Understanding the Cybersecurity Skills Gap:

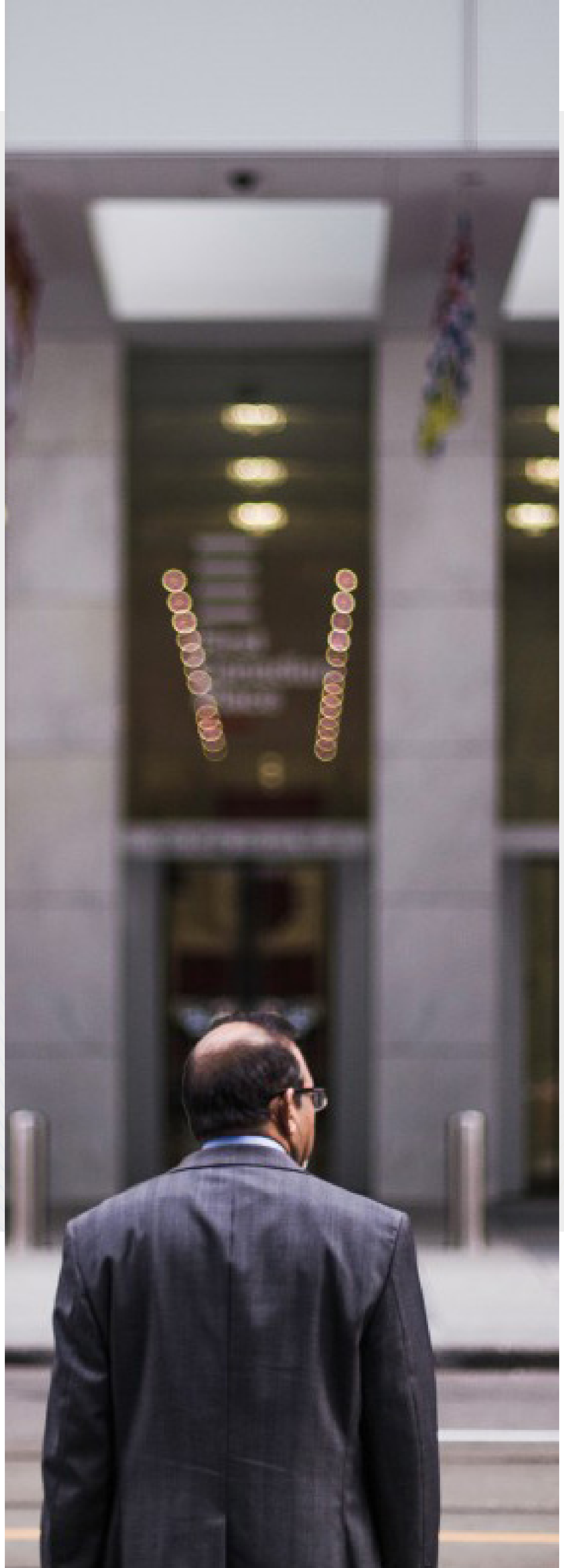
a CyberEd.io Survey Report

CyberEd.io

EXECUTIVE SUMMARY

Closing the Cybersecurity Skills Gap

To better understand the state of cybersecurity training and education across all types of organizations around the globe, CyberEd.io conducted an online survey of CISOs, Security Architects/Engineers, IT Directors, and other cybersecurity professionals in 2023.



HUNDREDS OF RESPONSES WERE RECEIVED IN LESS THAN 30 DAYS, which underscores the enormous need for information and insights about the state of cybersecurity training and what organizations are dealing with as they work to close the skills gap.

A few key highlights from our survey include:

- Finding qualified candidates for cybersecurity roles is challenging. More than half (55%) of respondents said the **availability of qualified candidates was inadequate or poor** to meet their needs for key cybersecurity jobs.
- Hiring difficulties definitely vary, but **only 20 of 393 respondents found hiring "extremely easy"** for any types of cybersecurity jobs.
- **Overcoming the ongoing talent shortage** (estimated at 3.5 million cybersecurity jobs worldwide in 2022) will require 'out-of-the-box' thinking across organizational levels and job roles.
- **Organizational visibility and budgetary constraints** were cited as the two biggest roadblocks to successful cybersecurity threat detection and response.
- Cybersecurity **awareness training lags behind the actual need** for such training. Only 36% of survey respondents said their organizations provide cybersecurity awareness training to all employees, while industry estimates emphasize phishing as the genesis of 90%+ of breaches.

Given the challenges involved in hiring for cybersecurity roles, along with severity of the cybersecurity talent shortage and rising threats often stemming from a lack of cybersecurity awareness, it's crucial to train and upskill employees, rather than relying on the hiring process alone, to close cybersecurity skills gaps.

Survey Respondent **Demographics**

More than 500 people responded to our survey, which was conducted in Q2 2023. A **total of 393 people** responded to all of the questions. Their responses were tallied to provide the data we used to build this CyberEd.io survey report.

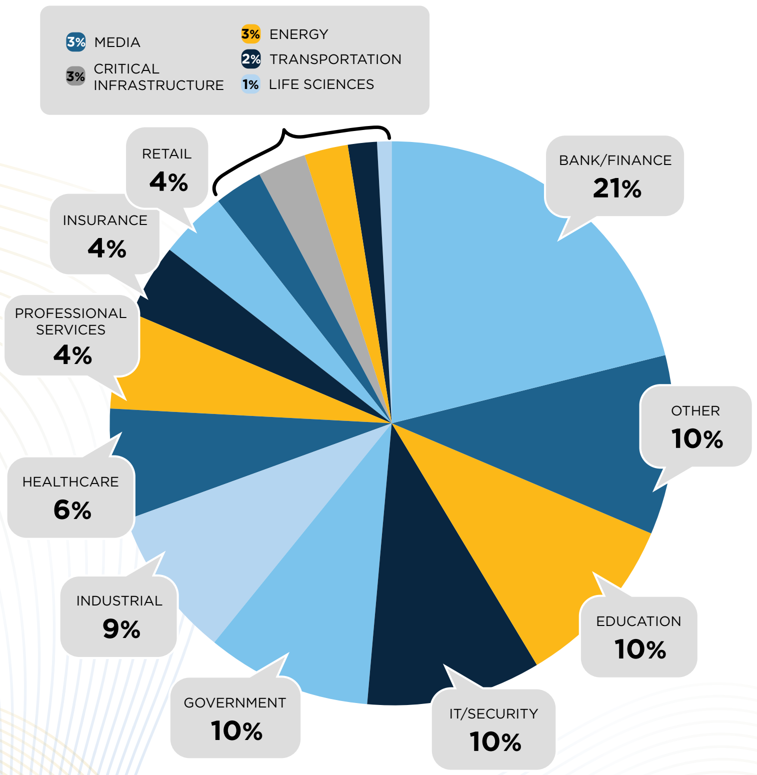


FIGURE 1
JOB INDUSTRY

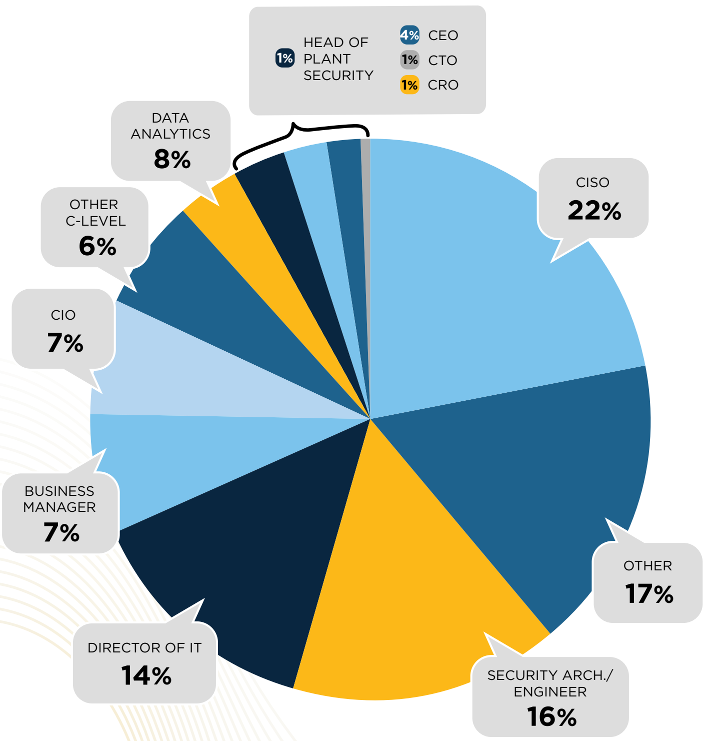


FIGURE 2
TITLE LEVEL

FIGURE 3
GEOGRAPHICAL LOCATION

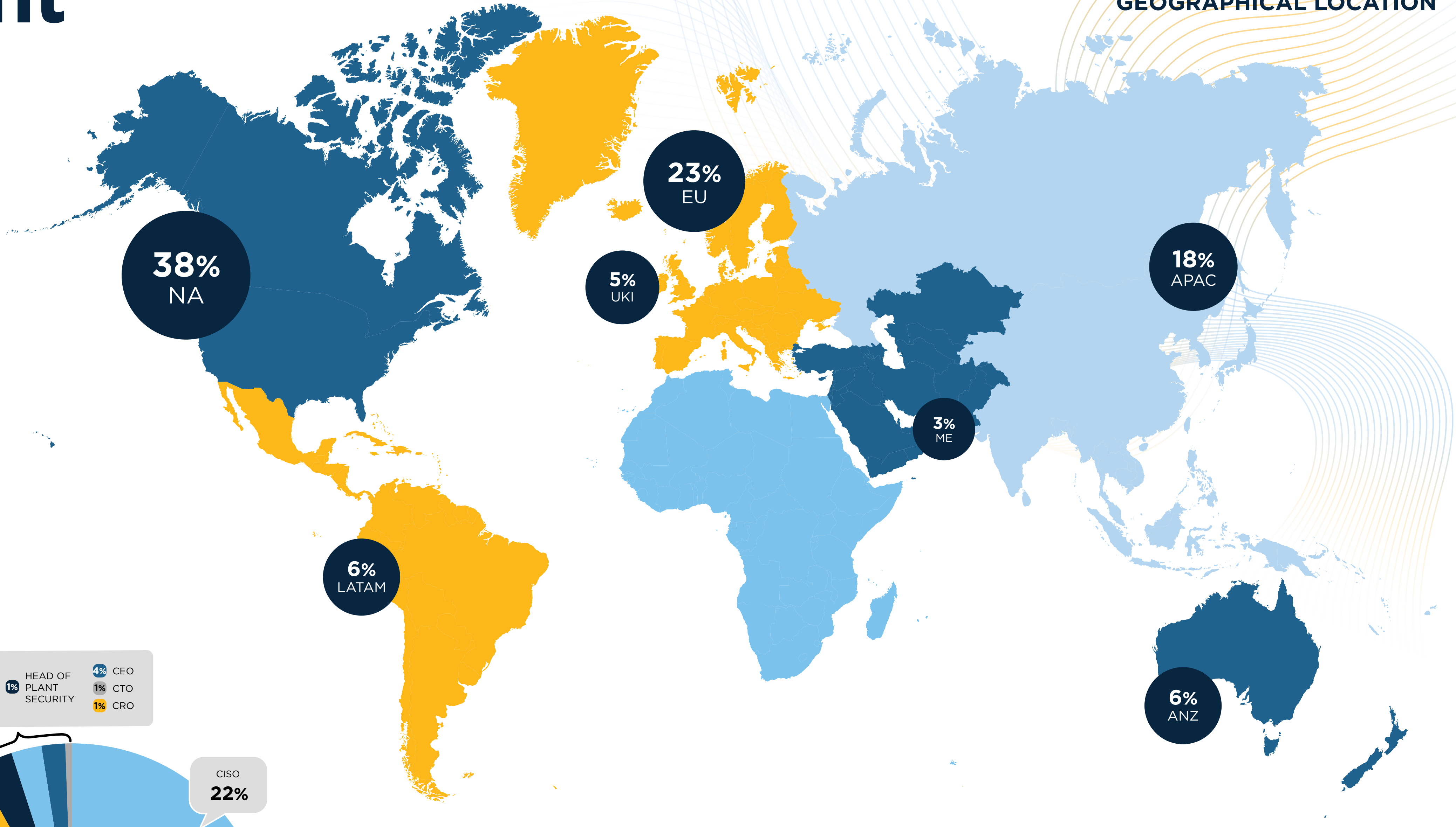


FIGURE 1
Respondents to the survey came from a variety of industries, most prominently from the Banking/Finance industry, followed by Education, IT/Security, and Government.

FIGURE 2
CISOs, Security Architects/Engineers and Directors of IT responded in the highest numbers to our survey.

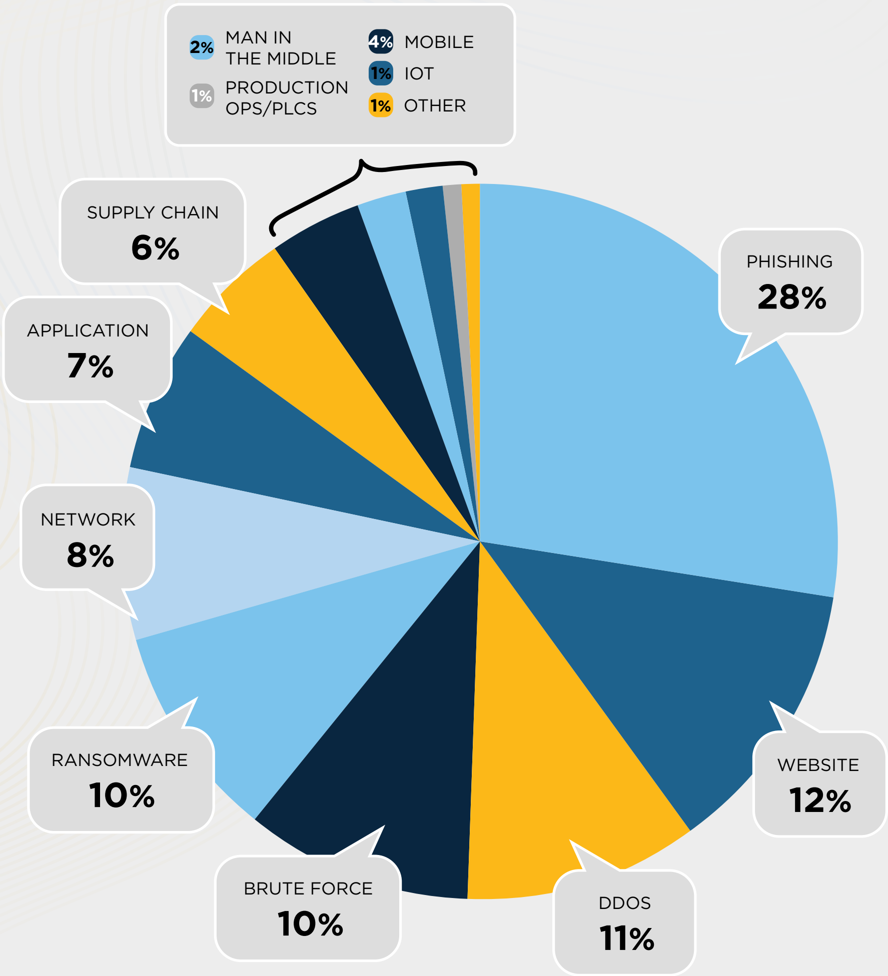
Survey Results and Key Findings

The urgent need for greater cybersecurity awareness

It is no secret that cyberattacks are becoming more frequent, which signals an urgent need for cyber education for all organizational members.

Survey respondents cited that the most common cyberattack attempts by far include Phishing (cited by 28%), followed by Website Attacks (cited by 12 %), DDOS (cited by 11%), Ransomware (cited by 10%) and Brute Force attacks (cited by 10%).

FIGURE 4
CYBERATTACKS IN 2022-2023



Cybersecurity Hiring

Survey respondents said their hiring of cybersecurity personnel is increasing in 2023.

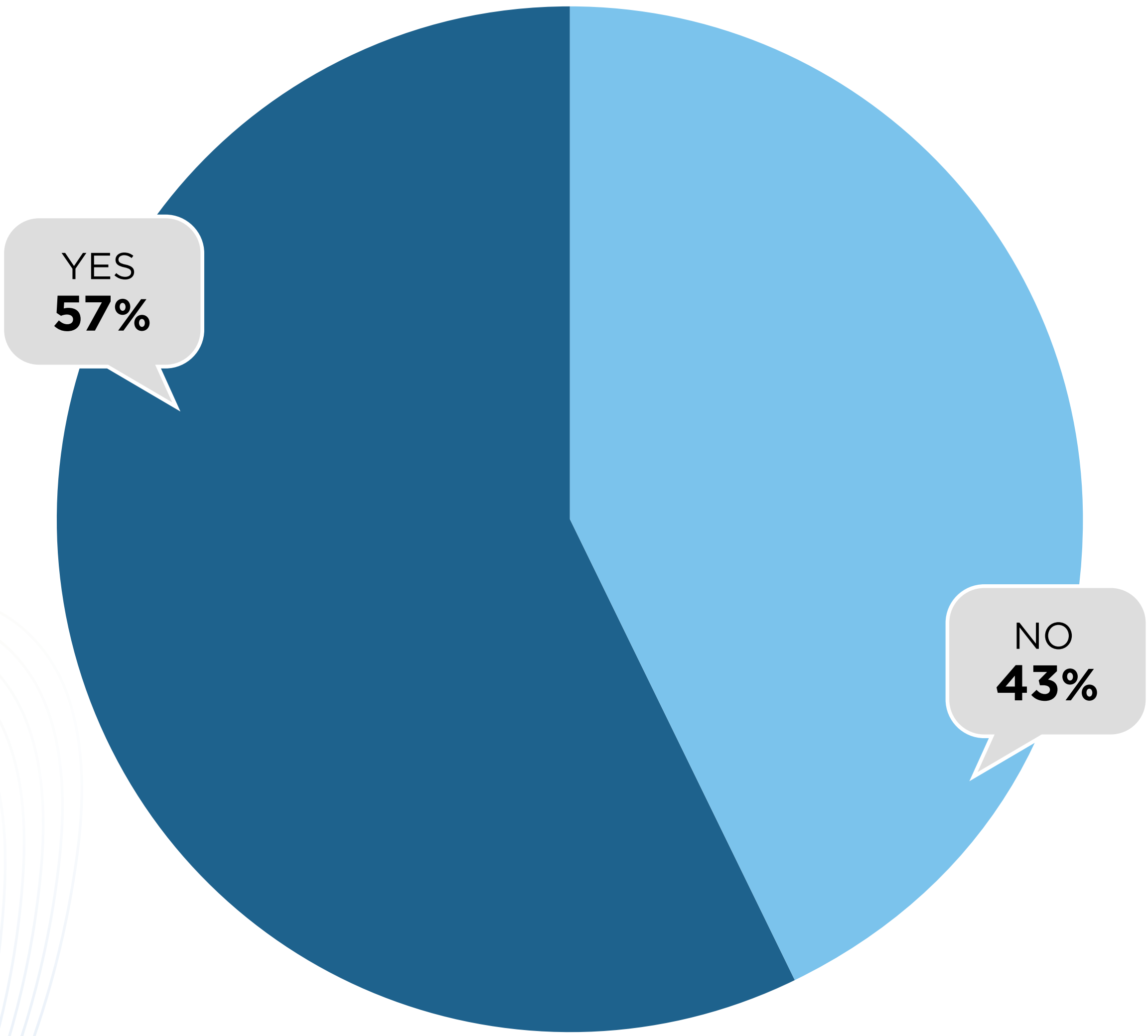


FIGURE 5
2022 HIRING

More than half of respondents (57%) said in 2022 they hired cybersecurity personnel.

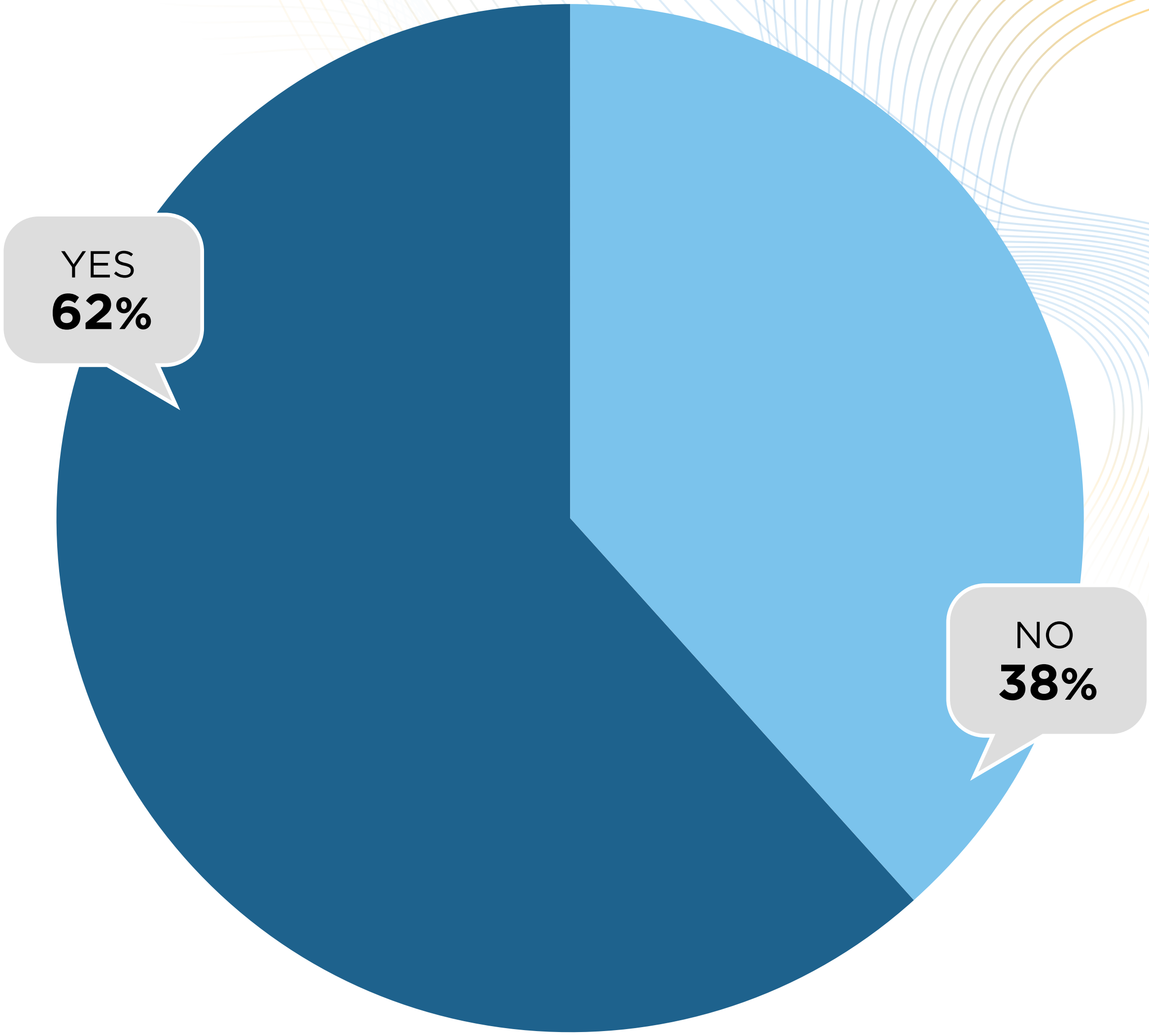


FIGURE 6
2023 HIRING

In 2023, nearly two thirds of respondents expect to hire cybersecurity personnel.

Availability of Candidates

A lack of qualified candidates underscores the need to 'close the gap.' This shortage of qualified candidates is only exacerbated by an ongoing absence of diversity in cybersecurity roles.

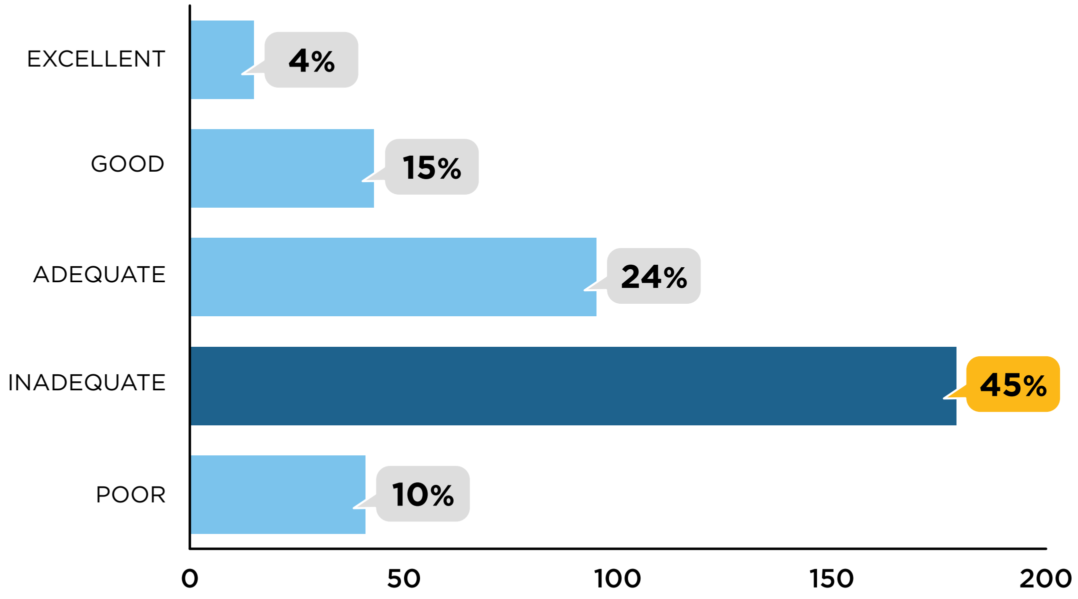


FIGURE 7 **AVAILABILITY OF QUALIFIED CANDIDATES**

In total, more than half of respondents (55%) cited an inadequate or poor availability of qualified candidates.

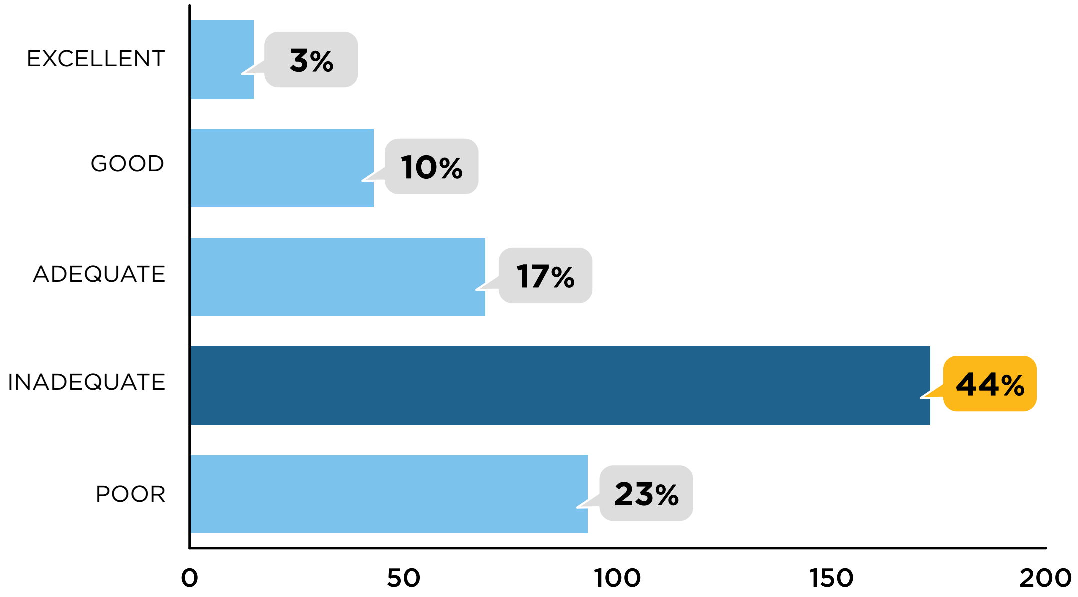


FIGURE 8 **AVAILABILITY OF QUALIFIED FEMALE CANDIDATES**

Approximately two thirds of respondents (67%) cited an inadequate or poor availability of qualified female candidates.

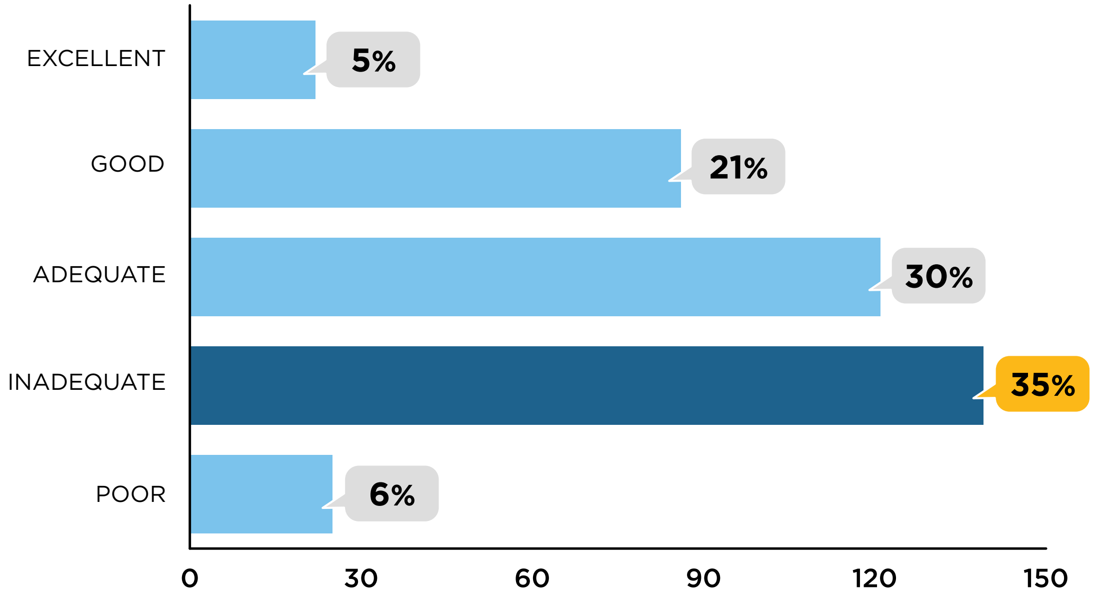
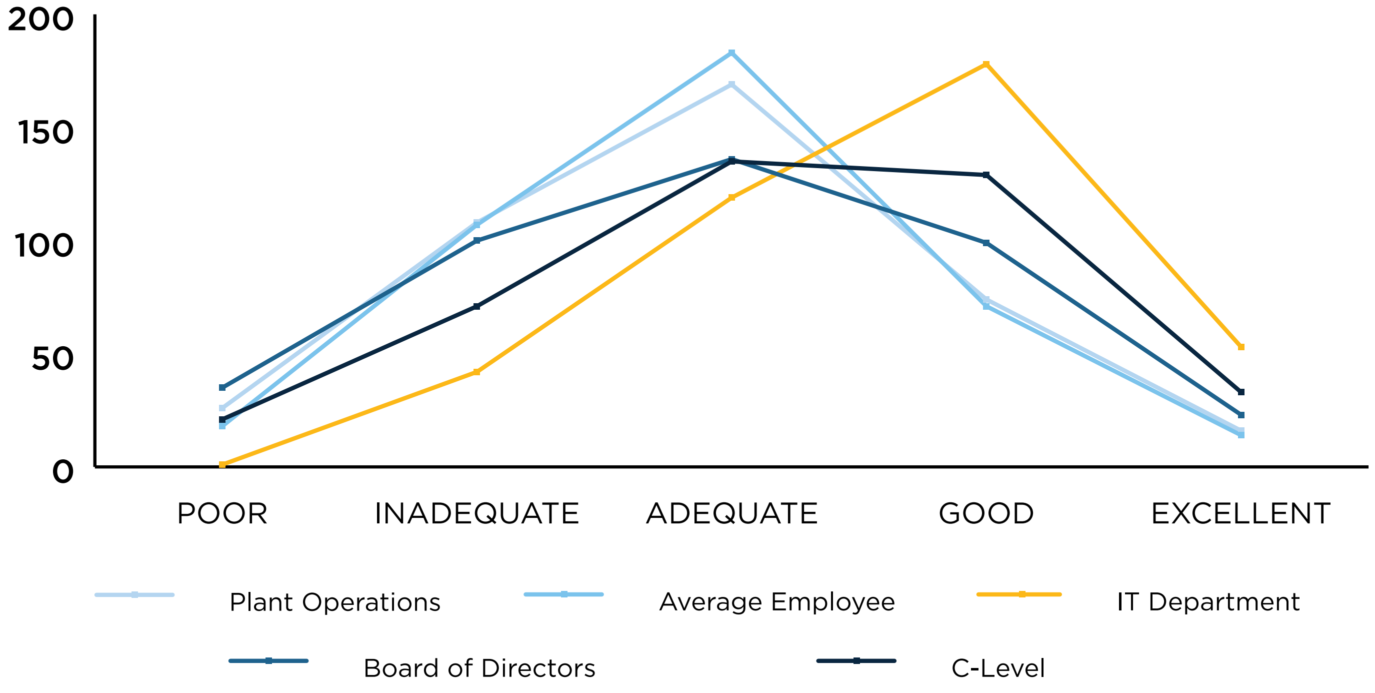


FIGURE 9 **AVAILABILITY OF EARLY CAREER CANDIDATES**

The availability of early career candidates was found to be adequate or better by 56% of respondents. This appears to coincide with recent growth in cybersecurity educational programs and providers, enabling more students to choose a cybersecurity career path, although it appears that the growing availability of training is still not enough to close the gap in filling early-career job roles.

Cybersecurity Competency

Most departments are perceived as 'cybersecurity competent,' with IT cited most often as having the highest competency. In addition to this, approximately 70% of respondents described their company-wide cybersecurity training as adequate or better. If this is the case, why are companies still suffering from increasingly worse cyberattacks?



	C-Level	Board of Directors	IT Dept.	Average Employee	Plant Operations
AVERAGE OR BELOW	58%	68%	41%	78%	77%
ABOVE AVERAGE	41%	31%	58%	21%	22%

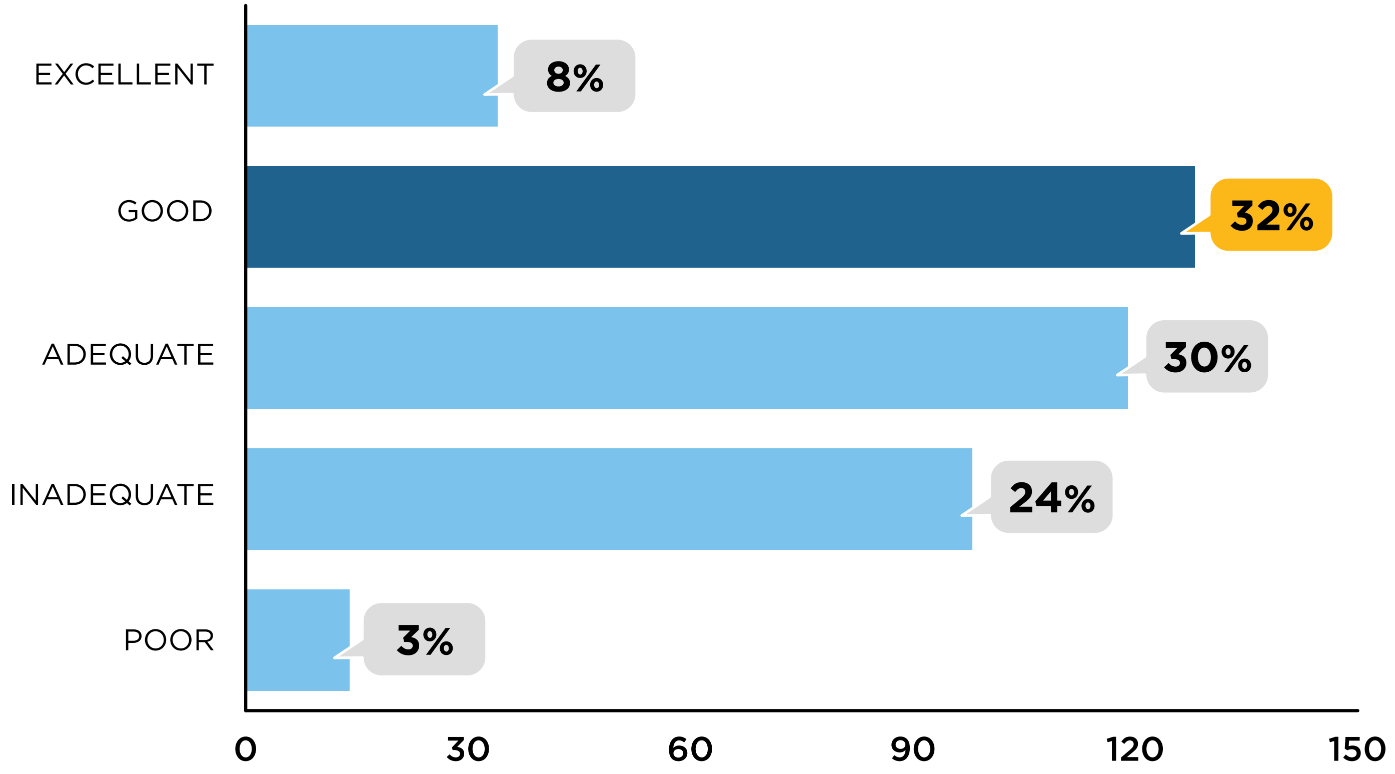
FIGURE 10 A (GRAPH) & B (CHART) **COMPETENCY BY DEPARTMENT**

Plant operations personnel and 'average employees' were most often cited for being 'average' to 'below average' in terms of cybersecurity competency. This provides a clear opportunity for training and education to help bring every employee's skills up, which is critical to protecting the organization against threats.

FIGURE 11 **ORGANIZATION-WIDE CYBERSECURITY TRAINING**

Unfortunately, responses regarding tilting toward 'adequate or better organization-wide cybersecurity training' demonstrate a clear disconnect between what's perceived as adequate or effective – and what's actually adequate.

The vast majority of cybersecurity breaches originate through phishing or associated social engineering attacks – 90% or more, according to industry estimates. Yet organizations typically perform awareness training activities once per quarter, or less often. And the survey indicated that only slightly more than a third of respondents (36%) said their organizations provide enterprise-wide cybersecurity awareness training. All of this falls short, failing to close 'inadequate cybersecurity awareness' gaps.



Hiring Difficulties

Hiring difficulties exist across all 15 cybersecurity roles queried. Fewer than 20 of 393 survey respondents stated that hiring for any of these roles is “extremely easy.”

Respondents found it most difficult to hire individuals for Critical Thinking and Design roles, Zero Trust Design, Security Analysis and Cloud Security roles. This makes sense due to the relatively recent advent of Zero Trust design / architecture roles and the strong demand for security analysts of all types, especially those with cloud security credentials and experience.

Also, more than half of respondents (52%) found it average or easy to hire for penetration testing roles. This area offers a career path that does not always require a university degree in computer science, information technology, or cybersecurity.

Training and certifications such as Certified Ethical Hacker (CEH), CompTIA PenTest+, GIAC Penetration Tester (GPEN), GIAC Web Application Penetration Tester (GWAPT), Offensive Security Certified Professional (OSCP), Certified Penetration Tester (CPT) can help job seekers get started as junior pen testers.

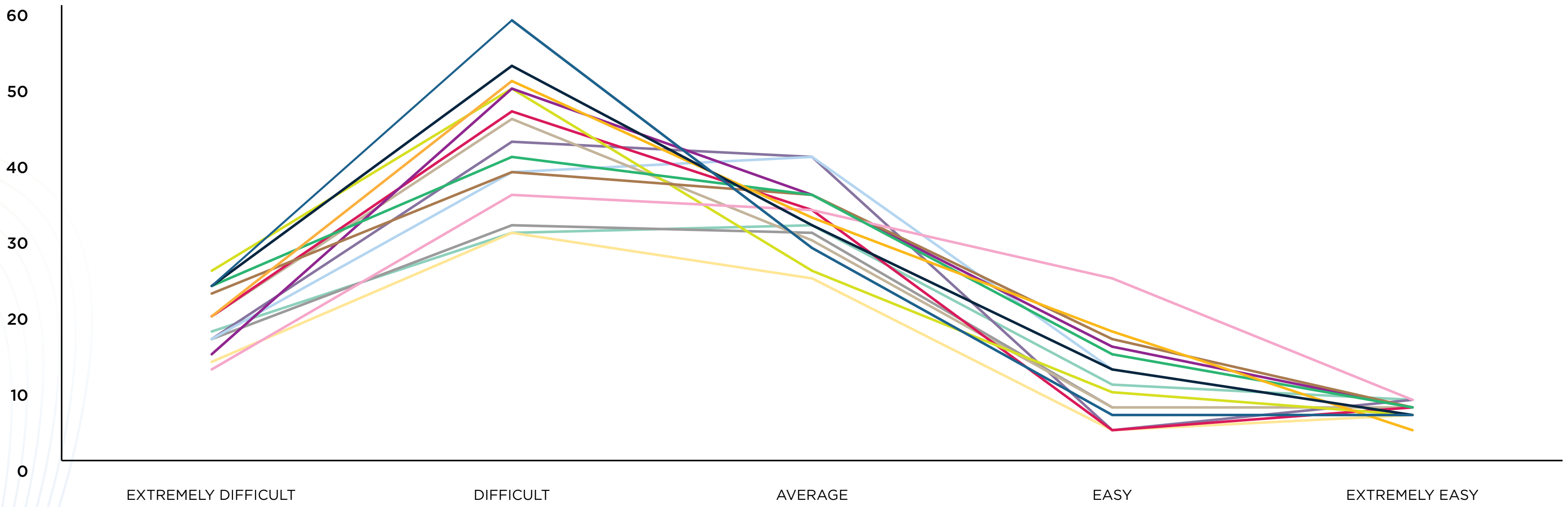


FIGURE 12 A (GRAPH) & B (CHART) **HIRING DIFFICULTY BY JOB ROLE**

JOB FUNCTION	DIFFICULT	AVG/EASY
Offensive Cybersecurity	**37%**	33%
Insider Threat Detection	**41%**	40%
Supply Chain Security	**32%**	32%
Mainframe Security	**30%**	24%
Application Security	**43%**	43%

JOB FUNCTION	DIFFICULT	AVG/EASY
DevSecOps	**47%**	34%
OT Cybersecurity	**45%**	32%
Zero Trust Architecture	**56%**	29%
Cloud Security	**50%**	41%
Network Security Architects	**47%**	42%

JOB FUNCTION	DIFFICULT	AVG/EASY
Penetration Testing	33%	**52%**
Incident Response	**45%**	44%
Audit & Compliance	**48%**	42%
Security Analysts	**56%**	37%
Critical & Design Thinking	**58%**	31%

Difficulties abound

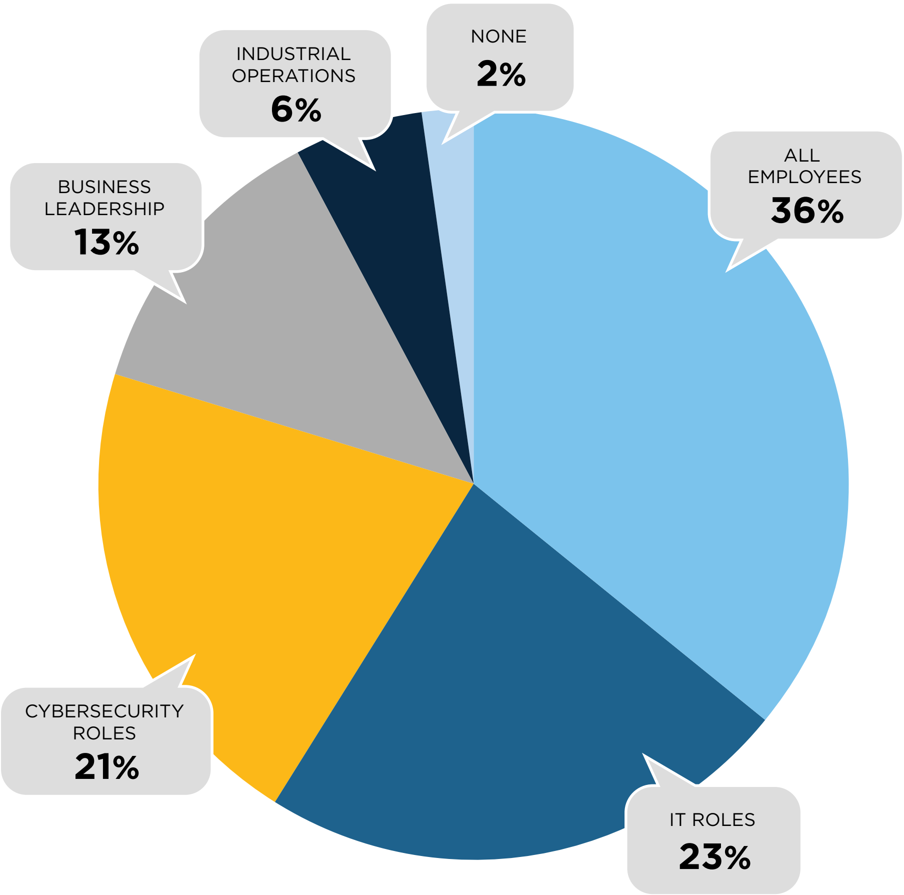
Advice for executives focused on hiring personnel for:

- **GENERAL CYBERDEFENSE** (Includes cybersecurity analysts, network security administrators and project managers.) Consider rethinking hiring criteria to be more flexible, especially in terms of non-negotiables such as years of experience, advanced degrees, expertise in specific technological tools. It will likely be easier to train someone to use specific tools.
- **CLOUD CYBERSECURITY** (Includes cloud security specialists, app sec specialists or cloud security architects.) Streamline hiring processes to move faster to bring a candidate through the hiring process and bring new cyber talent on board quicker.
- **SOC** (Includes vulnerability assessment analysts, cyberdefense incident responders and threat hunters.) Scout for new talent by partnering with universities and local STEM programs to encourage students to pursue careers in cybersecurity, especially if it helps to bring them into your organization.
- **ICS CYBERSECURITY** (Includes OT/ICS cybersecurity analysts and engineers and industrial control threat intelligence analysts.) Count on greater hiring difficulties because IT cybersecurity has had a decades-long head start in building expertise, along with a larger talent pool than those working in OT. Look for ways to train individuals for vertical and lateral career progression, and consider investing in automated detection tools as well.
- **RISK ANALYSIS AND RISK MANAGEMENT** (Includes identity and access risk analysts, vendor risk management analysts and cybersecurity risk managers.) Seek out internal team members who may be interested in changing or evolving from their current roles. Again, it will likely be easier to train experienced cybersecurity professionals for highly sought after, low availability risk management roles.

Availability of Cyber Training

Slightly over 1/3rd of respondents (36%) said cybersecurity training is offered for all employees. That leaves nearly 2/3rds of organizations without comprehensive cybersecurity training and education.

FIGURE 13
CYBERSECURITY TRAINING OFFERED BY ROLE



44% of respondents reported that training was offered for IT and cybersecurity roles, which is relatively low given the strong demand, and in light of requirements for ongoing education across all levels of IT and cybersecurity jobs.

Time to reconsider?

Given the rise in cyberthreats, it's a wise move to equip cybersecurity professionals with the latest training and certifications to keep their skills sharp. Training and reskilling programs are beneficial for employees and organizations alike, providing a positive impact on employee retention.

At the same time, all types of organizations benefit from well-trained, up-to-date cybersecurity teams.

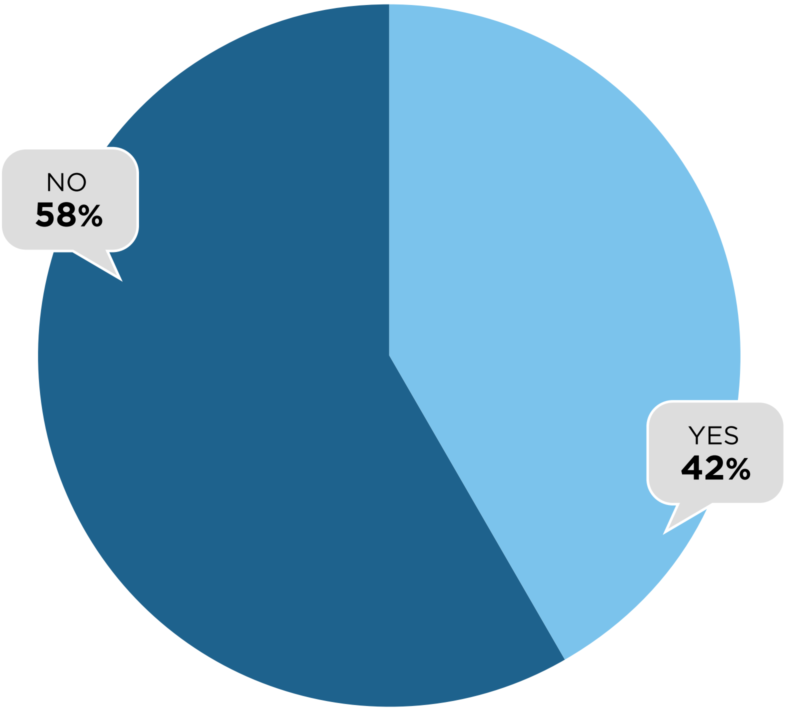
By investing in training programs and certifications, organizations can even help to foster non-cybersecurity personnel to consider moving into the cybersecurity field for career advancement opportunities. Employees are generally less tempted to seek new jobs if they believe their current employers are invested in their skill development and willing to provide opportunities for growth.

Training matters

Rising numbers of cyberattacks underscore the need for greater training across all departments and job roles. Since the onset of the global pandemic, for example, the FBI has reported up to an 800% increase in cyberattacks. Because the vast majority – roughly 90% of cyberattacks involve some form of phishing scam – it's important to increase your organization's focus on training for all employees.

Consider investing in a continuous managed service training approach, to keep your personnel informed, educated and updated on how to spot scams, and what to do to avoid such attacks.

FIGURE 14
TRAINING TUITION REIMBURSEMENT



Approximately 58% of respondents currently offer no cybersecurity training tuition reimbursement. This is something to reconsider as organizations work to mitigate risks and improve cybersecurity protections.

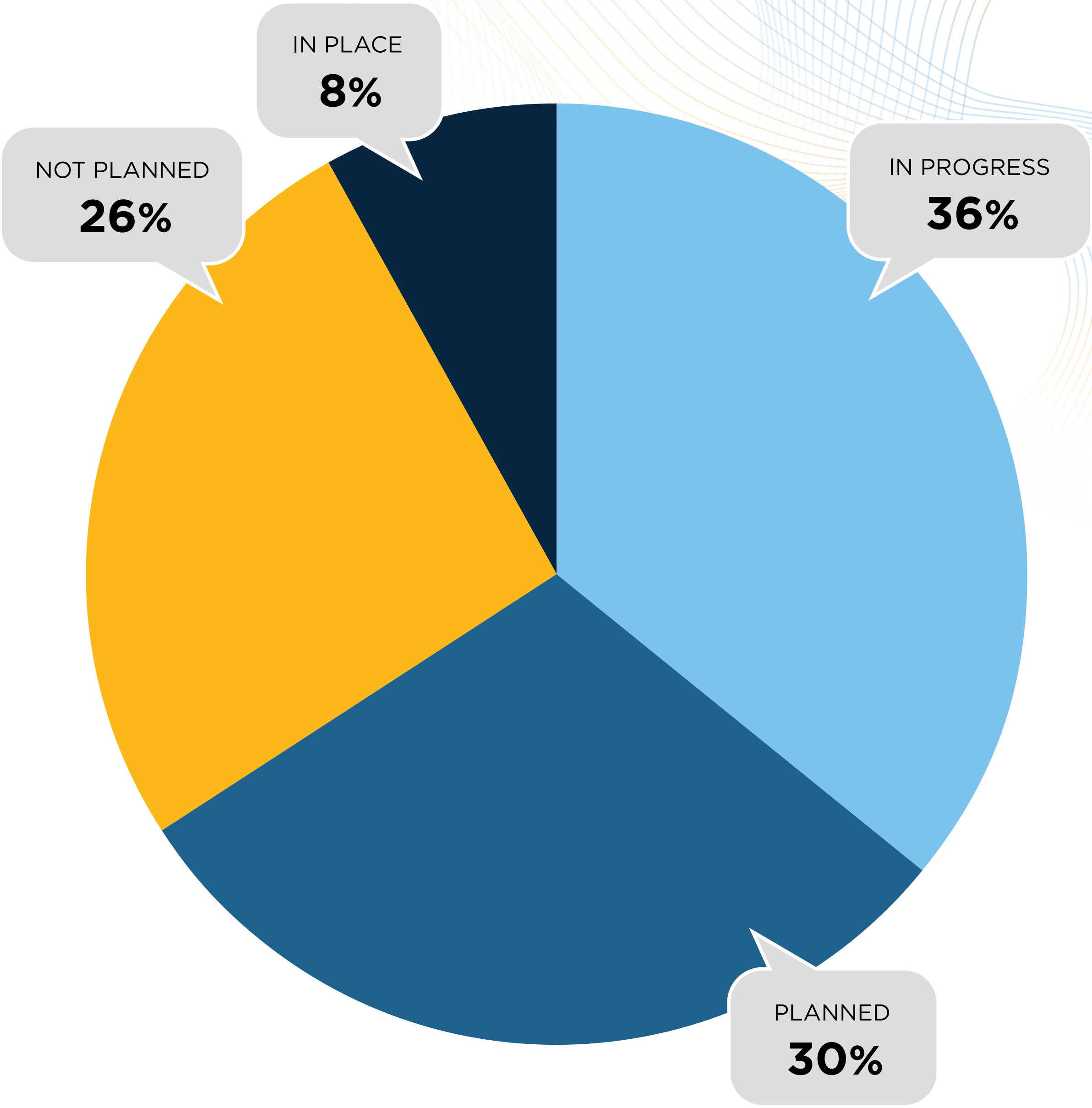
Zero Trust
In Organizations

Zero Trust is a strategic approach that helps prevent breaches by eliminating excess digital trust from your organization. Rooted in the principle of "never trust, always verify," the Zero Trust strategy can be deployed in both IT and OT organizations and at the highest levels within any organization, yet can be tactically deployed using off-the-shelf technology and the right procedural steps.

There are five primary steps to implementing Zero Trust, according to Zero Trust originator John Kindervag. These include:

1. DEFINE AND PRIORITIZE PROTECT SURFACES – the business critical assets requiring the most protection.
2. MAP TRANSACTION FLOWS – to understand how data, applications, assets, and services interact.
3. BUILD A ZERO TRUST ARCHITECTURE – placing security controls as close as possible to your protect surfaces.
4. CREATE A ZERO TRUST POLICY – to articulate who, what, when, why and how users can access your protect surfaces.
5. MONITOR AND MAINTAIN THE ENVIRONMENT.

FIGURE 15
STATUS OF ZERO TRUST IN ORGANIZATIONS



44% of respondents surveyed are either implementing Zero Trust or have a Zero Trust architecture in place. Meanwhile, nearly a third (30%) are planning to implement Zero Trust, underscoring the need for training and educational courses and content.

Roadblocks To Successful Detection & Response

Respondents cited organizational visibility challenges (21%) and lack of budget (20%) as the biggest roadblocks to successful detection and response.

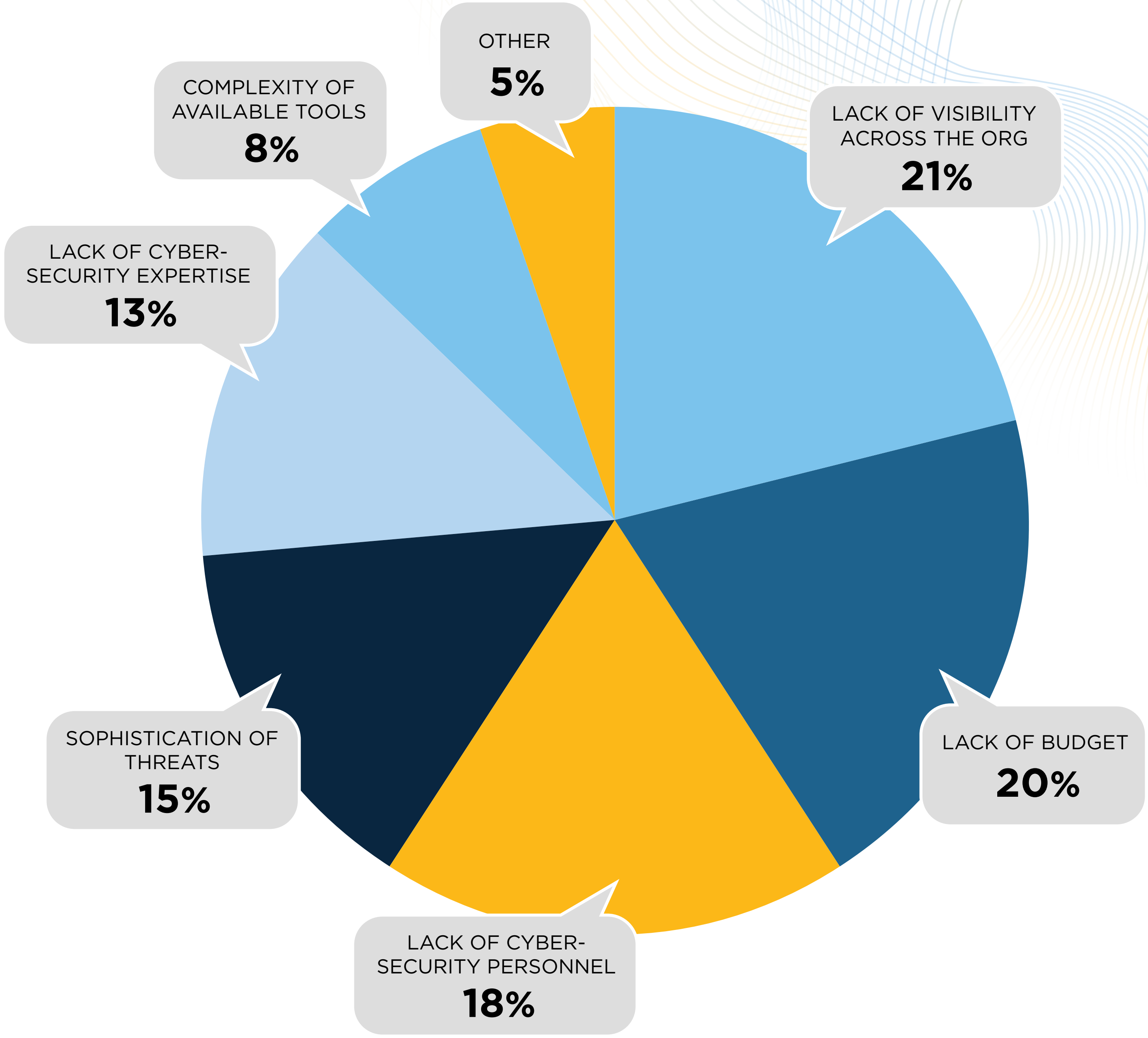
Overcoming obstacles

To help overcome the lack of budget for cybersecurity training noted by 20% of respondents, it's important to highlight the rising need for cybersecurity knowledge among today's boards of directors and business leadership, along with the increasing regulatory requirements levied on organizations around Governance, Risk, Compliance (GRC). These topics demand greater cybersecurity acumen and agility, both in operations and in the C-Suite (and beyond) to better manage and strengthen cybersecurity protections.

Consider exploring greater CISO and CEO engagement and understanding to overcome these challenges. This sentiment was echoed in respondent comments as well. "I'd like to see a stronger association promoted between the cybersecurity and GRC domains," said one North American Industrial Security Architect/Engineer.

"It seems there is far too much emphasis on tactical planning and response versus the organizational structures and processes which support a cybersecurity culture that mitigates risk."

FIGURE 16
DETECTION & RESPONSE ROADBLOCKS



Respondent Takeaways

To further understand the issues, it's important to consider a few more key concepts we learned from those who took the time to comment on our survey.

> "Cybersecurity education is too fragmented with new stacks of training coming all the time. We need to consolidate, not fragment training into multi-discipline qualifications. Only core service areas (e.g. pentesting) should be accepted as standalone qualifications, since the quality of individuals keeps declining due to quick fix hires with one or two certifications, but [without] foundational, risk-oriented thinking."
>
> AUSTRALIA/NEW ZEALAND BASED IT SECURITY BUSINESS MANAGER

> "Companies still [cut corners] a lot on the basics. We need to reinforce the need to [strengthen cybersecurity] processes, education, and implement effective penalties for non-compliance."
>
> LATAM CISO, RETAIL INDUSTRY

> "Cybersecurity is still seen as a responsibility unique to IT and those working within IT, not something that is everyone's responsibility. This change in culture needs to be led from the boardroom."
>
> U.K. IT DIRECTOR, EDUCATION INDUSTRY

> "There's a need for education and training across all organizational levels, especially given skyrocketing attacks. The problem is a serious lack of executive leadership awareness of the significance and prevalence of threats. Something needs to change."
>
> U.S. PROFESSIONAL SERVICES CYBERSECURITY SPECIALIST

> "Up-to-date security tools and appliances are not enough, especially if communicating cybersecurity to your respective organization and/or stakeholders is not part of your cybersecurity/business strategic plan."
>
> ASIA PACIFIC IT SECTION HEAD, GOVERNMENT SECTOR

> "It's stressful for IT staff because too much of what we suggest is misunderstood, and therefore ignored."
>
> ASIA PACIFIC BUSINESS ANALYST, MANUFACTURING INDUSTRY

> "Security should be foremost, and not an afterthought. Culture eats strategy for breakfast."
>
> ASIA PACIFIC IT DIRECTOR, MEDIA INDUSTRY

Results Appendix