CRA | Business Intelligence

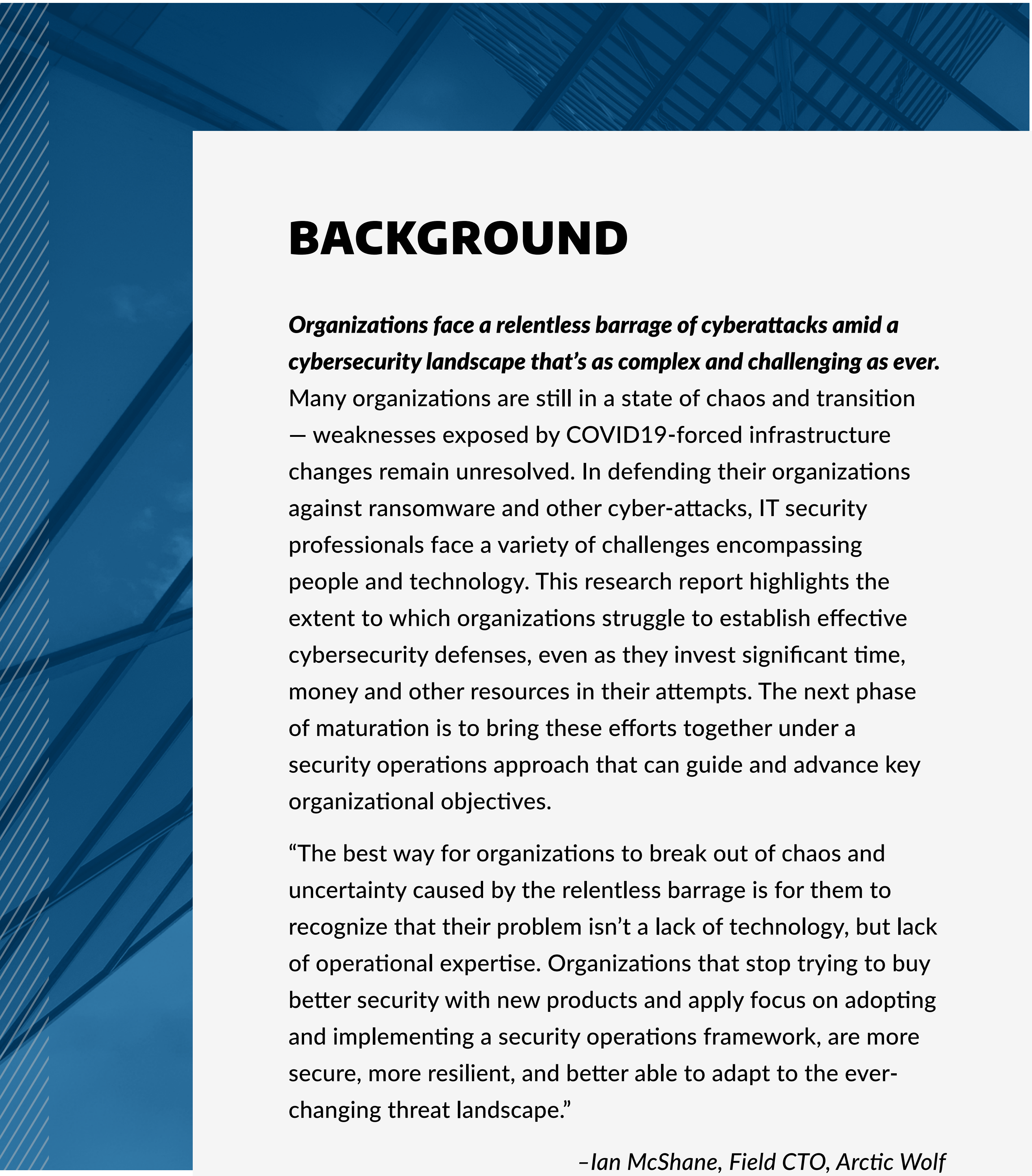
ARCTIC WOLF

END CYBER RISK

REPORT

The State of Global Security Operations

Table of Contents



BACKGROUND

Organizations face a relentless barrage of cyberattacks amid a cybersecurity landscape that's as complex and challenging as ever. Many organizations are still in a state of chaos and transition — weaknesses exposed by COVID19-forced infrastructure changes remain unresolved. In defending their organizations against ransomware and other cyber-attacks, IT security professionals face a variety of challenges encompassing people and technology. This research report highlights the extent to which organizations struggle to establish effective cybersecurity defenses, even as they invest significant time, money and other resources in their attempts. The next phase of maturation is to bring these efforts together under a security operations approach that can guide and advance key organizational objectives.

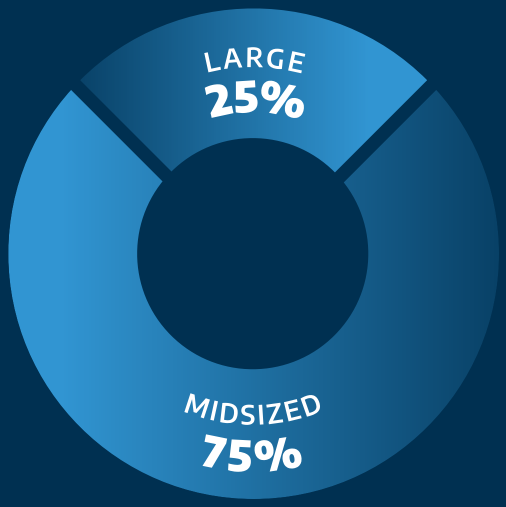
"The best way for organizations to break out of chaos and uncertainty caused by the relentless barrage is for them to recognize that their problem isn't a lack of technology, but lack of operational expertise. Organizations that stop trying to buy better security with new products and apply focus on adopting and implementing a security operations framework, are more secure, more resilient, and better able to adapt to the ever-changing threat landscape."

–Ian McShane, Field CTO, Arctic Wolf

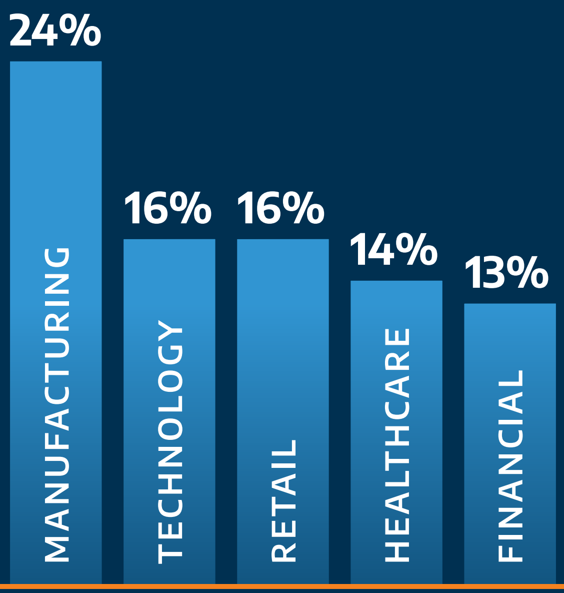
Research Methodology

This report is based on the findings of an online survey conducted in July and August 2021 among 314 IT and cybersecurity decision makers (65%) and influencers (35%). Respondents included C-level executives, vice presidents, directors and managers in North America (32%) and Europe (68%), specifically in the United Kingdom and DACH, Nordic and Benelux regions.

Three-quarters of respondents represented midsized organizations (200–2,999 employees), and one-quarter represented large organizations (3,000+ employees). The top industry sectors included manufacturing (24%); technology and business services (16%); retail (16%); healthcare (14%); and financial services (13%), together with education, government, legal and other sectors.



SIZE



INDUSTRY

EXECUTIVE SUMMARY

Research from CyberRisk Alliance and Arctic Wolf reveals that even as organizations take all the right steps to strengthen their cybersecurity defenses — training employees, investing in technology and engaging third-party experts — they are still not achieving the desired outcomes.

Key findings from the study:

01 ***Unsurprisingly, while lack of qualified staff, complicated solutions, ineffective training and regulatory compliance are all genuine challenges for the majority of organizations, carelessness or limited knowledge on the part of employees topped the list, cited by 57% of respondents.***

02 ***As organizations continue to rely on IT and security teams that are understaffed, under-resourced from a skills perspective and, in many cases, burned out, many (60%) have adopted a hybrid approach in managing their cybersecurity, handling some aspects of security internally while engaging an external partner to manage other areas.***

03 ***Despite their enthusiasm for new technology and innovation, organizations experience persistent challenges related to cybersecurity technology, ranging from product proliferation to difficulty in capturing meaningful security alerts. Many respondents have encountered challenges with cybersecurity technologies that are complicated (53%), and 51% said the number of security products is excessive or confusing. Missing alerts/notifications was a concern for nearly half (49%) of all respondents while alert fatigue concerned 43%.***

04 ***When asked to identify components of an effective cybersecurity strategy, technology, and innovation, building organization security culture through employee/IT staff training, and staffing/retaining qualified IT staff were ranked in the top two by well over one-third of all respondents.***

05 ***Organizations continue to face a relentless barrage of cyberattacks. On average, respondents reported that their IT and security teams had investigated an average of nearly 1,400 incidents over the past year, which is about three incidents per day. Nearly half of the respondents (48%) said their organization investigated one or two incidents daily during this timeframe.***

06 ***In the past year, the overwhelming majority organizations have steadily increased their spending on cybersecurity solutions – 80% have maintained or increased their cybersecurity budgets in 2021 or have indicated they are likely to do so. Many made it clear that future cybersecurity investments are driven by their need to keep pace with new risks and threats (47%) and the push to expand their cybersecurity capabilities (46%).***

The cumulative effect of organizations' challenges has been to undermine organizations' confidence in their ability to effectively defend against a cyberattack. This research reveals that simply increasing employee training and investing in technology solutions are not, by themselves, enough. Moreover, organizations cannot address challenges related to people and technology separately. These are mutually dependent areas that must be tackled through a security operations approach.

CYBERSECURITY CHALLENGES AND ISSUES FACING ORGANIZATIONS

01

People and technology, two of the pillars of cybersecurity, have proven to be a double-edged sword for many organizations. For example, employees, security experts and business leaders can be powerful allies in cybersecurity strategy, or they can become weak links. Employees may fail to follow best practices; security experts are hard to find amid staffing shortages and business leaders may approach security differently than IT leaders would prefer. Similarly, technology can be a critical enabler of threat detection and response, while also imposing new demands and complications that IT staff must manage and navigate.

A Staggering Volume of Attacks

One of the biggest challenges facing organizations is the unrelenting volume of attacks.

> ***On average, respondents reported that their IT and security teams had investigated an average of nearly 1,400 incidents over the past year, which is about three incidents each day. Nearly half of respondents (48%) noted their organization investigated one or two incidents daily during this timeframe.***

Further, many believed that cybersecurity challenges will continue to worsen as their organizations try to manage the ongoing, evolving stream of threats and risks.

Incident volumes were significantly higher for North American organizations and those in the vulnerable sector of technology and business services with 46% of respondents in this group indicating they had experienced more than 1,000 attacks during the past year, compared to only 13% of healthcare respondents.

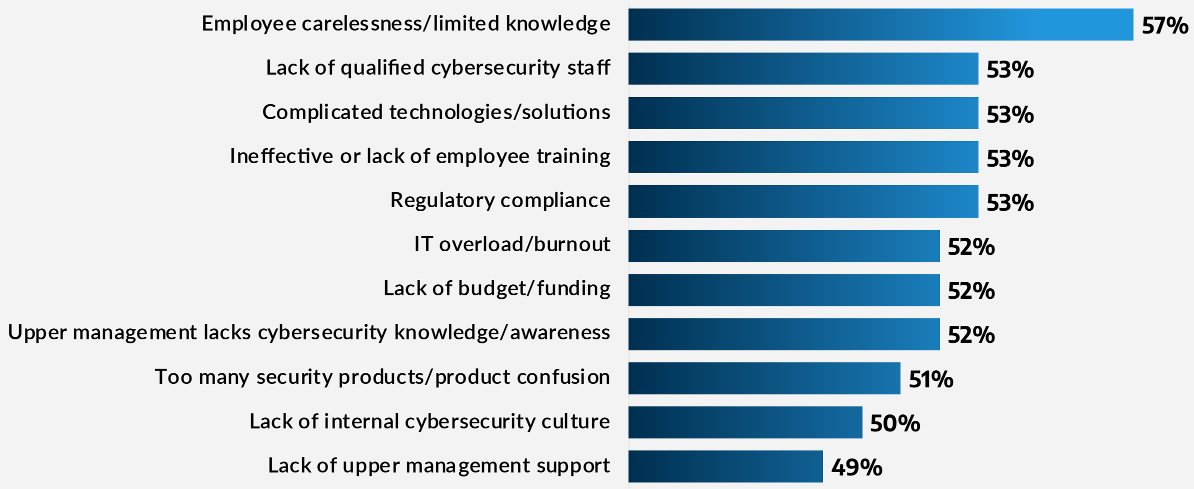
> “We are worrying the most about the increase in ransomware attacks and the fact that a lot of companies have no other choice than pay the ransom amount asked by the attackers.”
>
> *– CISO, manufacturing organization, Belgium*

Not surprisingly, while lack of qualified staff, complicated solutions, ineffective training and regulatory compliance are all genuine challenges for the majority of organizations, carelessness or limited knowledge on the part of employees topped the list, cited by 57% of respondents.

Cybersecurity Challenges

% of respondents indicating "somewhat challenging" or "very challenging"

Question: When thinking about improving your organization's security posture in the next 6 months, how challenging is each of the following?

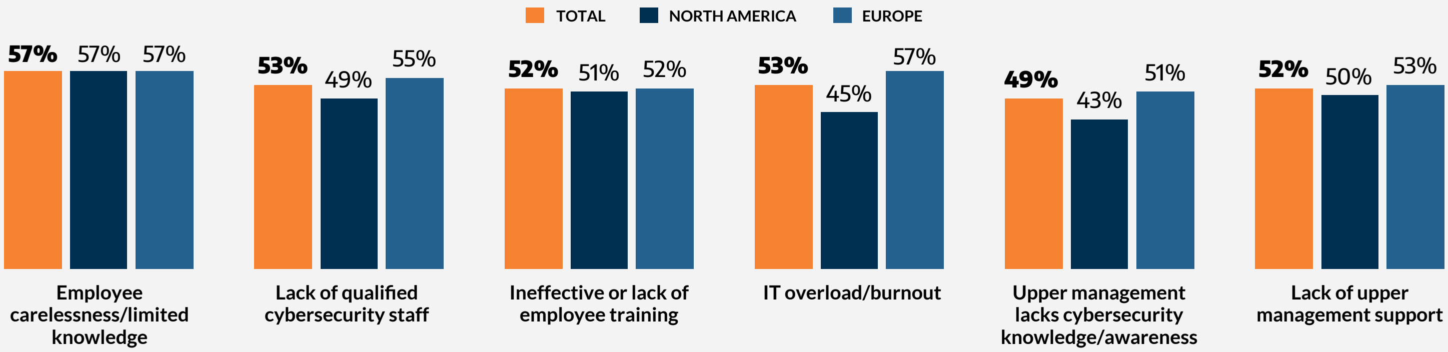


When comparing some of the challenges faced by European organizations to those in North America, the lack of qualified cybersecurity staff or specialty skills, as reported by 57% of European respondents, surpasses North America (45%). Additionally, in Europe, challenges related to regulatory compliance are significantly more common than in North American, as this issue was indicated by 57% of European organizations versus only 43% in North America. However, there are upsides to this greater regulatory involvement: European respondents were also more likely to cite regulatory requirements as a driver for new technology investments.

"People" Challenges, by Region

% of respondents indicating "somewhat challenging" or "very challenging"

Question: When thinking about improving your organization's security posture in the next 6 months, how challenging is each of the following?



By several measures, respondents identified “people” as a major cybersecurity challenge area, including a wide range of specific challenges, from employee carelessness about security to a lack of support from upper management. These trends were consistently higher for respondents in the retail sector.

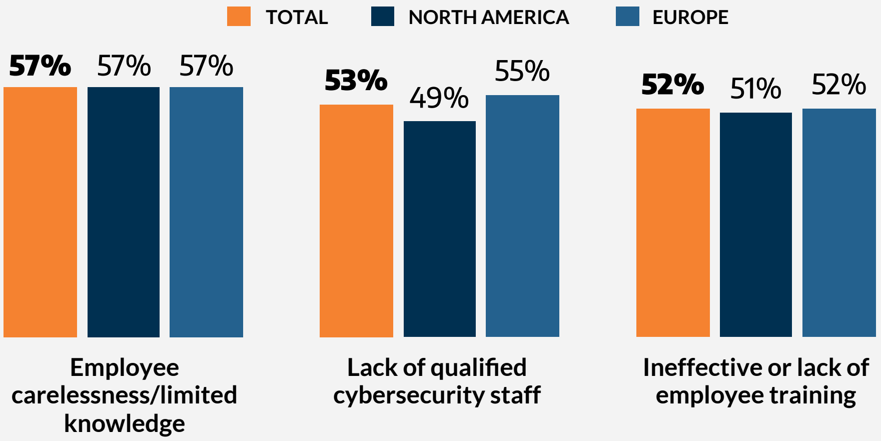
> ***For example, ineffective or insufficient employee training was a problem for 71% of retail respondents versus 53% overall; 69% of retail respondents also cited a lack of qualified security staff versus 53% overall.***

Retail and healthcare sectors reported their top difficulties were in the areas of budget, cybersecurity culture and regulatory compliance.

Process Challenges, by Region

% of respondents indicating “somewhat challenging” or “very challenging”

Question: When thinking about improving your organization’s security posture in the next 6 months, how challenging is each of the following?



Insights from this survey validate the breadth of cybersecurity challenges that continue to affect organizations. IT and cybersecurity staff, in many cases, have borne the brunt of them. Most organizations’ report their burdens are exacerbated by the lack of qualified cybersecurity professionals (53%), insufficient budgets (52%) and lack of cybersecurity knowledge among upper management (52%).

The combination of overwhelming threats and insufficient resources to combat them has been detrimental to organizations and damaging to IT staff. More than half (52%) said their IT staffs — the professionals charged with keeping their organizations safe from relentless cyberattacks—are overloaded and burned out.

> “Too much hesitation, no budget, and management only hears IT when the going gets tough.”
>
> *– Manager, high-tech organization (Germany)*

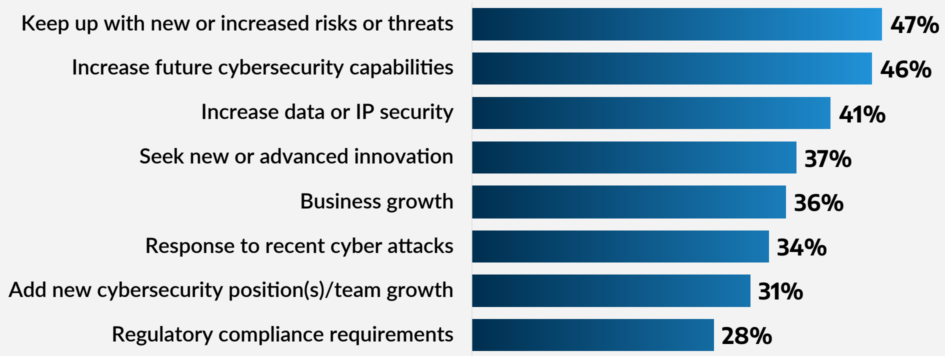
Technology Challenges: More Spending, Yet Benefits Can Be Elusive

Technology solutions continue to play a primary role in organizations' cybersecurity strategies. In the past year, many organizations have steadily increased their spending on these solutions.

> ***A large majority (80%) of organizations have maintained or increased their cybersecurity budgets in 2021 or have indicated they are likely to do so.***

Reasons for Future Investments in Cybersecurity

Question: Which of the following are the reasons your organization is likely to invest in cybersecurity or increase its cybersecurity budget?

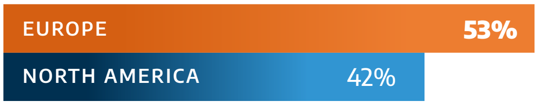


Many made it clear that future cybersecurity investments are driven by organizations' need to keep pace with new risks and threats (47%) and the push to expand their cybersecurity capabilities (46%). For well over one-third of all respondents, new or advanced innovation and business growth is also expected to spur cybersecurity investments. While the majority of all respondents (70%) indicate they are very or extremely likely to invest or increase their cybersecurity budgets in 2021, an even larger proportion of respondents from the high tech/IT/ business services (82%) and retail (84%) sectors say future investments in cybersecurity solutions is very or extremely likely.

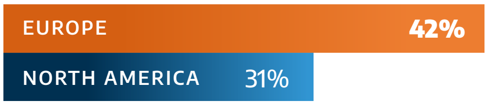
However, the availability of cybersecurity solutions and organizations' willingness to adopt them have not necessarily streamlined workflows and improved defenses. Many respondents have encountered challenges with cybersecurity technologies that are complicated (53%), and 51% said the number of security products is excessive or confusing, with more than two-thirds of all respondents from the retail sector (69%) reporting product confusion from too many security products.

Technology-related concerns also underscored respondents' top cybersecurity issues, where a majority of respondents said that cybersecurity solutions are decided by their organizations' business leaders vs. technology leaders (54%) and many viewed cybersecurity solutions as too complicated or having a poor UX (44%)

Worry about missing incident alerts/notifications



Receive too many alerts to know which ones to focus on

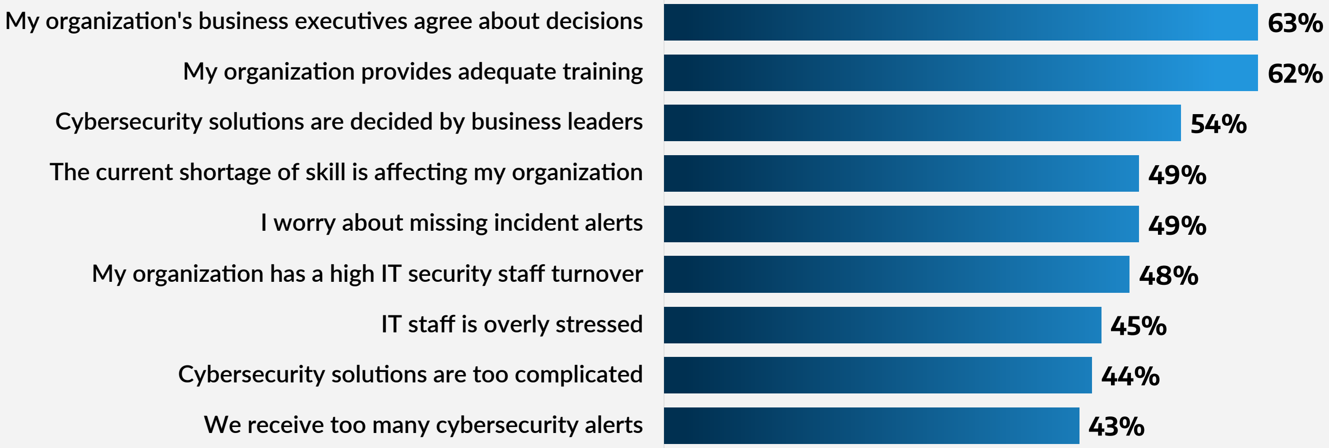


Missing alerts/notifications was a concern for nearly half (49%) of all respondents while alert fatigue concerned 43%. ***These results were notably higher in Europe, where 53% of respondents (vs. 42% in North America) said they worry about missing incident alerts/notifications, and 48% (vs. 31% in North America) said they receive too many alerts to know which ones to focus on.*** In North America and European retail organizations, missing alerts (76%) and alert fatigue (61%) concerns surpassed the other major sectors.

Cybersecurity Issues

% of respondents indicating "mostly agree" or "completely agree"

Question: How much do you agree or disagree with each of the following statements?



Echoing the findings related to IT staff burnout, respondents' top issues reflect the immense burdens that cybersecurity issues have placed on IT teams. Issues related to IT staff are consistently prevalent across the key industries, although higher than average for retail respondents with 63% reporting high turnover of security staff (vs. 48% overall) and 63% experiencing high stress from responding to cybersecurity issues (vs. 45% overall).

> "We seek new technologies and innovations to avoid as many cyberattacks as possible."
>
> *—Manager, manufacturing organization (U.S.)*

> "We have way too many false alerts, so the day it will be a real one, I'm worried that we will not know soon enough."
>
> *—IT administrator, regional government (Canada)*

SECURITY OPERATIONS AS A UNIFYING THREAD

02

Organizations have attempted to deal with their cybersecurity challenges by investing in technology solutions, training employees, and partnering with third-party security experts. However, this research reveals that multipronged approaches have failed to deliver the level of confidence that organizations need in their cybersecurity defense, their worries often exacerbated by concerns about the changing threat landscape and the formidable challenge they face in just keeping up with these threats.

Evaluating the Effectiveness of Employee Training

For virtually all respondents (96%), training employees is an integral component of their organization's cybersecurity strategy, whether employee cybersecurity awareness training (86%), IT staff training (89%) or both (78%). To achieve their training initiatives, most organizations are likely to use internal sources for employee awareness (72%) and third-party software, platforms or services to train their IT staff (60%). One out of three organizations seek to pursue optimal training through ongoing programs throughout the year; however, nearly half (47%) limit their cybersecurity training schedules to annual or bi-annual offerings. Simulation exercises are now included in roughly half of all organizational employee and IT cybersecurity training programs.

> ***Despite these efforts, 48% of respondents are still not convinced that their organizations' training is adequate to identify, prioritize and remediate security incidents.***

In addition to the challenges of establishing employee training initiatives in remote work settings, negative sentiments about managing security are often the harsh realities in organizations where cybersecurity awareness or knowledge is lacking among upper management, resulting in little or no support or investment for cybersecurity initiatives.

Augmenting Internal Resources With External Support

Another key cybersecurity strategy is the adoption of a hybrid approach to management. Sixty percent of organizations rely on this tactic, managing some aspects of security internally and engaging an external partner to manage other areas. This trend is generally consistent across in North America and Europe and among the key industries surveyed, reflecting organizations' universal need to address their lack of qualified cybersecurity staff.

Confidence Lags, Despite Increases in Security Efforts

Overall, respondents reported a lack of confidence that their organizations' cybersecurity efforts represented an effective defense again cyberattacks, with only one in five (21%) indicating they were "very confident" that their organizations could defend against a cyberattack in the next six months.

Although several factors contribute to respondents' uncertainty, one issue is the constant state of change and complexity related to cyberthreats and to technology itself. "My concerns are the ongoing and changing nature, operating across multiple countries and coping with a wholesale move to the cloud," noted one CISO in the U.K.

> "My concerns have been eased by involving external expertise in our security support."
>
> *—Manager, financial services (U.K)*

The persistent lack of efficacy speaks to a larger issue with cybersecurity that many organizations have struggled to address: the absence of a security operations component that steps in where tools and trainings fall short. Respondents are now voicing their concerns that simply increasing spending on cybersecurity technology will not solve the threat problem. That is particularly true when technology solutions create additional challenges, such as complexity, proliferation and incident alert fatigue.

GUIDELINES FOR FINE-TUNING SECURITY OPERATIONS

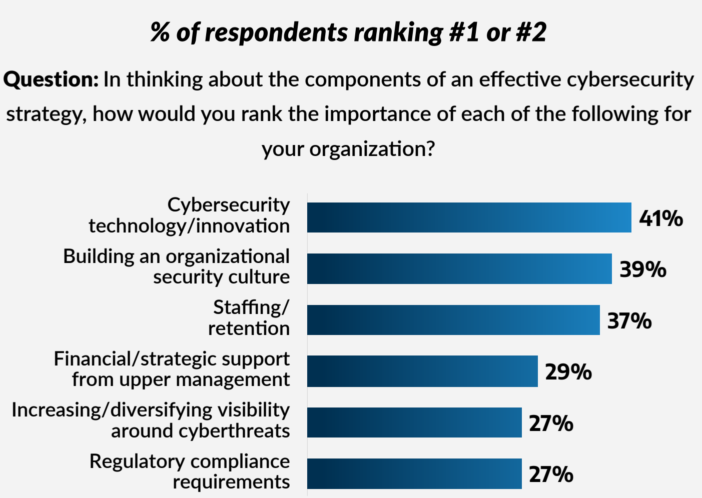
03

Clearly, the gaps must be filled. Organizations require a long-term strategy with a clear vision for success, supported by a security operations function capable of executing that vision and adapting it to changing circumstances.

When asked to identify components of an effective cybersecurity strategy, technology and innovation, building organization security culture through employee/IT staff training, and staffing/retaining qualified IT staff were ranked in the top two by well over one-third of respondents; this was universal across regions and industries.

> "Cyberattacks are increasing all the time. The damage is enormous. Our company is well-equipped, but there are still gaps."
>
> *—Manager, financial services organization (Germany)*

Cybersecurity Strategy Components Importance



To that end, organizations must address the shared cybersecurity challenges that span regions and industries, as well as the unique requirements of individual organizations. Healthcare organizations, for example, are largely driven by regulatory compliance, whereas the retail sector has a strong need for more qualified cybersecurity professionals.

As organizations move toward a security operations approach, priorities include:

01 ***Know your objectives***

02 ***Address your challenges***

- Get buy-in from senior leaders and board members to create a culture of security that includes ongoing training for all staff
- Budget to support cybersecurity strategy, including solutions and services
- Appropriate staffing levels
  - Invest in security leadership and vision
  - Optimize existing security tools

03 ***Engage with partners that understand the organization's unique objectives***

- Leverage insights based on their specific industry expertise

CRA | Business Intelligence

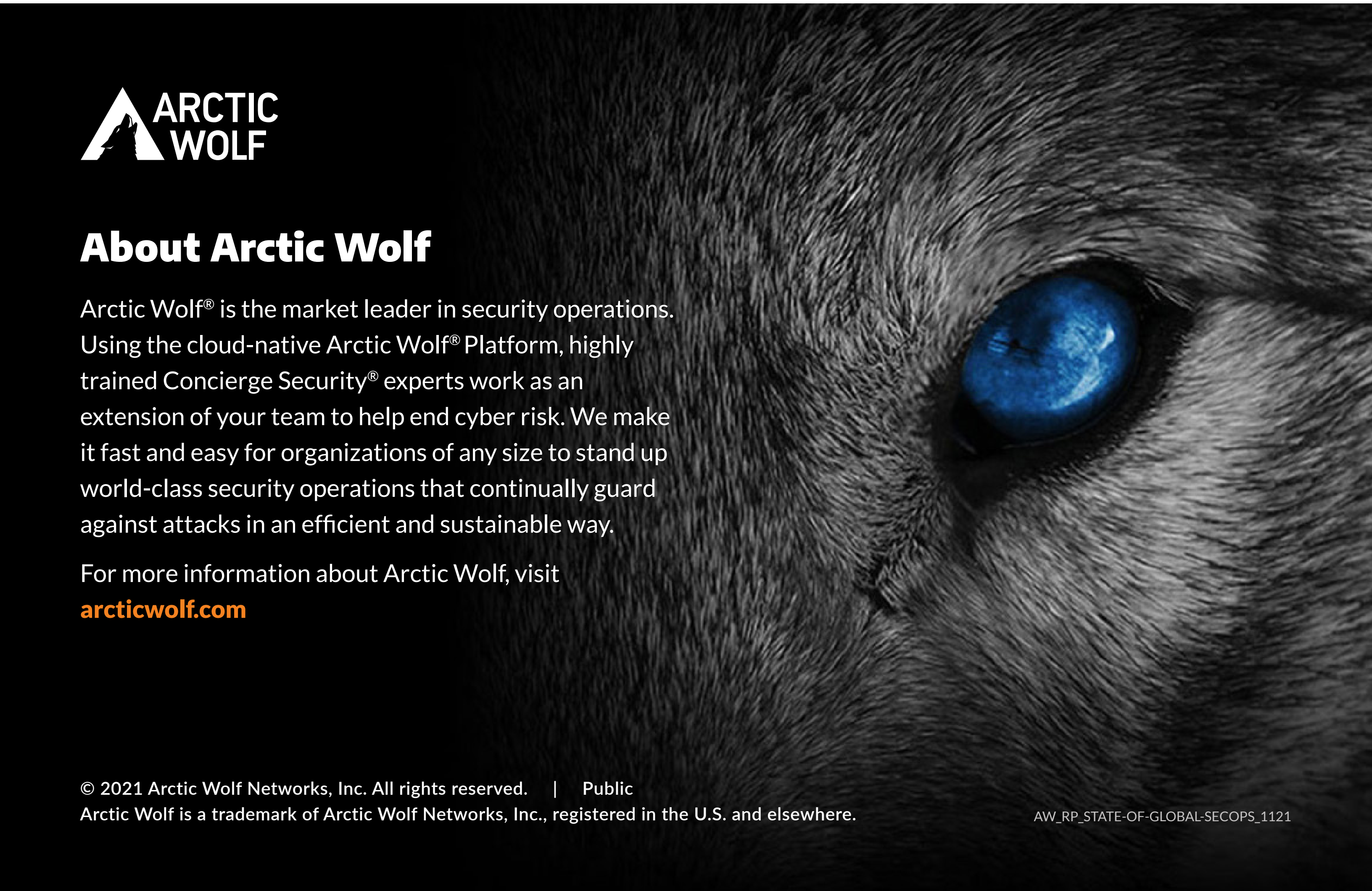
About CRA

CRA Business Intelligence is a full-service market research capability focused on the cybersecurity industry. Drawing upon CRA's deep subject-matter expertise and engaged community of cybersecurity professionals — along with a newly recruited, world-class market research competency — CRA Business Intelligence is unique in our industry.

These components together enable delivery of unparalleled data and insights anchored in our engaged community of cybersecurity professionals and business leaders eager to share their perspective on the market's most important concerns.

CRA Business Intelligence provides:

- Ground-breaking proprietary research to inform and engage our community
- Custom research to support strategic product and marketing initiatives
- Innovative thought-leadership content development and promotion
- Brand engagement through business activity indexes, interactive tools and assessments, and more



ARCTIC WOLF

About Arctic Wolf

Arctic Wolf® is the market leader in security operations. Using the cloud-native Arctic Wolf® Platform, highly trained Concierge Security® experts work as an extension of your team to help end cyber risk. We make it fast and easy for organizations of any size to stand up world-class security operations that continually guard against attacks in an efficient and sustainable way.

For more information about Arctic Wolf, visit **arcticwolf.com**