IMMERSIVELABS

FORRESTER
WAVE LEADER 2023
Cybersecurity Skills And Training Platforms

CYBER WORKFORCE BENCHMARK

2023

MEASURING THE STATE
OF GLOBAL CYBER RESILIENCE

Table of Contents

Foreword

Boards that don’t make cybersecurity a strategic priority fail their organizations

BY JACK HUFFARD
CO-FOUNDER OF TENABLE (NASDAQ: TENB), BOARD MEMBER

At the Board level today, there's much talk about building cyber resilience driven by an evolving threat landscape. Generative AI has created new threat vectors, supply chains face mounting cyber attacks, and ransomware incidents continue to make headlines.

Despite widespread awareness of the potentially catastrophic risks, directors often under prioritize cybersecurity as a strategic imperative, especially when it comes to preparing the workforce for threats. The lack of focus on the workforce’s cyber skills is surprising given most attacks target the human element.

What is particularly troubling is that 65% of directors anticipate a major cyberattack within 12 months, yet nearly half consider their organizations unprepared.* Moreover, many Boards and executive teams lack the metrics to identify workforce cyber capabilities, making it impossible to address skill gaps promptly.

Continued →

Foreword Continued...

Three notable Board-level pitfalls contribute to this problem:

Failure to adopt a people-centric cybersecurity strategy:

Many Boards view the investment in technology alone as the answer, but this approach can prove costly. Boards should encourage a formal people-centric cybersecurity strategy, empowering employees to become allies in the fight against cyber attacks.

Assumption that cybersecurity is solely the CISO's responsibility:

Placing the burden solely on the CISO or cyber lead is dangerous. Cybersecurity should be everyone's responsibility, requiring directors to partner with C-level executives to foster an organization-wide cybersecurity culture.

Lack of proof:

Insufficient proof of workforce cyber capabilities undermines cyber resilience. In fact, over 55% of cyber leaders lack data to demonstrate readiness for cyber threats and recovery for resilience. Directors should encourage organizations to engage in continuous practical exercises that provide proof of cyber capabilities across the workforce.**

To prepare for future uncertainties, organizations must make cybersecurity a strategic asset, with people at the core. This requires empowering teams and individuals to mitigate risk and respond swiftly to threats, while investing in continuous exercises that demonstrate organization-wide preparedness.

Boards that fail to recognize the importance of a long-term, measurable cybersecurity strategy and culture place their organizations at much greater risk.

*Source: "Cybersecurity: The 2022 Board Perspective Report," Proofpoint
**Source: Forrester Opportunity SnapShot: "Cyber Leaders Need a More Effective Approach to Building and Proving Resilience" – A custom study commissioned by Immersive Labs, March 2023

OVER VIEW

We partner with organizations around the world to build and prove their cyber resilience across the workforce, from front-line technical staff to Board members. We define cyber resilience as the ability and confidence to effectively prepare for, and respond to, cyber threats.

Every year, our customers - including the world's largest enterprises - use our platform to complete over a million realistic labs, threat simulations, and executive crisis response exercises to better prepare for threats.

While the primary purpose of these activities is for customers to develop and demonstrate cyber capabilities, the aggregated and anonymized results provide a unique snapshot of the overall state of cyber resilience globally.

This Cyber Workforce Benchmark report offers a unique look at organizations' resilience to threats (or lack thereof), revealed by analyzing this data over a one-year period. Our latest study builds on our research from our inaugural report in 2022.

The goal of the following report is to empower cyber leaders with insights to address strategy gaps, mitigate risk, and build lasting resilience to threats across the workforce.

KEY INSIGHTS

Cyber resilience is rising globally amid more sophisticated threats. We observed notable gains across numerous resilience metrics, such as verifying the skills of new talent and assessing security team capabilities in realistic scenarios. Organizations making continuous cybersecurity exercising a strategic focus saw consistent, measurable improvements in cyber risk mitigation, yet many still lag in areas such as expanding cyber framework coverage.

Organizations continue to accelerate response times to threats.

Organizations' median response time to emerging threats improved by one third, indicating a significant increase in the speed of response and continued progress compared to the year prior. Enterprises have enhanced their knowledge about newly discovered threats and vulnerabilities, enabling them to respond more rapidly than ever before. The Log4j crisis, for example, was a watershed moment that could well have been a catalyst for this urgency given its catastrophic impact on organizations around the world.

Seasoned cyber pros are more complacent in their skills than junior staff.

To effectively prepare for cyber threats, individuals at all stages of their career need to be prepared for the latest threats, yet our data suggest that junior staff tend to challenge themselves with more difficult exercises and are more likely to stay current with new threats compared to more-experienced cyber professionals.

Regulated industries only marginally outperform less-regulated peers.

With only a 6% difference across key resilience metrics, regulated industries on average are not substantially better prepared for attacks than less-regulated industries. Nevertheless, a few financial services firms were among the top individual performers. Our data suggest that - regardless of industry regulations - resilience depends on building a cybersecurity culture from within and providing consistent exercising of teams and individuals across the organization.

Organizations aren't preparing their workforces enough for after-incident responses.

To effectively reduce risk, organizations must be prepared both before, and after, an incident. While organizations are ensuring that cyber resilience activities span the MITRE ATT&CK® framework, we observed a notable bias towards the earliest stages of the attack lifecycle, suggesting cyber leaders have room for improvement and are potentially leaving their organizations exposed to after-incident risk.

Our methodology

Our research is based on Cyber Workforce Resilience activities and outcomes from:

1.1 million exercises and hands-on labs

Broad coverage from technical staff to executives

We analyzed the underlying data produced by these activities during the 12-month period from April 2022 to April 2023, as well as derivative metadata, to produce aggregated results, including such factors as:

Engagement rates

Decision-making effectiveness

Speed of learning

How we measure cyber resilience

Measuring cyber resilience is at the core of everything we do. For this report, we developed an overall industry benchmark based on the Immersive Labs Resilience Score, which measures an organization's preparedness for cyber attacks and breaches based on years of benchmarking data across industry verticals.

For the purposes of this report, we analyzed aggregated, anonymized resilience scores across our global customer base to assess overall trends in cyber resilience globally. Users on our platform tend to be more proactive about preparing their teams for threats than non-users, so resilience scores may be lower for a broader audience.

Each organization's individual score enables them to understand:

- **Their overall cyber resilience**
- **Trends and progress**
- **Comparisons to industry and best-in-class benchmarks**

Organizations achieved resilience gains despite a more complex threat landscape

Today, 72% of cyber leaders agree that the threat landscape is becoming more challenging over time. To keep pace with more sophisticated threats, organizations are investing in building cyber capabilities across the workforce.

The organizations that most successfully increased their cyber resilience have focused on the following three key areas in the last 12 months.

TAKEAWAY

Overall, the results indicate that organizations that make cyber resilience a strategic focus can achieve measurable improvements and reduce their overall risk exposure in meaningful ways on a yearly basis.

46%

Verify the Skills of New Talent

30%

Assess Security Team Capability in Realistic Scenarios

29%

Strengthen Executive Decision Making in Cyber Crises

Trailblazers are making strides on their resilience journey, while others lag behind

While we observed many notable advances in cyber resilience, our analysis focused on organizations that have already implemented a formal cyber resilience program. We also investigated how many organizations haven't yet taken this step.

A recent survey of cybersecurity leaders conducted by Forrester Consulting on behalf of Immersive Labs suggests that while organizations like the ones we studied are blazing an important new trail, many others are still early in their journey to cyber resilience.

32%

of respondents believe their organization has a formal strategy to ensure cyber resilience.

82%

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

60%

of respondents indicated that they plan to increase their investment in live simulations and online training moving forward.

Could AI put an end to cybersecurity?

BY MAX VETTER
VICE PRESIDENT OF CYBER, IMMERSIVE LABS

The leap forward in generative AI has left many companies rushing to make sense of its potential risks and benefits, including how AI will impact cybersecurity itself.

So far, commentary about AI tends to fall into two main camps, with one side contending that AI will offer intelligent tools so sophisticated that they will stop every cyber attack before they happen and enforce coding best practices to make software vulnerabilities a thing of the past. Others take the opposite perspective: that AI will bring about cyber attacks so powerful that organizations will be helpless to stop them. Either of these scenarios would have a profound impact on the business of cybersecurity.

While predicting the future is always precarious, one key observation is that defenders are generally playing catch up and are often slower, more restricted by laws and standards, and less well-funded.

Current AI defensive tools are good at spotting anomalies in traffic and stopping many attacks, but there's evidence organizations are actually getting worse at keeping cyber criminals out of our networks. Trials of AI coding assistants have shown that, while they make coding more efficient, they have at times introduced vulnerabilities, not reduced them.

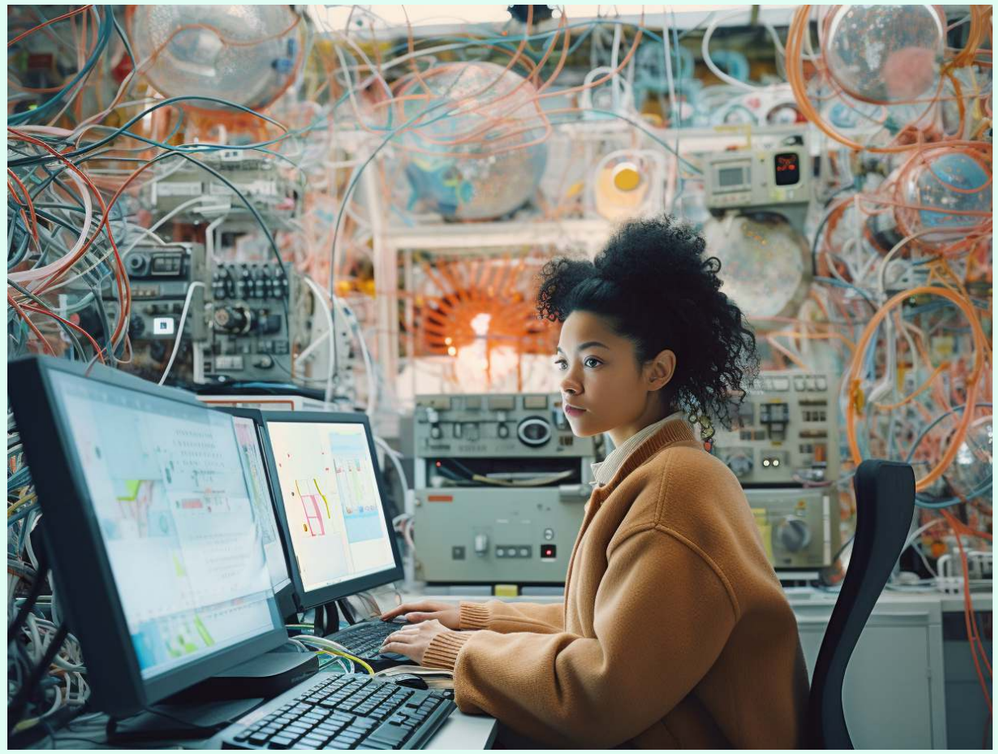
The reality is that criminals are already using AI to their advantage. If defenders are to make up the ground they've lost and have a chance of thwarting their efforts, they'll need to upskill their people as rapidly as possible to keep pace with attackers, as well as new advancements in AI technology.

Immersive Labs features a library of AI-related exercises and simulations for our enterprise customers. One of these unique exercises challenged users to convince a chatbot to reveal a password. More than 20,000 participated and many succeeded in beating the bot. This challenge underscores the point that AI can be hacked, exposing sensitive data.

To the point about whether AI will usher in a utopia or dystopia, I believe each side is half right. AI will most likely provide a mixed bag, simultaneously providing cyber criminals sophisticated new ways to attack organizations (like scripting realistic phishing emails), as well as offering defenders powerful tools to keep them out, such as new ways to identify anomalies. This game of cat and mouse is not new, but the scale and complexity of this interplay will only grow as each side gains advantages and countermeasures in rapid succession.

More than ever before, the difference between a secure, resilient organization of the future and one exposed to threats will be how quickly teams and individuals can learn new capabilities to keep up with both the benefits and risks of AI. Put another way: the more the robots rise, the more important it will be to empower people to keep the world safe.

Junior staff challenge themselves more than seasoned cyber professionals



We’ve observed that less-experienced cyber professionals are challenging themselves with more difficult labs than their more-experienced teammates, completing content that is on average 5% more difficult.

The results suggest a potential complacency problem, or a lack of organizational focus, on encouraging industry veterans to develop their skills against new threats.

Here are two notable examples:

Cybersecurity

Junior cybersecurity personnel are completing content that is harder than team members with eight or more years of experience.

Application Security

Team members with less than two years of experience narrowed the gap with their more experienced counterparts with the level of difficulty of content completed.

These findings are also supported by our recent commissioned study of cyber leaders conducted by Forrester Consulting, which found that despite high confidence in overall resilience, teams are insufficiently prepared for threats.

TAKEAWAY

Cyber teams have the most success maintaining strong security when all members stay current with industry trends and threats. Leaders should encourage junior and senior staffers alike to engage in continuous learning.

82%

agree they could have mitigated some to all of the damage of their most significant cyber incident in the last year if they were better prepared.

80%

don’t think, or are unsure, their teams have the capabilities to respond to future attacks.

Significant improvement in crisis response time

One of the most important ways that organizations can build lasting cyber resilience is to ensure cybersecurity teams have the knowledge and judgment to respond rapidly to new threats. Common examples include new forms of malware or newly published Common Vulnerability and Exposures (CVEs) that may be present in an organization’s IT environment.

Median response time

Organizations' median time to respond to new threats with the completion of relevant exercises and labs tells us a great deal about the overall state of cyber resilience. After all, a faster response means a smaller window of vulnerability and a lower risk of negative business impact, financial or otherwise.

This significant drop was likely influenced by multiple factors. However, lessons from the Log4j crisis and other high-profile vulnerabilities appear to have made a significant impact on ongoing urgency levels and response times.

TAKEAWAY

The Log4j crisis was a watershed moment that could well have been a catalyst for this urgency given its catastrophic impact on organizations around the world. Leaders benchmark team performance and work to reduce response times to new threats.

Log4j Remains Top of Mind 2+ Years Later

While the initial discovery of Log4j dates back to December of 2021, it continues to be a chart-topper among users of the Immersive Labs platform. Two of the top five most frequently attempted CVE labs over the last 12 months were Log4j-related.

1 CVE-2021-44228 (Log4j) – Defensive

2 CVE-2021-22205 (GitLab) – Defensive

3 CVE-2021-41773 (Apache) – Defensive

4 CVE-2022-22965 (Spring4Shell) – Offensive

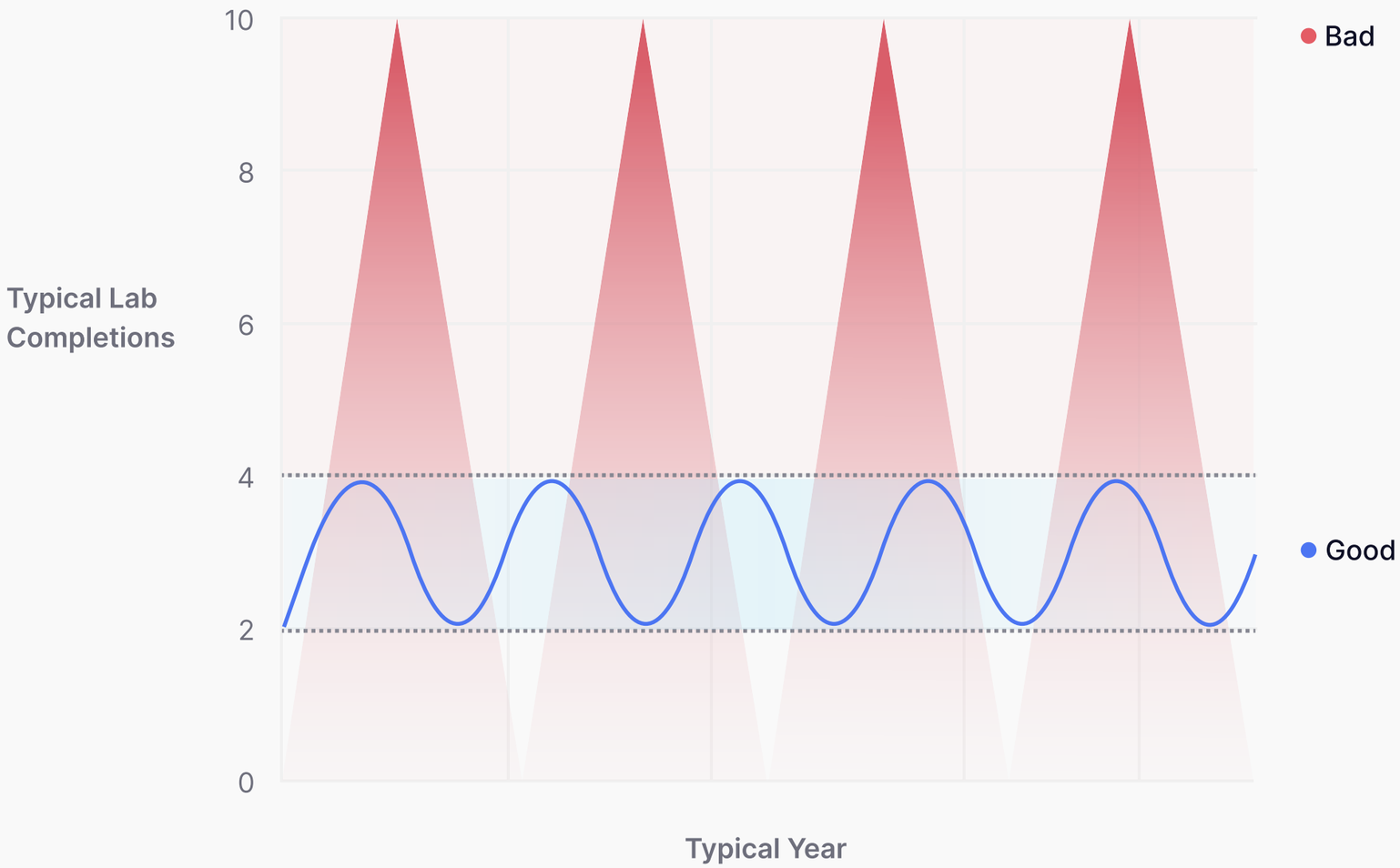
5 CVE-2021-44228 (Log4j) – Offensive

Internal cybersecurity culture - not industry regulations - is a better predictor of resilience

We looked at performance by industry to determine resilience trends. One would expect that more highly regulated industries would have higher resilience scores, but we found that with only a 6% difference in resilience scores, there is very little difference between regulated and less-regulated industries.

We also looked at the Top 10 best-performing organizations. What is notable is that they use the platform far more consistently than those outside this cohort.

A typical user in the Top 10 completes between 2-4 labs per week. By contrast, a typical user outside of this cohort completes labs far more erratically between 0-10 labs per week.



Consistent, habitual usage of the platform is a strong factor in why the top-performing organizations score higher overall in our measurement of cyber resilience.

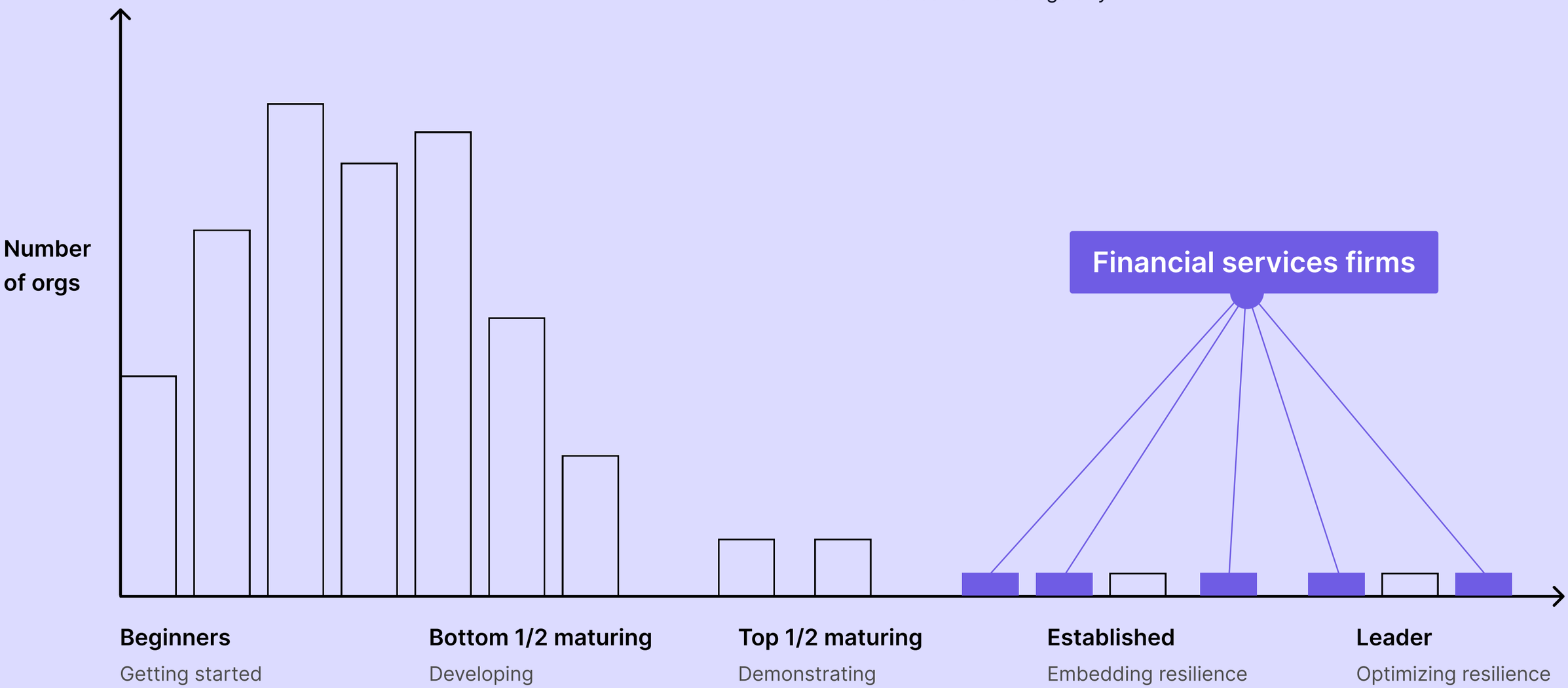
TAKEAWAY

The takeaway for Boards and other senior leaders is to make cybersecurity a deliberate, strategic focus, whether the organization does business in a regulated industry or not, and ensure teams consistently and regularly complete labs.

Financial services firms were among the top individual performers

Despite there being little difference in resilience scores across more and less-regulated industries, some verticals stood out among the top individual performers. A disproportionate share of the top individual scores during the period we studied came from the financial services industry. In fact, seven of the top 10 performers we observed were financial services firms.

These firms also made some of the most significant individual gains from the previous 12-month period, suggesting an increased level of focus and momentum with cyber resilience among the financial services leaders that often set the standard for cybersecurity best practices and also exercise their teams more regularly.



Organizations less prepared for events “after the boom”

Using MITRE ATT&CK® – a well-regarded industry framework that organizes and categorizes different types of threat actor tactics and techniques into distinct categories, providing a common language for cybersecurity professionals – we looked at organizations’ preparedness for events before and after an attack, or “boom.”

Analysis of the MITRE ATT&CK® data shows that companies are well prepared on the stages "before the boom." Typically as you move from left to right on the MITRE ATT&CK® framework the skills needed by the attacker increases. From this we can also infer that the skills of the defenders also need to be that much higher when dealing with "after the boom" techniques on the MITRE ATT&CK® framework. There could also be an over reliance on technology to do detection, leaving workforces less well prepared.

TAKEAWAY

Leaders should not overlook the critical capabilities needed during the middle and later stages of the MITRE ATT&CK® kill chain, such as the ability to detect attackers' efforts to establish persistence in the environment.

MITRE ATT&CK® Coverage

The Psychologist's View

Focus on people, not just patches, for greater resilience

By Dr. John Blythe, Director of Cyber Workforce Psychology, Immersive Labs

Since people are at the center of any effective cybersecurity strategy, it is important to take a closer look at the role human psychology and cyber culture play in building long-term cyber resilience. Organizations struggle when they focus too much on systems and processes at the expense of the pivotal role people – and their actions – play in responding effectively to threats.

The Psychologist's View

Unlike systems, people encounter challenges in recovering from setbacks and are susceptible to cognitive biases that impede their ability to detect security threats promptly and respond effectively during crises.

Cybersecurity brings further unique challenges because you are never truly "done." No matter how much progress you make, the deluge of threats keeps building. Meanwhile, even if you do thousands of things right, one mistake can be catastrophic.

This challenge is arduous, with considerable costs for businesses. Moreover, the impact on people is even more profound, as mental health concerns continue to escalate within the cybersecurity sector.

Yet, addressing people-centric cybersecurity cannot be approached in the same manner as tackling system or process flaws, nor can organizations expect that preparedness will arise without building a deliberate cybersecurity culture.

People cannot be patched like a system; instead, leaders must prepare them through engaging and measurable cyber exercises to cultivate resilience, rather than relying solely on technology.

Putting more focus on people necessitates adopting a psychological lens to develop cyber resilience. Research indicates that four main pillars underpin this approach.

The Psychologist’s View

Putting more focus on people necessitates adopting a psychological lens to develop cyber resilience. Research indicates that four main pillars underpin this approach.

Adaptation

It involves responding to adversity by adjusting thoughts and behaviors in alignment with the cyber threat. Positive adaptation is pivotal for resilience, while negative adaptation, such as denial, dithering, and delaying and inflexible thinking, indicates unproductive coping mechanisms. Cyber-resilient individuals adapt positively, learn from mistakes, and acknowledge their vulnerabilities to cyber attacks.

Confidence

Confidence encompasses an individual's perceived competence in dealing with cyber threats, encompassing both technical aptitude and emotional responses. Low self-confidence and organizational confidence are unlikely to lead to cyber resilient actions.

Social support

It refers to our connections with others, such as colleagues and professional networks, and their availability to assist us during times of crisis. They can serve as sources of information and emotional support. Many refer to this as social capital, but the significance of community —both internal and external to an organization—cannot be overstated.

Growth

Cyber threats serve as stressors, but also present opportunities for learning, self-development, and better preparation for the future. As attackers hold the advantage of making the first move, it is imperative that we continually strive to improve ourselves, set goals both before and after incidents, and embrace a mindset of continuous improvement.

By focusing on building a cybersecurity culture with more focus on preparing people, we can foster greater cyber resilience that encompasses adaptation, confidence, social support, and growth, ultimately strengthening overall cyber resilience.

Conclusion

Our analysis reveals several important cyber resilience trends that can inform how organizations mitigate risk amid more sophisticated threats. The findings of our report demonstrate that – while organizations are making some notable cybersecurity gains – there are still important gaps to fill. Ultimately, leaders must be proactive about driving cybersecurity strategy and building it into organization-wide culture to drive competitive advantages.

To increase your cyber resilience today, here is a checklist of 5 items supported by this year's report:

1/

Make cybersecurity a strategic Board and C-level priority. Making cyber a strategic priority means recognizing its importance and integrating it into the highest levels of the decision-making processes across an organization, including at the Board and C-level.

2/

Build a rock-solid cybersecurity culture across the workforce. Foster an environment where all employees understand and prioritize cybersecurity, promoting best practices, and encouraging a shared responsibility for protecting people and assets.

3/

Beware cybersecurity overconfidence or complacency. Seniority doesn't necessarily mean readiness for threats. To stay current with emerging threats, staff of all experience levels need to continue their skills development so they have the knowledge and judgment to effectively respond to threats.

4/

Don't be sporadic. Continuously exercise and prove capabilities. One-off cyber skilling fire drill won't do. Leaders need to regularly and consistently conduct cybersecurity exercises to assess skills gaps and fill them before it's too late.

5/

Ensure preparedness for both before, and after, an incident. Ensuring coverage across all of MITRE ATT&CK® framework means establishing workforce preparedness for before and after the boom to avoid weaknesses in any particular area.

Start your cyber resilience journey today

Immersive Labs is the leader in people-centric cyber resilience. We help organizations continuously assess, build, and prove their cyber workforce resilience for teams across the entire organization, from front-line cybersecurity and development teams to Board-level executives.

Immersive Labs is trusted by the world's largest organizations and governments, including **Citi, Pfizer, Humana, HSBC, the UK Ministry of Defence, and the NHS England.** We are backed by Goldman Sachs Asset Management, Summit Partners, Insight Partners, Citi Ventures, Ten Eleven Ventures, and Menlo Ventures.

To learn more, visit us at https://www.immersivelabs.com