Dr. John Blythe
Nick Cavalencia

Edition 002 - 2025

2025

immersive

Cyber Workforce Benchmark Report

Benchmark

Contents:

Unproven Confidence Will Not Survive a Real Crisis

By Oliver Newbury

Cybersecurity has never been more visible or more proactively managed than it is today. Boards receive regular risk updates, executives champion security initiatives, and organizations worldwide are investing at record levels. For many, it feels like maturity has finally arrived.

And yet, from experience, I know that confidence doesn't necessarily equal capability. This is the gap that defines our industry. While most organizations believe they're ready for a major incident, the underlying performance data often tells a different, more complicated, and sometimes more troubling story. We see indicators of readiness stagnating, even as our belief in our preparedness grows.

It's not that teams aren't working hard - they are. The problem is a systemic one: we're measuring readiness by activity rather than by outcome. We have become experts at counting training completions, audit results, and compliance checkboxes, but we're failing to measure demonstrated performance under pressure. We have mistaken preparation for proof.

This year's Cyber Workforce Benchmark Report provides the evidence we need to elevate the conversation with our boards and executive teams. It allows us to move beyond "Are we compliant?" and start asking the more critical question: "Are we capable?"

The 2025 Benchmark challenges all of us, leaders, practitioners, and boards alike, to confront the gap between how ready we feel and how ready we are. It provides the data to spark a crucial shift from confidence built on assumptions to confidence grounded in evidence.

Trusting confidence over capability results in a perilous illusion of readiness, one that will shatter the moment a real crisis hits, exposing the true and devastating cost of unproven confidence.

Oliver Newbury
Chief Strategy Officer, Halcyon
Immersive Board of Directors

Are We Compliant?

Are We Capable?

Why Believing You're Ready Isn't the Same as Being Ready

A Year Defined by Overconfidence

Cybersecurity has become an ever-present topic in the boardroom. Budgets have risen, roles have expanded, and leadership confidence has never been higher. Yet, as this year's Cyber Workforce Benchmark shows, many organizations remain dangerously unprepared when theory becomes reality.

Immersive's 2025 analysis reveals a widening gap between confidence and capabilities. While nearly every organization believes it can manage a major incident, measurable readiness metrics - accuracy, response time, and resilience scores - remain stagnant. The numbers point to a simple yet unsettling truth: perception has outpaced performance.

Moving Beyond Assumptions

Despite record training volumes and growing executive involvement, progress has stalled. This year's research explores why improvement has plateaued and where organizations are investing in effort without seeing the desired outcome.

The data reveals four root causes:

Each of these factors contributes to the illusion of readiness, activity mistaken for capability, measurement mistaken for proof.

01

Practicing the Past

Most exercises still focus on legacy vulnerabilities and outdated threats.

02

Fixating on Fundamentals

There's not enough learning around intermediate and advanced topics.

03

Excluding the Business

There's not enough focus on roles outside of IT/Security and cross-functional coordination.

04

Misaligning the Frameworks

MITRE ranks third, despite its direct application to threat actions and mitigations.

Evidence from Real-World Performance

This benchmark integrates findings from usage of Immersive One, Immersive's cyber readiness platform, comparing use from July 2023 - June 2024 with July 2024 - June 2025:

Including aggregated platform analytics and industry breakouts; survey data of cybersecurity leaders from 500 organizations from with the United States and the U.K.; and data from a controlled "Orchid Corp" crisis simulation exercise that tested 187 professionals across 11 global drills.

LOW

22%

Average Decision Making Accuracy

MEDIUM

60%

Average Confidence Score Rating

HIGH

29 hrs

Average Incident Containment Time

The results are sobering: average decision accuracy was just 22%, average confidence 60%, and average containment time 29 hours.

A New Measure of Readiness

Immersive defines readiness as the ability to prove, improve, and report cyber capability through evidence, not assumption. This year's benchmark applies that lens to uncover where progress has truly been made and where confidence continues to mask risk.

Each section that follows examines a dimension of this challenge: from leadership perception to skill currency, behavioural psychology, framework alignment, and live performance data.

Cyber Workforce Benchmark 2025

Confidence soars. Capability stalls. The 2025 data exposes the human reality behind cyber readiness.

THE CONFIDENCE SURGE

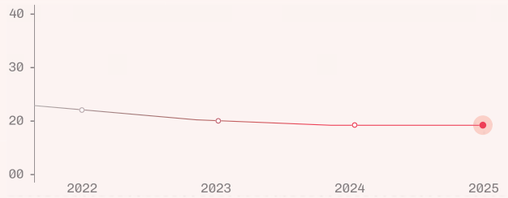
91% of leaders say their organization could handle a major incident, yet platform data shows resilience performance unchanged for a second consecutive year.

091 / 100

Takeaway: Confidence is trending up, but measurable capability is not.

FLATLINED PERFORMANCE

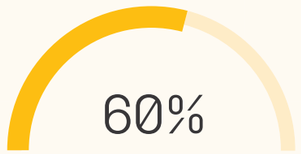
Resilience Scores have remained statistically flat since 2023, and the median response time to complete critical labs of 17 days hasn't improved despite increased spending and executive oversight.



Takeaway: Effort and investment alone aren't translating into faster or stronger responses.

PRACTICING THE PAST

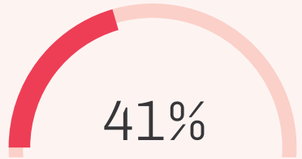
60% of all training activity focuses on vulnerabilities more than two years old, leaving teams over-prepared for yesterday's threats and under-practiced for today's.



Takeaway: Organizations are mastering outdated playbooks while new attack techniques evolve.

EXERCISING IN SILOS

Only 41% of organizations include non-technical roles in cyber simulations, meaning critical business decisions go untested until the real event.



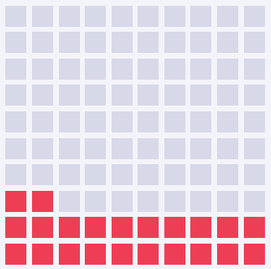
Takeaway: Crises are cross-functional, but the practice rarely is.

REALITY CHECK:

Across 11 global drills and a cyber range benchmarking exercise, participants averaged 22% decision accuracy, 60% confidence, and 29 hours to containment — proving that even mature programs struggle under pressure.

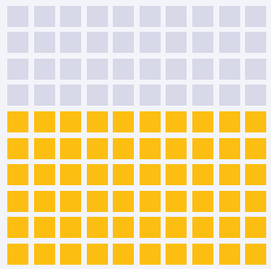
22%

AVERAGE DECISION MAKING ACCURACY



60%

AVERAGE CONFIDENCE SCORE RATING



HIGH

AVERAGE INCIDENT CONTAINMENT TIME

29Hrs

Takeaway: True readiness can't be assumed; it must be demonstrated and measured.

How We Measured the State of Cyber Readiness in 2025

This year's benchmark draws from three independent but complementary data sources to provide a comprehensive view of both perceived and proven cyber readiness.

Together, these datasets illuminate not just how organizations believe they would perform in a cyber crisis, but how they actually perform when tested.

Anonymized Cyber Resilience Data

Our largest dataset comes from 1.8 million exercises and hands-on labs conducted within the Immersive One platform between July 2024 and June 2025, compared with usage data from the previous 12 months. This anonymized dataset includes activity from technical cybersecurity staff, management, non-technical staff, and executives across industries and regions.

We analyzed the underlying data produced by these activities and derivative metadata to identify year-over-year trends in:

- **Engagement rates and participation by role**
- **Decision-making effectiveness and improvement velocity**
- **Areas of readiness focus**
- **Speed of response and skill development**
- **Alignment of readiness to current threat categories**

Simulated Exercises

To evaluate how teams perform under real-world pressure, Immersive conducted two controlled exercises: a crisis simulation exercise that tested 187 professionals across 11 global drills, and a cyber range benchmarking exercise that was run with 29 organizations.

The exercises tested decision-making, coordination, and communication across technical and business functions in a simulated ransomware incident, revealing key behavioral and process gaps that contribute to the confidence–capability divide.

Cyber Readiness Perception Survey

Finally, Immersive commissioned a survey of 500 cybersecurity professionals and leaders between August and September 2025. The survey captures how organizations perceive their readiness - providing the attitudinal context that complements empirical platform data and simulation performance.

It measures factors such as:

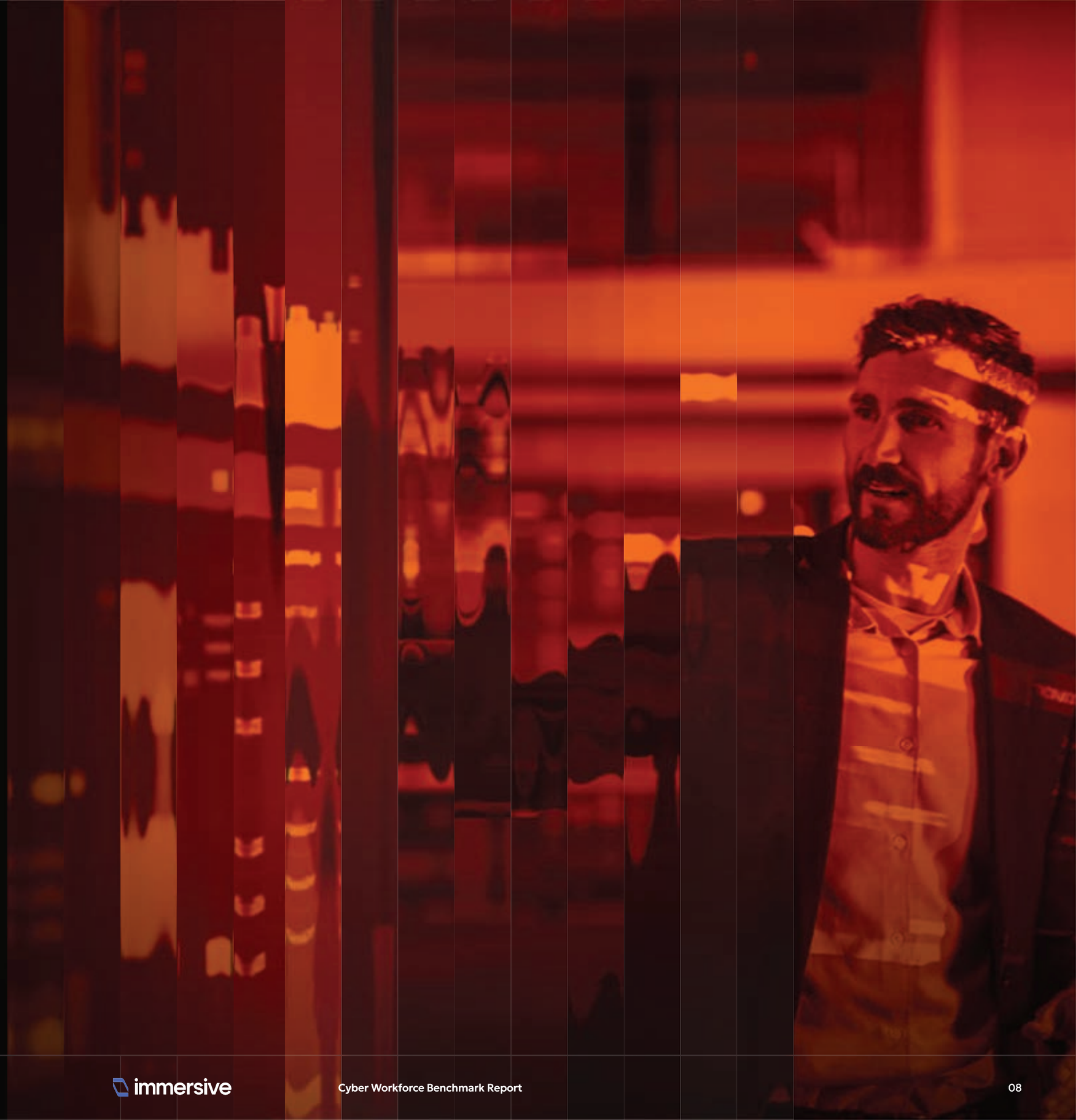
- **Confidence levels in incident response and recovery**
- **Reported maturity of readiness programs**
- **Metrics organizations use to define and measure "readiness"**

How We Measure Cyber Resilience

At the core of this analysis is the Immersive Resilience Score, a benchmark derived from years of real-world data designed to quantify an organization's preparedness across people, process, and technology by aggregating multiple dimensions: skills, practices, decision-making performance, framework coverage, and adaptability to new threats.

For this report, we analyzed aggregated, anonymized Resilience Scores from the global customer base to evaluate trends in readiness maturity and performance by role and industry.

While organizations using Immersive One typically represent proactive security cultures, these findings highlight broader patterns that likely extend across the wider market - meaning true global readiness levels may be even lower than this dataset suggests.



01

CONFIDENCE VS CAPABILITY:

The Gap Widens

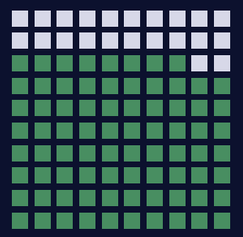
CONFIDENCE IS HIGH:

When Readiness Feels Stronger Than It Is

Across boardrooms and SOCs alike, a striking confidence permeates today's cybersecurity landscape. Nearly every organization believes it's prepared for the next major incident - but the data tells a different story.

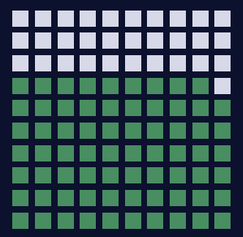
Yet when readiness is measured through performance – not perception – the optimism fades. Immersive's cyber readiness analysis shows average Resilience Scores remain flat year over year, while median response time to complete a readiness lab holds steady at 17 days.

Confidence has grown, capability has not.



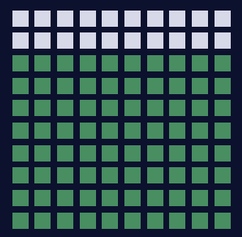
78%

of boards and senior leaders view cybersecurity as a major business priority



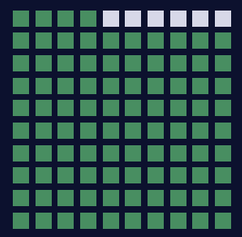
69%

of cybersecurity teams feel greater pressure to prove cyber resilience now than 3 years ago to cyber insurers, leadership, and the board



80%

of cybersecurity teams believe their organization is ready to handle a significant attack



94%

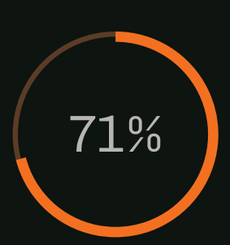
of orgs believe they will detect, prevent, respond to, and recover from a cyber incident effectively.

CONFIDENCE IS HIGH:

The Growing Confidence–Capability Gap

The data reveals a widening chasm between perceived and proven readiness. 71% of respondents describe their cyber readiness programs as “very” or “extremely mature,” yet performance data tells another story.

Metric	Perception	Reality
Readiness Confidence	94% believe they will be effective in a crisis	Orchid Corp crisis simulation response accuracy was only 22%
Response Speed	85% feel their performance in a cyber drill/ assessment/exercise met or exceeded their expectations	Average completion of the Orchid Corp crisis simulation was 81% and took 29 hours
Program Maturity	94% rank their cyber readiness program as some degree of “mature”	Resilience Scores flat YoY



71% of organizations would label their readiness program “extremely mature,” or better

The Hypothesis

Part of this dynamic stems from the intensifying scrutiny from boards, executives, and cyber-insurance carriers to prove resilience.

To satisfy that demand, many turn to tools and metrics that look impressive, like awareness-training completion rates, tabletop attendance, and policy adherence scores, but few measure true crisis performance. Boards see green dashboards while human weaknesses persist.

In the Orchid Corp simulation, teams achieved a dismal 22% accuracy, took 29 hours to contain, with only 31% of orgs actually completing the entire simulation.

02

THE HARSH REALITY:

Flat Performance & False Metrics

immersive

The Data Behind the Confidence Crisis

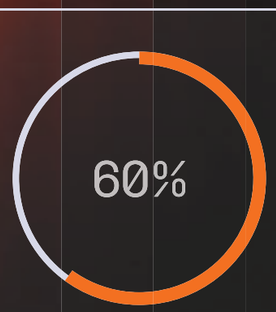
Despite record investment and training activity, objective benchmarks show cyber readiness has stalled.

Data from Immersive's cyber readiness platform shows little to no improvement in the core readiness metrics that actually matter.

Resilience Scores are flat to slightly lower YoY (with an average decline of -3%)	Median Response Time remains unchanged at 17 days	Industry Performance shows over 60% of sectors declining in response times	Confidence Scores of "OK", "Good", and "Great" answers all average around 42.5%

Industry Analysis of Improvement in Lab Response Times

Despite the massive 60% of industries effectively demonstrating worse response times, not all industries are on the decline; material improvements were seen in Manufacturing (48% improvement), Government (45% improvement), and Healthcare (44% improvement), with incremental improvements in Technology and Financial Services.



60% of industries effectively demonstrated worse response times

Industries that made significant material improvements;

MANUFACTURING:

48% IMPROVED

GOVERNMENT

45% IMPROVED

HEALTHCARE:

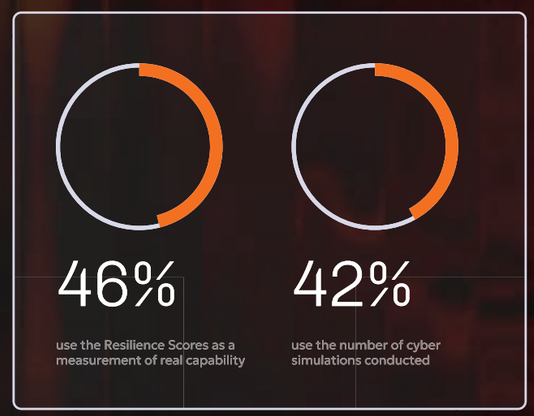
44% IMPROVED

"

Completion is not competence. Without real-world assessment, progress is just paperwork.

The Danger of False Metrics

Organizations are measuring activity instead of ability. The most-used metrics in cyber-readiness dashboards focus on training and completion, not competence.



Most used indicators of readiness within existing organizations:

01 SECURITY AWARENESS TRAINING

02 CYBERSECURITY EXERCISE

These numbers help explain why readiness scores remain stagnant even as organizations celebrate program maturity. When success is defined by attendance instead of outcome, cyber leaders gain confidence without proof. Boards receive slide decks full of percentages, but none of them predict how fast a team can contain a ransomware outbreak or restore operations after a breach.

Beyond the Dashboard:

The Psychology of "Cyber Dunning-Kruger" and How to Break It

By Dr. John Blythe

This research that fueled this year's report reveals a striking paradox: cybersecurity confidence is at an all-time high, but actual performance is stagnant.

Our survey shows that 71% of organizations rate their cyber readiness programs as "very" or "extremely mature" and 94% believe those programs will prove effective in the midst of a crisis. Yet, the performance data tells a different story.

While the capability gap is cause for concern, the illusion of confidence is what represents real danger.

The Problem: The Psychology of Overconfidence

This disconnect is driven by powerful cognitive biases. We see evidence of the Dunning-Kruger effect, a bias where a lack of knowledge in a specific area leads to an overestimation of ability.

The data shows teams are building confidence by mastering the wrong things. Organizations are practicing against old threats, with 60% of all training activity focused on vulnerabilities more than two years old, and not pushing themselves to understand advanced threats, with 36% of all labs taken being beginner-level. By mastering these basic and old threats, teams build high confidence. However, they don't know what they don't know about new or advanced threats, like AI, an area where senior staff participation has notably dropped.

The Enabler: False Metrics and Confirmation Bias

This false confidence is fueled by optimism bias (the belief that a major incident won't happen) and confirmation bias (seeking out data that confirms our belief in our own readiness).

Leaders are relying on false metrics. The report shows the most-used indicator of readiness is the "Security Awareness Training completion rate". While this metric feels good, it proves nothing about performance under pressure. Measuring "completion" is not measuring "competence". It's just checking boxes.

The Solution: From Assumption to Evidence

The only way to break this cycle is to seek objective, data-driven feedback.

01

Reset Confidence with Reality:

Use high-pressure simulations (like Cyber Drills) to provide a necessary shock to the system. A 22% accuracy score is a painful but essential dose of reality that moves teams beyond assumption.

02

Shift Culture from Checking the Box to Measurable Improvement:

A failed drill is not a failure; it is a successful identification of a critical gap. This mindset reframes exercises as an opportunity for improvement, not a test to be passed

03

Report on Capability, Not Activity:

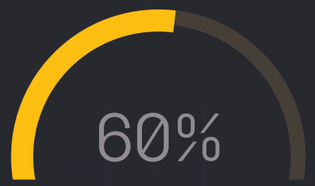
Stop reporting "completion" to the board. Start reporting true capability through better benchmarking. This includes critical decision-making accuracy, decision speed, and real-world detection and response metrics like Mean Time to Detect (MTTD) and containment time.

03

THE READINESS RUT:

Why Progress Has Stalled

The Four Barriers Holding Readiness Back



of training exercises focus on vulnerabilities more than two years old, and four of the top five most-practiced CVEs stem from legacy issues.

MISSTEP 1

Practicing the Past

Our data shows that organizations are not accelerating readiness. Resilience scores remain flat or slightly declining year-over-year, indicating stagnation directly tied to an overemphasis on outdated threats.

The result: Organizations cultivate superficial preparedness for past threats, leaving themselves blindsided by novel attack vectors, reduced adaptability, and escalating exposure to emerging risks

"Organizations aren't failing to practice—they're failing to practice the right things."

MISSTEP 2

Fixating on Fundamentals

Many organizations remain mired in beginner-level readiness, never graduating to maturity or resilience. Interest in labs considered "Beginner/Entry" level saw a slight increase over the previous year, indicating a flat-to-slight decline in Intermediate and advanced threat-hunting or scenario-based modules.

The result: Without progression beyond basics, teams fail to develop deeper judgment, tactical agility, or the ability to respond to multi-stage, novel attacks - leading to brittle defenses when stress and novelty collide.

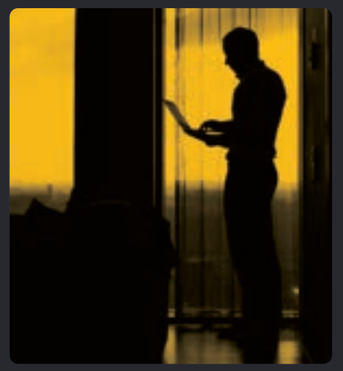
01 FUNDAMENTAL LABS:

36%

02 DEFENSIVE CYBER

18%

"Mastering the basics is useful - but when everyone stops at fundamentals, maturity stalls."



MISSTEP 3

Excluding the Business

Readiness remains technical and siloed, reducing its real-world efficacy as crises span the entire organization.

We also found that non-technical roles more likely to stick to fundamentals 1.7 times more than technical users, demonstrating that, when participating in simulated drills, non-technical users lack the ability to swiftly and accurately make the right decisions that will impact their part of the business' response to an incident.

The result: Organizations cultivate superficial preparedness for past threats, leaving themselves blindsided by novel attack vectors, reduced adaptability, and escalating exposure to emerging risks

"Resilience isn't built by technologists alone, it's built when business roles know how to act under crisis."

The Myth of the Technical-Only Response: Why Siloed Drills Fail

By Jon Paul Gabriele

A major cyber incident is not an IT problem. It is a business crisis that unfolds in minutes. In this "golden hour" of a breach, the actions of your legal counsel, communications team, and executive leadership are just as critical as those of your technical responders.

Unfortunately, this report's findings reveal a dangerous disconnect: 90% of organizations feel their cross-functional communication between technical and non-technical teams is effective. Yet, only 41% of organizations actually include non-technical roles in their cyber simulations.

This means that for nearly 60% of organizations, their crisis communication plan is pure theory. It has never been tested under pressure.

In a real attack, the technical response (finding the malware, isolating systems) runs in parallel to a high-stakes business response:

- **Legal** is on a 72-hour clock for regulatory disclosure
- **Communications** is fielding calls from journalists and drafting statements for anxious customers
- **Executive Leadership** is facing a $5 million ransom demand and must make a "pay/don't pay" decision that could define the company's future

These are not technical problems; they are leadership, legal, and financial crises. A 29-hour average containment time is not just a technical failure. It is a symptom of decision-making bottlenecks, unpracticed handoffs, and siloed teams.

As the data shows, when non-technical roles do participate, they are 1.7 times more likely to stick to fundamentals, meaning these teams are only being tested in basic, low-pressure drills. They are not being battle-tested in the advanced, chaotic scenarios where their leadership, legal, and communications decisions are most critical.

Organizations are failing not for a "lack of knowledge," but for a "lack of practiced coordination". To fix this, you must practice the handoffs, not just the technical response.

01

Integrate Every Function: A simulation that doesn't include injects for Legal (e.g., a mock regulatory query), Comms (e.g., a fake journalist email), and the C-suite (e.g., a live ransom video) is incomplete

02

Practice Business Decisions: The goal isn't just to "find the breach." It's to "approve the public statement in 30 minutes" or "decide on the ransom payment in one hour."

03

Build Shared Empathy: Practice is the only way for the technical team to understand why Legal is being so precise, and for Legal to understand why the tech team can't be 100%

Misaligning the Frameworks

Alignment between training, measurement, and operational threat models is weak, limiting the actionable value of readiness.

Despite the MITRE ATT&CK Framework being held as one of the best tools for mapping threat tactics, techniques, and procedures to defenses, it surprisingly ranks third in framework adoption among surveyed organizations. Many firms instead lean on broad regulatory standards that include ISO 27001 or frameworks like NIST that don't directly translate into threat-response capability.

The result: The misalignment causes teams to prepare against compliance checkboxes—not real adversary behavior—undermining readiness by failing to build skills directly relevant to attack paths actually used in the wild.

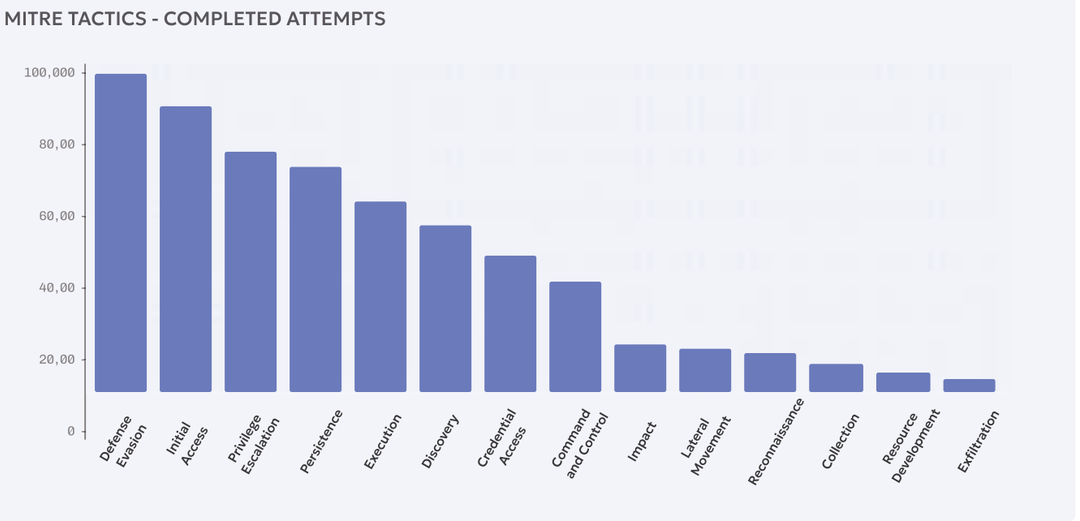
MITRE's ATT&CK Framework breaks down actual threat actions into 14 tactics— overarching goals threat actors are attempting to achieve using various malicious techniques and procedures, providing real-world examples, methods of detection, and mitigating steps to be taken.

Organizations that map their cyber readiness to the ATT&CK framework are better preparing themselves for specific kinds of threat actions and the appropriate responses (remember, even if the "next" attack uses a novel method, it's still limited by the environment in which it runs, so keeping up with the latest that ATT&CK has to offer will give responders a leg up).

We found that organizations are relatively consistent in the ATT&CK tactics they are focusing on year over year. As shown at right, organizations have been and continue to be interested in the earlier stages of an active cyber attack—specifically those tactics they can either prevent, stop, or at least detect on the network.

This lack of focusing on the same threat tactics each year creates a potential resilience gap with organizations not knowing how to respond to threat actions categorized within other tactics.

> **You can train to a framework, but if it doesn't map to real attacks, you're training in the dark**



By Dan Potter

Stuck at the Start: Why Your Framework Choice Creates Critical Blind Spots

What is your organization preparing for? For many, the honest answer is "an audit." This year's benchmark data reveals a critical misalignment in how organizations approach readiness.

Compliance-based frameworks like ISO 27001 and general-purpose frameworks like NIST are being prioritized, while the threat-based MITRE ATT&CK framework ranks third in adoption.

Look at the data from the report. Organizations are overwhelmingly focused on practicing tactics like "Initial Access" and "Defense Evasion." These are the start of an attack—the moments before and during the initial breach. This focus, which is consistent year over year, has created massive blind spots for what happens after an attacker has established a foothold.

This is where the real damage occurs. Tactics like "Collection" (stealing your data), "Lateral Movement" (finding your crown jewels), and "Exfiltration" (shipping your data out) receive minimal practice. Teams are training to win the initial engagement while completely ignoring the main event.

This isn't just an academic preference; it has a direct, negative impact on performance. Choosing a compliance framework over a threat-based one means you are "training in the dark"—preparing against static checklists, not dynamic adversary behavior. The consequence is a myopic focus on only the first links of the attacker kill chain.

This misalignment is a root cause of the "readiness rut" this report identifies. You can be 100% compliant with a standard like ISO 27001 and still be 100% vulnerable to a real-world attack path. You are practicing almost exclusively for the prevention of a breach, a battle you will inevitably lose at some point. You are not practicing for the response.

To build true resilience, organizations must adopt an "Assumed Breach" mindset.

01

Train Like an Adversary, Not an Auditor: Use compliance frameworks (NIST, ISO) to build your defenses (the "what"). Use a threat-based framework like MITRE ATT&CK to prove your defenses work against real-world behaviors (the "how").

02

Cover the Full Kill Chain: Use the ATT&CK framework as a diagnostic tool. Look at the chart in this report and ask your team, "When was the last time we practiced detecting 'Collection' or 'Exfiltration'?"

03

Run "Assumed Breach" Scenarios: The most valuable exercises assume the initial compromise has already occurred. Start the simulation inside the network. This immediately shifts the focus from "prevention" (a hope) to "response" (a plan) and forces your team to practice the middle and end of the kill chain, where resilience is truly proven.

Experience vs. Adaptability

When Experience Helps vs. When It Hurts

Veteran practitioners outperform newcomers on known threats. In 2025, analysts with 11 or more years of experience achieved ≈80% accuracy in classic incident-response labs and cut median recovery to 21 days (for reference, those with zero years of experience took a median of 64 days). This is obviously good news for organizations with tenured security staff. However, notice that they are achieving these scores on threats they know. The real question is, then, are they keeping up with new threats, like AI?

The data shows that when put against AI-enabled or novel attack vectors, experienced teams lag in experimentation and cross-domain thinking. Immersive data shows senior staff participation in AI-scenario labs dropped 14% YoY, while non-technical managers increased participation by 41%.

Rethinking Seniority:

Are Your Experts Ready for What's Next?

When it comes to known threats, experience will always be king. Our data shows a clear correlation between years of experience and the accuracy and speed of response to known vulnerabilities. However, when you look at the breakout of our comparative data around the proportion of intermediate and advanced level drills and labs taken by purely years of experience, those same senior staff (with the 11+ years under their belts) did not invest themselves further into more difficult training, whereas every other grouping based on years of experience saw increases in more advanced skills being developed.

Experienced technical experts, while masters of yesterday's threats, may be developing a critical blind spot to the most significant threat of tomorrow. It's a compelling reason for CISOs to ensure their entire team, especially seasoned practitioners, is engaged in continuous, forward-looking skill development.

> **Experience teaches what to do next — until the next thing has never happened before**

What's Next?

AI Based Threats

In keeping with the theme of IT and security staff—regardless of experience level—adapting to new threats, we can't gloss over one of the fastest and potentially most-dangerous new threats: AI.

Most security professionals believe the use of AI will increase. Specifically:

80%

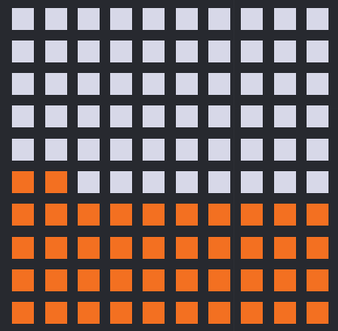
Think threat actors will use generative AI to increase the sophistication of cyber threats against their organization over the next 12 months

76%

Think threat actors will use generative AI to increase the frequency of cyber threats against their organization over the next 12 month

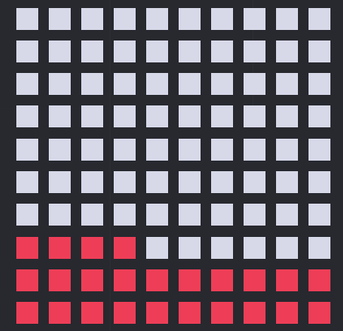
The types of AI-based threats organizations are concerned about cast a wide net of threat actions that only require further adaptability by organizations to ensure they can be detected and responded to accordingly:

We are glad to report that the completion of labs tagged as being AI-related increased year-over-year by nearly 42% (for comparison, non-AI labs only saw an increase in completion of 24%). Additionally, a correlation between years of experience and the percentage completion of AI-related labs shows those with 11+ years of experience completing more than double the labs of those with 0 years.



42%

Increase in the Completion of Labs Tagged as Being AI-Related



24%

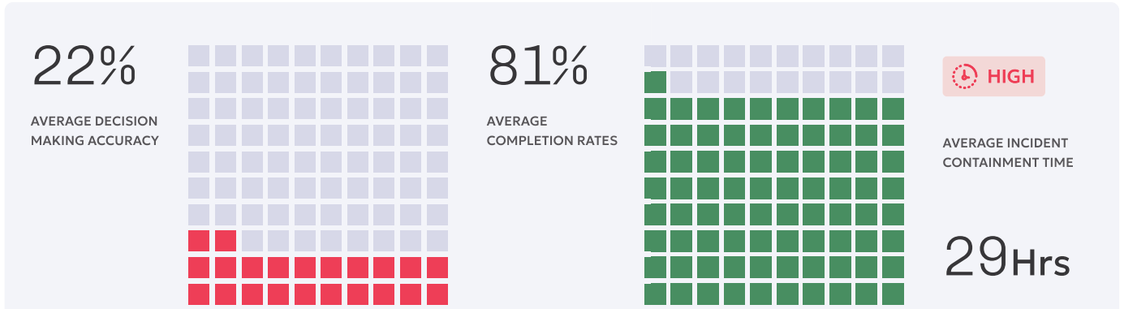
Increase in the Completion of Labs Tagged as Non-AI Related

Turning Confidence into Competence

As this report has revealed, many organizations harbor strong confidence in their cyber readiness even when tested performance metrics (22% decision accuracy, 29-hour containment durations, 81% completion rates) expose persistent gaps.

The following recommendations translate those findings into concrete steps, bridging the distance between belief and capability. Each recommendation is paired with practical actions, and all align under Immersive's strategic pillars of Prove, Improve, and Report, so you can embed sustainable readiness across your enterprise.

Taking into account the detail shared in this report, we offer the following recommendations.



Work Towards Continual Readiness Training

Organizations that train only sporadically tend to plateau, yet the data shows that more years of experience correlate with higher decision accuracy. Sustained training helps lift both confidence and performance:

01

Establish a regular training cadence (e.g., monthly micro-drills or quarterly full simulations) to keep muscles sharp, not just exercised once a year

02

Track training exposure by experience band (junior, mid, senior) and monitor how decision accuracy improves over time for each band

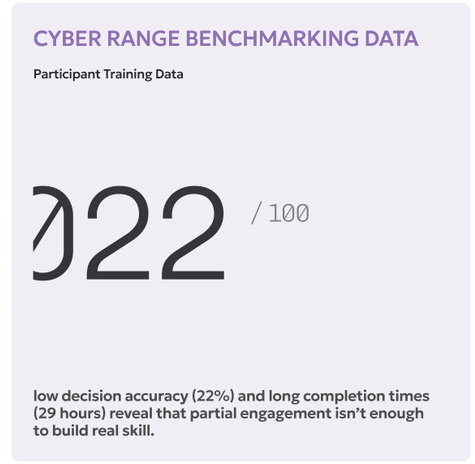
03

Rotate scenario types (e.g. AI-enabled attacks, supply chain compromise) to prevent overfitting to a narrow threat set and keep training fresh

Ensure Training is Fully Completed, not Just Attempted

Many participants start training but don't see it through. In the Cyber Range benchmarking data, low decision accuracy (22%) and long completion times (29 hours) reveal that partial engagement isn't enough to build real skill.

- Attempt more structured progression, where a user must complete a module before advancing to the next, with automated reminders or escalation paths for stalled participants
- Monitor completion vs attempt rates and flag users under the 81% threshold (report's average) for coaching, review, or targeted support
- Conduct post-training audits, sampling labs to check who actually finishes vs abandons, and collect feedback about why users drop off (complexity, time constraints, UX friction)



Involve the Board and Senior Leadership Directly

Leaders often see cybersecurity through dashboards, but they seldom feel the pressure of real decisions. Engaging them in readiness training ensures alignment, accountability, and better-informed investment choices:

Run executive-level simulations or tabletop exercises where board members or C-suite participants make actual crisis decisions in controlled conditions.

Provide readiness briefings using side-by-side metrics (accuracy, completion, time) so leadership understands capability, not just compliance.

Rotate scenario types (e.g. AI-enabled attacks, supply chain compromise) to prevent overfitting to a narrow threat set and keep training fresh

Expand readiness beyond IT / Security

A cyber incident isn't a technical problem alone. It requires decisions from Legal, Comms, HR, and executives.

If non-technical roles aren't rehearsed, coordination breaks down when real pressure hits.

- Include representatives from Legal, Communications, HR, Operations, and executive functions in every simulation, not just in postmortem reviews
- Run role-swap drills in which non-technical participants attempt security-impact decisions to build empathy and awareness of what those teams face
- Map and rehearse decision handoffs and communication protocols (e.g., how Legal escalates to Exec or how PR coordinates with IT) during drills

Shift focus dynamically to current threats

If over 60% of training focuses on older CVEs, teams are practicing for battles already fought. New threat vectors and exploit techniques demand timely, relevant content to maintain readiness.

- Regularly retire outdated CVE labs and replace them with modules tied to recent exploits (6–18 months window), keeping exercises aligned with the threat landscape
- Track CVE-to-fix timing internally and benchmark whether lab coverage is keeping pace; prioritize labs for vulnerabilities that are fixed rapidly in the wild
- Integrate threat intelligence feeds into the training roadmap so new TTPs or exploit chains automatically generate new lab content

Expand readiness beyond IT / Security

By aligning each recommendation under one of these pillars, organizations can transform readiness from a one-off initiative into an enduring, measurable capability.

At Immersive, we regard readiness not as a single event, but as a cycle of

→ Prove → Improve → Report

These parts of a cyber readiness cycle give structure and sustainability to the recommendations above:

- **Prove:** This is where individuals test their capabilities under stress. Frequent, cross-role training and leadership participation are the proving grounds to expose real gaps
- **Improve:** Once weaknesses are revealed, improve is about closing those weaknesses with targeted, relevant training—especially for non-technical functions and emerging threats
- **Report:** This translates the performance of proving and improving into credible evidence. Presenting accuracy, completion, and time metrics to decision-makers builds accountability and trust and serves as the basis to start the cycle over to prove readiness as new threats emerge

Conclusion:

As we've seen throughout this report, confidence in cyber readiness has never been higher, but real proof of that readiness remains elusive.

Organizations overwhelmingly believe they are prepared, but when tested under pressure, performance metrics tell a different story: decision accuracy hovers near 22%, containment can require 29 hours, and training completion rates average just 81%.

The divergence between belief and capability is not a minor gap. It's a structural fault line in how we think about resilience.

To move beyond illusion and toward true readiness, organizations must commit to a new model: one where capability is proven regularly, gaps are improved precisely, and performance is reported transparently.

That requires embedding readiness across roles (not just in security teams), enforcing completion of real-world training, engaging leadership in the process, and updating content to reflect evolving threats. Only by turning confidence into evidence and converting intention into repeatable performance, can any organization hope to stand up to the next breach with certainty rather than hope.

Authors:

Dr. John Blythe
Director of Cyber Psychology
Immersive

Nick Cavalencia
CEO
Conversational Geek

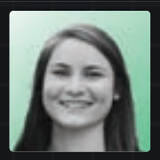
Acknowledgements:

James Hadley
Founder & Chief Innovation Officer
Immersive

Oliver Newbury
Board of Directors
Immersive

Will Bloor
VP, Brand and Creative Director
Immersive

Dan Potter
Senior Director of Cyber Resilience
Immersive



Suzy Dolan
Marketing & Communications Lead
Immersive

Expert Contributors:

Michael Sampson
Principal Analyst
Osterman Research

Roberta Bradshaw
Data Analyst
Immersive

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

www.immersivelabs.com | sales@immersivelabs.com