FORRESTER®

Cyber Leaders Need A More Effective Approach To Building and Proving Resilience

Get started ⟶

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY IMMERSIVE LABS | MARCH 2023

Overview

With an expanding tech footprint, hybrid work, and a constantly evolving threat landscape, it's impossible for companies to be impenetrable. But cybersecurity leaders who focus on people-centric cybersecurity increase their cyber resilience and protect their data, reputation, and bottom line.

In December 2022, Immersive Labs commissioned Forrester Consulting to understand how global cybersecurity training strategy decision-makers perceive their company's cyber resilience and how they hire and upskill their teams. For this study, we defined cyber resilience as the ability and confidence in a cybersecurity team to prepare for and quickly detect, defend, respond, adapt, recover, and learn from a security breach or unexpected and unknown threats. We found that leaders still feel their cybersecurity teams are unprepared and ill-equipped to protect their companies — and that a people-centric cybersecurity culture shift needs to happen for companies to be better prepared.

Key Findings

Eighty-four percent of respondents agree that cybersecurity teams feel increasing pressure to be prepared for the next cyberattack.

Over 80% also agree they could have mitigated some to all of the damage of their most significant cyber incident in the last year if they were more cyber resilient.

The main obstacle to cyber resilience is insufficient security expertise. Rather than rely on certifications and traditional training practices, leaders need to hire high-potential candidates, evaluate preparedness processes gaps, and invest in continuous and more effective upskilling approaches.

Cybersecurity Teams Face Mounting Pressure To Be Cyber Resilient

Security and risk professionals have a lot to juggle; not only are their roles and responsibilities increasing over time, but the threat landscape is continually changing — and becoming more challenging. According to our study, 84% of respondents agree that cybersecurity teams feel pressured to prepare for the next attack. Furthermore, respondents agree that top executives at the board and C-suite levels pressure them to prove their cyber resilience more than they did a few years ago.

But the question remains: *Are* teams ready for the next cyberattack?

Cybersecurity Teams Face Mounting Pressure From All Fronts

61% agree the roles and responsibilities of cybersecurity professionals are increasing over time.

72% agree the threat landscape is becoming more challenging.

84% agree their organization's cybersecurity team is feeling increasingly pressured to prepare for the next cyberattack.

65% agree their organization's board is placing more pressure on the cybersecurity team to prove cyber resilience than they did a few years ago.

78% agree their organization's C-level executives are placing more pressure on the cybersecurity team to prove cyber resilience than they did a few years ago.

Base: 316 global decision-makers of cybersecurity training strategies
Source: A commissioned study conducted by Forrester Consulting on behalf of Immersive Labs, December 2022

Cybersecurity Teams Have An Overconfidence Problem

Survey data suggests that cybersecurity leaders are conflicted in their confidence of their organization's cybersecurity team. At first glance, they seem confident that their cybersecurity team is cyber resilient, but when asked specifically about how well prepared the team is for another attack or how effectively the team responds to and resolves incidents, their confidence plummets.

Furthermore, only 17% of respondents consider their cybersecurity team to be fully staffed and nearly half of respondents admit they aren't able to measure the cybersecurity team's abilities to address cyberattacks nor is the team well-trained. Therefore, confidence in the cybersecurity team's resilience is questionable. If cyberattack prevention and damage control are both lacking, organizations are more vulnerable than they initially thought.

"On a scale of 1 to 5, how much does each term describe your organization's cybersecurity team today?"

Base: 316 global decision-makers of cybersecurity training strategies
Note: Total percentages may not equal separate values due to rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Immersive Labs, December 2022

Cybersecurity Teams Are More Confident In Their Abilities Than Their Coworkers

In terms of incident response, only 60% of respondents think their cybersecurity team responds and resolves incidents effectively (see previous figure). Companies cannot risk having poor incident response capabilities because a security breach can have devastating financial and reputational repercussions. Yet as it stands, over 80% of respondents either don't think or are unsure that their cybersecurity team has the needed abilities to respond to attacks. Even worse, over three-quarters of leaders don't think their security team has confidence in themselves. What is clear is other stakeholders lack confidence in their cybersecurity teams' incident response capabilities. Cybersecurity teams need better metrics to justify their confidence in their incident response capabilities.

Employees Lack Confidence In Firms' Incident Response Capabilities

82%

don't think their organization's cybersecurity team has all the abilities it needs to effectively respond to the next cyberattack.

Only 23%

think their organization's security team is confident in its incident response capabilities.

Only 17%

think their organization's workforce is confident in its incident response capabilities.

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY IMMERSIVE LABS | MARCH 2023

Base: 316 global decision-makers of cybersecurity training strategies
Source: A commissioned study conducted by Forrester Consulting on behalf of Immersive Labs, December 2022

Leaders Need Proof Of Cyber Resilience

Cyber risk is a top priority leadership cares about and wants managed like any other risk.[1] Whether it's a recurring meeting or a postmortem after a major cyber incident, security professionals can expect more face time and increasing pressure from the board and C-suite to prove their firms' cyber resilience. Boards of directors rarely have security expertise, so instead of a count of attacks, alerts, and events, an evidence-based assessment of the firm's security program's maturity would be much more accessible and valuable.[2]

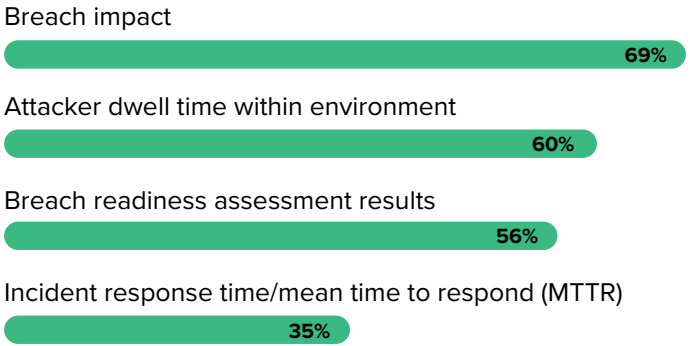
According to our study, security leaders are selective about the metrics they share. They should be sharing breach readiness and incident response results to a greater degree, but fewer than 60% do so today. These results tend to be largely qualitative and anecdotal and, therefore, are difficult to share. Security and risk professionals might be more encouraged to share their security maturity if they had better methods to assess and prove their capabilities and resilience.

Firms Are Selective About The Metrics They Share With Leadership

89%
of respondents are tracking all four metrics.

82%
share two or more metrics with board and leadership.

They track and share the following metrics with the board and leadership:

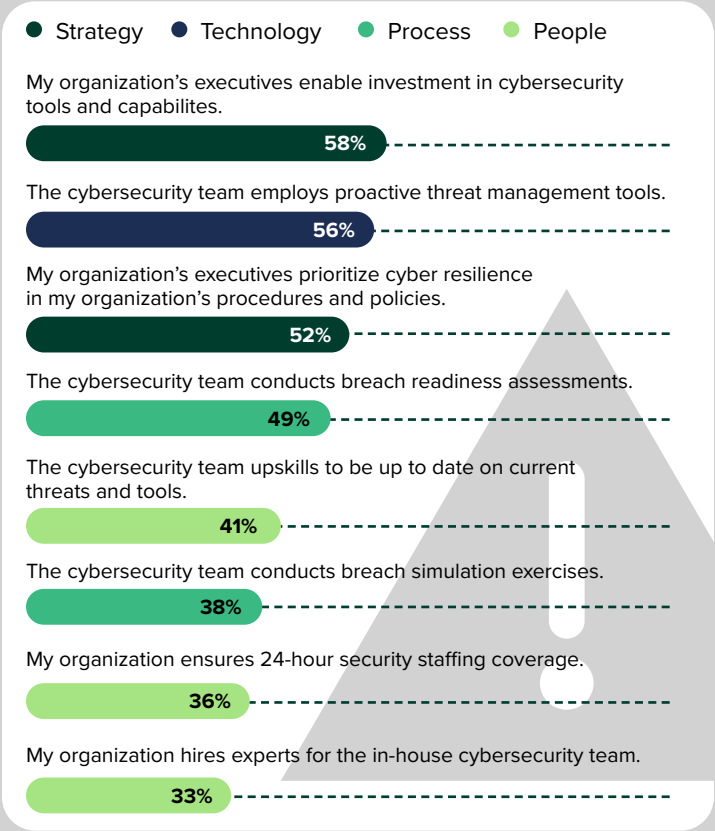


Base: 316 global decision-makers of cybersecurity training strategies
Source: A commissioned study conducted by Forrester Consulting on behalf of Immersive Labs, December 2022

Teams Aren't Strategically Equipped To Maintain Cyber Resilience

Preparing against cyberattacks is no simple task. While security leaders might have leadership's backing — or even the right cyber risk management tools — execution is lacking. Less than one-third (32%) believe their organization has a formal strategy to ensure cyber resilience, and over half (55%) agree their cybersecurity team doesn't have the data needed to demonstrate readiness for cyber threats. Cybersecurity teams are not sufficiently assessing, hiring, or training for resilience.

"Which of the following describes how your organization ensures cyber resilience?"

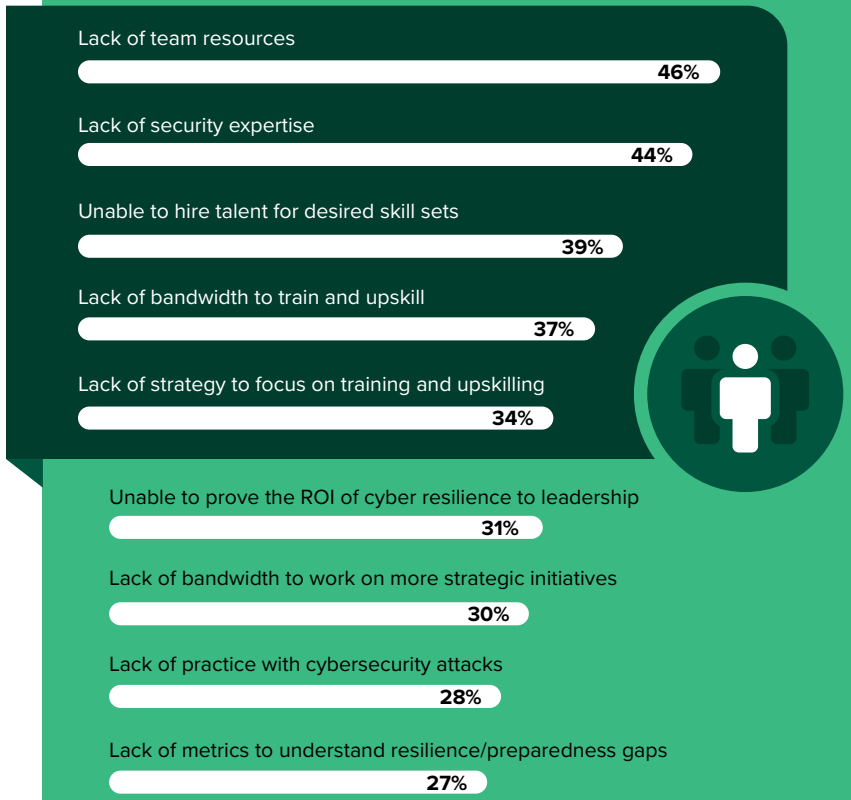


Base: 316 global decision-makers of cybersecurity training strategies
Note: Showing top 8 responses
Source: A commissioned study conducted by Forrester Consulting on behalf of Immersive Labs, December 2022

Firms Lack The Talent To Maintain Cyber Resilience

Over 90% of respondents report experiencing at least one challenge to maintaining cyber resilience with the top five challenges relating to people. Firms have many considerations to optimize for from the team size and acquiring the desired skill sets to having the bandwidth and strategy needed for upskilling. The latest gadgets and tools are useless without the people and knowledge to unleash the power of the technology.

"What are challenges your organization's cybersecurity team face to maintain cyber resilience?"



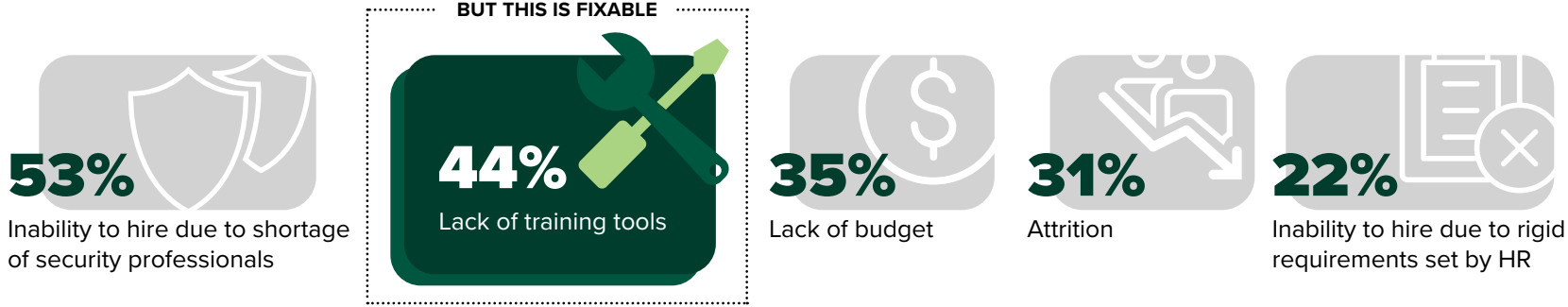
Base: 316 global decision-makers of cybersecurity training strategies
Source: A commissioned study conducted by Forrester Consulting on behalf of Immersive Labs, December 2022

Cybersecurity Faces Talent Shortages

Eighty-three percent of respondents think their cybersecurity team is understaffed, and 94% experience at least one talent management challenge with the cybersecurity team. The top challenge is inability to hire due to a shortage of security professionals, which over 40% agree is negatively impacting their company's cyber resilience. The more vacancies there are, the more vulnerable the company is and the more breaches the company will experience.[3]

The second-ranked talent challenge is the lack of training tools, which can be more easily addressed. Chronically underskilled security teams fare no better than an understaffed one, and poor security succession planning is costly in more ways than one — the departure of one key employee can mean institutional knowledge leaves with them.[4] Firms can mitigate the potential damage of attrition or an underskilled team through improved hiring, training, and retention practices.[5]

"Which of the following challenges does your organization experience with talent management within the cybersecurity team?"



Base: 316 global decision-makers of cybersecurity training strategies
Source: A commissioned study conducted by Forrester Consulting on behalf of Immersive Labs, December 2022

Cybersecurity Needs A Cultural Shift To Recruit Talent With Potential

Decision-makers want to hire cybersecurity experts with the experience (85%) and skills to hit the ground running (78%), but they also hire with certifications in mind (63%). But decision-makers have the opportunity to hire cybersecurity experts based on their aptitude or future potential. Unfortunately, HR and hiring managers are over-relying and overemphasizing certifications and, as a result, reject qualified applicants or create a costly barrier to entry for early career and diverse security talent.[6] While HR might be responsible for hiring and development, they don't always understand the expertise cybersecurity roles require.[7]

While over 60% of surveyed respondents think their cybersecurity team is well certified, 48% agree their team lacks expertise in specific security domains. Existing recruiting processes are potentially weeding out hires with high potential that companies can invest in and develop.

"How important are each of the following to your organization's cybersecurity hiring decisions?"

85%
Cybersecurity experience

78%
Demonstrable cybersecurity skills

69%
IT background or experience

63%
Cybersecurity certifications

OPPORTUNITY

62%
Aptitude/potential

56%
Higher-education degree

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY IMMERSIVE LABS | MARCH 2023

Base: 316 global decision-makers of cybersecurity training strategies
Source: A commissioned study conducted by Forrester Consulting on behalf of Immersive Labs, December 2022

Investing In In-House Upskilling Is Critical

Given the talent shortage and budget-tightening efforts for most organizations, firms are better served using a cybersecurity upskilling training platform to 1) test candidates for desired skills during recruiting and 2) equip early career and in-house talent to handle threats. Improved hiring and training practices would eliminate lengthy vacancies and skill gaps, which can lead to more vulnerabilities and breaches.[8]

Building quality in-house and people-centric cyber resilience programs is essential. It allows leaders to close the expertise gap in their organizations; create a succession plan to prevent disruptions; demonstrate investment in its employees and provide paths for advancement; and, ultimately, promote retention.[9] In addition, organizations can better track hands-on cybersecurity capabilities and career progression when performing continuous exercises. Seventy percent of respondents agree their firm will be making investments to improve in-house cybersecurity training in the next year.

70%

agree their organization is making investments to improve in-house training of the cybersecurity team in the next year.

Base: 316 global decision-makers of cybersecurity training strategies
Source: A commissioned study conducted by Forrester Consulting on behalf of Immersive Labs, December 2022

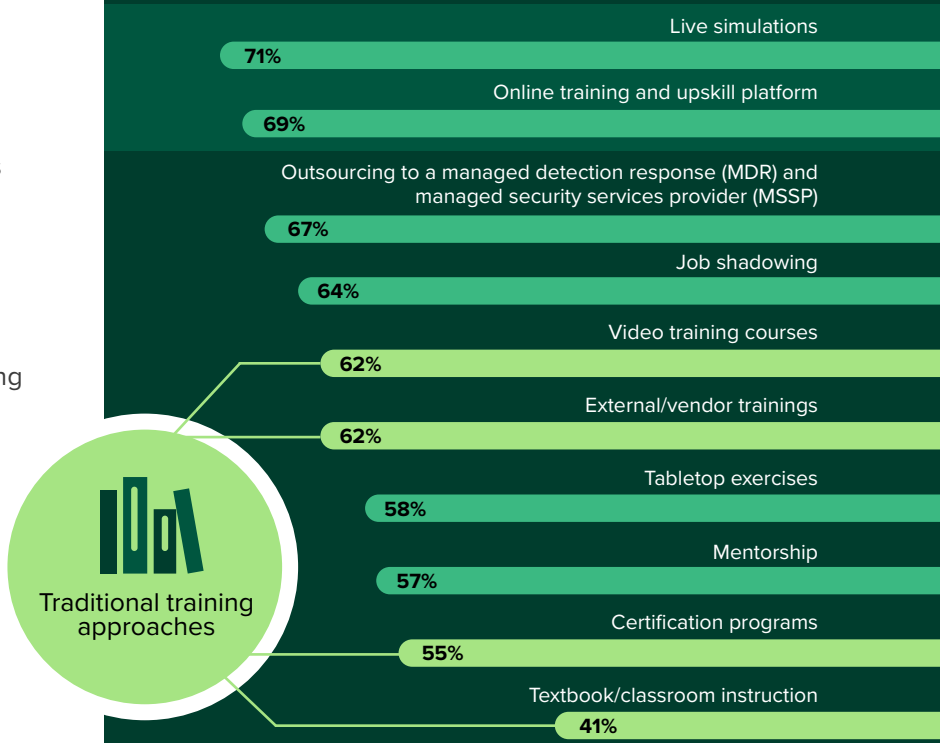
Cybersecurity Teams Are Not Using The Most Effective Upskilling Approaches

Nearly all surveyed respondents use video training courses and external/vendor training, potentially because they are the most accessible and the least expensive; but these traditional training approaches are not the most effective. In fact, 64% of respondents agree that traditional cybersecurity training methods (e.g., certifications, video training courses, classroom instruction) are insufficient to ensure cyber resilience.

According to cybersecurity training decision-makers, the most effective training approaches are live simulations and online training and upskill platforms, which over 60% of respondents plan to increase investment in.

"How effective are the following cybersecurity training approaches in building cyber resilience capabilities for your organization's cybersecurity team?"

(Showing "Very effective/Effective")



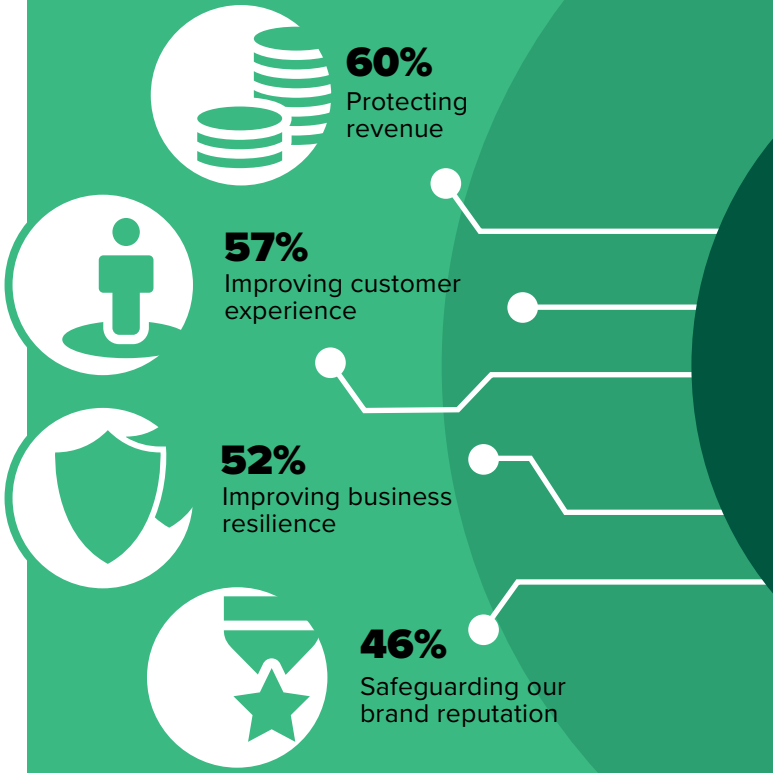
Base: 316 global decision-makers of cybersecurity training strategies
Source: A commissioned study conducted by Forrester Consulting on behalf of Immersive Labs, December 2022

Reap The Business Rewards Of Effective Cybersecurity Upskilling

Security leaders recognize that being ill-prepared to take on cyber risk will increase cyber incidents, financial losses, and a need to turn to third-party partners for assistance. In contrast, improving cybersecurity skills on the team and individual level will result in operational, brand, and financial benefits. Eighty-two percent of respondents agree that if their teams were better prepared to address the most significant cyber incident they experienced last year, they could have mitigated some to all damage or impact.

As one survey respondent said, “By solving cybersecurity incidents, a company gains a competitive advantage over its competitors.” A comprehensive and effective cybersecurity training program will invite new and retain existing talent, bolster readiness against cyberthreats and attacks, and secure operational resilience for the business.

Top 4 Benefits Of Improving Hands On Individual And Team Cybersecurity Skills



Base: 316 global decision-makers of cybersecurity training strategies
Note: Showing top 4 responses
Source: A commissioned study conducted by Forrester Consulting on behalf of Immersive Labs, December 2022

Conclusion

Cyber risk is costly if poorly managed, so the name of the game is to be as prepared as possible to address cyberattacks as they come. Cybersecurity teams are currently ill-equipped to protect their companies or even diffuse the impact of cyber incidents. They lack cyber capabilities and judgment to respond effectively. To alleviate the staffing shortage and the lack of in-house cyberskills, firms must reevaluate hiring practices to recruit and test for high-potential hires. They must also invest in a culture that leverages effective people-centric approaches, such as live simulations, and progressive, career-path aligned online training and upskilling to bolster their cybersecurity teams' capabilities and, in turn, their organization's cyber resilience.

Project Director:

Sandy Liang,
Market Impact Consultant

Contributing Research:

Forrester's Security and Risk research group

Methodology

This Opportunity Snapshot was commissioned by Immersive Labs. To create this profile, Forrester Consulting supplemented this research with custom survey questions asked of 316 global decision-makers of cybersecurity training strategies. The custom survey began in November 2022 and was completed in December 2022.

ENDNOTES

[1] Source: "How To Talk To Your Board About Cybersecurity," Forrester Research, Inc., August 2, 2021.

[2] Source: Ibid.

[3] Source: "Succession Planning Is A Business Resilience Imperative," Forrester Research, Inc., June 30, 2022.

[4] Source: Jess Burn (host), "Succession Planning For The Security Org," What It Means, September 15, 2022.

[5] Source: "The Security Skills Shortage Takes Its Toll On Organizations," Forrester Research, Inc., January 20, 2023.

[6] Source: "Rethink Your Reliance On Cybersecurity Certifications," Forrester Research, Inc., October 24, 2022.

[7] Source: "How To Manage Your Vulnerability Risk Program Amidst Skill And Labor Shortages," Forrester Research, Inc., October 28, 2022.

[8] Source: "Reverse Cybersecurity's Self-Inflicted Staffing Shortage," Forrester Research, Inc., August 2, 2021.

[9] Source: "Succession Planning Is A Business Resilience Imperative," Forrester Research, Inc., June 30, 2022.

Demographics

GEOGRAPHY	
US	**60%**
UK	**15%**
Germany	**11%**
Sweden	**9%**
Canada	**6%**

ANNUAL REVENUE	
$1B to $2.9B	**46%**
$3B to $4.9B	**23%**
$5B to $9.9B	**20%**
$10B or more	**12%**

TOP 4 INDUSTRIES	
Financial services, excluding fintech	**19%**
Fintech	**18%**
Retail	**5%**
Manufacturing and materials	**5%**

TITLE	
C-level	**5%**
Vice president	**34%**
Director	**60%**

Note: Percentages may not total 100 because of rounding.

ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key transformation outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute on their priorities using a unique engagement model that tailors to diverse needs and ensures lasting impact. For more information, visit forrester.com/consulting.


FORRESTER®