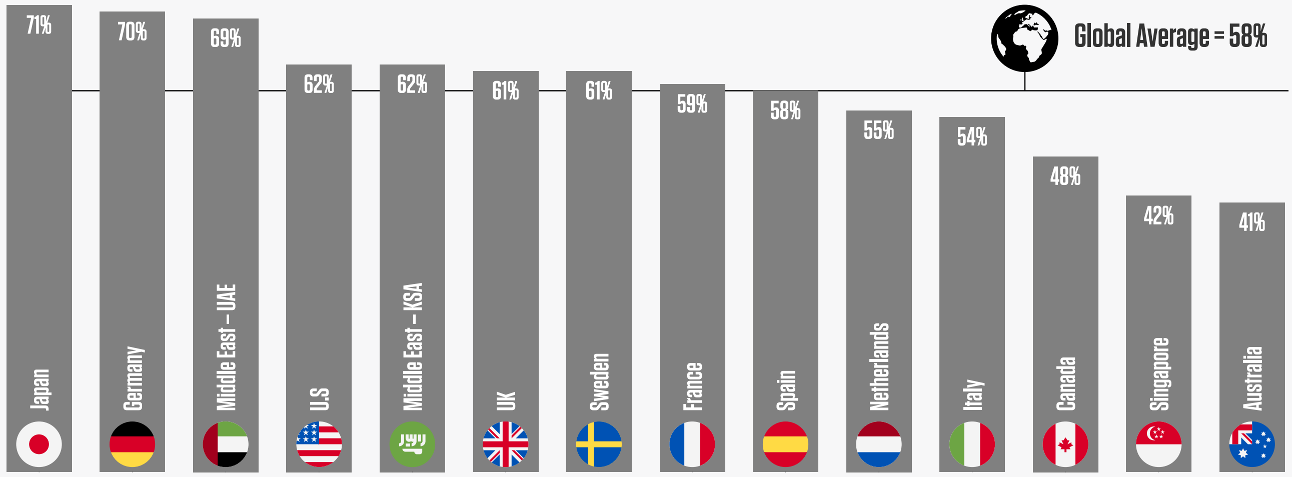
Over half of CISOs are more concerned about the repercussions of a cyberattack in 2021 than they were in 2020 – with one in four strongly in agreement.

> *As security leaders, we continuously re-evaluate the effectiveness of our controls in order to identify new gaps and mitigate risk. Security automation and orchestration, as well as consolidating redundant tools are some of the priorities that enable us to drive operational efficiencies in our organizations.*
>
> **Krishnan Chellakarai, CISO, Gilead**

CHAPTER 2: TECHNOLOGICAL VERSUS HUMAN VULNERABILITY

Despite the distraction and disruption of 2020, most CISOs believe that employees understand the role they play in protecting their organizations against cyber threats. Over half (**58%**) agree with this statement, with about a quarter (**26%**) in strong agreement.

Percentage of CISOs believing that employees understand their role in protecting the organization against cyber threats

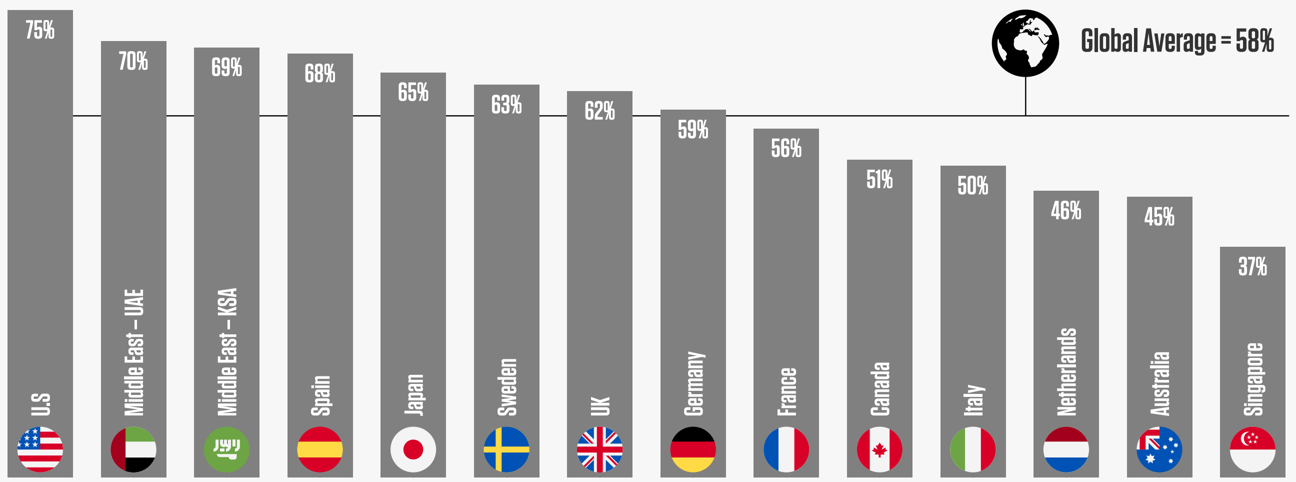


However, this belief is at odds with the view of most CISOs that human error is their organization's biggest cyber vulnerability. This raises several red flags. For one, that so many CISOs believe employees understand their role but still pose a risk suggests an acknowledgement that end users are not adequately skilled or equipped for cyber defense.

58% of CISOs believe employees understand their role in protecting against cyber threats, yet also pose the biggest risk.

> *Attackers used to focus on exploiting infrastructure. Now they target people. Our focus has shifted to protecting people, which illustrates the changing boundary of security. That boundary has gotten very personal, very quickly.*
>
> **Seth Edgar, CISO, Michigan State University**

Percentage of CISOs in agreement that human error is their organization's biggest cyber vulnerability



We know that more than **90%** of successful cyberattacks require some level of human interaction. Many CISOs, therefore, significantly underestimate the degree of risk posed by their users. Only **37%** of Singapore CISOs consider their employees to be their biggest cyber vulnerability, followed by Australia (**45%**) and the Netherlands (**46%**).

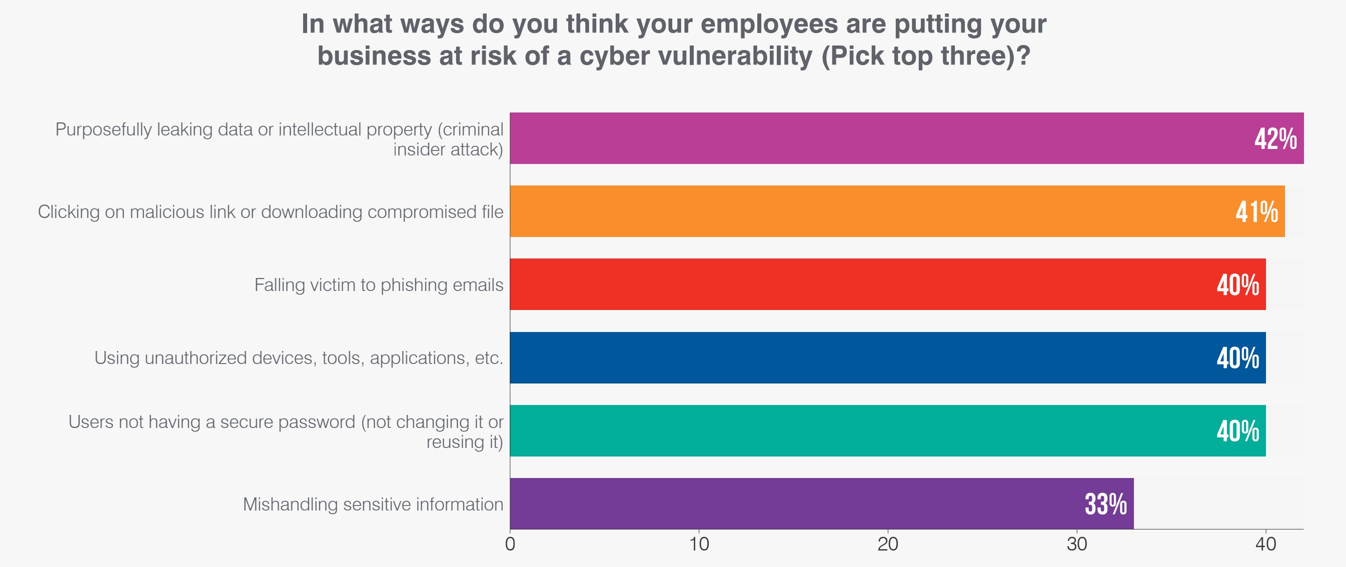
73% of CISOs from the retail sector consider human error as their organization's biggest cyber risk.

Financial services CISOs agreed with their retail peers with **61%**.

Global CISO from the public sector, education, and healthcare sectors seem to have a low level of awareness when it comes to human error and cyber risk with **54%**, **53%**, and only **48%** respectively.

Of those who believe employees are the greatest threat to security, there are several issues causing concern. But, as is the case with external attacks, CISOs face a struggle to pinpoint which potential threat poses the highest risk.

Intentional foul play is the most pressing concern for most, with **42%** believing that the purposeful leaking of data or IP is the biggest threat posed by employees. Negligent threats also rank high: **41%** fear that users will click on malicious links or download compromised files, while **40%** are wary of phishing, the use of unauthorized applications, and poor password hygiene.



Concern about user vulnerability is highest in France. **65%** of CISOs worry about users' password hygiene, and **52%** fear the purposeful leaking of data and phishing attacks.

Security concerns are not based solely on the human element of our defenses. Many of the world's CISOs also have similar misgivings over technical protections.

Fewer than two-thirds are confident that their organization has the capability to detect a cyberattack or data breach. This leaves many feeling both unprepared and ill-equipped for the modern threat landscape.

A major reason for this lack of confidence appears to be the patchwork approach to cybersecurity in recent years. An approach that was exacerbated by last year's rush to deploy and secure remote environments, often without adequate training or technical protections.

This is likely why two in three CISOs believe technical debt to be a significant cause of security vulnerability, with one in three strongly agreeing with this position.

Technical debt concerns **74%** of CISOs in the UK, followed by Germany (**71%**), Middle East (**71%**), and Australia (**71%**).

Unfortunately, making up the lost ground between good and good enough security won't be easy. There is a shared belief among CISOs and cybersecurity teams (**61%**) that increasing security to the level required for the modern threat landscape will negatively impact performance and business agility.

Only **1%** of CISOs strongly disagree that increased security impacts agility, confirming that there is always a perceived trade-off between the two.

CHAPTER 3: LONG TERM HYBRID WORKING: A SEISMIC SHIFT FOR CYBERSECURITY

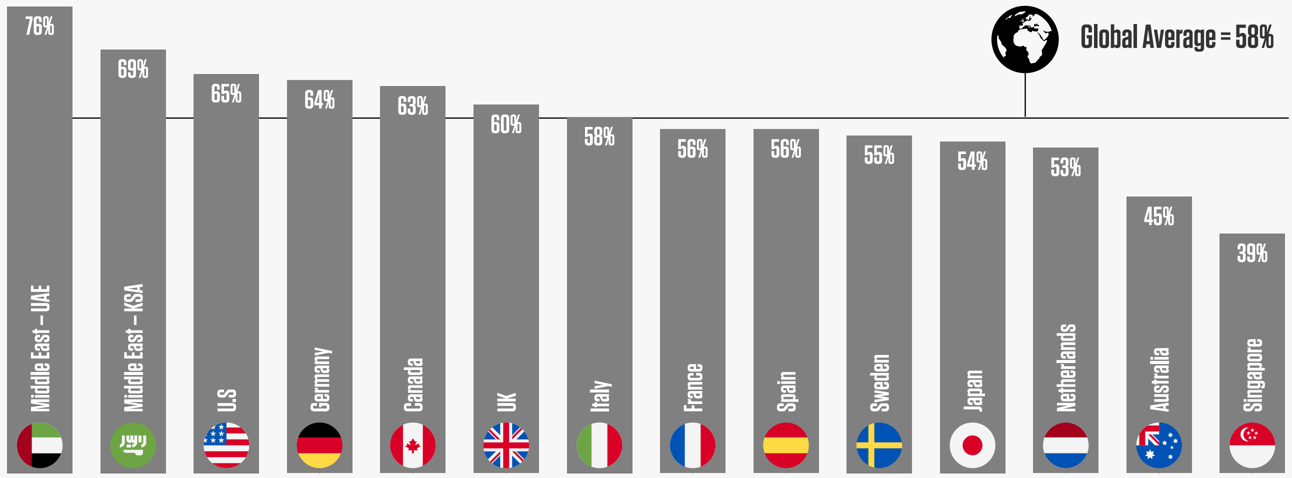
The CISO's ability to balance the interests of agility and security will take on increasing importance in the future. As more organizations have seen what remote working offers from a cost-saving and flexibility point of view, many will now look to adopt this approach with hybrid models.

This challenges the CISO to convince their boardroom that the "good enough" approach of the past 12 months will not work in the long term. There's plenty of evidence to bolster this point of view.

Almost two in three CISOs across all regions agree that remote working makes their organization more vulnerable to cyberattack. As the same number report an increase in targeted attacks since the mass rollout of remote working, it's easy to see why they share this opinion.

58% of CISOs have seen more targeted attacks since enabling widespread remote working

Percentage of CISOs saying their business has seen more targeted attacks since enabling widespread remote working



A staggering **69%** of CISOs from companies with 5,000+ employees said their workforce had been targeted more since they started remote working. The most impacted industries include IT, technology, and telecoms (**69%**).

CISOs in the Middle East – UAE (**76%**) and KSA (**69%**) – have seen the biggest increase in targeted attacks since switching to widespread remote working.

In Singapore, on the other hand, only **39%** of CISOs report more targeted attacks. The number is also below average in Australia (**45%**).

A greater reliance on home networks, a need to prioritize continuity over security, and a rapid increase in points of attack will always make an organization more vulnerable to cyber threats.

However, many other factors also add to concerns around remote working. For more than half (**56%**) of surveyed CISOs, allowing remote access to company information negatively impacts their ability to manage the control and classification of sensitive business data.

Slightly more, **58%**, said that staff using personal IT equipment increases the risk of data breaches.

User preparedness is also a cause for concern. Working from home brings with it many security implications. The use of personal networks or devices, added distractions, and less formal surroundings call for heightened protections that many do not have in place. Forty percent of CISOs state that their employees are not appropriately equipped to work remotely.

In response to the longevity of the new and enforced working environment, **57%** of companies have strengthened the security policies put in place at the beginning of the pandemic. However, with business unlikely to ever return to “normal,” further strengthening is mandatory.

> *The global pandemic has necessitated a re-evaluation of security programs across many industries and mandated changes in policies and technologies. The network edge has become a fluid entity that follows every remote worker. As security professionals, we have to remain nimble to respond to the evolving attack surface, dynamic ransomware and evolving insider threats.*
>
> **Martin Littmann**
> **CTO and CISO at Kelsey-Seybold Clinic**

German CISOs are most satisfied with the impact of their updated security policies, with **72%** agreeing that they have strengthened their ongoing support of remote work in 2021. They are closely followed by CISOs from the UAE (**69%**) and Spain (**66%**).

Singapore and Canadian CISOs, however, are least in agreement, with only **40%** and **43%** respectively agreeing that they have strengthened their security posture to better support remote working.

CHAPTER 4: A POSITIVE OUTLOOK INTO 2022/2023

Despite widespread acknowledgement of the struggle to stay secure last year, most CISOs are hopeful in their outlook for the years ahead. Assuming appropriate strengthening and strategizing, two in three (**65%**) CISOs worldwide believe they will be better able to resist and recover from cyberattacks by 2022/23.

This optimism is felt more keenly across certain industries.

Almost three-quarters (**74%**) of CISOs in retail are confident they will be better positioned to battle cyberattacks by 2023. Among those less hopeful are CISOs in transport and media (both **56%**).

CISOs in the UAE (**77%**), Germany (**76%**), and the U.S. (**73%**) either strongly or somewhat agree that organizations will be better able to resist and recover within two years.

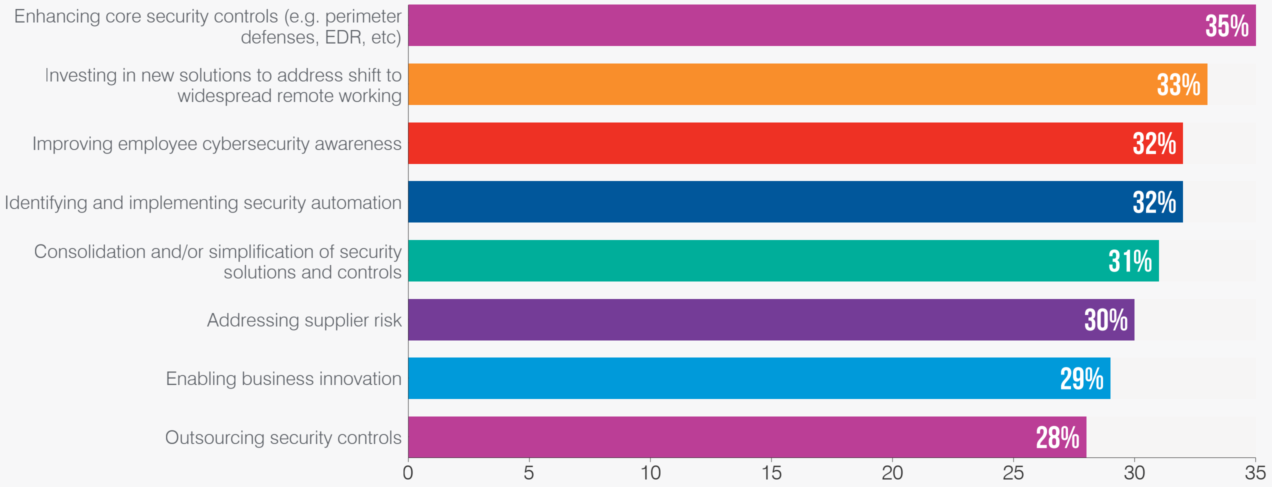
In France, **25%** disagree with such optimism, the highest number by far overall.

Disagreement is lowest in the U.S. (**3%**), Spain (**4%**) and the UK (**5%**).

For most CISOs, efforts to adapt to the new way of working and the evolving threat landscape will focus on four key areas.

Almost two-thirds of CISOs intend to enhance core security controls (**35%**), support remote working (**33%**), improve security automation (**32%**), and increase security awareness (**32%**). Enabling further business innovation and outsourcing security controls is of lesser concern.

What are the top priorities for your organization's IT security department over the next two years? (Select up to three)



Naturally, these priorities differ across industries and organizations. Many larger companies (**47%**), those with 5,000+ employees, are focused on supporting remote and hybrid working. For those in financial services and manufacturing, security awareness is the most pressing concern. Conversely, mitigating supplier risk is the top priority in the public sector.

The UK's top priority is educating their users – **44%** said security awareness was key.

Addressing supplier risk is of most concern to North American CISOs. In Canada, **39%** of CISOs list it as a top priority, while **37%** of U.S. CISOs agree it is a top concern their team will be addressing in the next two years.

Efficiency is top of mind for CISOs in Germany. Their top priority is security automation (**39%**), followed by consolidation and simplification of security solutions and controls.

The majority expect to see cybersecurity budgets increase by at least **11%** over the next two years to support this process. While this news is certainly positive, it is disconcerting to learn that almost a third (**32%**) are expecting budgets to decrease between now and 2023.

> *The global pandemic has brought the topics of business resilience and cyber security into very sharp focus. I have received both strong engagement and unequivocal support from my board as we have worked to adapt our security posture to dynamically balance risk and reward during the emergency. Maintaining safe business operations and supporting our displaced workforce across a now amorphous corporate perimeter has become both business critical and strategically significant.*
>
> **Paul Watts**
> **Group CISO at Kantar**

Larger budgets are not the only reason behind the collective optimism of the world's CISOs. There is a common view, held by **64%** of respondents, that public awareness of cybersecurity risks will increase in the future. There is also a belief that cybersecurity regulations will become more specific and less outcome-based.

This bright outlook for the immediate future appears warranted. Tighter, more manageable regulation, increased user awareness, and bolstered technical controls should all increase organizational security.

However, the outlook is somewhat bleaker for the organizations that fail to adapt to the new normal. 2020 was a bumper year for cybercriminals, and they are more emboldened than ever in their efforts to harm organizations around the world.

So much so that two-thirds (**63%**) of CISOs believe that cyber-crime will be even more profitable over the next two years, and those that fall victim may suffer even greater consequences. **61%** of CISOs believe that organizational penalties for being breached will increase in 2022 and 2023.

More than two-thirds of UAE (**76%**) and German (**73%**) CISOs agree that penalties for breaches will likely grow.

Agreement with this statement is lowest in Singapore (**47%**) and Sweden, where just **34%** of CISOs strongly agree.

CHAPTER 5: CISO SATISFACTION, CHALLENGES, AND EXPECTATIONS

The lasting impact of cybersecurity in 2020 is the elevated importance of the CISO. The incredible demands of the past year encouraged CISOs to make their voices heard, loud and clear.

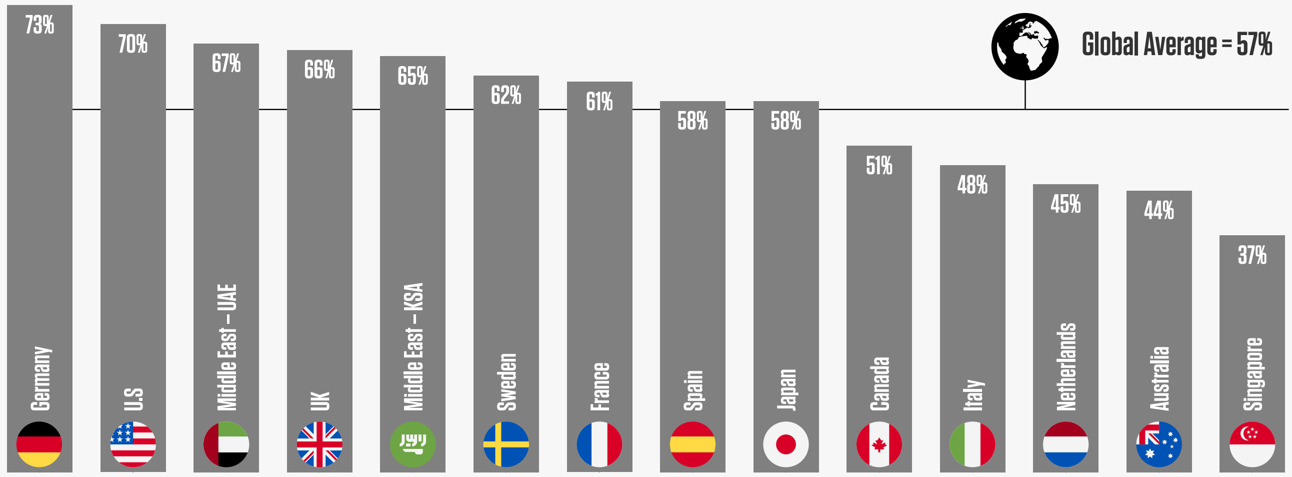
Overall, CISOs across all regions believe that the expectations of their superiors and colleagues are excessive. However, there is considerable variation in this view among CISOs in different countries.

Feeling the pressure: **73%** of CISOs in Germany agree that expectations on the CISO/CSO role are excessive, followed by the U.S. with **70%** and UAE with **67%**.

Belief that perceived expectation is excessive is lowest in Singapore (**37%**), Australia (**44%**), and the Netherlands (**45%**).

> *The number of priorities that CISOs have continues to grow, but if everything is a priority, nothing is. It's important to focus on the ones that deliver the most value to your organization and that are synchronized with the overall business strategy.*
>
> **Paige H. Adams**
> **Global CISO at Zurich Insurance**

CISOs stating that they face excessive expectations in their current role



57% of CISOs agree that expectations on their role are excessive

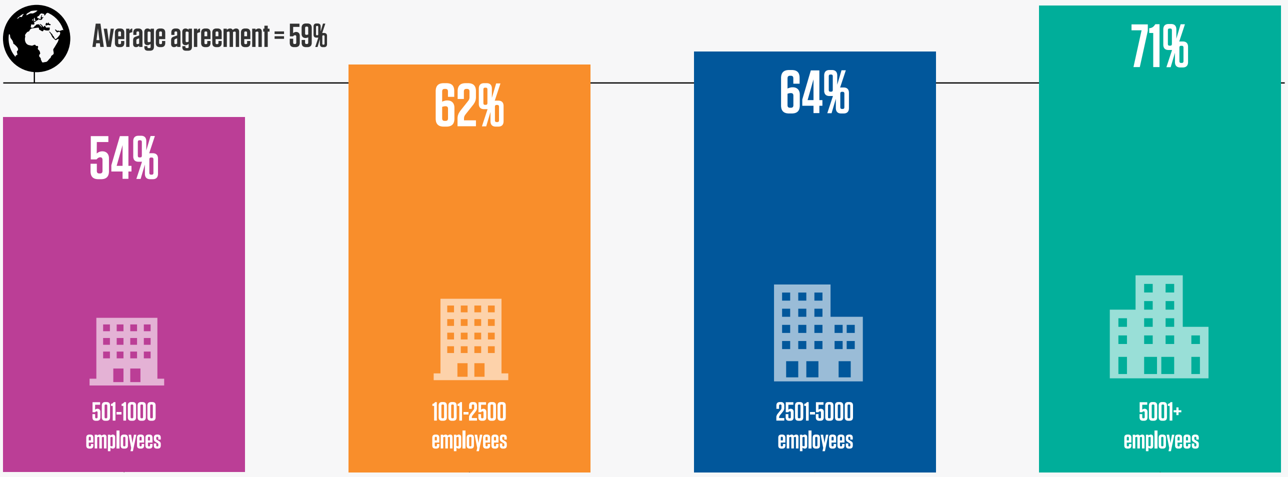
Expectations, and the opinion of the reasonableness of such expectations, depends on the size of the company. The larger the company, the higher the expectation. In organizations with 500-1,000 employees, just over half agree that there are excessive expectations on them and their team. This number increases to **66%** in companies with headcount over 5,000.

Across verticals, CISOs from technology (**71%**) companies feel the pressure of excessive expectations the most.

Adding to the demanding and often thankless workload of the CISO is a perceived lack of support from the boardroom. Fewer than two-thirds of global CISOs agree that they see eye-to-eye with the board on cybersecurity matters.

This figure aligns with company headcount, highlighting the difficulties faced by CISOs at smaller organizations.

Percentage of CISOs who agree that their Board sees eye-to-eye with them on the issue of cybersecurity – By company size



This lack of support and agreement doesn't just impact buy-in and budgets. Many CISOs report that their superiors can also directly impact their ability to perform their roles.

Fifty-nine percent of global CISOs agree that their reporting line can hamper their job effectiveness. This view is most prominent in the world of technology, where three in four CISOs agree with the sentiment. It is much less of an issue in the public sector, where just **38%** agree.

The result of this apparent disconnect between CISOs and the rest of the C-suite is that many feel they are unable to perform to the best of their ability. Nearly half of global CISOs do not believe that their organization positions them to succeed. Even more alarming, **24%** strongly agree that this is the case.

While the challenges of their role are felt worldwide, CISOs still find fulfilment in many ways, although perhaps not in the areas that many outside cybersecurity teams would expect.

Topping the job satisfaction list are a clear sense of purpose in helping society (**44%**) and in the responsibility of crafting a response from tech/ people/process to address evolving risk (**44%**). The breadth of the CISO's role is also a positive factor. Curiosity about technology (**38%**), the excitement of battling on the frontline (**38%**), and financial reward (**35%**) make up the rest of the top six list.

> *As a CISO, you need to address and explain risks to the board as well as to the tech people in order to be effective. You need to understand the technical side as well as the strategic side of the organization. You are like one of a handful of spiders in a big web that feels the vibrations or influences them at the edges.*
>
> **Roeland Reijers**
> **CISO, University of Amsterdam**

CONCLUSION

A blanket approach by cybercriminals ramped up the pressure during a difficult year for CISOs. Battling a constant stream of threats old and new, many struggled to prioritize resources and build effective defense strategies.

While such challenges may have been surmountable in any other year, this was a year like no other. It's not unusual for cybersecurity to feel like a high stakes game of whack-a-mole. But it's much harder to play when you're also tasked with security across hastily deployed remote environments and employees ill-prepared to work there.

Within this context, it should not come as a surprise that both human error and technical debt are serious concerns to CISOs worldwide. What should ring alarm bells is how many admit that this new working environment seriously hampers their ability to secure sensitive data and keep their organizations safe.

Despite the unprecedented disruption of the past year, there are many positives to take forward. CISOs understand that hybrid working is here to stay and soon expect to be better able to accommodate it securely near term. Many also believe that they will have the budget to achieve this goal.

However, cyber strategy concerns remain. Across the board, CISOs feel more vulnerable to cyber-attack despite strengthening policies. This suggests a lack of certainty around effective security controls and initiatives.

> *Cybercriminals are getting increasingly sophisticated in how they execute their attacks and are constantly developing new techniques to compromise our networks; even with the most advanced tools and techniques implemented to protect your organization, you need to be aware that your staff are now part of your 'attack surface' and are being used by bad actors to launch their attacks.*
>
> **David Cripps**
> **CISO at MONEYCORP**

While this is understandable in the context of the past year, it is hugely detrimental to future cyber-defense. Targeted protection and tailored awareness training are the cornerstones of any robust cybersecurity strategy.

Lastly, CISOs continue to feel the pressure of excessive expectations, as well as a lack of support from the boardroom. This underscores the need for cybersecurity oversight at the board level.

Only by fully understanding the style, tactics, and motives of the attacks we face and achieving boardroom buy-in can we equip those on the front line to defend against them.

Methodology

The Proofpoint 2021 Voice of the CISO survey, conducted by research firm Censuswide in Q1 2021, surveyed 1,400 CISOs from organizations of 200 employees or more across different industries in 14 countries. One hundred CISOs were interviewed in each market which consisted of the U.S., Canada, the UK, France, Germany, Italy, Spain, Sweden, the Netherlands, UAE, KSA, Australia, Japan, and Singapore. Censuswide complies with the MRS Code of Conduct and ESOMAR principles.

Contact us at info@proofpoint.com to better protect your business.