CEO • DIGITAL

STRENGTHENING BUSINESS RESILIENCE

An industry report 2023

A CEO.digital report commissioned by Dataminr®

TABLE OF CONTENTS

IN THIS REPORT, WE'VE CAPTURED A VIVID PICTURE OF A RISK LANDSCAPE SHIFTING TOWARDS A MORE RESILIENT FUTURE.

Ch.1 INTRODUCTION

In the last few years, the risk landscape has undergone many seismic shifts. Beginning with COVID-19 and culminating with the war in Ukraine, global enterprises have faced serious business disruptions. The frequency, complexity and persistence of threats have increased in both the physical and cyber realms.

How are forward-thinking chief security officers (CSOs) and chief information security officers (CISOs) recalibrating their response? This report, commissioned by Dataminr, answers that question.

We surveyed both physical and cyber security leaders in Europe, the UK and the US, to identify the biggest technical and organisational challenges they face in strengthening their security posture and business resilience. In follow-up interviews, we also asked how they planned to navigate this complex new terrain.

An illuminating picture emerged from the results. Lack of resources and skilled staff, budget cuts, and corporate retrenchment – all created a scenario in which effectively responding to threats became even more challenging. It also made it much more difficult for businesses to bounce back from disruptions.

Further, having too much data without the right context and not knowing how to extract and prioritise the most relevant information has slowed down decision making.

As one participant trenchantly put it, "Visibility is a double-edged sword."

Most interestingly, security leaders are already keenly aware of their challenges and potential solutions. They see AI as a great aid in making sense of things on the ground in real time. Equally, they view public data sources as a valuable well-spring of insight. They also realise that their businesses can benefit from greater collaboration between cyber and physical security teams. Many of the participants are already taking tangible steps in that direction.

> “SECURITY REQUIRES THE ABILITY TO DISCERN WHICH ALERTS MATTER AND WHICH DON’T. AND IT’S A SKILL THAT TAKES TIME TO CULTIVATE.”

SETTING THE STAGE

The survey approached the question of business resilience from both physical and cyber security perspectives. Respondents came from two types of organisations: Those in which these two security functions operated separately, and those with collaboration between the two. We were interested in uncovering how different ways of working affect their overall effectiveness.

To draw out this nuance, responses throughout this report have been broken down across the job functions.

Throughout the survey, we’ll also be using the term ‘alert’ to mean ‘a brief, human-readable notification regarding current risk events, vulnerabilities, exploits, and other security issues.’ Alerts provide information that security teams need to respond to threats and mitigate the risks associated with them.

METHODOLOGY:

Total number of people surveyed:	2700
Total number of responses:	~500
Total number of responses accepted:	50
Total number of interviews conducted:	5

Industries where the interviewees are from:

Corporate insurance
Information technology
Financial technology

Risk detection maturity is the degree to which security teams can identify and assess risks in a way that helps them mitigate the negative repercussions of any given threat—using real-time information to inform decisions regarding security operations.

On an average, respondents had a risk detection maturity score of 6.7 on a scale of 10.0 which meant they had no reliance on real-time event detection to make decisions, while 10 meant that they had complete reliance on real-time data.

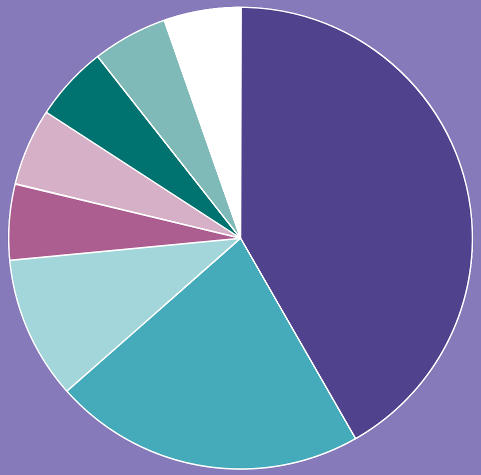

FIG. 1

RESPONDENTS’ JOB FUNCTIONS

- Executive Board Member
- Security Operations Director
- Physical Security Specialist
- CEO, Founder
- CRO
- CISO
- CSO
- Analyst

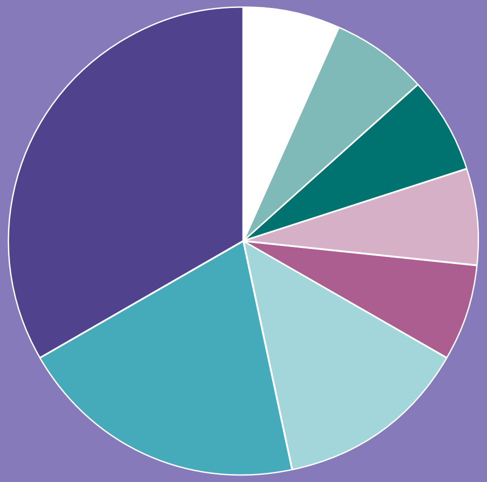

FIG. 2

WHERE DO RESPONDENTS COME FROM?

- Estonia
- Lithuania
- France
- Ukraine
- Romania
- United States
- Spain
- United Kingdom

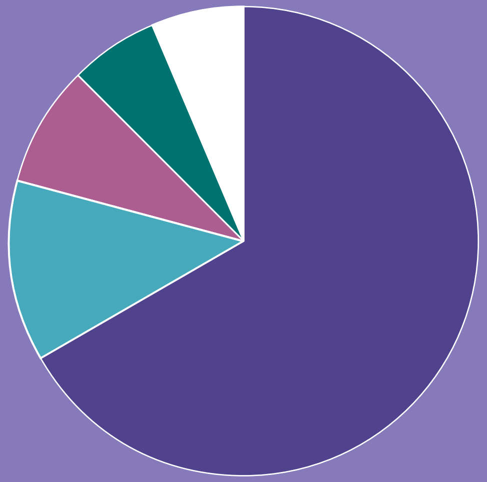

FIG. 3

RESPONDENTS’ ORGANISATION SIZE

- <20,000
- <10,000
- <50,000
- <100,000 and more
- <5,000

IN THE LAST 12 MONTHS, WHICH FACTORS HAD THE MOST IMPACT ON YOUR SECURITY POSTURE AND BUSINESS RESILIENCE?

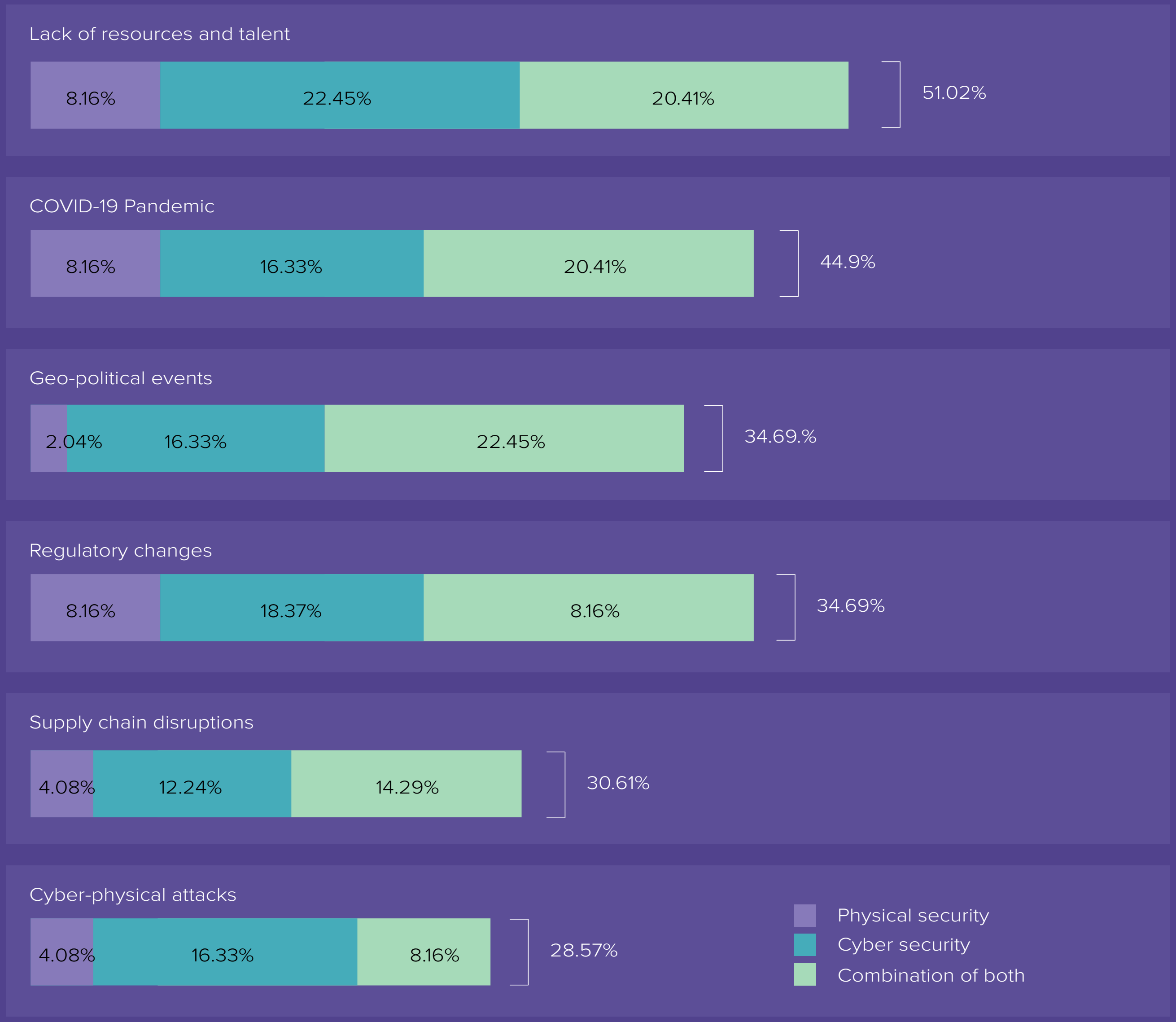

FIG. 4

Main Takeaway

Talent shortage is a major stumbling block for both cyber and physical security leaders in strengthening business resilience.

More than half the respondents cited 'lack of resources and talent' as having had the most negative impact on their security operations and business resilience over the last 12 months. The lack of a consistent and skilled workforce has made it more difficult to identify threats, mitigate risks, maintain business continuity and strengthen business resilience.

ONE CISO BASED IN THE UK EXPLAINED THE SITUATION IN THE FOLLOWING WORDS:

"Security isn't guess work. It requires the ability to discern which alerts matter and which don't. And it's a skill that takes time to cultivate. But today, the job market has tilted towards the candidate, and it has become much harder for us to attract and retain candidates who have this skill."

ANOTHER UK-BASED CISO CONFIRMED THIS VIEW:

"We saw a challenging period when skilled employees were leaving companies. If you lookat the market today, you'll see that many senior analysts have become consultants who work independently. We're seeing lots of 'fractional' employees, who move from company to company because they're in such high demand."

The phenomenon of 'great resignation' is now spreading and taking a toll on cybersecurity in particular. According to research by BlackFog, nearly 90% of CISOs report being "moderately" or "tremendously" stressed. The average tenure of a CISO in an organisation is just over 2 years.

In the following sections, we'll explore how this lack of resources, coupled with other challenges identified in the figure 4, creates a formidable hurdle to strengthening business resilience.

THE SITUATION IS LIKE HEARING A WINDOW BREAK IN YOUR HOME IN THE MIDDLE OF THE NIGHT. UNTIL YOU GO AND EXAMINE EACH WINDOW, YOU WON’T KNOW WHERE YOUR HOME HAS BEEN BREACHED – OR IF IT WAS EVEN A REAL BREACH.

Ch.2
CHALLENGES AND SOLUTIONS

The challenges and solutions split across two areas: technical and organisational. The technical area pertains to the procedural aspects of security operations. From where do they gain threat intelligence? How quickly are they able to operationalise this information?

The organisational area pertains to the structural aspects of the whole business. How does budgeting affect security operations? Are silos helping or hindering business resilience?

Making this distinction allowed us to extract a richer picture of the problems that security leaders face.

“GRANULARITY IS IMPORTANT BECAUSE IT ALLOWS US TO OBSERVE WHERE THE THREAT IS EMANATING FROM AND MITIGATE IT AS QUICKLY AS POSSIBLE.”

TECHNICAL CHALLENGES

More than half of those surveyed reported that having ‘too many disparate tools and platforms’ is the single biggest technical challenge in strengthening their security posture and business resilience.

Security analysts spend the better part of their day keeping track of alerts and correlating data from multiple platforms.

ONE PARTICIPANT EXPLAINED:
“This leads to alert fatigue. Not having the right tooling negatively impacts job performance and productivity. It can be quite stressful to work in a chronically reactive environment. People just leave.”

WHEN ASKED HOW THE RESPONDENT’S TEAM DEALT WITH THE PROBLEM, THE CISO EXPANDED:
“We manually consolidate our platforms. Our metrics team sets up the data feed from various tools we use; it takes time, and the data we have isn’t always granular... Granularity is important because it allows us to observe where the threat is emanating from and mitigate it as quickly as possible.”

ONE RESPONDENT COMPARED THE SITUATION WITH THE “TOOL WHICH CRIED WOLF”:
“We have all this information on our hands and no way of sifting through it to get the full picture. Frequent low-quality alerts mean we have no idea which ones to prioritise. It can make people complacent.

“The situation is like hearing a window break in your home in the middle of the night. Until you go and examine each window, you won’t know where your home has been breached – or if it was even a real breach. But let’s say you hear a window break every day. On a night that you’re particularly tired, you may decide to sleep through it. That may be when you’re actually burgled.”

In other words, the more context an alert has, the less effort it takes to make sense of an evolving threat and the faster your security team can act.

Main Takeaway

Lack of granular, real-time data within a common operating picture is slowing down security teams and costing time, effort and money.

WHAT ARE THE BIGGEST TECHNICAL CHALLENGES YOU FACE IN IMPROVING YOUR SECURITY RESPONSE AND BUSINESS RESILIENCE?

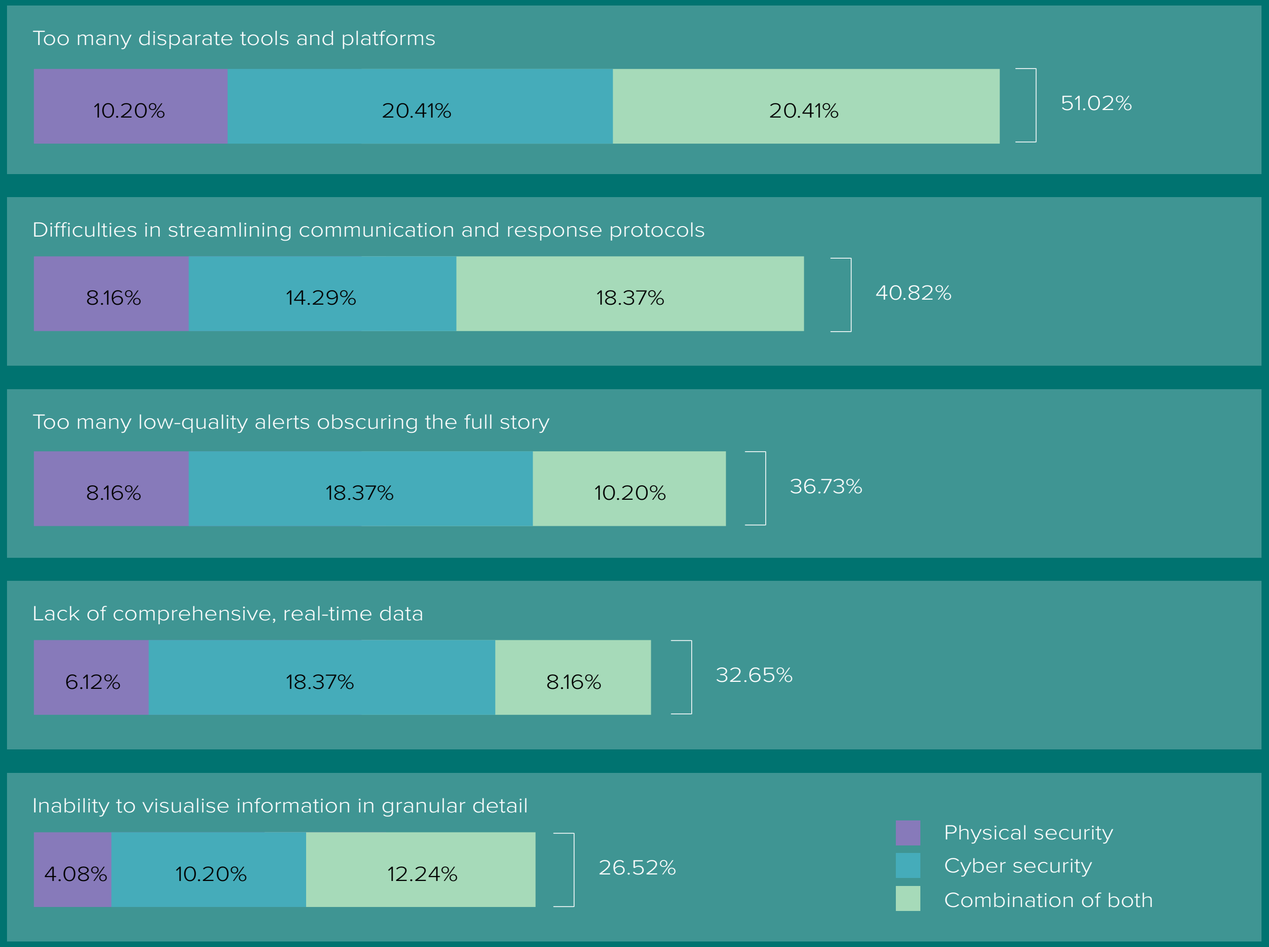

FIG. 5

WHEN WE ASKED WHAT THE IDEAL SOLUTION WOULD LOOK LIKE, THE RESPONDENT HIGHLIGHTED ABOVE EXPLAINED:

“It would first of all focus on quality rather than quantity. It would provide the complete picture... How and when is a threat likely to affect us? How long do we have before we respond? Whom should we alert and where exactly are they now?”

Knowing these vital details upfront means security teams can make rapid decisions that save lives, protect infrastructure and ensure business continuity. But gathering them manually can be self-defeating. Even well-resourced security teams cannot manually go through the sheer volume and variety of information available and pick out the most relevant indicators of risk in real time. This is precisely where AI can help.

But building the capabilities to extract such context-rich information through AI requires buy-in from management as well as budget and time.

The next section considers how these factors pose a challenge to security teams.

> “SECURITY TEAMS HAVE HIGHLY SPECIALISED PERSONNEL WHO ARE VERY GOOD AT SPECIFIC TASKS. WHEN THEY LEAVE, IT BECOMES MUCH HARDER TO HIRE THEM.”

ORGANISATIONAL CHALLENGES

The economic crisis, catalysed by COVID-19 and accelerated by the war in Ukraine, has forced many enterprises to take a harder look at their expenditure and cut costs.

More than half of those surveyed reported that they were unable to procure more funding for security operations.

This meant they were unable to acquire new solutions, hire new employees, or upskill existing ones. Coupled with the talent scarcity noted in the first section of this report, it becomes easy to see why lack of new investment is so disruptive to security operations.

Budget cuts exacerbate the problem of talent deficit in two very difficult ways. On one hand, it becomes much harder to hire people with the right skill levels; on the other hand, employees who don’t see growth in the team leave for greener pastures elsewhere. It’s a problem that’s not unique to security, of course, but nonetheless a thorny issue for the industry.

To circumvent the problem, many enterprises are also weighing the benefits of moving security from capital expenditure to operational expenditure models (OPeX). Outsourcing security operations (or buying subscription-based security tech) allows enterprises to avoid large capital investments, simplify their budgeting, scale more quickly, and offload the responsibility of staying up to date with service providers. It also means they no longer must worry about staffing shortages.

But even the shift to OpEx cannot solve the problem of silos, which appeared as the second biggest organisational stumbling block to better security and resilience.

ONE FINLAND-BASED LEADER WHO OVERSEES BOTH PHYSICAL AND CYBER SECURITY EXPLAINED:

“Security teams have highly specialised personnel who are very good at specific tasks. When they leave, it becomes much harder to hire them at a salary offered by the market for a person of that competency.”

Main Takeaway

Budget cuts and entrenched silos are negatively impacting security response and business resilience.

WHAT ARE THE BIGGEST ORGANISATIONAL CHALLENGES YOU FACE IN IMPROVING YOUR SECURITY RESPONSE AND BUSINESS RESILIENCE?

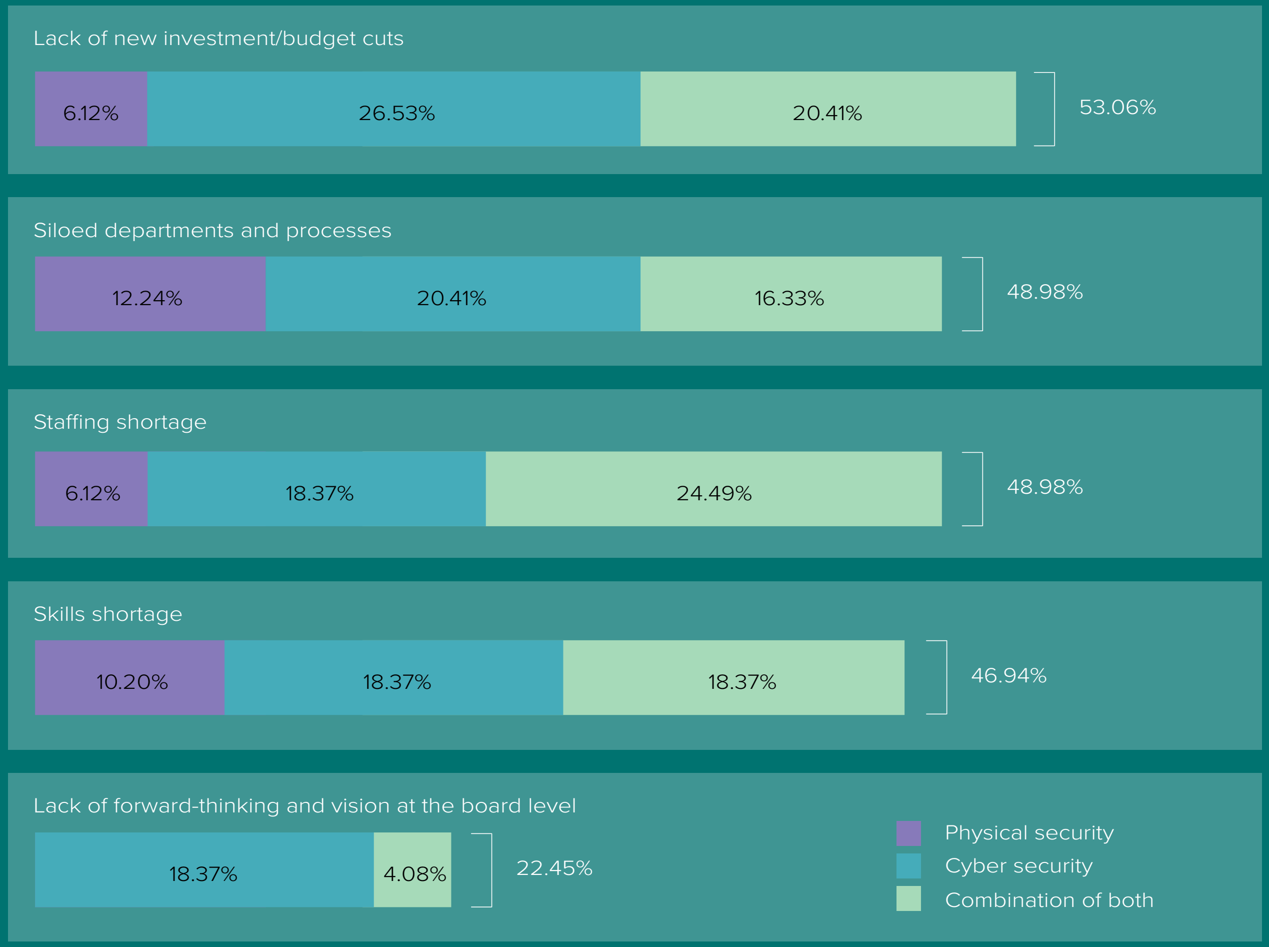

FIG. 6

EXPLAINING HOW SILOS CAN AFFECT BUSINESS, THE SAME FINNISH LEADER FROM ABOVE COMMENTED:

“Silos are where vulnerabilities hide. It leads to wasted effort. Different teams could be trying to mitigate the same threat. For instance, the HR team could be aware of an employee terminated for policy violation. The same person may end up committing workplace violence or leaking vital information.”

To find the way forward, a holistic approach to security is required at the board level. Businesses now operate in a hyperconnected world where the chances of cascade effect from high-impact events are extremely high. To keep everyone safe in such a situation, security leaders must think about how they’re going to share the right information with the right stakeholders at the right time – without overburdening their limited resources.

In the pages that follow, we’ll explore how security leaders are recalibrating their strategy in response to the shifting risk landscape.

"WHAT DO WE DO WHEN WE LEARN OF A POTENTIAL THREAT? WE CAN'T LOSE TIME BY PLANNING AT THAT MOMENT WHO IS GOING TO DO WHAT."

TECHNICAL SOLUTIONS

Geopolitical events, changes in regulation (for example the Supply Chain Due Diligence Act), and the shift to hybrid working have widened the threat landscape for global enterprises. Furthermore, expansion through acquisition also brings in new unknowns for security leaders. It's a major challenge to deal with this ever-evolving profile of risks using limited expendable resources. To cope, security leaders are increasingly turning towards AI and public data as a source of powerful additional insight.

AI can reduce the amount of work needed to gather intelligence, minimise the margin of human error and speed up decision making. It can allow your teams to quickly correlate vast amounts and varieties of data and surface the most relevant signs of risk in real time.

ONE CHIEF SECURITY & SAFETY OFFICER, SPEAKING FROM GREECE, EXPANDED:

"[AI] is now sophisticated enough to rapidly make sense of vast mountains of data. It is helping us pick out patterns which would fly under the radar of human attention. At a time when we don't have enough resources, this is a great time saver for us, and when it comes to crises, time is everything."

WHEN WE ASKED FOR AN EXAMPLE OF HOW AI HELPED THEIR TEAM MAKE SENSE OF THE DATA AND TURN IT INTO ACTIONABLE INSIGHT, THIS RESPONDENT SPOKE OF THE PROTESTS IN GREECE OVER THE TRAGIC TEMPI TRAIN CRASH:

"The AI solution we use picked up on certain threats. Our [global] security team alerted the team leaders in the city. We closed the office in anticipation of potential violence and the employees were advised to work from home."

Another UK-based leader spoke of a scenario in which AI can be quite useful. They cited the example of the 'Act on Corporate Due Diligence Obligations in Supply Chains' that kicked-in on 1 January 2023.

This Act covers an expansive range of human rights and environment-related legal positions and requires German companies and subsidiaries to account for a host of new challenges in the high-risk countries in which they operate. These issues include child labour, forced labour, slavery, occupational health and safety obligations and freedom of association, among others.

Main Takeaway

Security leaders view AI-based solutions as a force multiplier for their teams. AI helps supplement the talent deficit and create more business value with less.

IN THE NEXT 12 MONTHS, HOW DO YOU PLAN TO SOLVE THE TECHNICAL CHALLENGES YOU'RE FACING?

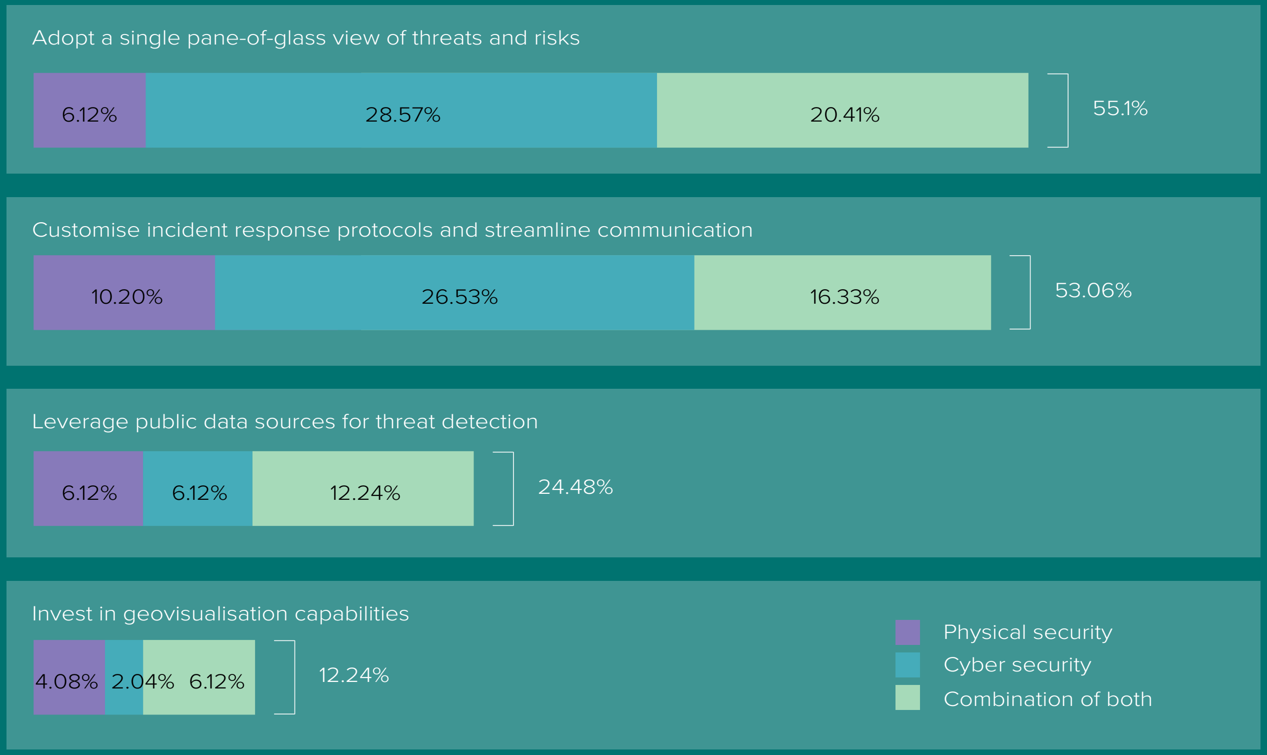

FIG. 7

EXPLAINING THE SITUATION, THE SAME LEADER SAID:

"If security and compliance teams had to keep track of all the risks implied in this law, that's all they'd be doing each day. But with AI, we can scour the media for potential problems and surface exactly those things that are likely to burst into flames later.

"What do we do when we learn of a potential threat? We can't lose time by planning at that moment who is going to do what. We need to already know who will do what, almost like muscle memory."

Intentional or negligent violations of due diligence obligations can be punished with a fine of up to EUR 8 million. A company with an average annual turnover of more than EUR 400 million can be fined up to 2 percent of its average annual turnover.

AI is indeed a great aid to decision making, but it's only the beginning. To seamlessly operationalise AI-generated insights, a scenario-based incident response protocol that accounts for the various eventualities is a prerequisite.

In simple terms, it's not just what you know, but how quickly you can act on it when you find out.

But this discussion of the technical solutions is incomplete without an understanding of how security leaders are planning to solve their organisational dilemmas. We'll see in the next section how security leaders use a data-driven approach to impress upon their C-suite peers the value they create for the enterprise.

IN THE NEXT 12 MONTHS, HOW DO YOU PLAN TO SOLVE THE ORGANISATIONAL CHALLENGES YOU'RE FACING?

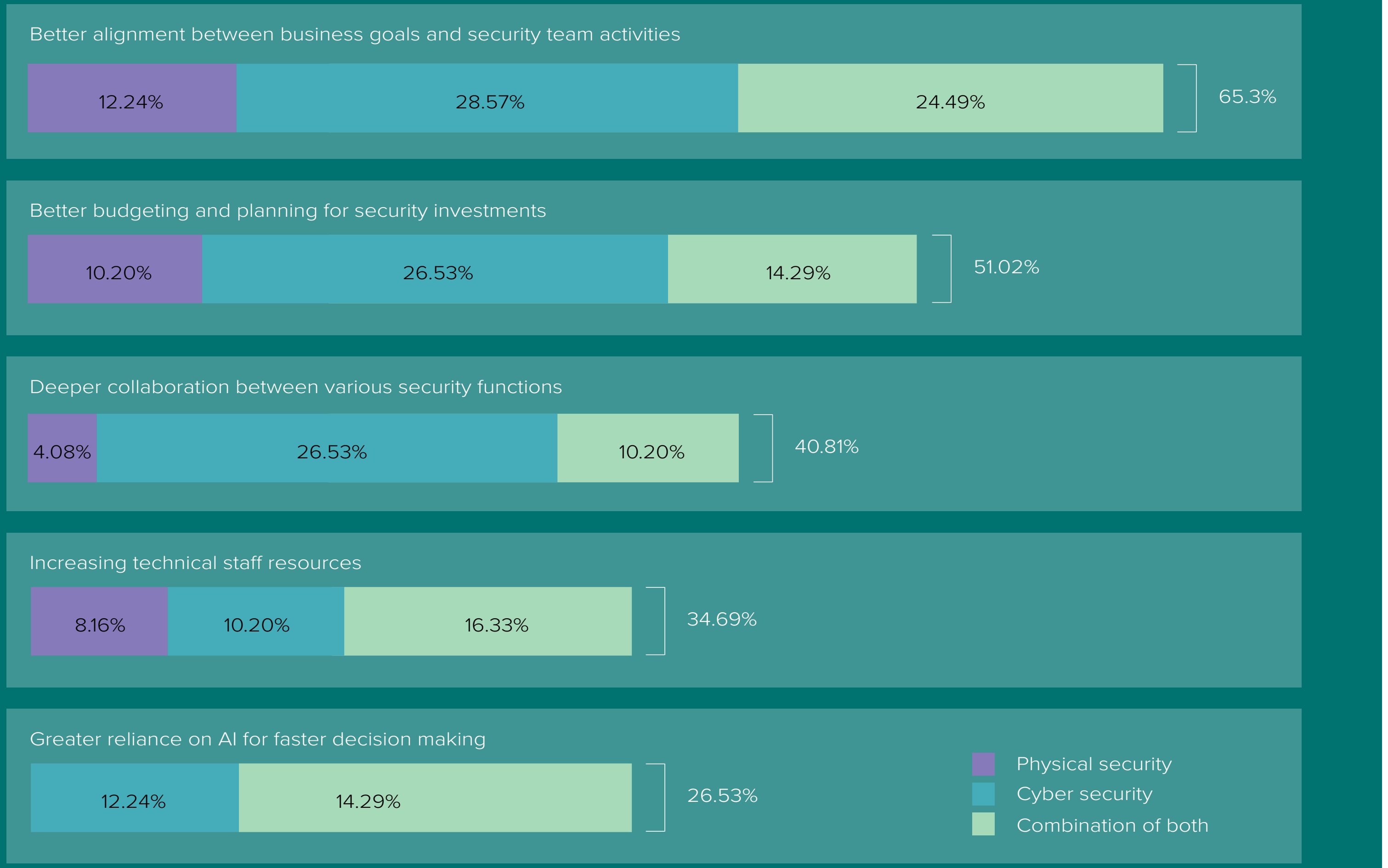

FIG. 8

ORGANISATIONAL SOLUTIONS

While directly making a case for "better budgeting and planning for security investments" may seem like the obvious first choice, security leaders solve their organisational challenges differently.

FOR INSTANCE, A CISO IN ESTONIA', SPOKE OF ALIGNING BUSINESS GOALS BY PROVIDING THIRD-PARTY RISK REDUCTION:

"I demonstrate the business value of better risk management and compliance by showing how they give us more clients, especially in Estonia which is driven by e-services. Proving risk management and compliance gains us more trust from the clients. It means that we're more likely to be chosen as the next partner among many."

"We provide services to healthcare, telcos, fintech and governmental organisations... There's a very high probability that we'll be used as a proxy. It means that we have to be extremely careful about not endangering clients with the operations we do.

"There have been cases like the Lockheed Martin attack where the security token company (RSA Security) was compromised. . . Third party became the vector of attack on governmental agencies, and we don't want to be that."

Directly correlating security activity with mitigated risks, saving lives and protecting the bottom line are what matter most to CEOs, CIOs and CFOs, who are becoming the three most consequential figures on organisations' boards for security and risk oversight and decision making.

AS CISO OF CUSTOMERS BANK, ENDRE WALLS, NOTES IN THIS FORBES ARTICLE:

"The CSOs and CISOs may have a more difficult task, especially if their CEOs aren't yet sold on the idea of elevating them. They must understand their companies inside and out so that they can communicate effectively across the C-suite about how their expertise and responsibilities are vital to maintaining a secure business."

So how can CSOs and CISOs ensure that their agenda remains a priority for the board? They must find ways to insert themselves into ever greater leadership environments and become a part of the innovation chain for the entire enterprise. They must not allow themselves to be pigeonholed into parts of business that just deal with technology and risks.

Letting your data do the talking can be a powerful way to break through the ceiling and seize the attention of top-level executives.

This is precisely where AI-based solutions are helping leaders by unearthing meaningful data through which they can demonstrate that their security teams are making a difference on a daily basis.

However, this is only a part of the solution. To fully align with business goals, security leaders are also questioning the conventional wisdom of siloing cyber and physical security. After all, hybrid threats—also known as the convergence of cyber-physical risks—are blurring the boundaries between cyber and physical domains. We asked how they expect their organisations to be affected by such threats. Figure 9 shows how they responded.

Cyber-physical threats can play out from both ends. A threat can start in the cyber domain and spill over into the physical, or vice versa. For example, a cyber attack on a factory's operational technology [OT] can cripple its production, bringing business to a standstill. Equally, a geopolitical conflict can trigger a cyberattack to exfiltrate confidential information.

Business leaders in asset-intensive organisations are keenly aware of a rise in hybrid threats. According to a 2023 PwC survey, 29% of organisations expect an increase in attacks on their operational tech. This includes access control devices, HVAC systems, monitoring and control devices, and programmable logic controls, among others.

IN THE NEXT 12 MONTHS, HOW DO YOU EXPECT YOUR ORGANISATION TO BE AFFECTED BY A CYBER-PHYSICAL HYBRID THREAT?

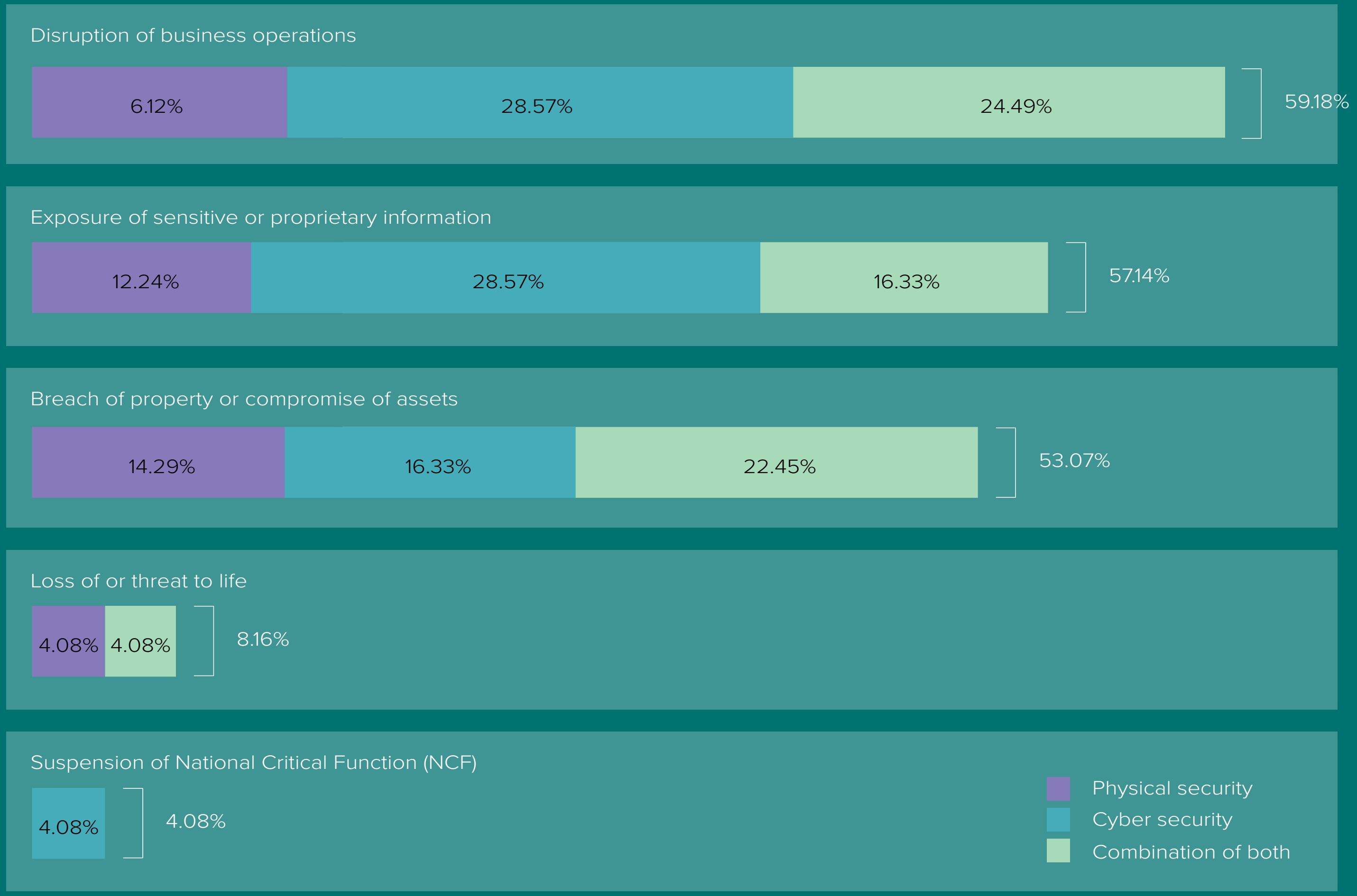

FIG. 9

ONE UK SECURITY LEADER EXPLAINED:

"Attackers used to scan the brands they're interested in for weaknesses. This has now changed. With new automation capabilities, bad actors now scan everything [including OT] to see if it is exploitable, identify what's worth taking and find a point of entry."

Consider for example the 2014 attack on Sony Pictures Entertainment. It was carried out by a group of six people, including at least one former Sony Pictures employee. Sony was made aware of the attack on 24 November 2014. But disgruntled employees had provided physical access to Sony's network months earlier. One of the hackers was even reported saying, "Sony left their doors unlocked, and it bit them. They don't do physical security anymore."

What began as a physical intrusion ended in a devastating cyberattack. The hackers claimed to have acted on behalf of North Korea with the cooperation of insiders. In the current political climate, security leaders are aware that similar scenarios can play out if they don't share information and work in tandem with their cybersecurity peers.

Main Takeaway

Security leaders are gaining senior management buy-in through a data-driven approach.

HOW DO YOU EXPECT YOUR ORGANISATION TO BENEFIT FROM GREATER COLLABORATION BETWEEN THE SECURITY FUNCTIONS?

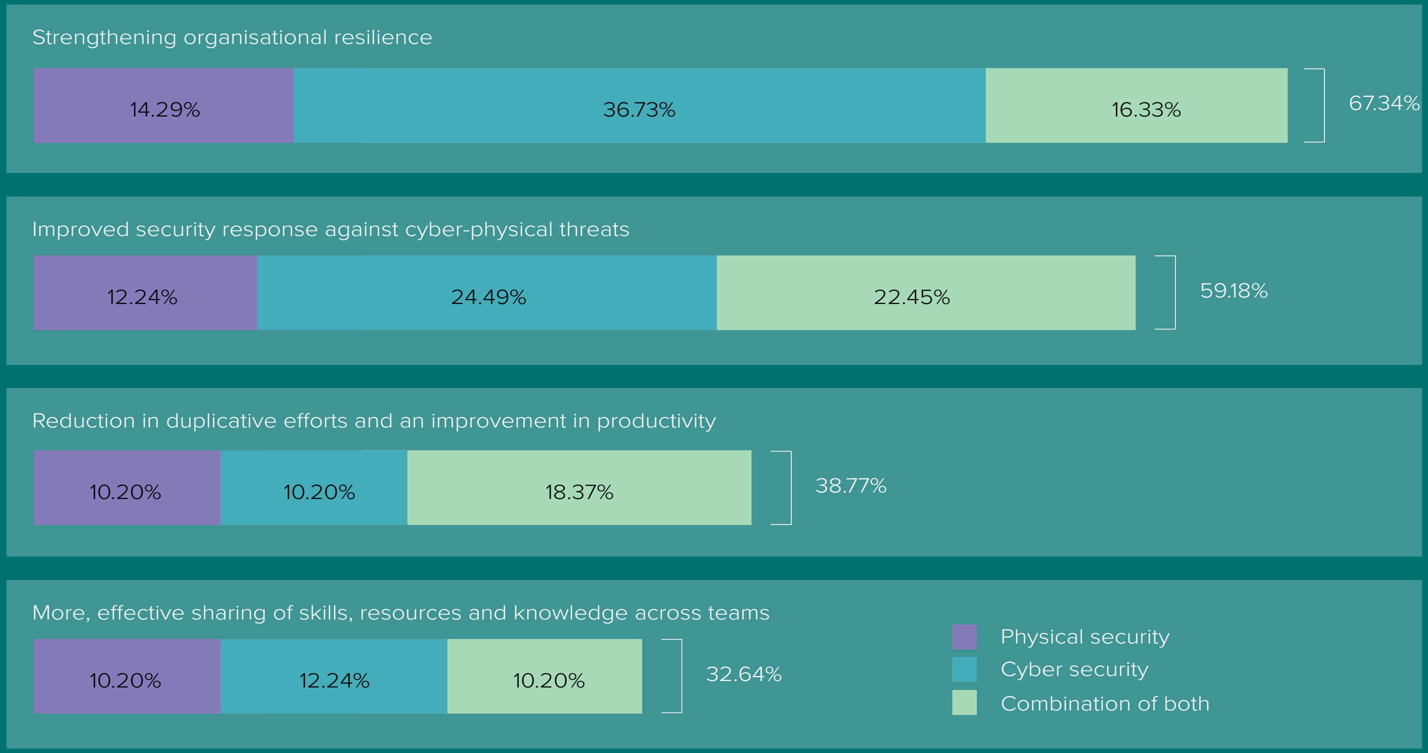

FIG. 10

AS ONE SECURITY LEADER EXPLAINED:

“People are moving around in the offices, like say, fire system technicians, cleaners, or whoever. Their background is not 100% checked. People can simply walk into your office and insert a USB device. You must be aware of those things.”

To protect against such hybrid threats, security leaders must cultivate a free flow of information between cyber and physical teams, identify overlapping vulnerabilities in their ecosystem, and coordinate response during crises.

Some organisations have responded by creating a single unified security function comprising both cyber and physical security teams, reporting to the same security leader.

Regardless of what approach is taken, de-siloing cyber and physical security teams is now timely as their worlds are colliding. Here’s how survey respondents see their organisation benefitting from greater collaboration between security functions:

In the next section of this report, we will consider these benefits in greater detail. We’ll also see how despite the many benefits of greater collaboration between cyber and physical security functions, there are several hurdles to overcome along the way.

COLLABORATION HAS INCREASED PRECISELY IN THOSE ORGANISATIONS WITH A FORWARD-THINKING CEO IN A PERIOD OF INTENSIVE GROWTH.

Ch.3

CYBER-PHYSICAL SECURITY COLLABORATION

Security leaders we spoke with almost unanimously agree that greater collaboration between security functions improved their business resilience.

HERE'S ONE LEADER EXPLAINING WHY COLLABORATION IS NEEDED GIVEN TODAY'S MODERN RISK LANDSCAPE:

"The traditional view that physical security begins where cyber security ends no longer works. We live in a very connected world. Imagine that one of your employee's information is doxed online. If you simply stop with just fixing the data breach, only half your job is done. Who's going to make sure that the employee is safe and doesn't fall victim to identity theft? You need to let this information flow to all the right people. Business continuity teams, physical security teams, HR."

ANOTHER LEADER EXPLAINS HOW TIGHTER COLLABORATION ACROSS TEAMS HELPED THEM UNCOVER HIDDEN VULNERABILITIES:

"When we began to collaborate with [physical] security, certain gaps became immediately apparent. We realised that both [the teams] assumed that the other team would be on top of these risks. So really, nobody was in-charge. Simply sharing information has helped us close the gaps and improve our overall security posture."

Thus, sharing information across teams not only improves security posture, it also reduces the amount of work each team has to do in order to track threats – especially during a time of dire talent crunch. Given all these benefits, how do organisations fare when it comes to protecting against cyber-physical threats? The picture presented in figure 11 emerged from our survey.

Over the last 12 months, collaboration between physical and cyber security has steadily increased. But this doesn't tell us the full story. We also asked why it had increased and Figure 12 shows our respondents answers.

An interesting correlation appears between C-suite mandate and an increase in collaboration between the two teams. Collaboration has increased precisely in those organisations with a forward-thinking CEO in a period of intensive growth.

There are several reasons for this. When a business is expanding, it becomes more justifiable to review the organisation's approach to security and set a new direction. But this requires the executive function of a bold, security-sensitive CEO willing to challenge the status quo and ask new questions. This is not incidental, as security leaders previously identified as an organisational challenge a 'lack of forward-thinking and vision at the board level'.

Furthermore, because the directive for increased collaboration was coming from the highest level of the organisation, it was also likely to override 'turf guarding'; when a team may feel strongly about others cutting into their territory.

Problems around "Culture & Skillsets" and "Turf & Silos" were also identified by ASIS International's detailed 2019 research on security convergence. As you'll see in the graph below, these findings line up perfectly with our survey results, illustrating why collaboration stayed the same or decreased over the last 12 months among a small group of organisations.

Entrenched silos and differing reporting structures are two main reasons where collaboration eludes many organisations.

In global organisations, the directive may come from above, but implementing it locally can still be a difficult problem. Team members can feel insecure about losing budget, resources and prestige by sharing it with the other team. Therefore, any conversation of de-siloing and collaboration must first address cultural challenges. Leaders must be willing to re-evaluate their goals, priorities and key performance indicators.

IN THE LAST 12 MONTHS, HOW HAS THE COLLABORATION BETWEEN THE SECURITY FUNCTIONS CHANGED?

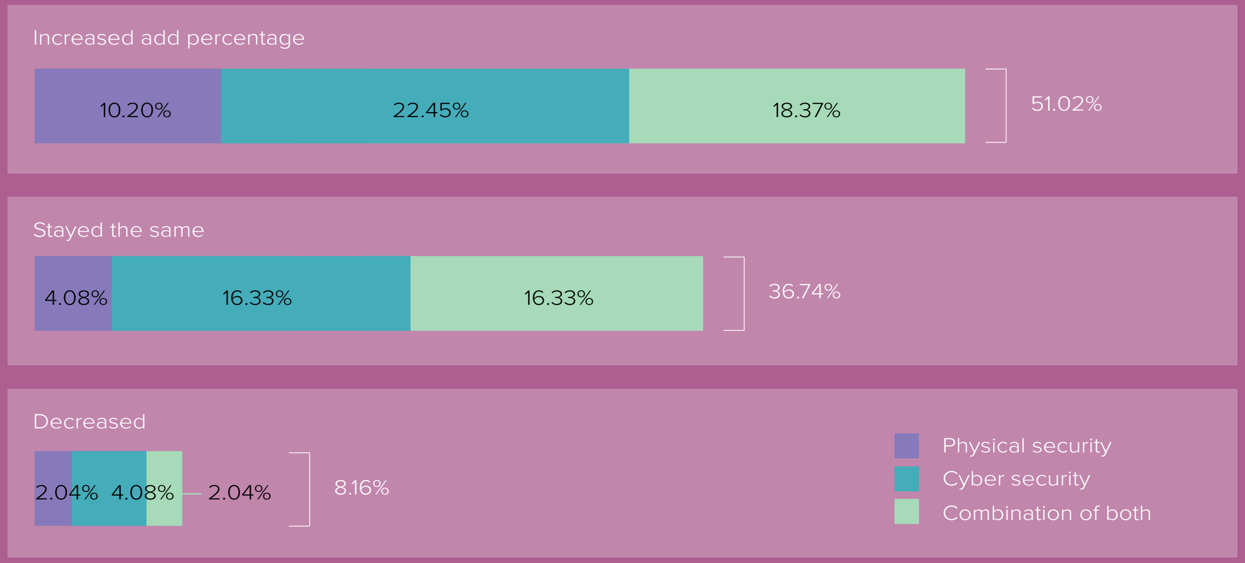

FIG. 11

WHAT WERE THE REASONS THAT COLLABORATION INCREASED?

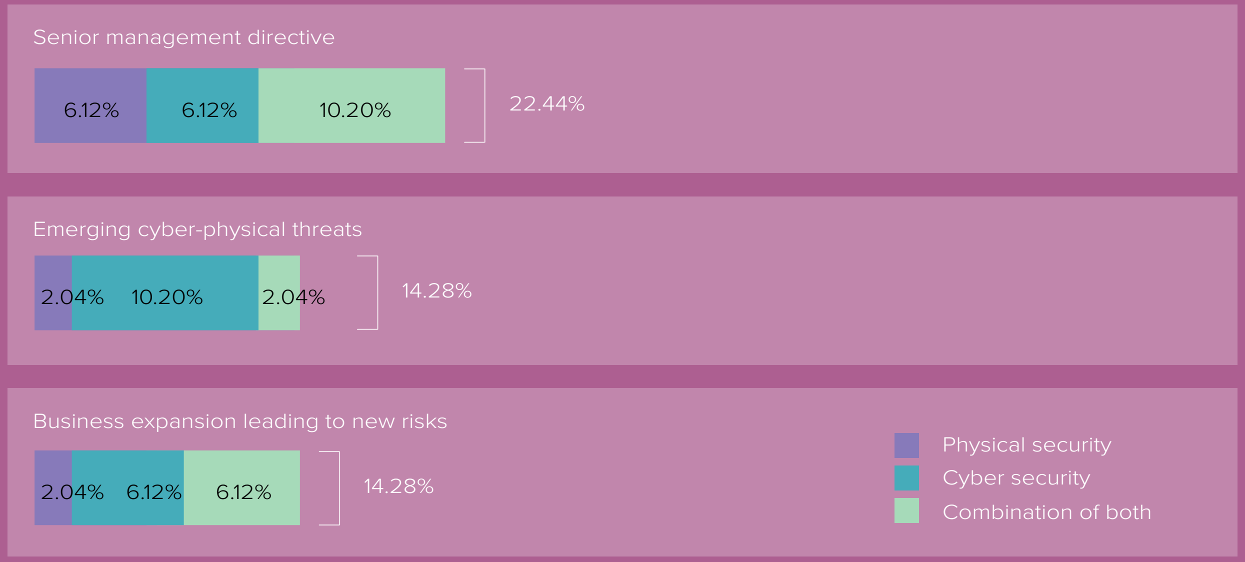

FIG. 12

Main Takeaway

Collaboration is increasing between the security functions, but cultural issues and silos stand in the way.

WHAT WERE THE REASONS THAT COLLABORATION DECREASED OR REMAINED THE SAME?

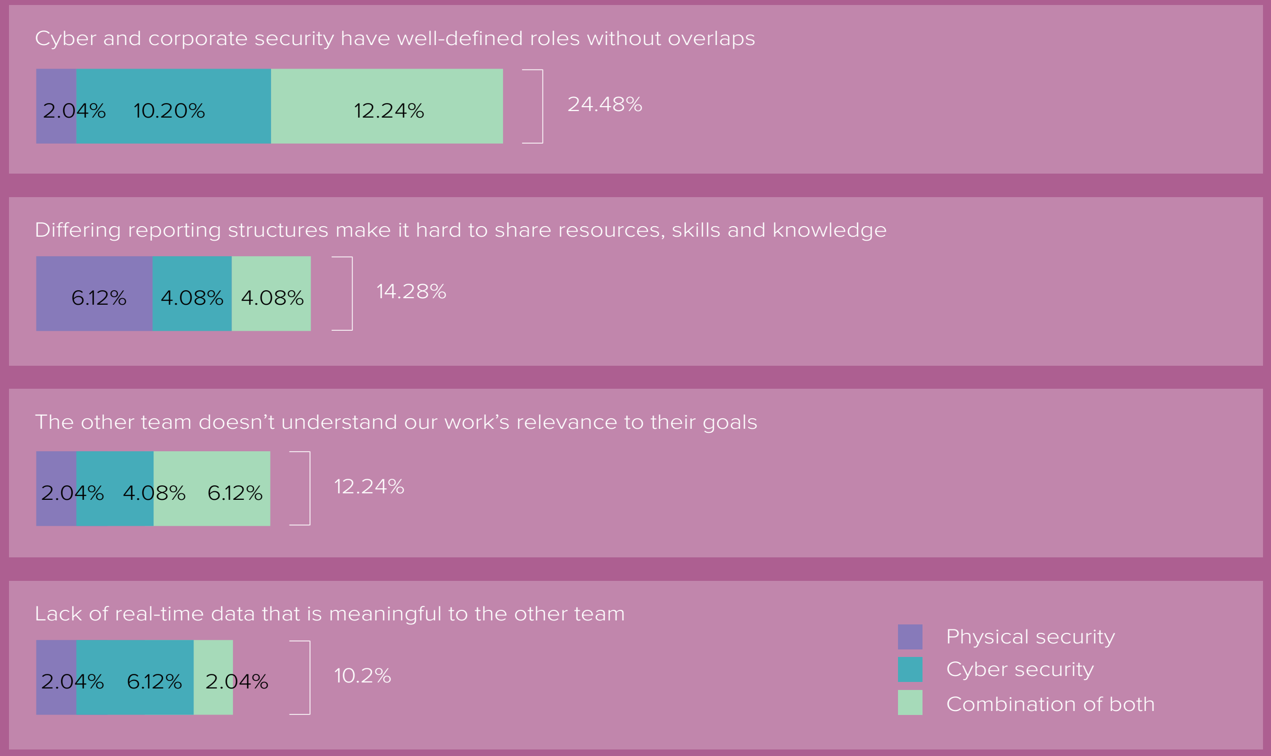

FIG. 13

AS NOTED BY THE US GOVERNMENTAL CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (CISA):

"A culture of inclusivity is vital to successfully converging security functions and fostering communication, coordination, and collaboration. Organizations of all sizes can pursue convergence by developing an approach that is tailored to the organization's unique structure, priorities, and capability level."

In short, there is no one formula for increasing collaboration. However, a vital ingredient in ensuring success is data. Without real-time data that is meaningful to the other team, security collaboration will remain, in the words of one respondent, "a board-level fantasy".

AI is helping organisations find this piece of the puzzle. By detecting risks and critical events in real-ime and by sharing this information to their security counterpart, security teams can augment their resources, elevate their talent, and maximise their overall impact.

Main Takeaway

Market leaders are using AI alongside increased security collaboration to manage talent scarcity and widened attack surface.

Ch.4

TYING IT ALL TOGETHER

The one consistent thread running throughout the report is this: Talent scarcity, coupled with a widening attack surface and economic downturn, has negatively impacted security teams' ability to proactively respond to threats.

With an explosion of data, it has become much harder to pick out patterns that matter and far easier to miss red flags. So, what are security leaders doing?

They're turning increasingly towards AI to elevate their threat response and streamline security operations. Sophisticated AI algorithms are now capable of mining public data sources to bring out the full story and visualise insights. Armed with this in-depth, context-rich information, security leaders can prioritise and act effectively to protect their organisation's employees, infrastructure and operations.

But AI is helping solve more than security dilemmas. It is also allowing leaders to demonstrate the business value they create to their C-suite peers and steer the internal narrative about security. They do this using data to demonstrate how much loss is prevented, how much reputation is preserved and how many risks are mitigated.

Equally, AI is also helping uncover insights that are relevant to both cyber and physical security, thereby minimising the amount of work each security team must do in tracking and managing hybrid threats. Especially in a time of dire talent drought, this is not a triviality.

Finally, with the right tooling that brings together all the functionalities in one place, security leaders are able to seamlessly operationalise the insights they've gathered, trigger incident response protocols, and communicate with their employees before, during and after a crisis.

But AI is just one part of the equation. The other equally vital part of the equation is a more holistic approach to security, which is impossible without de-siloing. To protect against cyber-physical risks, leading enterprises are cultivating greater levels of collaboration between security teams.

To strengthen business resilience and security posture, collaboration and a greater reliance on public data sources for threat intelligence are the two best starting points.

THANK YOU FOR READING

Dataminr®

Recognized as one of the world's leading AI businesses, Dataminr delivers the earliest warnings on high-impact events and critical information far in advance of other sources. Its corporate product, Dataminr Pulse, helps organizations strengthen business resilience with the real-time information and integrated tools needed to respond faster, mitigate risks more effectively and better manage crises.

Dataminr is one of New York's top private technology companies, with approximately 800 employees across seven global offices. It has been recognized for its groundbreaking AI platform and rapid revenue growth by Forbes AI 50 and Deloitte Fast 500, and has been named to the Forbes Cloud 100 for six consecutive years.

CEO • DIGITAL

Dataminr®

FIND CEO.DIGITAL ON SOCIAL MEDIA

🌐 🐦 in