



CYBER IN SECURITY THE NEW NORMAL:

Securing the
distributed workforce
and remote operations

CONTENTS

- Introduction
- Key findings
- The distributed workforce is here to stay
- The move to remote working has introduced new risk
- Deprioritized security tasks can lead to increased risk
- Overconfidence in security changes can lead to increased vulnerabilities
- Radical changes necessitate security transformation
- Six steps to transform your security organization
- Survey methodology

INTRODUCTION

By Gidi Cohen, Skybox Security CEO and founder

Enterprises can't keep up with the pace

New vulnerabilities are projected to exceed

20,000 in 2020

(this is up from 6,000 in 2016); this is a leading indicator for future attacks

Enterprises are unable to stop greatest risks to the organization

New ransomware samples are up

72% in 1H 2020

and are exploiting multiple vulnerabilities

New vulnerabilities

are expanding across multiple OS, SW, device types including:

Android, Windows, Chrome, OS X, iOS, Edge Chromium, iPod OS, RedHat OpenShift, IBM API Connect, Oracle E-Business Suite

Very few people could have predicted the events of 2020, or the radical changes it has brought about for the cybersecurity industry. While the world stays focused on finding a cure for COVID-19, there is another crisis growing – a cybersecurity crisis.

The World Economic Forum aptly brings this to the forefront: “We should prepare for a COVID-like global cyber pandemic that will spread faster than a biological virus, with equal or greater economic impact.”¹

The situation is beginning to escalate. The FBI has seen a four-fold increase in cybersecurity complaints since the beginning of the COVID-19 pandemic.² INTERPOL has also seen an alarming rise in cybercrimes.³ In particular, they found “a significant concentration in the use of data harvesting malware with COVID-19 related information as a lure. Threat actors deceive users into executing malware such as remote access Trojans, info stealers, spyware and banking Trojans to compromise networks, harvest data, divert money, and build botnets.” The Skybox research lab also saw a 34% increase year-over-year in vulnerabilities, which is a leading indicator for the growth of future attacks.

Many organizations invest millions in security controls to block, detect, prevent, or respond to attacks. However, hackers often exploit vulnerabilities and misconfigurations across hybrid environments, leaving exposure to material cybersecurity and compliance risks.

¹ What the Covid-19 pandemic teaches us about cybersecurity – and how to prepare for the inevitable global cyberattack, World Economic Forum, June 2020

² FBI sees spike in cybercrime reports during coronavirus pandemic, The Hill, April 2020

³ Cybercrime: COVID-19 impact, Interpol, August 2020

In a post-pandemic era, what was once 'good enough' will no longer suffice.

Compounding this situation, the frantic shift to support a remote workforce and operations – sometimes within 24 hours – has introduced new risks for organizations in this time when cybercrime is on the rise.

The rapid expansion to cloud and accelerated growth of IT assets, together with a severe shortage of security personnel, leaves organizations struggling to deal effectively and proactively with potential attacks that could significantly damage their business and reputation.

For example, initial lockdowns forced many organizations to adopt new solutions and collaboration tools (e.g., Microsoft Teams, Slack, or Zoom) to accommodate employees and customers during the critical period. This rapid-pace adoption exposed several shortcomings associated with the remote workforce's home networks and routers – a significant concern considering the WHO's report that there has been a five-fold increase in cyberattacks during 2020.⁴

As a result of the crisis and the evolving role of security within businesses, Skybox surveyed the market to investigate what security practitioners worldwide think about the implications of the distributed workforce. Based on this analysis, we have found that C-level executives are greatly concerned about new risks. Yet, their organizations may be overconfident in their abilities to handle change. Further, the distributed workforce is not a short-term phenomenon. KPMG's CEO outlook study 2020 found that 69% of CEOs plan to downsize office space moving forward.⁵

Remote working is here to stay. This means that already-stretched thin security teams will have to manage existing responsibilities while supporting the new digital transformation initiatives.

But the reality is that current security practices are not keeping up with the changing security landscape. In a post-pandemic era, what was once 'good enough' will no longer suffice. Massive fragmented networks, decentralized, inconsistent configurations and change management processes, unsafe cloud and network configurations, and the continual increase in vulnerabilities have created the perfect storm.

CISOs have a starring role in the new normal. Cybersecurity has become a central part of how businesses grow and operate. Their influence with the CEO and board has greatly increased.⁶ Radical change brings an opportunity for a dramatic shift in how organizations are approaching their security programs. Moving forward, the most successful programs will have full visibility across their infrastructure, intelligence around potential risk and compliance exposures, and the insights necessary to make informed decisions on their future security strategy and programs.



“We should prepare for a COVID-like global cyber pandemic that will spread faster than a biological virus, with equal or greater economic impact.”¹

⁴ WHO reports fivefold increase in cyber-attacks, urges vigilance, WHO, April 2020

⁵ CEO Outlook Study 2020: Special COVID-19 edition, KPMG, 2020

⁶ Digital Trust Insights Pulse Survey, PwC, May 2020



KEY FINDINGS

The distributed workforce is here to stay

A third of respondents believe that a significant portion of their workforce will not return to the office in the future. This means that the risks introduced by supporting a remote workforce will become pervasive. Paired with the accelerated digital transformation that will continue to expand the attack surface, security teams must establish new strategies to reduce risk.

Security transformation is necessary for organizations to stave off increasingly energized threat actors

The complexity created by supporting an all-remote workforce and operations, combined with an exponential increase in vulnerabilities and ransomware, requires a radical new approach to cybersecurity programs. To mitigate risk, create efficiencies, and enable businesses to operate at scale and speed, security programs must focus on building prescriptive vulnerability threat management capabilities, rather than simply relying on traditional detect and respond methodologies.

The move to remote working has introduced new risk

Seventy-three percent of C-level executives are concerned that the distributed workforce has introduced new vulnerabilities and increased exposures. On top of this, only 11% are very confident in their ability to gain full visibility over their growing security environment. To address the significant rise of threats and vulnerabilities, CISOs will need to prioritize investments that help them gain the visibility and context they need to combat this increasingly complex environment.

Organizations are over-confident about the risk-level of changes made during the pandemic

Despite almost a third of respondents sharing that it was difficult for them to validate that network and security configurations did not increase security risk, 93% expressed at least average confidence that changes were validated correctly. If organizations made changes without a full understanding of their attack surface, they could have inadvertently introduced new risks to environments. Now is the time to assess those changes and ensure proper actions are taken to address new vulnerabilities.

Security teams deprioritized crucial security tasks to quickly support a remote workforce

Security teams deprioritized BYOD policies at a time when mobile vulnerabilities have increased by 50% with more personal devices connecting to corporate assets.⁷ While understandable at the time, it is crucial that security practitioners now assess decisions that were made during that time of crisis, understand potential risk, and take necessary actions to bolster their security posture moving forward.

The DISTRIBUTED WORKFORCE

is here to stay

Concerns currently held by CISOs about the security surrounding the distributed workforce will continue. The way that people work has been changed forever by the pandemic. One-third of respondents project that a significant number of their employees will not be returning to the office within 18 months.

This has several significant repercussions for cybersecurity practitioners:

- Attack surfaces will continue to expand at pace as remote work becomes a defining feature of the new normal. Organizations will strive to maintain business continuity by accelerating their digital transformation initiatives.
- New perspectives are needed to determine the best way to secure a long-term, distributed workforce.
- Complexity of cybersecurity has increased.

70% say at least
**1/3 of the workforce will
remain remote 18 months
from now**

Q: What percentage of your workforce do you expect to remain remote 18 months from now?

The move to remote work and operations has introduced

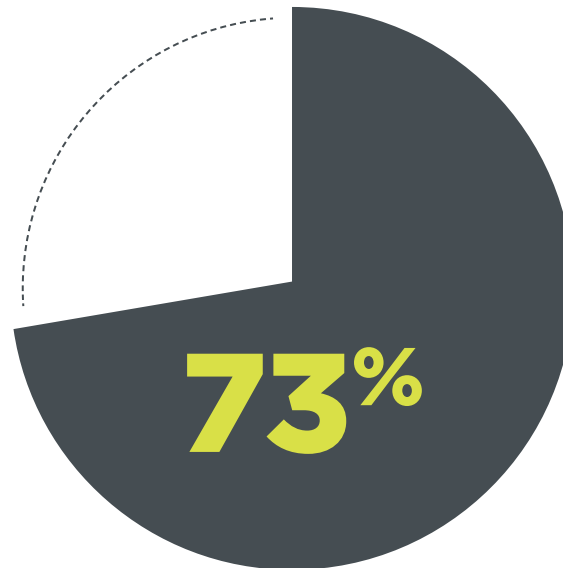
NEW RISK

With almost three-quarters of C-level executives very concerned about the distributed workforce introducing new vulnerabilities and allowing new exposures, just over one-tenth were confident in their network visibility capabilities.

As a result of the move to a distributed workforce and the acceleration of digital transformation, the CISO now has a lot more to protect. New technologies and services supporting the distributed workforce have left them with more access points to configure, more technologies to secure, and more changes to validate correctly.

If security practitioners cannot gain visibility of their expanded attack surface and lack contextual insights into vulnerabilities and assets within their networks, they could be inadvertently introducing new risks. In fact, 73% of C-level security and IT executives were concerned that new vulnerabilities and exposures have been introduced by the distributed workforce. Only 11% of executives stated they were very confident in their ability to maintain a holistic view of their organizations' attack surfaces. Without proper visibility, it will be impossible for them to track any unauthorized access created by remote employees – something that 70% of C-level executives are at least moderately concerned about.

C-level executives share concerns that the distributed workforce has introduced new vulnerabilities and allowed exposures



Q: Are you concerned that the distributed workforce has introduced new vulnerabilities, allowing exposures to your organization?

C-level executives who are very confident in their ability to maintain a holistic view of their organization's attack surface



Very confident

Q: On a scale of 1-5 (1 being not confident, 5 being very confident), how confident are you that you are maintaining a holistic view of your organizations attack surface as you enable a growing remote workforce?

Skybox Research Lab discovered that 2020 will be a record-breaking year for new vulnerabilities with a 34% increase year-over-year – a leading indicator for the growth of future attacks.⁸

Already-stretched security teams are struggling to properly manage this influx of new vulnerabilities on top of enabling business-critical digital transformation initiatives.

To address these challenges, CISOs must transform security programs to fit the new normal. CISOs need to have visibility and insight across infrastructure and assets to see the bigger picture of where threats could originate and the pathways they could take. A new approach to cybersecurity is required; this includes a fresh look at people, process and technology.

To start, security practitioners are operating with many blind spots across their networks that have only been exacerbated by an immediate switch to support a distributed workforce and remote business operations. Complete visibility, analytics and automation to quickly map, prioritize and remediate vulnerabilities across their organization are needed. This will provide the intelligence required to optimize security policies, actions, and change processes across all corporate networks and cloud environments.

Organizations in Asia are highly concerned about the remote workforce introducing new vulnerabilities

Respondents in Asia were more concerned that the distributed workforce has introduced new vulnerabilities and allowed more exposures to their organization than their North American and European counterparts.

Q: Are you concerned that the distributed workforce has introduced new vulnerabilities, allowing exposures to your organization?

Deprioritized security tasks can lead to

INCREASED RISK

1 Scheduled reporting

2 Software updates

3 BYOD policies

Top tasks deprioritized since the onset of the COVID-19 pandemic

Q: Check to indicate "yes" if you've had to downgrade any of the following since the COVID-19 pandemic to enable the remote workforce?

The sophistication of hacking techniques is growing by the day, as are threat actors' confidence that they will be successful in their attempts to gain ransom.

Bad actors are fully aware of how important it is for businesses to maintain continuity during the current crisis and are energized to take advantage of any weaknesses.

The creation of new ransomware samples increased by 72% over the first six months of 2020.⁹ KPMG has warned of "evidence that remote working increases the risk of a successful ransomware attack significantly."¹⁰

⁹ Vulnerability and Threat Trends Mid-Year Update, Skybox Security, July 2020

¹⁰ The rise of ransomware during COVID-19, KPMG, 2020

The EU cybersecurity network cautioned that “the pandemic offers cyber attackers unique opportunities to leverage existing attack tactics, techniques and procedures to exploit new opportunities...with a massive increase of employees working from home increasing risk levels.”¹¹ Further, an INTERPOL assessment of the impact of COVID-19 on cybercrime found “a significant target shift from individuals and small businesses to major corporations, governments and critical infrastructure.”¹²

In addition to the rise in ransomware samples, trojans experienced a similar growth trajectory,¹³ raising the possibility of an increase in chained attacks. Hackers exploit non-critical vulnerabilities with trojans. Bad actors know that organizations without risk-based remediation practices are unlikely to prioritize the remediation of these lower-level flaws. Cybercriminals can laterally move across the network to enact a more devastating ransomware attack.

Many security teams do not have context-informed vulnerability and threat management practices in place. Instead, they operate with detect-and-respond methodologies and are more susceptible to these kinds of attacks.

With this in mind, it is concerning that securing the distributed workforce has led to the deprioritization of important security tasks.

Around a third of respondents shared that they had downgraded software updates and BYOD policies.

The downgrading of BYOD policies is particularly alarming. In fact, mobile OS vulnerabilities increased by 50% over the first half of 2020,¹⁴ which is worrying considering the increased connection between personal devices on home networks and the corporate security environment.

42% of all respondents shared that they had deprioritized reporting since the onset of the pandemic.

This means that security practitioners may not be getting as much insight into their data, and thus making decisions based on incomplete information. While this deprioritization is understandable due to limited resources and the compressed timeframe organizations had to support the remote workforce, it only emphasizes the criticality of automation. During times of intense workloads, greater automation allows security organizations to have the insights they need to make the decisions that are crucial to their business.

European firms prioritize firewalls during the pandemic

The split between deprioritized tasks resulting from the distributed workforce is fairly evenly distributed within North America. There are, however, points of difference between Europe and Asia, with most European companies prioritizing firewalls and VPNs: Only 6% of respondents said that they downgraded firewalls and VPNs this year. Most companies in Asia prioritized phishing and social engineering tests: Only 7% said they had downgraded these efforts during the pandemic.

¹¹ The COVID-19 Hackers Mind-set: White Paper of the ECHO Network of cybersecurity centres, 2020

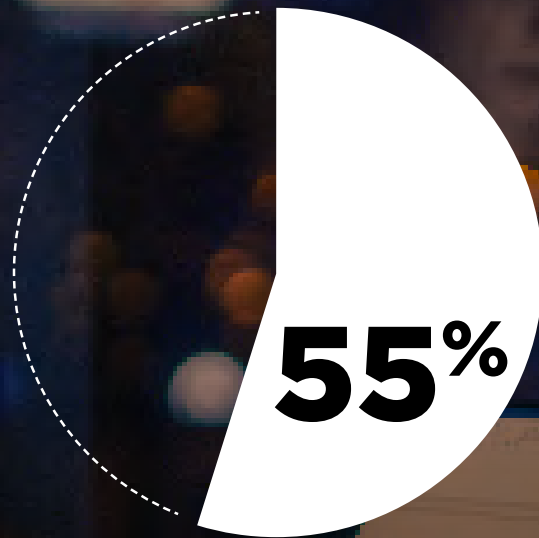
¹² INTERPOL COVID-19 Cybercrime Analysis Report, August 2020

¹³ Vulnerability and Threat Trends Mid-Year Update, Skybox Security, July 2020

¹⁴ Vulnerability and Threat Trends Mid-Year Update, Skybox Security, July 2020

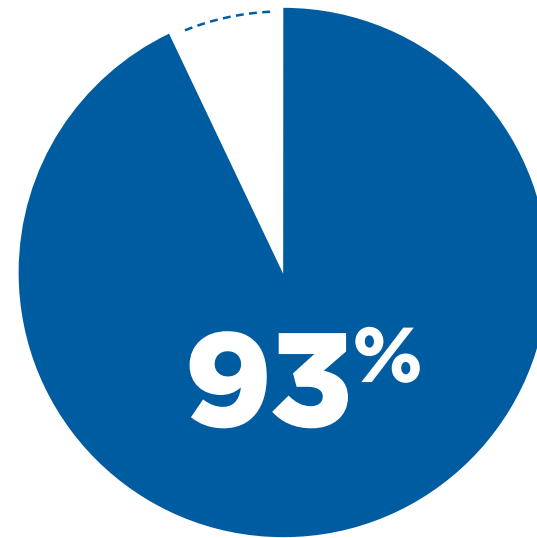
Overconfidence in security changes can lead to increased

VULNERABILITIES



Find it at least moderately difficult to validate that network and security validations did not increase security risk

Q: On a 1-5 scale, (1 being very easy, 5 being very hard), please rate how difficult it was to validate that network and security configurations supporting remote employees did not increase security and/or business risk



Yet 93% have higher than average confidence that changes are validated correctly

Q: On a scale of 1-5 (1 being not confident, 5 being very confident), how confident are you that changes were properly validated so as not to lead to security issues in the next 12 months?

Sixty-two percent of respondents are concerned that distributed workforces have introduced new vulnerabilities. Shockingly, 93% expressed at least average confidence that changes were validated correctly. Yet, over half of respondents said that it was at least moderately difficult for them to validate that network and security configurations did not increase security risk.

There is an apparent disconnect here. If organizations are truly confident that all changes were properly validated, then it should follow that change management processes were handled with relative ease and they would not have concerns about new vulnerabilities. This is not the case.

Change management issues cannot be divorced from the introduction of new vulnerabilities and exposures. If changes are properly applied, there is a limited scope for new flaws to be introduced to the security environment. Likewise, if there are known or expected issues with changes, organizations should expect to see an increase in vulnerabilities and exposures.

Traditional approaches to change management – treating each change manually and on a case-by-case basis – are now unmanageable. Limited staffing and compressed change cycles result in changes increasing the risk level. Limitations of manual-led processes have been known for years, with 90% of all breaches attributable to human error.¹⁵ The pandemic has put a finer point on this issue.

In a rush to enable newly remote workforces, security teams may have neglected to incorporate existing network topologies and configurations into analysis before implementing new policies. Combined with siloed vulnerability and policy management technologies, this could have contributed to blind change and automation processes. Consequently, unvalidated new policies and rules could have exposed vulnerabilities and introduced systemic risk across organizations.

Yet, many organizations are overconfident about the strength of their security postures. Considering that 91% of enterprises have reported an increase in cyberattacks during the pandemic,¹⁶ it is clear that this confidence is misplaced. The new normal requires more agility and change than ever before. As such, organizations need to rethink long-held practices.

Where automation was once a nice-to-have, it is now a must-have. Where network visibility was once considered an aspiration, it is now a necessity. Where security teams could rely on antiquated change management capabilities, they now need to modernize.


Securing the distributed workforce in financial services

Managing cybersecurity at a large financial institution is a mammoth task. It is not uncommon for a bank to have hundreds of staff members working exclusively on security, invested heavily in best-of-breed point solutions, and strict policies to dictate security standards. Despite this, the industry has faced some of the greatest challenges during lockdowns. It was critically important that they did not allow any possibility for threat actors to gain unauthorized access to sensitive data. Still, they had to move as rapidly as other industries. Even with enhanced capabilities, the potential for new risk to have been introduced is still apparent. Here are a couple of stand-out statistics that highlight how changes during COVID-19 are perceived within financial service institutions and banks:

- 68% of banking and financial service organizations are concerned that the distributed workforce has introduced new vulnerabilities, allowing exposures to their organizations.
- 55% say reporting has increased in their organizations due to distributed workforces or other COVID-related changes.

Q: Are you concerned that the distributed workforce has introduced new vulnerabilities, allowing exposures to your organization?

Q: Have auditing/reporting for internal policy/regulatory standards increased in your organization due to distributed workforces or other COVID-related changes?



A radically different cybersecurity
landscape paves the way to security

TRANSFORMATION

This is a pivotal time for security leaders.

As we enter the new normal, leaders need to think about establishing a new approach to cybersecurity. Old ways of working will slow progress and could open up new attack vectors. **A radical new approach is needed** – one that is rooted in the development of preventative and prescriptive vulnerability and threat management practices.

The distributed workforce here to stay. As the acceleration of digital transformation continues to gain pace, the CISO will have more assets to protect, more vulnerabilities to manage and more changes to secure. The CISO has also gained more influence – they now have an opportunity to enforce wide-scale transformation within their function and change overarching approaches to security.

It is clear that traditional approaches to managing cybersecurity rooted in detection and response no longer apply within the current security context. Instead of basing their security programs on detecting threats at the extremities of the network perimeter, leading CISOs are developing proactive capabilities that better enable them to prevent threats. This approach is centered on visibility, context-rich insights, focused automation, and data integration across their entire fragmented estate.

What we will see is the emergence of stronger, more resilient security programs. The CISO will be focused on developing a holistic view of their fragmented environment, one that enables them to see the bigger picture and limit opportunities for increasingly-energized threat actors. This will allow them to be confident in their ability to avoid regulatory fines, significantly limit the chance of falling foul to a data breach or ransomware attack and allocate more resources to focus on securing digital transformation.

SIX STEPS

to transform your
security program

1 Evolve the tech stack

To maximize investments, security leaders need to evolve their technology stack to deliver critical business outcomes and long term value. When CISOs are dealing with bloated stacks that deliver restricted value, they can devote too much time to trying to fortify legacy infrastructure when the focus could be better placed elsewhere. Rather than buying point solutions that tackle hyper-specific security issues, CISOs should adopt technology that provides a holistic understanding of their infrastructure. When considering which technology investments to make, CISOs need to prioritize solutions that enable them to integrate data, gain visibility of all vulnerabilities and assets within their expanded infrastructure, and deliver insights that will empower them to take decisive action.

2 Gain full visibility

IDC predicts that by 2021, over 90% of enterprises worldwide will be relying on a mix of on-premises/dedicated private clouds, multiple public clouds, and legacy platforms to meet their infrastructure needs.¹⁷ Security and IT organizations need complete visibility and analytics to quickly map, validate and remediate vulnerabilities across these hybrid and multi-cloud infrastructures. This is not an easy task. It requires establishing a mature and tightly connected security management framework that spans across planning, implementation and ongoing change management workflows.

17 IDC Expects 2021 to Be the Year of Multi-Cloud as Global COVID-19 Pandemic Reaffirms Critical Need for Business Agility, March 2020



3 Eliminate silos

By unifying vulnerability and policy management capabilities with the aggregation of data sets from a wide range of security, cloud and networking technologies, teams can validate network, cloud and security configurations together to remediate vulnerabilities faster. Gaining insights also helps them to break down silos to understand the big-picture view. To advance change, it is integral that everything – including data and talent – is working towards enriching the security program as a whole. Insights that show how each process connects will be invaluable in achieving this.

4 Make changes with context

To ensure security policy changes are adequately analyzed and properly deployed without introducing new risks, organizations need context-aware change management that coalesces the decision-making process across enterprise security and network teams. To ensure policy changes are adequately analyzed and properly deployed without introducing new risks, organizations need prescriptive analytics to quickly map and remediate vulnerabilities while making rule changes that improve overall security.

5 Introduce targeted automation

By leveraging automation, organizations can strengthen their security postures and help optimize and control their increasingly complex infrastructure, both on-premises and in the cloud, while efficiently meeting key compliance requirements across any environment. Automation can clean up and optimize firewalls, spot policy violations, ensure proper segmentation, assess vulnerabilities without a scan, match vulnerabilities to threats, simulate attacks, proactively assess rule changes, and more. It also right-sizes resources, freeing up talent to focus on supporting more strategic business initiatives.

6 Remediate based on risk exposure

Once visibility is achieved, it is important to build capabilities to discover all vulnerabilities within the security environment. This can be achieved when disparate data repositories are brought together with data normalized and modeled to infer the presence of vulnerabilities.

Insights should then be enhanced with more information from a wide range of sources to better understand the implications of current vulnerabilities. All of this information should be used to determine how exposed the vulnerability is within a network by simulating attacks on the network model created during the initial visibility phase.

With effective discovery and prioritization practices in place, organizations are left with a smaller and more manageable number of vulnerabilities that they know require immediate attention. Vulnerabilities on important assets, exposed to a threat origin, and with an active exploit are top priorities. At this stage, security practitioners are better able to focus remediation where it is needed most.

Over 700 of the largest and most security-conscious enterprises in the world rely on Skybox Security for the insights and assurance required to stay ahead of their dynamically changing attack surface. We don't just serve up data and information, we provide the intelligence and context to see the biggest picture possible and make informed decisions, taking the guesswork out of securely enabling your business at scale and speed.

Our unified security posture management platform provides Security and IT teams complete visibility, analytics and automation to quickly map, prioritize and remediate vulnerabilities across your organization. Plus intelligently optimize security policies, actions and change process across all corporate networks and cloud environments. With Skybox, your security team can now focus on the most strategic business initiatives while ensuring your business remains protected.

Research methodology

The survey was conducted by the Information Media Security Group during September and October 2020. 295 cybersecurity professionals at organizations with 5,000+ employees were surveyed.



295
cybersecurity
professionals



Organizations with
5,000+
employees

Including:

- 44** C-Level executives
- 111** respondents in North America
- 72** respondents in Europe
- 43** respondents in Asia
- 47** respondents in Financial service organizations

[Contact us](#)