Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **May 2023**
Commissioned by **Immersive Labs**

Cyber Workforce Resilience Trend Report

Executive Summary

With a steady increase in cyberattacks each year and a constantly evolving threat landscape, more organizations are turning their attention to building long-term cyber resilience: the ability of the workforce to adapt, respond, and recover from cybersecurity incidents, not merely the ability to detect and prevent them. To learn more about the state of cyber resilience, we surveyed senior security and risk leaders and found that cyber resilience indeed tops their list of strategic and spending priorities for organizations in 2023, driven largely by concerns about ransomware, supply chain and third-party attacks, and coding vulnerabilities.

While a majority of these leaders have cyber resilience programs in place, they are falling short and failing to prove teams' real-world cyber capabilities. Half of organizations are not prepared for any kind of cyberattack and current confidence levels in cyber resilience are low. And although confidence in technical teams for cyber resilience is much higher than for the general workforce, many organizations continue to rely on ineffective and ad hoc methods for building cybersecurity competence and assessing resilience.

These findings suggest that organizations must urgently embrace a new approach to building cyber resilience, including implementing more effective ways to develop and prove cyber capabilities across teams, measure improvement , and cultivate a workforce with the expertise to handle the real-world impact of a cyber incident.

Cyber resilience is a top priority for organizations, yet most lack confidence that they are prepared for a cyberattack.

KEY TAKEAWAYS

The key takeaways from this research are:

- **Cyber resilience tops the list of strategic priorities for organizations**
  It is the highest-ranked strategic priority and spending priority in 2023.
- **The threat of cyberattacks and vulnerabilities are driving these priorities**
  Ransomware, supply chain risks, and vulnerabilities are chief among security leaders' concerns.
- **Current cyber resilience programs are falling short**
  Half of organizations are flying blind across a wide range of cybersecurity indicators despite having cyber resilience programs in place.
- **Organizations have a questionable reliance on industry certifications, classroom training, and ad hoc learning pathways**
  While almost all organizations encourage industry certifications, only 32% say they are effective at mitigating cyberthreats. Classroom training is offered too infrequently to be effective. Many rely on ad hoc and reactive learning pathways for cybersecurity team members to get up to speed on the latest vulnerabilities. None of these approaches work at the speed of cyber.
- **Most lack a framework for measuring cyber capabilities**
  Organizations are attempting to cobble together an assessment framework using indicators, tests, and metrics unrelated to resilience.
- **Organizations need better ways to assess, build, and prove cyber resilience—but they're making some progress**
  To increase cybersecurity, organizations need to be able to identify skills gaps, fill them, and prove cyber resilience to senior leaders. Some are making some early steps towards effective cybersecurity.

ABOUT THIS WHITE PAPER

The survey and white paper were commissioned by Immersive Labs. Information about Immersive Labs and details on the survey methodology are provided at the end of the paper.

The Importance of Cyber Resilience

Strengthening cyber resilience of cybersecurity teams and the general workforce is high on the priority list for organizations in 2023.

CYBER RESILIENCE TOPS STRATEGIC PRIORITIES FOR 2023

Our research found that cyber resilience tops the list of strategic priorities for organizations in 2023, with improving both the cybersecurity team and the general workforce the two highest-ranked strategic priorities for 80% of organizations. Cyber resilience is the ability of the workforce to detect and prevent cybersecurity incidents (including breaches), and also to adapt, respond, and recover from incidents.

Three input factors that contribute to increased cybersecurity resilience rank highly as enablers for achieving the outcome. These input factors are deploying new software solutions, upskilling teams, and hiring qualified cybersecurity professionals. Rating these input factors as less important than the outcomes is the proper emphasis. See Figure 1.

Managers see upskilling existing teams and/or individuals as a higher priority than hiring new cybersecurity professionals. This strategic emphasis highlights the skills gap in the market, the benefit of staff knowing the organization's culture, and the value of driving resilience with better team-level skills and experiences rather than merely adding new people with untested resilience capabilities.

Strengthening cyber resilience of cybersecurity teams and the general workforce tops the priority list for organizations in 2023.

Figure 1
Priority of People-Centric Strategies in 2023
Percentage of respondents indicating "high priority" or "essential priority"

Source: Osterman Research (2023)

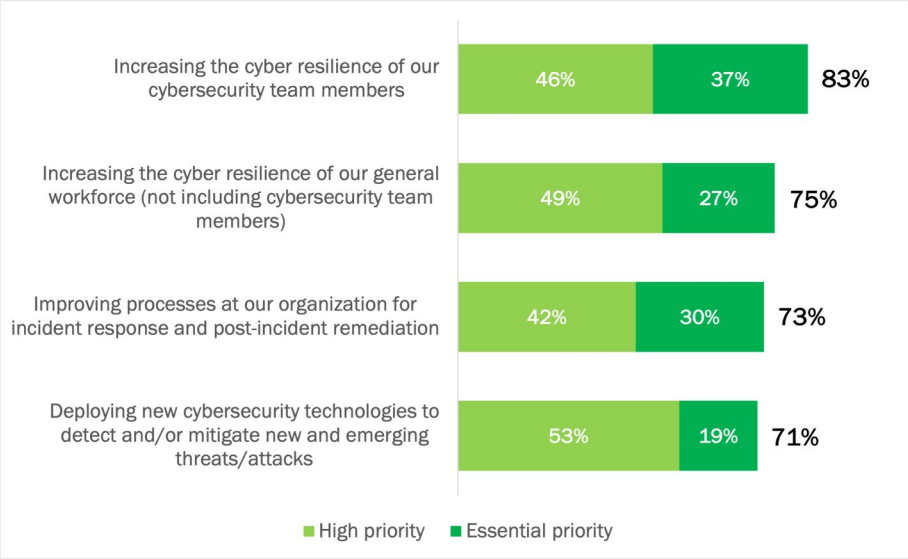
CYBER RESILIENCE TOPS IT AND SECURITY SPENDING PRIORITIES IN 2023

The strategic priority of improving cyber resilience is reflected in how organizations approach spending on IT and security in 2023. Increasing the cyber resilience of cybersecurity team members (83%) and the general workforce (75%) are the two areas with the highest overall priority. If we isolate the "essential priority" ratings, the highest value is assigned to increasing the cyber resilience of cybersecurity team members (37%), followed by improving processes for incident response and post-incident remediation (30%). These two areas of spending work together: trained and aware cybersecurity professionals plus robust processes for incident response and post-incident remediation.

Of the four spending priorities covered by our study, deploying new cybersecurity technologies was rated in last place, and only 19% of respondents indicated this was an "essential priority." Rating tools as less important than the outcomes is the proper emphasis. Organizations intend to drive the resilience outcome through spending aligned with their strategic priorities, not by merely deploying new cybersecurity technologies or chasing standalone inputs.

See Figure 2.

Figure 2
Areas of Priority Spending in 2023
Percentage of respondents indicating "high priority" or "essential priority"



Source: Osterman Research (2023)

Organizations intend to drive the resilience outcome through spending aligned with their strategic priorities, not by merely deploying new cybersecurity technologies or chasing standalone inputs.

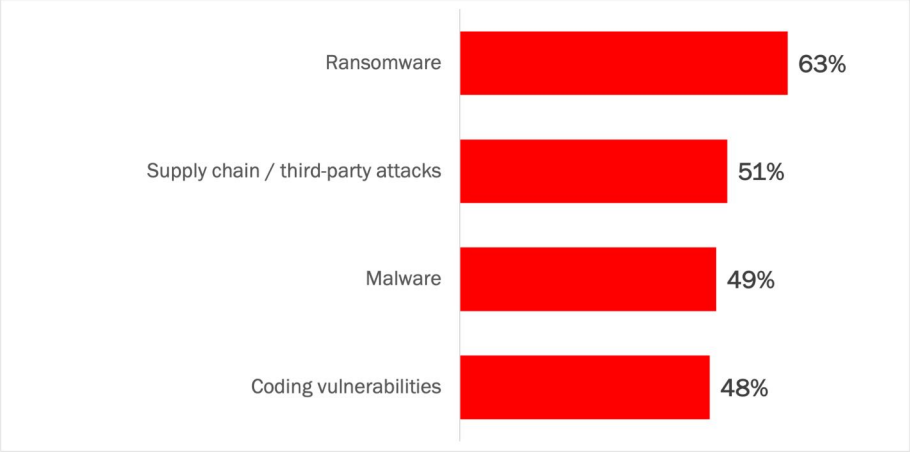
EXTERNAL THREATS DRIVING THE CYBER RESILIENCE AGENDA

Organizations are concerned about multiple cybersecurity threats and issues, with ransomware, supply chain/third-party attacks, and coding vulnerabilities among the top four cyberthreats or issues (see Figure 3). These threats and issues are significant, and without a robust cyber resilience story, they threaten the organization's viability. For example:

- **Ransomware (63% of respondents "concerned" or "extremely concerned")**
  The threat dynamics with ransomware continue to worsen, with individual threat actors transitioning into highly organized ransomware gangs, the embrace of supply chain and division of labor models, and ransomware-as-a-service offerings.[1] Suffering a ransomware attack leads to operational disruption to the organization and its customers/citizens, high-profile media coverage, and financially punitive business and regulatory consequences.
- **Supply chain and third-party attacks (51%)**
  Organizations face high uncertainty with supply chain and third-party attacks. The tools available for defensive measures are still rudimentary, with many relying on security posture assessments undertaken by yet another third party rather than anything even approaching a direct line-of-sight view into the security posture of significant business and supply chain partners. The lack of capabilities for better pre-attack strategies will continue to be a major risk for organizations. Hence, organizations must shift their focus to preparedness and resilience to mitigate an incident rapidly and fully if/when it occurs.
- **Coding vulnerabilities (48%)**
  81% of development teams at large organizations admit they are knowingly releasing vulnerable applications with insecure code.[2] While unpatched applications and software vulnerabilities from the wider software supply chain are frequent causes of breaches, an organization's development teams are also frequently at fault. Strengthening development processes and the organization's security culture are critical steps on the defensive side of the equation. However, these must be supported by an equal emphasis on the recovery and response side if/when a coding vulnerability is compromised.

Ransomware, supply chain and third-party attacks, and malware are driving the cyber resilience agenda.

Figure 3
Cyberthreats and Issues of Concern to Organizations
Percentage of respondents indicating "concerned" or "extremely concerned"

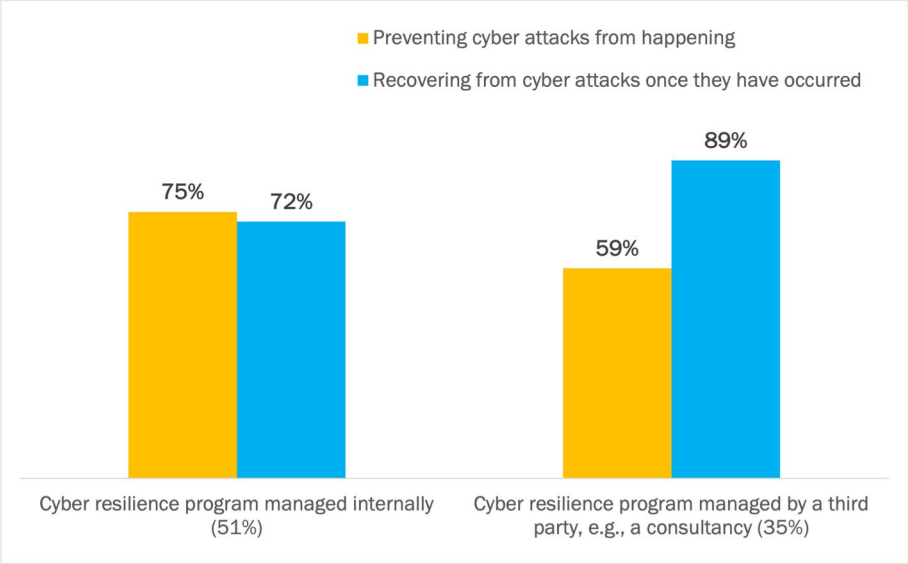


Source: Osterman Research (2023)

MOST ORGANIZATIONS HAVE A CYBER RESILIENCE PROGRAM, BUT LACK CONFIDENCE AND DATA

While 86% of organizations have a cyber resilience program, more than half of respondents say their organization lacks a comprehensive approach to assessing cyber resilience. These programs include some mix of a cyber resilience strategy, plan, and/or infrastructure. Most cyber resilience programs are managed internally by the organization (51% of organizations), with the remainder managed by a third party, such as a consultancy (35% of organizations). See Figure 4.

Figure 4
Efficacy of Achieving Outcomes of Cyber Resilience Programs
Percentage of respondents indicating "effective" or "very effective"



Source: Osterman Research (2023)

While organizations generally have these programs in place, they aren't as effective as they could be, because they lack metrics to identify and fill skill gaps.

HALF OF ORGANIZATIONS WITH NO METRICS ON CYBER RESILIENCE REPORT TO THE BOARD OF DIRECTORS SEVERAL TIMES A YEAR ON CYBER RESILIENCE. WE HOPE THEY'RE TELLING THE TRUTH

54% of senior security and senior risk leaders say they have the metrics they need to fully demonstrate their workforce's resilience in the face of a cyberattack. By implication, 46% do not.

Of this 46%, just under half report to the board of directors several times a year on their organization's cyber resilience for cyberattacks. The only valid report under these circumstances is to say "we have no idea." If anything else is claimed, senior security and security risk leaders are deceiving the board of directors and setting the organization up for massive failure.

All boards receiving regular reports on the cyber readiness of their organization need to start asking the messenger a question: How do you know?

All boards receiving regular reports on the cyber readiness of their organization need to start asking the messenger a question: How do you know?

ORGANIZATIONS ARE TAKING HAPHAZARD STEPS IN DEVELOPING A FRAMEWORK FOR MEASURING CYBER CAPABILITIES

We asked respondents how they measured the cyber capabilities of the teams and individuals at their organization. Of the 570 total respondents, 215 provided an open-ended answer. We coded, grouped, and correlated the answers.

The answers show organizations are taking haphazard steps towards a framework for measuring cyber capabilities. They are relying on questionable methods and approaches for cobbling together a framework.

The five most common responses were:

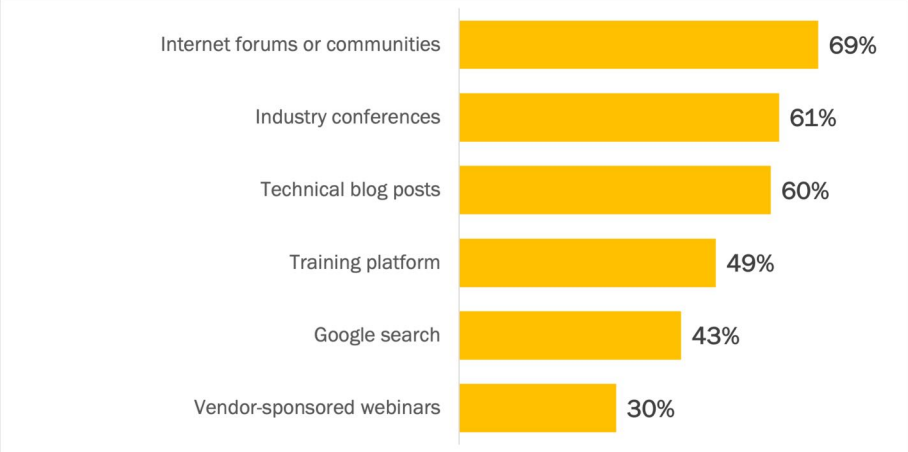
- **Response times to historical cyberthreats (9.8% of responses)**
  Looking at the trend line for historical response times provides a quantification that offers only an approximate assessment of cyber capabilities for future incidents.
- **No framework for assessment (9.3% of responses)**
  These organizations are not measuring cyber capabilities and have no approach for getting better. They are leaving cyber resilience entirely up to chance, which has repeatedly proven to be a short-sighted strategy worldwide. Shockingly, many organizations in this group believe nonetheless that their cybersecurity team and the general workforce will be able to perform the relevant tasks needed to recover from the next cyber incident—based on no evidence.
- **Some type of testing method (6.5% of responses)**
  Individuals are tested alone or pitted against their peers. About one fifth rely on phishing simulation tests. These methods are questionable because measuring cyber capabilities requires assessing cooperation across a team, not competitive stack ranking of individuals. And phishing simulation tests only provide insight about how an individual responds to a single type of cyberthreat, not an assessment of readiness against many types of threats.
- **NIST Cybersecurity Framework (6.0% of responses)**
  The NIST Cybersecurity Framework offers standards, guidelines, and practices for organizations to manage and reduce their cybersecurity risk.[3] The use of the framework is voluntary for most organizations and requires a tailored approach by each organization embracing the framework. NIST does not offer a certification program or endorsement of implementation.
- **Cybersecurity metrics (5.6% of responses)**
  A range of cybersecurity metrics are used by 5.6% of organizations, such as response times to addressing vulnerabilities, tracking intrusion rates, metrics on internal data loss, and incidence rates of various threat types. Visualizations, graphs, maps, and ratios are tracked to provide insight into how the organization deals with cybersecurity threats and incidents.

Organizations are taking haphazard steps toward a framework for measuring cyber capabilities, with 9.8% relying on response times (a lagging measure), 9.3% doing nothing, and 6.5% using some type of "testing."

LEARNING PATHWAYS FOR CYBER RESILIENCE ARE AD HOC

Cybersecurity team members are predominantly relying on ad hoc and reactive learning pathways to get up to speed on the latest vulnerabilities, such as Log4Shell. The formal learning programs at their organization is not addressing what they need to know. Internet forums and communities are the most frequently used pathway, followed by industry conferences and technical blog posts. See Figure 5. The efficacy of these pathways relies on cybersecurity professionals discovering the best internet forums/communities, attending the right industry conferences, and following the best technical blog posts. While these can be engaged with using a "best efforts" approach by individuals to drive continuing professional development, how these pathways contribute to cyber resilience is unverified.

Figure 5
Pathways for Learning About the Latest Vulnerabilities
Percentage of respondents



Source: Osterman Research (2023)

Weaknesses of these approaches for improving cyber resilience include:

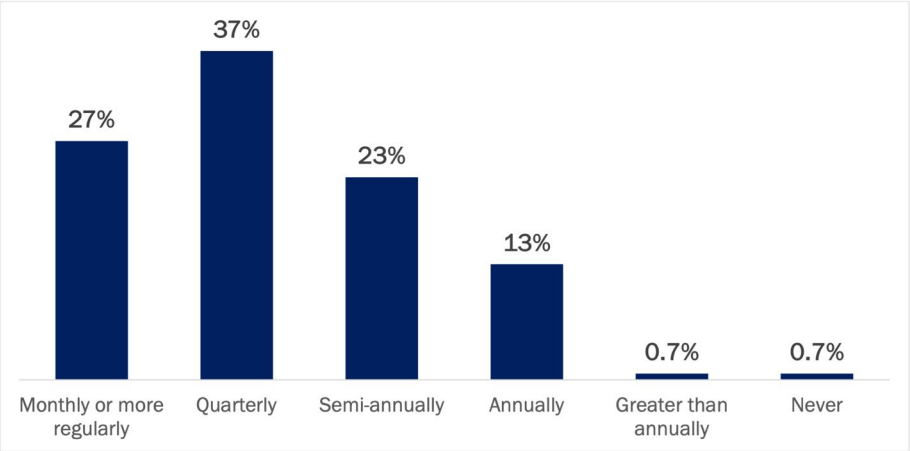
- **Lack of timeliness in content selection**
  Many industry conferences are held only annually and face a significant time gap between the selection of speakers and the conference itself. Talks that are approved for presentation months before the event is held will be outdated by the time the conference finally rolls around. Conferences are often better at distributing swag and hosting wild parties than upskilling cybersecurity professionals on the latest vulnerabilities—let alone improving resilience.
- **No contribution to team learning or assessing team dynamics**
  The learning interests of the individual rise above what the organization needs to know about the cybersecurity team. The approaches do not offer a structured mechanism for engaging the cybersecurity team as a whole, and therefore the organization has no way of assessing and improving how the cybersecurity team works together during an incident.
- **Learning and experimentation is disconnected from the resilience objective**
  Individual learning via these methods is commendable, but it does not provide a structured method for developing and assessing the cyber resilience of the organization. Reliance on these methods also signals that the organization is leaving a critical input to cyber resilience up to chance.

Formal learning programs at organizations are not addressing what cybersecurity professionals need to know about the latest vulnerabilities.

CLASSROOM TRAINING IS OFFERED TOO INFREQUENTLY TO BE EFFECTIVE

Classroom-based training represents a common approach to increase competence among employees, executives, and specific teams. Almost all respondents in this research indicate their organization offers classroom-based training annually or more regularly. See Figure 6.

Figure 6
Frequency of Classroom Training in Cybersecurity
Percentage of respondents



Source: Osterman Research (2023)

In attempting to make classroom training an effective approach for addressing cybersecurity threats, organizations must wrestle with the following dynamics:

- **Cyberthreats move at the speed of cyber, classroom training does not**
  Cyberthreats evolve, develop, and change more quickly than content for classroom training sessions can be developed, tested, and embedded across the organization. Running classroom training sessions on cyberthreats that were active three months ago (the reality for 37% of organizations) is reactionary and ineffective. The timeline between the disclosure of vulnerabilities and active attacks beginning is measured in hours and days, not weeks or months, so classroom training will always lag behind cyberthreats.
- **Addressing the challenges of frequency and reach**
  Classroom-based training is costly to offer frequently and difficult to scale across an organization to reach everyone. Only 27% of organizations provide classroom-based cybersecurity training monthly or more regularly—which was the most frequent cadence asked about in this research.

Organizations need to find an approach to developing cyber resilience that aligns with the speed of cyberthreats. Any approach that cannot deliver continuous training is not fit for purpose given the realities of cyberthreats.

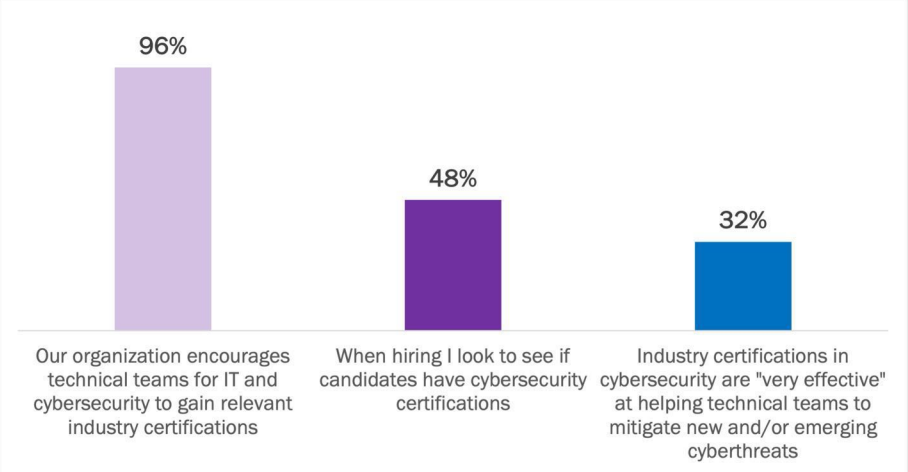
Running classroom training sessions on cyberthreats that were active three months ago (the reality for 37% of organizations) is reactionary and ineffective.

INDUSTRY CERTIFICATIONS ARE INADEQUATE TO ADDRESS EMERGING CYBERTHREATS

Almost all organizations encourage IT and cybersecurity teams to gain industry certifications to develop competence to mitigate new and/or emerging cyberthreats (96%). Such a high emphasis seems misplaced when considering two research-based realities of industry certifications (see Figure 7):

- **Certifications are considered in less than half of hiring decisions**
  Hiring processes look for the presence of cybersecurity certifications at only 48% of organizations, which is a significant drop from the 96% that indicate they "encourage" IT and cybersecurity teams to earn certifications. The disparity positions certifications as a check-box disqualification method in hiring decisions, not an approach that is treated by the organization as fundamental to success.
- **Certifications lack effectiveness in mitigating cyberthreats**
  Given the high emphasis placed on industry certifications (96%), it is alarming that only 32% of respondents rate industry certifications as "very effective" at helping technical teams to achieve the outcome of mitigating new and/or emerging cyberthreats. Organizations face financial outlay and lost productivity for technical teams to achieve and maintain industry certifications, yet these certifications are proving ineffective at mitigating cyberthreats.

Figure 7
Reliance on and Realities of Industry Certifications
Percentage of respondents



Source: Osterman Research (2023)

Cyberthreats move at the speed of cyber, but industry certifications do not.

The primary weakness of industry certifications is that cyberthreats move at the speed of cyber, but industry certifications do not. New cyberthreats hit organizations daily, yet industry certifications are revised much less frequently (e.g., annually). This means that industry certifications provide—at best—a lagging signal of baseline competence to deal with historical types of threats. Certifications may provide general direction to cybersecurity professionals on how to approach threats, but cannot be relied on to drive awareness and preparedness to mitigate specific current threats. The second weakness is that certifications signal lagging competence and dedication by technical individuals to achieving the certifications, not a sense of readiness, preparedness, and cyber resilience of the organization.

Early Progress Toward Cyber Resilience

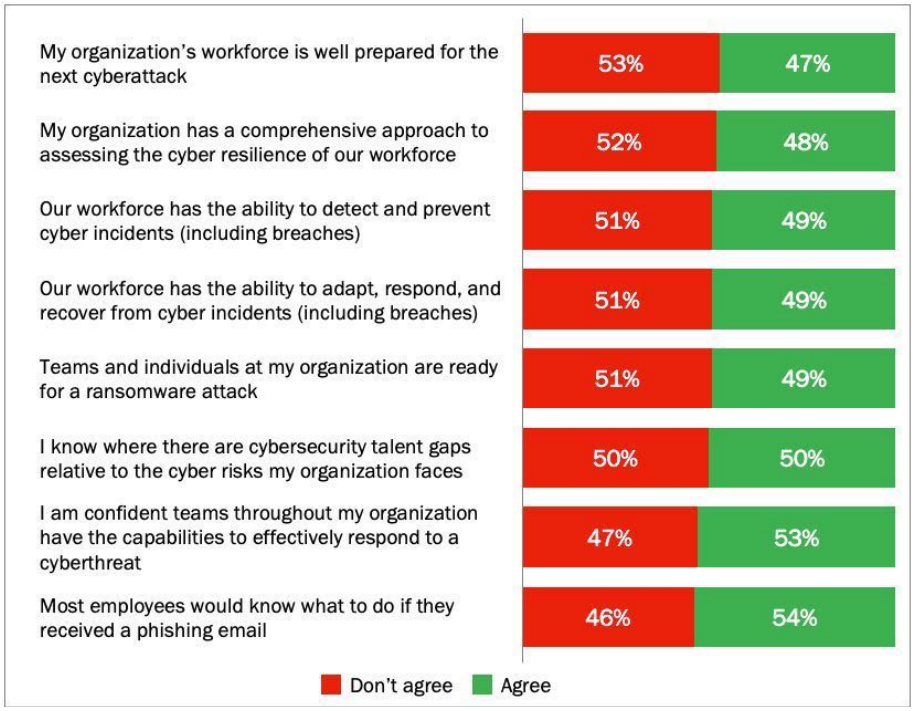
Some organizations have made promising early steps toward the cyber resilience outcome, despite setbacks. Across a wide range of indicators of cyber resilience, half of respondents indicate that employees, cybersecurity teams, and the organization are under-prepared. In sum, while respondents indicate cyber resilience is a strategic priority, current indicators present a poor showing (see Figure 8). These include:

- **Preparedness and assessment are lacking at more than half of organizations**
  53% of respondents indicate the organization's workforce is not well-prepared for the next cyberattack (of any kind), and 52% say their organization lacks a comprehensive approach to assessing cyber resilience.
- **Half of organizations are not prepared for a ransomware attack**
  Despite high-profile media coverage, despite increasing government alarm, despite calls for stronger defensive and recovery strategies for ransomware across multiple industries, just over half of respondents say their organization is not ready for a ransomware attack.
- **Almost half say employees still don't know what to do with phishing emails**
  Phishing messages are the most common initial attack vector for stealing credentials to breach data or plant ransomware. Almost half of respondents (46%) say their employees would not know what to do if they received a phishing email, despite years of security awareness training and phishing tests.

While these indicators are concerning, some organizations are making limited progress.

Half of respondents indicate that employees, cybersecurity teams, and the organization are under-prepared for cyberattacks.

Figure 8
Organizational Status and Progress Toward Cyber Resilience
Percentage of respondents indicating "agree" or "strongly agree"



Source: Osterman Research (2023)

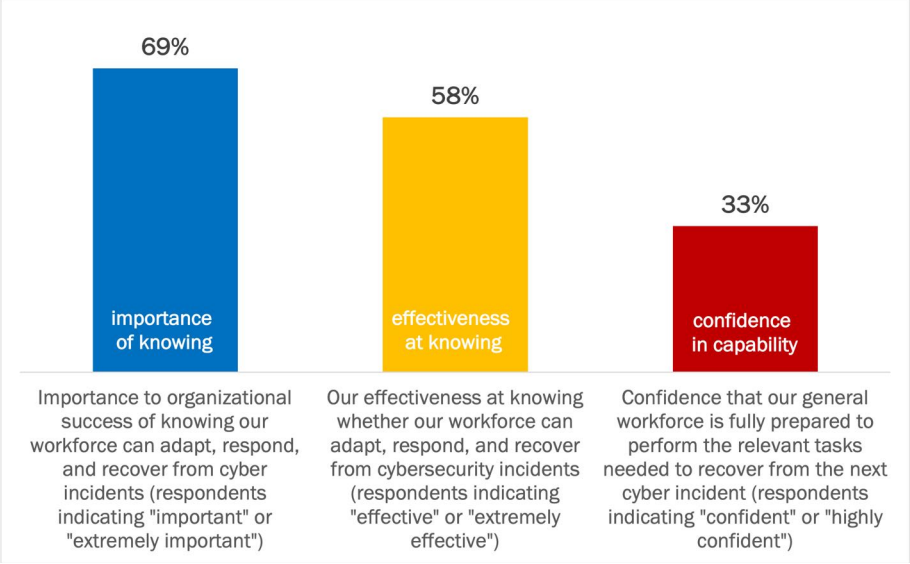
CONFIDENCE IN THE ABILITY TO RECOVER IS DRASTICALLY LOWER THAN ITS IMPORTANCE

There is a significant gap between three interrelated measures of cyber resilience. This gap strongly indicates that organizations know they have more work to do to strengthen cyber resilience (see Figure 9):

- **Importance of "knowing" is the highest number**
  69% of respondents see a strong linkage between knowing that their workforce has cyber resilience and the success of their organization. In other words, the organization knows that if their workforce cannot adapt, respond, and recover from cyber incidents, the success of the organization will be compromised.
- **Effectiveness at "knowing" trails the importance of doing so**
  A lower number of respondents say their organization is effective at assessing cyber resilience. Only 58% indicate they have the ability to know if their workforce can adapt, respond, and recover from a cybersecurity incident. The remainder lack an assessment methodology, rely on weak or useless metrics, or have low trust in the current assessment methodology.
- **Confidence—or the current "knowing" level—is the lowest of the three**
  Only 33% of respondents are confident their workforce is fully prepared to perform the relevant tasks needed to recover from a cyber incident. This means only one third currently have a cyber resilience assessment methodology that provides an accurate picture of resilience in the event of a cyber incident.

Only 33% of organizations are confident their general workforce is fully prepared to perform the relevant tasks to recover from a cyber incident.

Figure 9
Achieving Cyber Resilience: Importance, Effectiveness, Confidence
Percentage of respondents



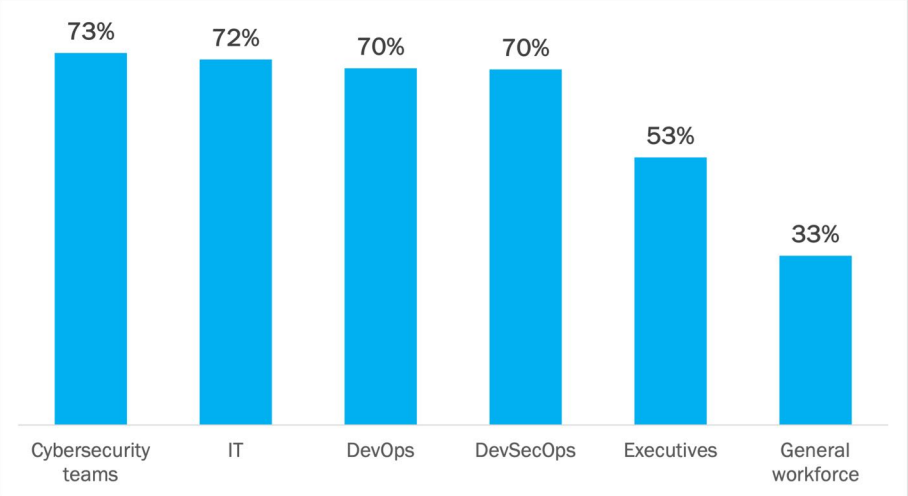
Source: Osterman Research (2023)

The actions of employees—the general workforce—is frequently cited as a contributing factor in cyber incidents. Hence, a lack of confidence that employees are fully prepared to perform the relevant tasks needed to recover from the next cyber incident is worrisome. The likelihood that the general workforce will miraculously stumble on the right path to take is much lower than the likelihood that they will exacerbate the extent and duration of the cyber incident by acting contrary to recovery.

PREPAREDNESS IN TECHNICAL TEAMS IS "FAIR," BUT "TERRIBLE" FOR EVERYONE ELSE

The high-water mark for confidence in the ability of a team or group to be fully prepared to perform the relevant tasks needed to recover from the next cyber incident is 73% for cybersecurity teams, followed by very similar confidence levels for IT (72%), DevOps (70%), and DevSecOps (70%). In other words, three out of ten organizations lack confidence that the teams responsible for executing the technical tasks to recover after a cyber incident know what to do. See Figure 10.

Figure 10
Confidence in the Cyber Resilience of Teams and Groups
Percentage of respondents indicating "confident" or "highly confident"



Source: Osterman Research (2023)

The level of confidence for the two groups beyond the technical teams is worse and potentially more damaging and costly to the recovery process for an organization:

- **Half of organizations lack confidence that executives will respond well**
  A cyber incident demands a strong, informed, and measured response from executives. High-priority tasks include coordinating the public response, giving direction to the general workforce, liaising with regulators and data protection authorities, and engaging with the financial markets. Strategic errors and avoidable missteps during these critical processes can inflict long-run costs.
- **Two in three organizations lack confidence that the general workforce will know how to respond to a cyber incident**
  In combination, the technical teams and executives at an organization can compose 5% of the workforce. For two out of three organizations, there is a lack of confidence that the other 95% of the workforce will know how to recover from a cyber incident. High-priority tasks for this much larger group include maintaining business operations without the availability of core IT systems, handling urgent tasks using manual processes, and not exacerbating the recovery process by connecting compromised devices to the network.

Recovery processes rely to a high degree on technical teams executing a series of recovery tasks after an incident. But as incidents become more severe and extended, executives and employees must also know what to do.

Three out of ten organizations lack confidence that the teams responsible for executing the technical tasks to recover after a cyber incident know what to do.

Pursuing the Cyber Resilience Outcome

Organizations need a better way of strengthening the cyber resilience agenda. In this section, we look at the pathway forward.

CYBER RESILIENCE IS A FUNCTION OF TRAINING, TOOLING, PEOPLE, BUSINESS RISK MANAGEMENT, AND CULTURE

We asked respondents to share their viewpoint on what action would make the largest positive difference to the cyber resilience of their workforce. Of the 570 total respondents, 330 provided an open-ended answer. After coding, grouping, and correlating the answers, five main themes stood out:

- **Training (21% of responses)**
  Training was the most frequently cited viewpoint, with recurring sub-themes of the training mandate including greater frequency and regularity, more engaging and innovative forms of training, a comprehensive approach, and content that is up to date. Respondents say that training needs to cover both cybersecurity professionals and the workforce in general.
- **Better cybersecurity tools (14% of responses)**
  Access to better cybersecurity tooling was the second most common viewpoint, with recurring sub-themes of a comprehensive approach (e.g., "Intelligent strategies, solutions, and services to protect critical data and quickly recover from a cyberattack to resume normal business operations"), continuous monitoring (enterprise-wide/of all systems), and zero trust (to proactively reduce the threat and vulnerability space).
- **Cybersecurity professionals (10% of responses)**
  Hiring more and better-qualified cybersecurity professionals who have the expertise to handle the demands of the role were the main subthemes around cybersecurity professionals. Respondents wanted to hire experts who started with a better baseline of training and competence, along with structured encouragement/incentives for cybersecurity professionals to extend their proficiency and expertise.
- **Business risk management program (7% of responses)**
  How an organization should approach cyber resilience is pictured through a business risk management lens, with comprehensive visibility to identify gaps, categorize risks, proactively reduce the threat surface, and prioritize interventions and mitigations based on business and financial implications. Approaching cyber resilience through a business risk management program elevates the emphasis away from discrete threats and isolated technologies to a strategic, business-driven framework that aligns with the interests of senior executives and the Board.
- **Security culture (4% of responses)**
  Open communication on security, all employees accepting responsibility for cybersecurity, and fostering a security-first mindset were posited as the missing links in 4% of responses to this question. The answers we coded as security culture carried a wistful and hopeful sense, albeit without much direction on how to get there.

As isolated inputs, the above themes will make some contribution. Finding an approach that works at the intersection of these five is even better.

More effective training, better cybersecurity tools, and hiring cybersecurity professionals with the expertise to handle the demands of the role are the three most cited actions for improving cyber resilience.

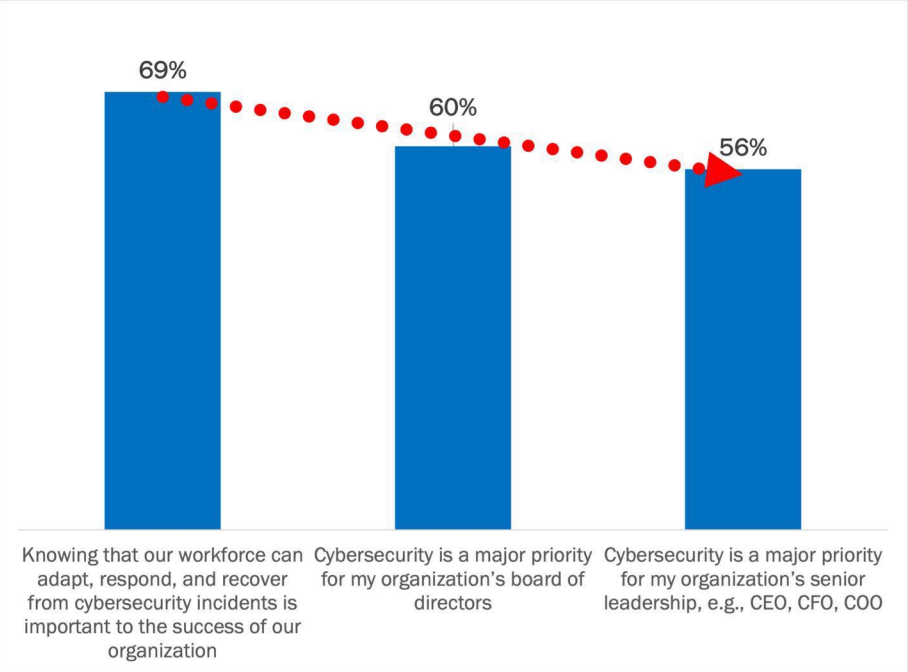
TO INCREASE SUPPORT, FOCUS ON THE IMPORTANCE OF CYBER RESILIENCE

The level of support by the board of directors (60%) and senior leadership (56%) is lower than the importance of cyber resilience to the success of the organization (69%)—see Figure 11. This makes sense given the governance and leadership roles of these two groups. Neither group will make something a priority that does not connect with the success and viability of the organization. Therefore, make this dynamic work in your favor by raising awareness of the importance of cyber resilience, which will drag up the support of the two groups. Raising the heat includes:

- **Communicating with the board and senior leadership on cyber resilience**
  Embrace cyber resilience messaging in communicating with the board and senior leadership, rather than focusing on the status of piecemeal inputs such as deploying new cybersecurity solutions. Everything should be placed in the context of cyber resilience, including the organization's major gaps in achieving the cyber resilience outcome.
- **Ensuring the board and senior leaders know about attacks on other high-profile organizations**
  Brief the board and senior leaders on the cyberattacks faced by high-profile and well-known organizations, including consequences faced. Make a particular effort to uncover the weaknesses and shortcomings in how other organizations have responded to cyber incidents, especially if those shortcomings are also reflective of your organization.

Raise awareness of the importance of cyber resilience to increase support by the board and senior leaders.

Figure 11
Raising the Importance of Cyber Resilience
Percentage of respondents



Source: Osterman Research (2023)

Conclusion

Cybersecurity focused on building skills, knowledge, and judgement across the workforce, while being able to prove it, helps build lasting cyber resilience. Unfortunately, many organizations lack some of these key elements in their preparedness for cyberthreats. To prepare for future threats, organizations urgently need to implement ways to better evaluate current resilience levels and fill cyber skills gaps. In driving the cyber resilience agenda, a comprehensive approach that assesses competence, builds team-level skills, and highlights gaps is essential. Legacy approaches that don't move at the speed of cyber and that rely on historical threat data can never provide what organizations need to address new and emerging threats.

About Immersive Labs

Immersive Labs empowers organizations to equip, exercise, and evidence human cyber capabilities. We provide metrics that give security leaders insight into human cyber skills and readiness levels across their organization. We improve these through dynamic labs and crisis scenarios that track the threat landscape. Goldman Sachs and Summit Partners back Immersive Labs, and our customers include some of the largest companies in financial services, healthcare, and government, amongst others.

For more information on Immersive Labs' offering, please visit www.immersivelabs.com

IMMERSIVELABS

www.immersivelabs.com

@immersivelabs

+44 20 3893 9101 (UK)

+1 508 500 6111 (US)

Methodology

This white paper was commissioned by Immersive Labs and conducted by Osterman Research. 570 respondents in senior security and risk roles were surveyed in November 2022. To qualify, respondents had to work at organizations with at least 1,000 employees. The surveys were conducted in the United States, United Kingdom, and Germany, with the survey in Germany fielded in German. The survey was cross-industry, with a particular focus on financial services, technology, and consulting.

JOB ROLE

CISO	38.8%
VP of Security	25.4%
Senior Director or Director of Security	15.8%
Chief Risk Officer	16.1%
VP of Risk	3.9%

GEOGRAPHY

United Kingdom	36.3%
United States	34.7%
Germany	28.9%

INDUSTRY

Financial services	29.5%
Technology	29.5%
Consulting	27.9%
Manufacturing	3.0%
Energy or utilities	2.8%
Education	2.6%
Pharmaceuticals	1.8%
Infrastructure	1.6%
Government	1.4%

[1] Osterman Research, Ransomware Attacks: Strategies for Prevention and Recovery, October 2022, at https://ostermanresearch.com/2022/10/14/orwp_0355/

[2] Osterman Research, Imperfect People, Vulnerable Applications: The Human Elements Contributing to Cyber Risk, May 2021, at https://www.immersivelabs.com/resources/ebooks/research-imperfect-people-vulnerable-applications/

[3] NIST, NIST Cybersecurity Framework, January 2023, at https://www.nist.gov/cyberframework