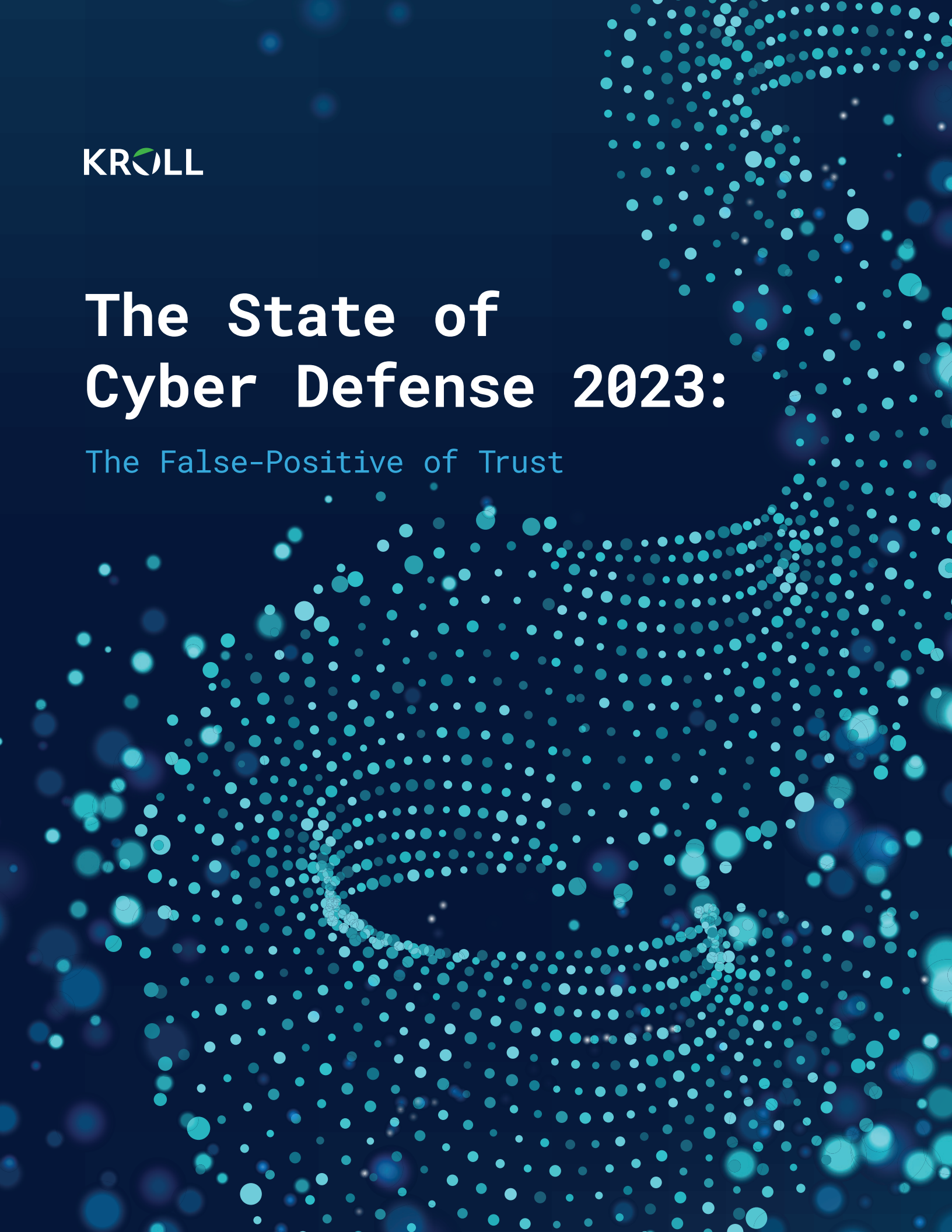
KROLL

# The State of Cyber Defense 2023:

## The False-Positive of Trust



# Table of Contents

# Introduction

With cyber threats increasing in number and sophistication, organizations are using multiple cybersecurity platforms, ingesting threat intelligence from various sources, leveraging the cloud at a massive scale, and outsourcing key services.

To navigate this landscape, trust is imperative. There needs to be trust in teams, trust in technology, trust in intelligence sources and trust with suppliers or third-party providers. The degree in which businesses trust their technology can have wide-ranging impacts on how effectively organizations deal with cybersecurity challenges. Further, where trust is lacking, there are far-reaching consequences for cyber resilience.

It is clear that there is a critical balance in how much and where trust should be placed. Organizations that report high levels of trust also claim that they have high levels of cyber maturity. However, when looking deeper, the actions of these self-reported mature organizations seem to suggest that their cyber defense should be improved. The challenge being faced is what cyber maturity truly means, and how this can be used to build trust across key stakeholders.

Throughout this e-book, we will look to understand the current state of cyber defense, the levels of organizational trust and how true cyber maturity links to trust in facilitating organizations to stay ahead of the curve in a constantly evolving threat landscape. This report is based on the responses from 1,000 senior security decision-makers, based in North and South America, APAC and EMEA.

# Key Findings:

**Trust is clearly an issue:** Over a third **(42%)** of information security decision-makers reported a lack of trust as their biggest challenge, and **95%** do not feel as though senior leadership trusts their security teams to protect their organizations from threats.

**Trust is also misplaced:** Trust in employees to stop a cyberattack **(66%)** is ranked higher than the ability of the security team to identify and prioritize security gaps **(63%)**, the accuracy of data alerts **(59%)**, the effectiveness of cybersecurity tools and technologies **(56%)**, and the accuracy of threat intelligence data **(56%)**.

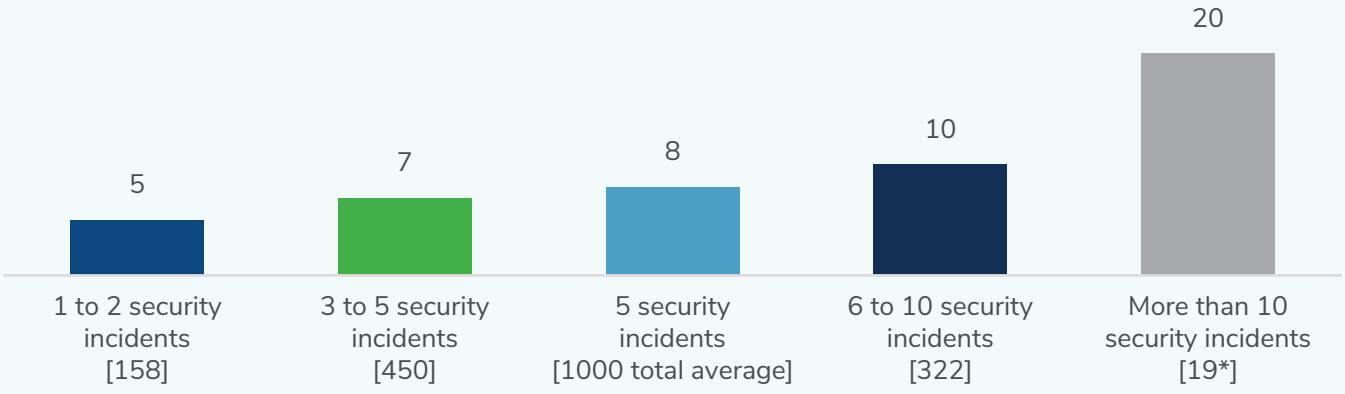
**A lack of communication is the most frequent cause for a loss of trust, as reported by 47% of information security decision-makers.**

**It's hard to trust what you don't fully understand:** While **99%** agree that endpoint detection and response (EDR) plays a key role, responses show limited understanding of its full function. Approximately **22%** of respondents believe that EDR prevents reinfection and **38%** believe all responses can be made with EDR, neither of which are wholly accurate.

**Outsourcing cybersecurity services is gaining popularity:** **98%** of those that do not already outsource their cybersecurity services have (or are considering) plans to do so. However, **89%** of IT and security decision-makers say improvement is needed in the transparency between their security teams and security vendors.

**Multiple security tools aren't solving the problem:** The higher the average number of platforms used, the more cybersecurity incidents organizations have experienced. The number of incidents and the fact that only **24%** have MDR show that having the right tools, and not the number of tools, is an important factor in cyber protection.

**Average Number of Platforms Used, By the Number of Security Incidents Experienced in the Past Year**



# 1 - The Current State of Cyber Defense

## Part 1: Over-Confidence in the Current Cyber Defense Landscape

Information security decision-makers place trust and confidence in their teams and technology to protect their organizations but many display an "over-confidence."

Over a third (37%) of senior security decision-makers interviewed report that they "completely" trust that their organization is protected and can successfully defend against most/all cyberattacks, indicating a level of over-confidence in being able to defend against all potential threats in this ever-changing threat landscape.

**Trust in Organization's Cybersecurity Defenses**

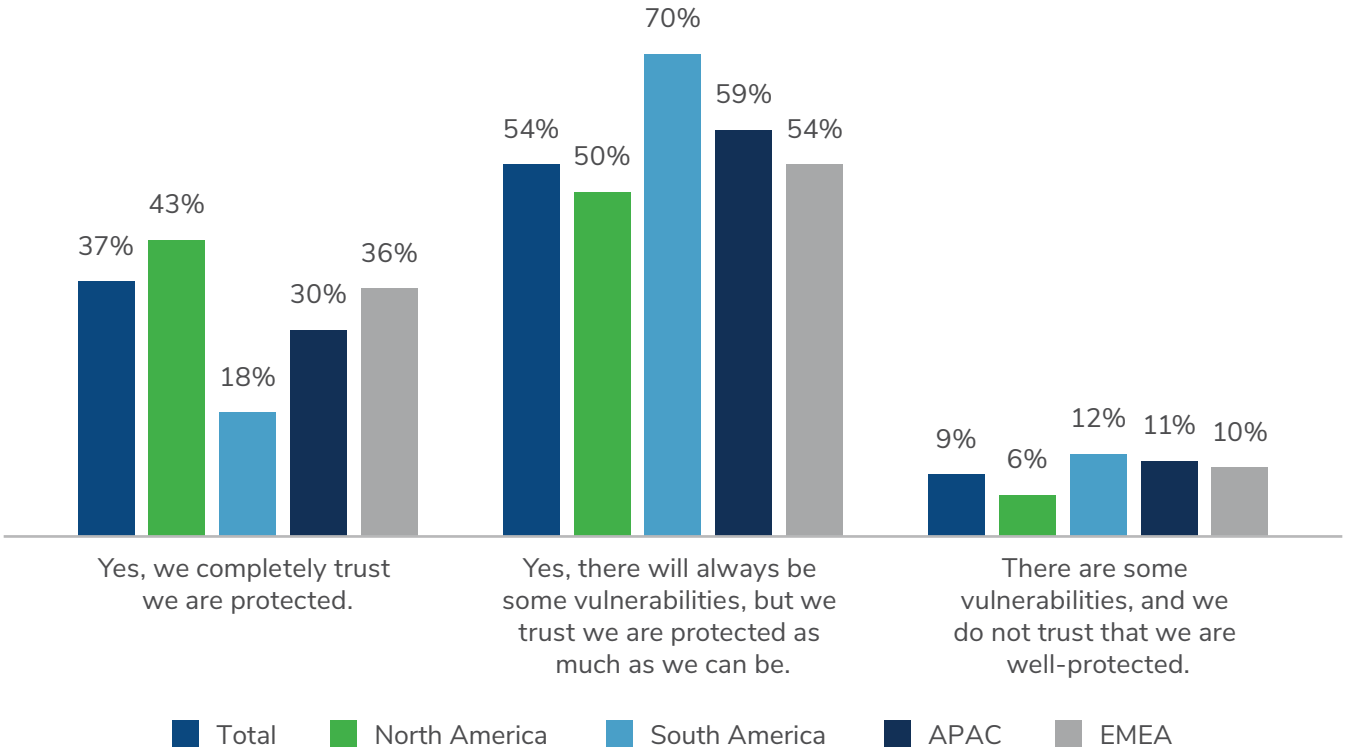



*Figure 1: Do you trust your organization's cybersecurity defenses to successfully defend against most/all cyberattacks? [1000], split by region, omitting some answer options*

The extent to which infosecurity decision-makers trust the level of protection offered by their cybersecurity defenses is surprising, considering that organizations have experienced an average of five major security incidents (that resulted in data compromise or financial impact) in the last year. With only 4% of respondents reporting no incidents of this nature, a high level of trust in their organization's cyber defense may be misguided.

This ties to the clear link found with CFOs also being over-confident in their companies' abilities to defend against cybersecurity incidents, as per research conducted by Kroll in 2022 - CFO Cyber Security Survey: Over-Confidence is Costly. This being the case, do senior leadership teams really know how well-protected their organizations are?

## Part 2: Not All Security Leaders Understand What their Security Tools are Protecting Against

For any organization looking to effectively defend against cyber threats, it is essential they understand what they are protecting against and which tools to implement to protect themselves in the long term.

Most organizations are using multiple platforms for cybersecurity—with eight platforms used on average.

**Average Number of Cybersecurity Platforms Used**

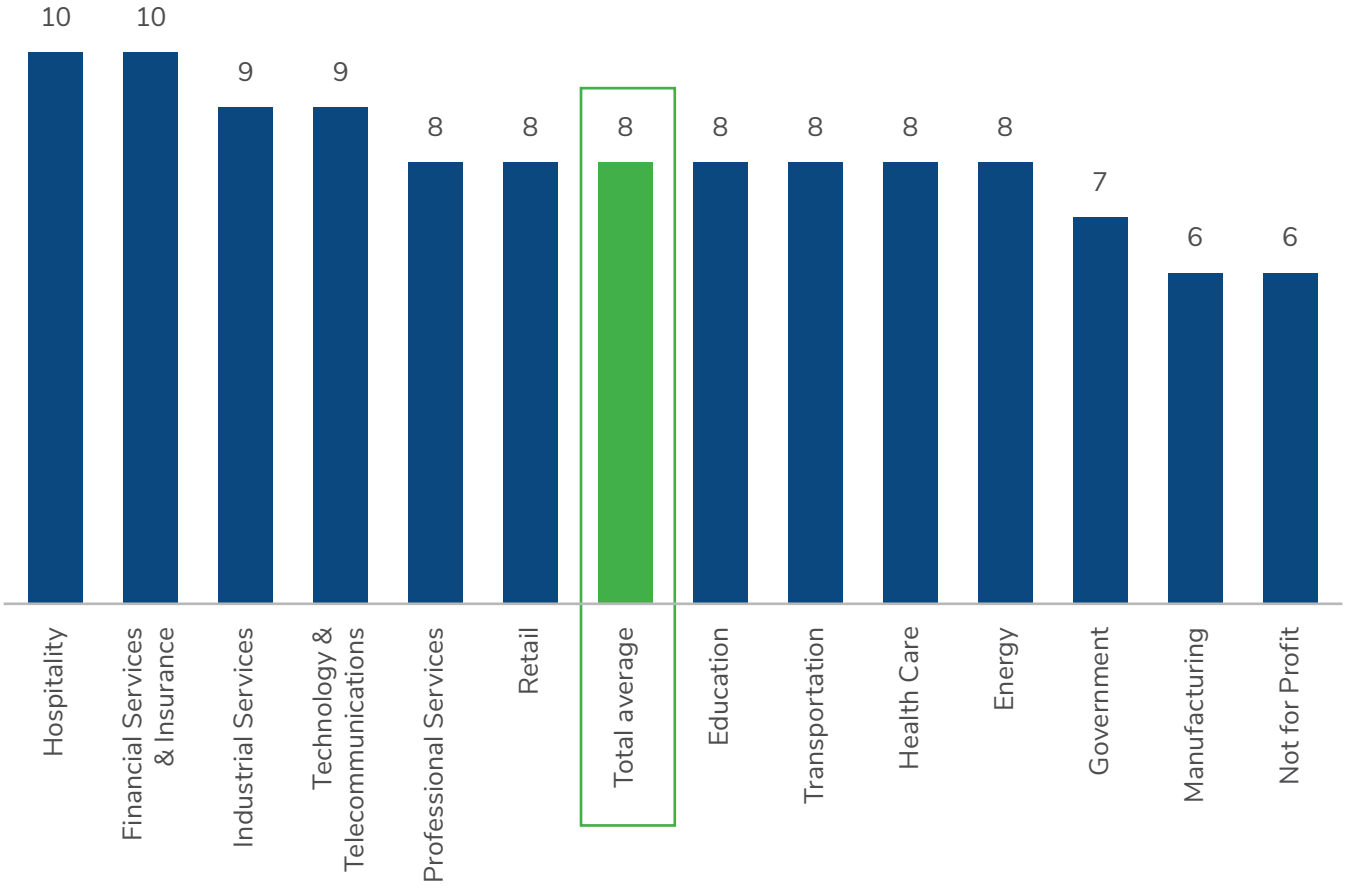



*Figure 2: How many cybersecurity platforms does your organization use regularly to monitor cybersecurity alerts? [1000], split by sector*

Interestingly, **the higher the average number of platforms used, the more cybersecurity incidents the organizations have experienced.** This could imply a combination of factors, namely that organizations are struggling to understand and fully utilize all the aspects of the many platforms they rely on. This combined with the sheer volume of data that security teams deal with in their environment can cause teams to feel like they are drinking from a firehose, unsure where to begin. A lack of management of these tools could then be over-complicating organizations' security measures and creating vulnerabilities in their cyber defenses.

Truly effective cyber defense is developed and maintained by an overarching strategic security architecture which is answerable, measurable, quantitatively defined, and supported by data drawn from appropriate reporting. Of paramount importance, therefore, is a holistic, risk-driven approach, propelled by controlled operational effectiveness.

Further to this, almost all (99%) agree that the endpoint detection and response (EDR) technology plays a role in response to cyber threats, but the responses clearly suggest that the understanding of its full function is not fully realized. Just under a quarter of respondents (22%) believe that EDR prevents reinfection and 38% believe all responses can be made with EDR, neither of which are wholly accurate. With businesses not apprised of the capabilities and potential of security technology, their cyber maturity and preparedness for an attack will be miscalculated.

**What Respondents Believe the Role of EDR is in Response to Cyber Threats**

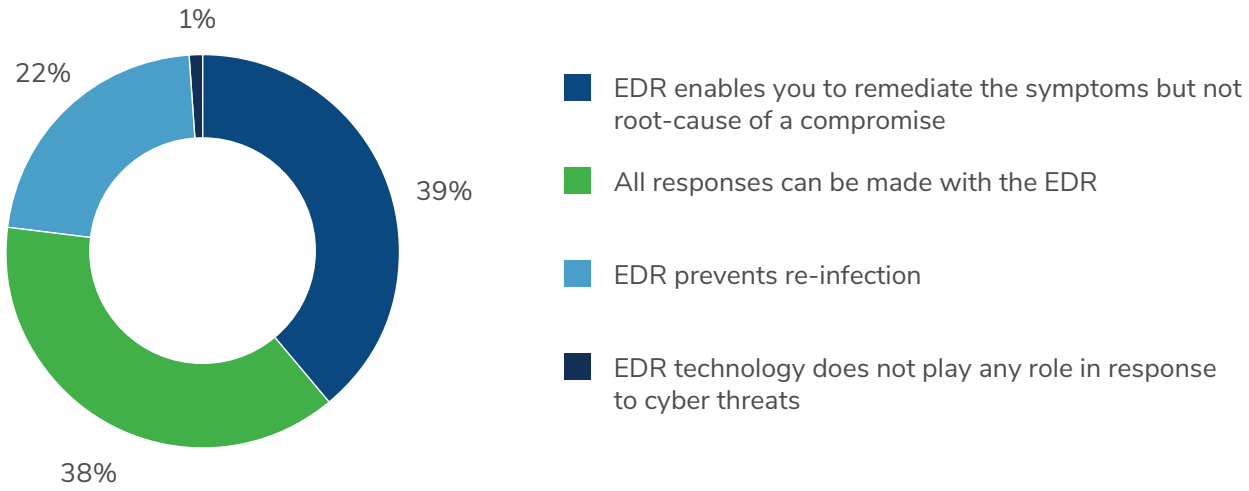



*Figure 3: In your opinion, what role does Endpoint Detection and Response (EDR) technology play in response to cyber threats? [1000], omitting some answer options*

KROLL

## Part 3: Limiting Factors on the State of Cyber Defense

### Team size

To handle ever-increasing threats, respondents report that they have an average of 25 personnel involved in cybersecurity in their organizations, with larger organizations (over 3,000 employees) averaging 30 personnel.

### Insurance

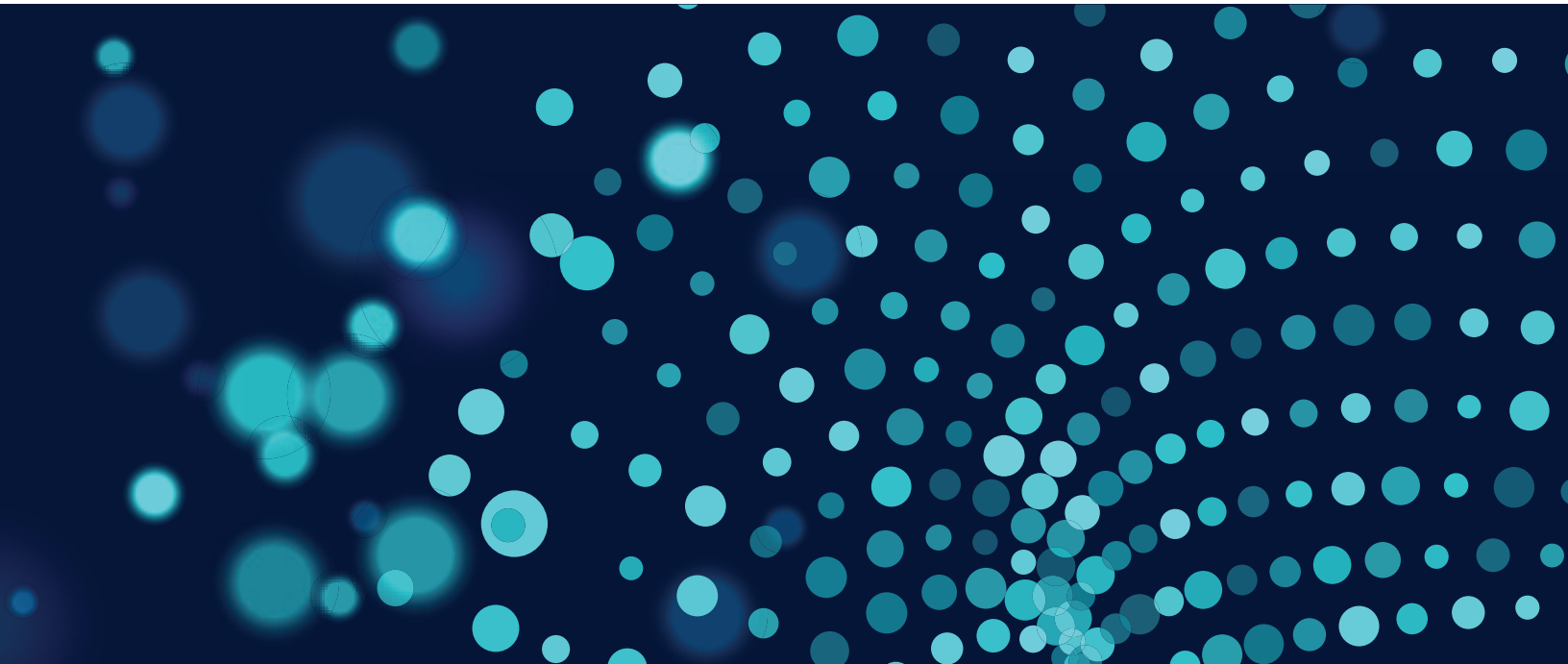
Organizations use an abundance of elements in their defense programs, however, only just over one in five currently have the benefit of specific cybersecurity insurance cover (23%). Further, only 20% of IT and security professionals who say that their security operations are cyber mature have cyber insurance.

This is noticeably lower in countries such as Italy and Japan (both at 16%). Looking by industry, hospitality (10%), not-for-profit (13%) and transportation (17%) are also lacking such insurance. Cyber insurance is more prevalent in sectors such as technology and communications (34%) and education (27%). However, two-thirds of companies in these sectors still do not have any form of cyber insurance.

Clearly, with the prevalence of cyber incidents in the past year, cyber insurance should not be overlooked nor dismissed by organizations.

### Trust

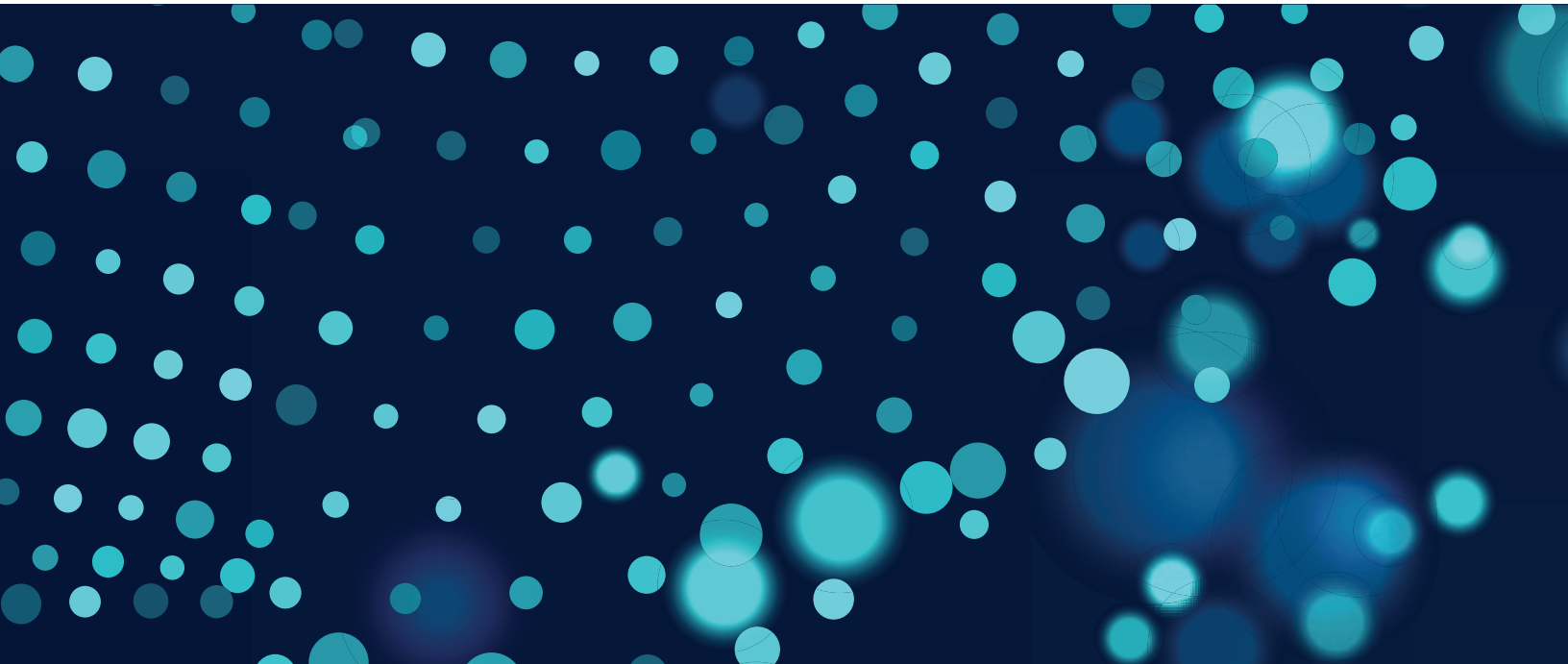
The complex task of protecting organizations against cyber threats is challenged by many deterrents but a lack of trust reportedly outranks all others.



**Biggest Cybersecurity Challenges for Organizations**


*Figure 4: What are the biggest challenges for your organization currently when thinking about cybersecurity? [1000], combination of responses ranked first, second and third, omitting some answer options*

Over a third of information security decision-makers reported a lack of trust as their biggest challenge. Addressing this deficit must be a priority for organizations to comprehensively review, restore and elevate their security posture. Let's dive deeper into this over the next section.



# 2 - Cyber Defense and Organizational Trust

## Part 1: Senior Leadership Have Cautious Trust in their Cyber Defenses, However Security Teams 'Over-Trust'

Ninety-five percent of information security decision-makers do not feel as though senior leadership trusts their security teams to protect their organizations from threats.

**Is Improvement Needed in the Level of Trust from Senior Leadership**

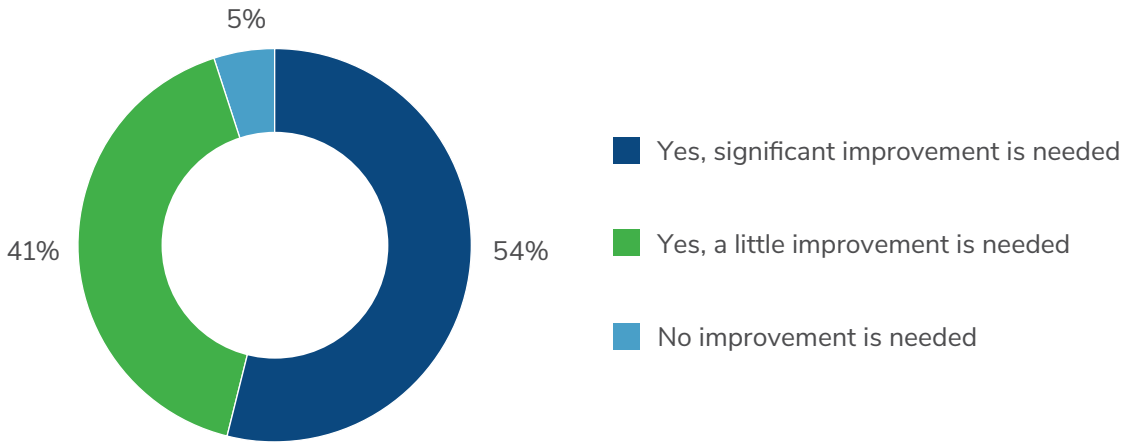



*Figure 5: Do you feel that the level of trust the senior leadership team has in your team to keep the business secure from threats could be improved in your organization? [1000], omitting some answer options*

Perhaps, this is not surprising considering the repeated number of security incidents that are experienced by organizations. However, with the earlier reported over-confidence of senior information security decision-makers in their organizations' defenses, why are we seeing this disparity?

This could tie into a scenario of "over-trust," where those closest to the day-to-day security of organizations lack a complete understanding of what is involved in the implementation of "true cyber maturity," combined with a lack of resources for the necessary maintenance of the cyber technology at their disposal.

## Part 2: Humans are Trusted More than Technology

When it comes to specific departments, IT and security decision-makers have understandably significant levels of trust in IT and infosecurity teams (94%). While protecting an organization from cyberattacks should be a company-wide effort, there are potential pitfalls for over-trust in the methods used to remain vigilant.

When looking at the methods to prevent a cyberattack, the majority of respondents state that they trust their employees' abilities to avoid falling victim to a cyber incident (66%) above all else.

Trust in employees is ranked higher than the ability of the security team to identify and prioritize security gaps (63%), accuracy of data alerts (59%), effectiveness of cybersecurity tools and technologies (56%), and the accuracy of threat intelligence data (56%).

**Most Trusted Methods by IT and Security Decision-Makers**

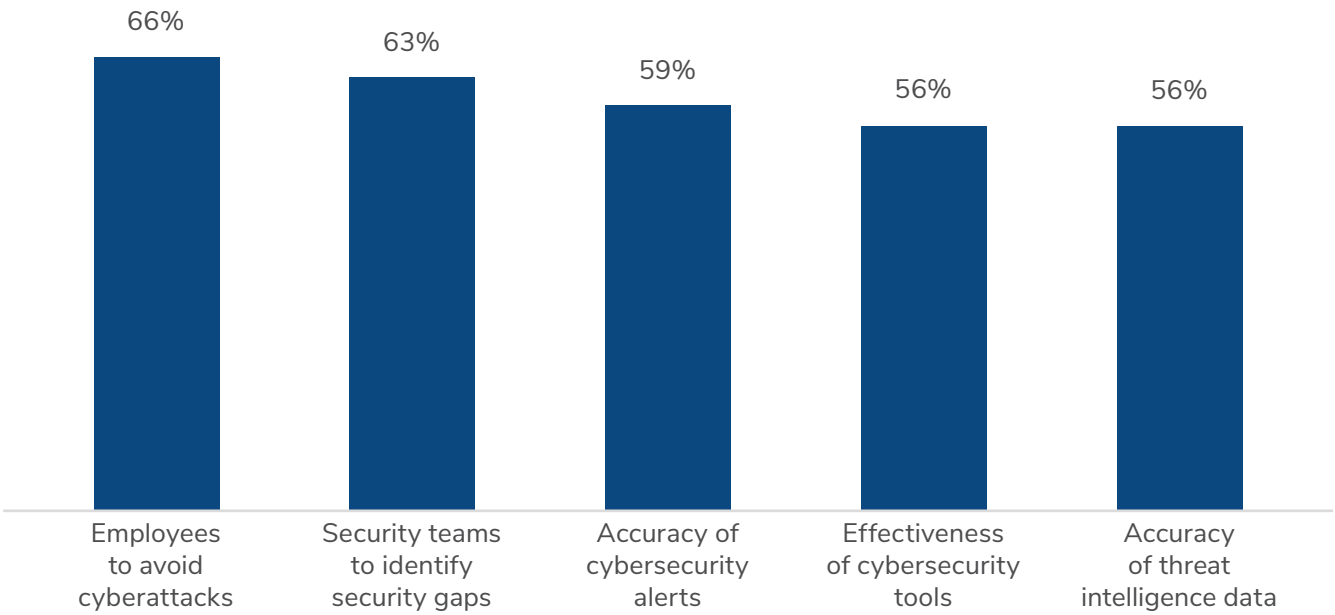



*Figure 6: Which of the following do you trust the most within your organization? [1000], combination of responses ranked first, second and third, omitting some answer options*

Respondents find it easier to trust people (and their ability to help mitigate a vulnerability) than technology. While employees may be the first line of defense against a cyberattack, it cannot be assumed that they will avoid falling victim to a cyber incident. Of course, businesses need to have up-to-date and recurring cybersecurity training for employees so that they remain aware of potential threats. However, people are understandably fallible, and without the necessary technology in place, businesses will inevitably be woefully unprepared.

## Part 3: Demand for Outsourcing is Rising but Organizations Need to Work to Build Trust

Currently, over three quarters (77%) of organizations use an element of outsourcing for cybersecurity services, with 49% of these co-sourcing (both in-house and outsourced solutions are used). Further, 98% of those that do not already outsource their cybersecurity services have (or are considering) plans to do so, with 51% intending to do so in the next 12 months.

**Organizations' Current Sourcing Model for Cybersecurity Services**

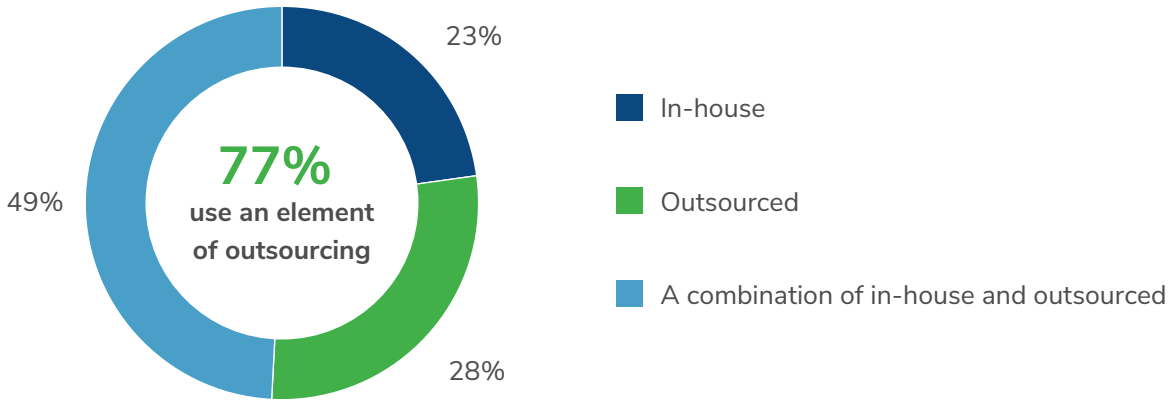



*Figure 7: What is your organization's current sourcing model for cybersecurity services? [1000], omitting some answer options*

Outsourced security and trust are quite closely linked. Indeed, 40% of security and IT decision-makers believe that having closer collaboration between in-house security teams and external service providers can help build trust in cybersecurity. Further, the biggest benefit felt (40%) when outsourcing cybersecurity services is gaining confidence in your cyber defenses.

However, 89% of IT and security decision-makers say improvement is needed in the transparency between their security teams and security vendors. This demand for transparency comes from a disconnected security ecosystem—organizations reported an average of eight security tools (see section 1, part 2) deployed in their system, but only 24% have a managed detection and response (mdr) or managed security service provider solution (MSSP) in place to act as the glue between a variety of tools.

This, combined with the previously mentioned fact that organizations have experienced an average of five serious security breaches in the last year, supports the premise that trusting security tools alone may be misguided. Businesses need to routinely manage and update their security monitoring solutions—something a strong MDR provider would be able to do.

To improve transparency with security vendors, security teams can establish regular touchpoints with a qualified technical account management team, which can act as strategic advisors, while acting as client advocates to escalate requests within the vendor organization. A customer portal where security activities, service requests and reporting can be tracked would not only be an asset but also enhance the customer experience. Working with a provider that can provide remediation guidance regarding specific types of threats is crucial. In addition, having vendor insights as to how they are protecting your business, as well as the roles and responsibilities between their different teams and yours will help bolster the levels of transparency, and in turn trust.

# 3 - The Benefits of Trust are Overshadowed by the Lack of It

## Part 1: The Reasons for Trust Depreciation are Wide-Ranging

A lack of communication is the most frequent cause for a loss of trust, as reported by 47% of information security decision-makers. This is a concern because communication is crucial when coordinating cyber teams to defend against threats. Limited technical capabilities (45%), experiencing numerous incidents (44%), and not having enough people in the team (43%) are also significantly impacting trust levels.

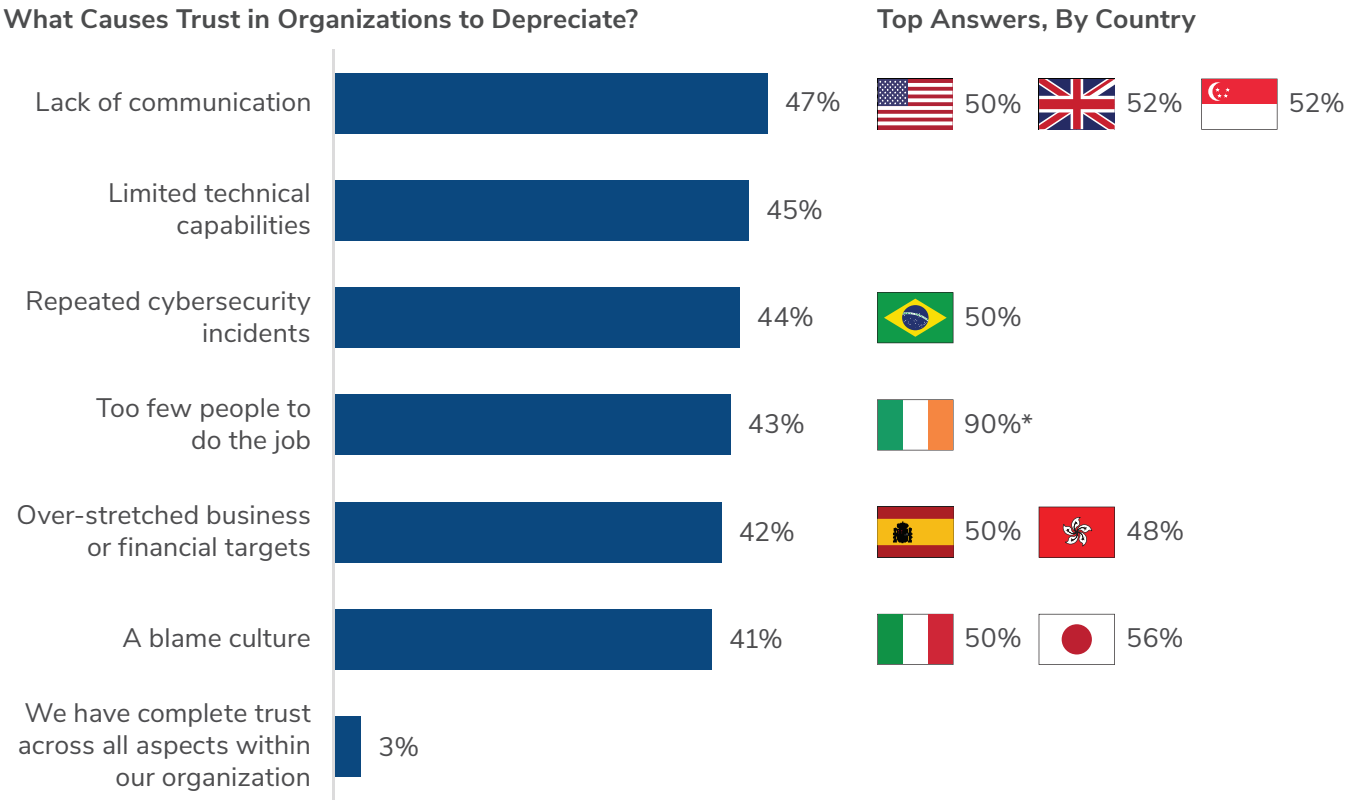



*Figure 9: What causes trust in your organization to depreciate? [1000], omitting some answer options, showing the top selected answer option by country. Note low base size, less than 30 respondents (Ireland)**

Looking at countries individually, the U.S., the UK and Singapore report a lack of communication as their top reason for trust depreciation, with a blame culture reported in Italy and Japan, and repeated cyber incidents cited in Brazil.

With almost all (97%) reporting that they *do not* have complete trust across all aspects of their organization, this is clearly a widespread concern for IT leaders with potentially damaging consequences, as we outline in the next section.

## Part 2: Everyone Agrees there are Negative Consequences of a Lack of Trust

An overwhelming majority (98%) agree that there is a cost to a lack of trust in the workplace, and this cost can be far-reaching.

**Consequences of a Lack of Trust in the Cyber Environment**

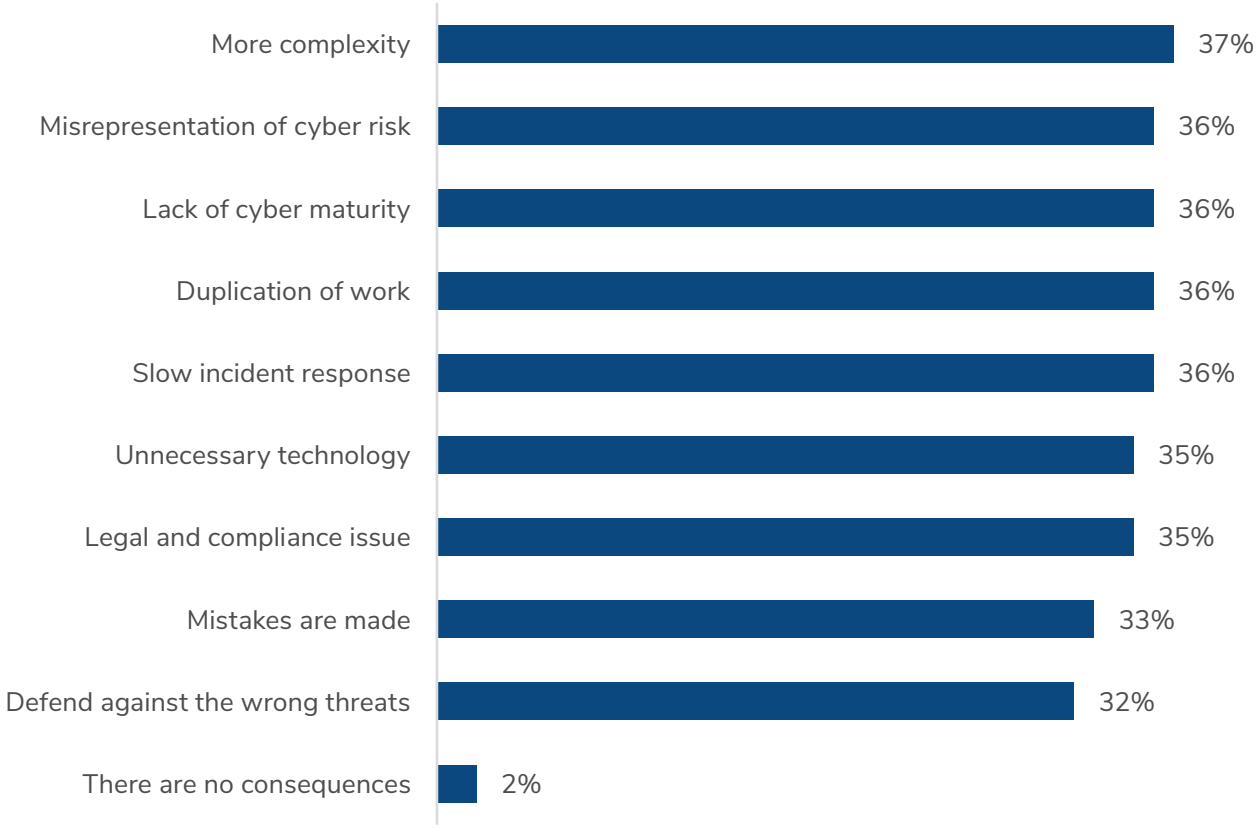



*Figure 10: In general (thinking about other organizations as well as your own), what do you believe are the consequences of a lack of trust in the cyber environment? [1000], omitting some answer options*

Over one-third of respondents cite factors such as duplication of work, wasting resources and heightened costs (36%), slow incident response (36%) and unnecessary technology (35%) as the top consequences.

Different countries experience these varying consequences more deeply, with duplication of work most keenly felt in Spain and Hong Kong (42% and 40%, respectively), slow incident response in Japan and Brazil (both 48%), and unnecessary technology in the UK and Singapore (43% and 46%, respectively). Defending against the wrong threats is equally of most concern in Hong Kong (40%), and the U.S. reports more complexities as their highest perceived consequence (37%).

## Part 3: How can Trust be Built?

Nearly half (48%) of IT and security decision-makers suggest that an all-encompassing cyber defense strategy with both preparedness and response processes is a successful way to build trust along with having a better understanding of the root cause of cyberattacks (40%).

As we saw earlier, greater understanding can only serve to improve cyber defense. Building a closer collaboration between in-house security teams and external security service providers (40%) is also recognized as being an important part of building trust. This means that organizations appreciate the expertise of external providers.

Further to this, improving processes and ensuring clarity will also assist organizations in their quest for trust. Our findings show that information security teams processes can be improved in three quarters of cases (74%) and aligning expectations with all users will increase confidence in how organizations respond to and deal with cyber threats.

**Are Improvements Needed in Your Organization's Security Teams' Processes**

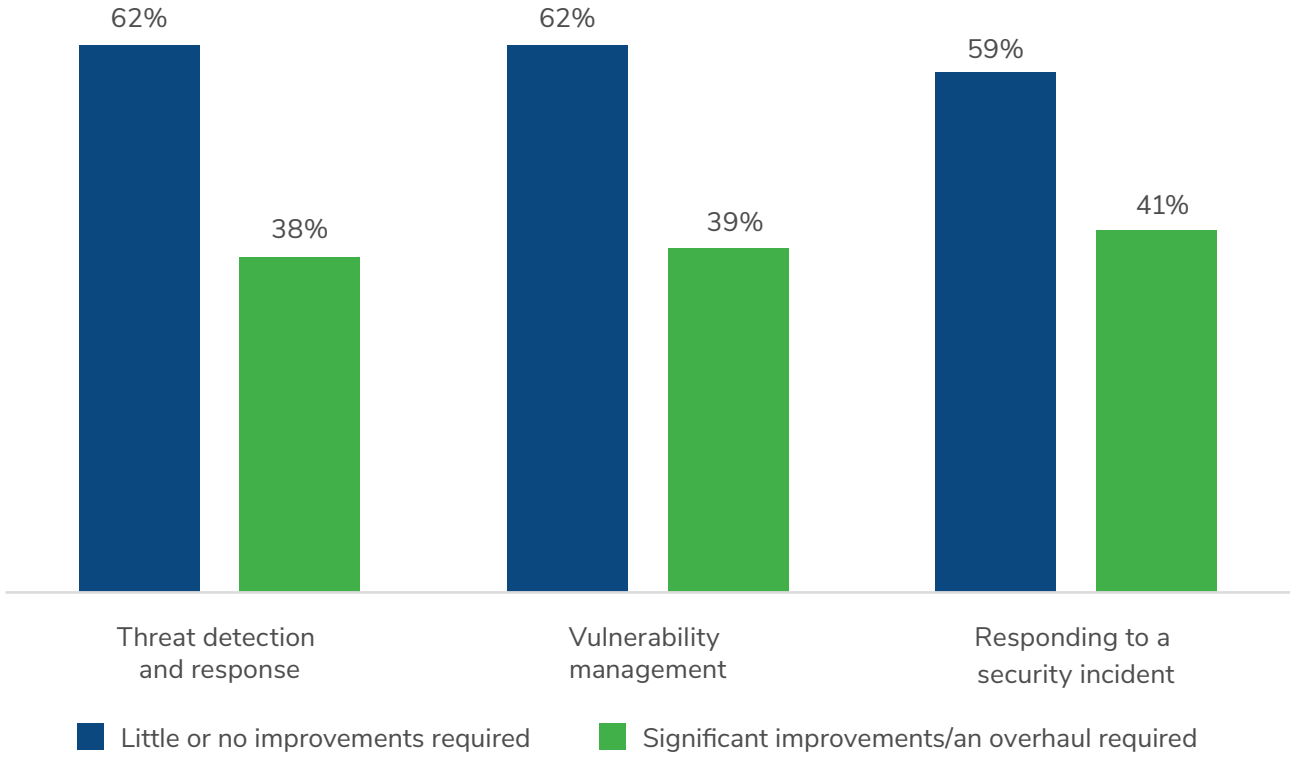



*Figure 11: How do you feel your organization's IT/Security teams' processes could improve for the following? [1000], omitting some answer options*

# Mitigating the False-Positive of Trust

Trust is critical to cybersecurity. Yet, our findings reveal a concerning inconsistency between the level of trust organizations have in their readiness to achieve true cyber resilience. Of course, without confidence in their security tools and teams, organizations cannot attain a robust security maturity. However, when trust in people and processes is misplaced or excessive, it can itself present further security threats to organizations. While organizations are cognizant of the potential risks and the importance of taking action, it would appear they don't always apply this awareness in practical terms.

This organizational cognitive dissonance is putting companies at significant risk, suggesting an incomplete understanding of what is involved in true cyber maturity. This is further demonstrated by the fact that the higher the average number of platforms used, the more cybersecurity incidents experienced by the organizations. Clearly many organizations are motivated to invest in security solutions to address their issues, however, these cannot be relied upon without an effective strategy backed with proven expertise.

## Moving From Assumptions to Assurance

So, how can companies move beyond unsafe assumptions about their cybersecurity to become fully cyber resilient? Making this step forward involves staying up-to-date about evolving cyber threats, gaining in-depth understanding of what their security tools can actually defend them against and maximizing tooling in response. Organizations can achieve this by working with a trusted external partner to gain an independent and accurate perspective on their security status. Specialist support will provide the critical viewpoint needed to help businesses avoid internal security siloes and enhance their knowledge with constantly updated threat insight.

An effective MDR solution delivers comprehensive insight and greater ability to respond to threats. Organizations should ensure that the MDR solution they choose includes EDR technology as many businesses surveyed are still not using it to its full potential.

In a security landscape characterized by constantly diversifying threats, it is imperative that organizations ensure that their trust in people, processes and security tooling is matched with real-world strategy. This means moving away from long-held assumptions and moving toward greater self-awareness about gaps in knowledge and practices. Further, by leveraging proven partners and resources to consistently address potential threats, businesses can progress beyond the false-positive of trust to become truly cyber mature.

## Advance Your Cyber Defenses with Kroll

As a leading provider of end-to-end cybersecurity, digital forensics and breach response services, responding to over 3,000 security events every year, Kroll is well-placed to help you benefit from full confidence in your cyber defenses. Kroll Responder, our industry-leading managed detection and response solution, is powered by a team of seasoned incident response experts and frontline threat intelligence to deliver unrivaled response. Kroll Responder is now one of the only solutions in the market that delivers MDR with "Complete Response." You can rely on Kroll's prioritized response and global resources in a crisis with our cyber risk retainer which offers maximum flexibility with transparent pricing. With Kroll on your side, you can trust in your cyber defenses against the threats of today and tomorrow.

**Learn more about Kroll's services.**

# Methodology:

Kroll commissioned independent market research agency Vanson Bourne to conduct research into the state of cyber defense.

The study surveyed 1,000 senior IT security decision-makers in February and March 2023, all of whom had some responsibility or knowledge of cybersecurity within their organization. Respondents were from USA, UK, Ireland, Spain, Italy, Singapore, Hong Kong, Japan and Brazil.

Respondents were from organizations with between $50 million and $10 billion in revenue, across the following sectors: manufacturing, education, technology and telecommunications, healthcare, retail, financial services and insurance, energy, professional services, transportation, hospitality, government, not for profit, and industrial services.

All interviews were conducted using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.

## About Kroll

As the leading independent provider of risk and financial advisory solutions, Kroll leverages our unique insights, data and technology to help clients stay ahead of complex demands. Kroll's global team continues the firm's nearly 100-year history of trusted expertise spanning risk, governance, transactions and valuation. Our advanced solutions and intelligence provide clients the foresight they need to create an enduring competitive advantage. At Kroll, our values define who we are and how we partner with clients and communities. Learn more at Kroll.com.

## About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision-makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com.

KROLL

For the latest insights, threat intelligence, and analysis from Kroll check out kroll.com/cyberblog

## TALK TO A KROLL EXPERT TODAY

**North America**
T: 877 300 6816

**UK**
T: 808 101 2168

**Hong Kong**
T: 800 908 015

**Additional hotlines at:**
kroll.com/hotlines

**Singapore**
T: 800 101 3633

**Australia**
T: 1800 870 399

**Brazil**
T: 0800 761 2318

**Or via email:**
CyberResponse@kroll.com

---

**About Kroll**

As the leading independent provider of risk and financial advisory solutions, Kroll leverages our unique insights, data and technology to help clients stay ahead of complex demands. Kroll's global team continues the firm's nearly 100-year history of trusted expertise spanning risk, governance, transactions and valuation. Our advanced solutions and intelligence provide clients the foresight they need to create an enduring competitive advantage. At Kroll, our values define who we are and how we partner with clients and communities. Learn more at Kroll.com.

*M&A advisory, capital raising and secondary market advisory services in the United States are provided by Kroll Securities, LLC (member FINRA/SIPC). M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Kroll Securities Ltd., which is authorized and regulated by the Financial Conduct Authority (FCA). Valuation Advisory Services in India are provided by Kroll Advisory Private Limited (formerly, Duff & Phelps India Private Limited), under a category 1 merchant banker license issued by the Securities and Exchange Board of India.*