Enterprise Strategy Group™ by TechTarget

WHITE PAPER

# Legacy Cybersecurity Training Strategies Are Failing, Leading to a Lack of Resilience

## A New, Evidence-based Approach Is Needed

By Dave Gruber, Principal Analyst
Enterprise Strategy Group

February 2023

# Contents

# Securing Modern Businesses Requires a People-centric Approach

Cybersecurity program investments have long been comprised of a people, process, and technology cocktail, requiring ongoing investments in each. As these risk mitigation strategies evolve in the face of a growing and more complex and sustained threat landscape, a new level of cyber and operational resilience is needed. New considerations are required that shift priorities from event-based, point-in-time trainings to fully operationalized preparedness and adaptability models.

### Few Can Measure the Preparedness of Their People or Teams

Legacy cybersecurity training strategies are failing to prepare the individuals and teams they operate within for modern, advanced threats.

While cybersecurity technology investments are still needed, a new focus on increasing the cyber acumen of people and teams—from the super-technical to C-level business leaders—will dramatically improve cyber resilience. While once considered almost solely the responsibility of a handful of technical IT and security professionals, modern attacks and the response actions needed to mitigate them all too regularly involve people from all aspects of an organization, from top-level executives and line-of-business decision makers to staff in sales, finance, manufacturing operations, and more.

Legacy security-related processes have traditionally been focused on operationalizing key, well-defined security functions, often referred to as security operations, spanning functions that include daily alert triage and investigation, proactive and reactive threat detection and response, security assessments, vulnerability assessment and management, security tools configuration and management, and more. Yet, more advanced cyber-risk mitigation for threats like ransomware require a significant expansion in the scope of readiness activities and the people involved. Adapting and responding to unknown situations requires not only technical skills but also rapid judgment and decision making for both line-of-business and security operations.

And while a variety of measurements exist for security tools and tech, most security leaders have no way to measure the preparedness of people and teams involved. Common uncertainties include:

- I don’t know what the current capabilities are across my organization.
- Are my people and teams always up to date and ready to handle any threat? Can I prove it?
- Is every individual ready? In every role?
- Are teams ready to work together?
- How do you vet what people know and don’t know, including within my hiring process?

Legacy cybersecurity training strategies are failing to prepare the individuals and teams they operate within for modern, advanced threats, leaving security leaders uncertain and organizations exposed. New strategies capable of increasing and measuring the cyber acumen of all types of people required to mitigate and respond to modern threats, inclusive of line-of-business, IT, security, and senior leadership, are needed. Given this new reality, the growth of cybersecurity acumen takes on an important role in risk mitigation strategies.

# Where Legacy Training and Readiness Approaches Are Failing

Legacy cybersecurity education, training, and readiness strategies fall into two categories:

- Technical security skills training and certifications.
- End-user security awareness training (general threat information, phishing simulation, etc.).

Most legacy strategies are focused on a limited set of readiness skills and are generally activity- or event-based, meaning that they require periodic engagement in scheduled training activities designed to educate each audience on both general and more detailed security principles and activities.

**Legacy Technical Training Strategies Are Flawed**

The pace of change within modern cyberattacks requires a transformation in the way we think about training—moving from a scheduled, online, or classroom-style approach to a continuous, real-world learning environment.

## Technical Security Training and Certifications

An ongoing commitment to technical training has always been a way of life for IT and security pros. But limited, outdated methods and training resources continue to be in use for most. It is commonplace for security professionals to attempt various training "classes" offered by legacy cybersecurity certification organizations or educational institutions, in an online or classroom-style environment. These periodic "classes" offer a combination of general and tactical strategies to help prepare security pros for "real-life" situations.

Measurements are implemented through certifications, which quickly become outdated and are typically based on simulated, staged attacks modeled after known, historical attack techniques. The pace of change within modern cyberattacks requires a transformation in the way we think about training—moving from a scheduled, online, or classroom-style approach to a continuous, real-world learning environment. And with 45% of organizations reporting a problematic shortage of cybersecurity skills,[1] new strategies are needed to close the skills gap.

Other challenges include:

- People often don't retain knowledge over time, and what is learned is prone to quickly becoming obsolete.
- Passive video training and online exams lack engagement and often don't reflect real-life experiences.
- Event-based training lacks continuous readiness refresh.
- Certification-based training doesn't measure the ongoing readiness of people and teams.
- Multiple-choice exams and paper certificates are not evidence-based and do not ensure that participants have acquired practical knowledge.

## End-user Security Awareness Training

Security awareness training programs have taken a generalized approach to educating non-technical people about potential threats and offering recommendations for how to avoid them. Typical online training resources provide limited actionable guidance and often instruct people to notify either their IT teams, security teams, or managers when they encounter potential security risks.

Yet, these same people will play a much more critical role in responding to cyberthreats to sustain key operations. Virtually every individual within an organization will, at some point, participate in response activities and, therefore, must understand the specific role they will play and how they must work together with other teams and team

[1] Source: Enterprise Strategy Group Research Report, *2023 Technology Spending Intentions Survey*, November 2022.

members to respond effectively and efficiently. General awareness training further lacks focus for critical roles, such as business leaders, executives, and other critical decision makers involved in crisis response situations.

New strategies and methods capable of preparing, exercising, and measuring the people and teams that must work together to mitigate cyber-risk are needed. In the face of an ongoing growth in cyberattack volumes and complexity, these methods must be operationalized to ensure continuous readiness and growth in cybersecurity acumen across organizations over time.

# Can Security Leaders Confidently Prove Workforce Readiness?

Many cybersecurity leaders believe that their teams will be able to respond to threats, yet few know for sure, and few can prove it. Beyond paper cybersecurity certificates and regulatory compliance-reporting mechanisms loosely based on security awareness training tools, only security leaders who have lived through a serious cyberattack can honestly report whether their organization is prepared. And even then, are they prepared for the *next* unknown threat? The only way to truly be confident is to trust in the knowledge, skills, *and* judgment of your people to be able to respond effectively in any situation.

### Organizational Readiness Measurements Are Lacking

As impactful as a serious cyberattack can be on overall business operations, few C-level execs or BoD members have an ability to effectively measure their organization's readiness.

As impactful as a serious cyberattack can be on overall business operations, few C-level execs or Board of Directors (BoD) members have an ability to effectively measure their organization's readiness. This lack of confidence flows through to shareholders, who only hear about readiness issues post-breach—once the damage is already done.

As in most operational functions, **improvement can only be recognized when the function can be effectively measured**. Measurements begin with a baseline of performance, compared to an expected set of outcomes, and are further understood when compared to the performance of other similar organizations and individuals.

Cybersecurity readiness is often measured in the context of cybersecurity frameworks, guided by NIST,[2] MITRE ATT&CK, and others. Yet, while helpful in guiding architectural and investment strategies, these frameworks lack formalized measurements that would enable security leaders to accurately assess overall readiness across their organizations.

When it comes to the assessment of the cybersecurity acumen of the people and teams involved, few have an ability to assess more than "participation" in required training activities, beyond a "post-attack" analysis to determine what succeeded and what failed. This reactive measurement approach leaves security leaders unprepared to report to their boards, C-suites, and regulators with any sense of accuracy on the preparedness of their function.

# A Path to Effective Cyber Resilience

With crisis only *one cyberattack away* from every organization, preparedness is more important than ever before. Yet while 97% of organizations report planning on continuing investments in cybersecurity programs and technology,[3] most lack strategies that go far enough to properly prepare the people and teams needed to mitigate cyber-risk. This is further exacerbated as adversaries turn their attention to human-assisted attacks, leveraging readiness weaknesses to accelerate ransomware and other advanced attack success rates.

[2] Source: National Institute of Standards and Technology, *Cybersecurity Framework*.
[3] Source: Enterprise Strategy Group Research Report, *2023 Technology Spending Intentions Survey*, November 2022.

Effective cyber resilience requires investment in people, process, and technology. But these strategies must evolve and expand to support the people and teams needed to effectively protect, respond to, and mitigate cyber-risk. Security leaders must expand strategies to operationalize continuous awareness, training, and measurement processes for all people and teams within their organizations. When they do, security leaders can:

- Measurably reduce cyber-risk.
- Improve operational resilience, leading to better business outcomes.
- Demonstrate compliance to regulatory requirements.

## A Systematic Methodology Is Needed

### People-centric Cybersecurity Must Be Continuous and Measurable

CISOs need to ensure they have the coverage and required acumen across their entire organization. Business and technical leaders need to have confidence in their preparedness across the AppDev, security, IT/cloud operations, legal, communications, and executive teams.

Implementing a comprehensive cybersecurity workforce resiliency strategy requires a systematic methodology capable of driving continuous improvement of cyber acumen across all individuals throughout an organization. This includes every person involved in any facet of business and technical operations.

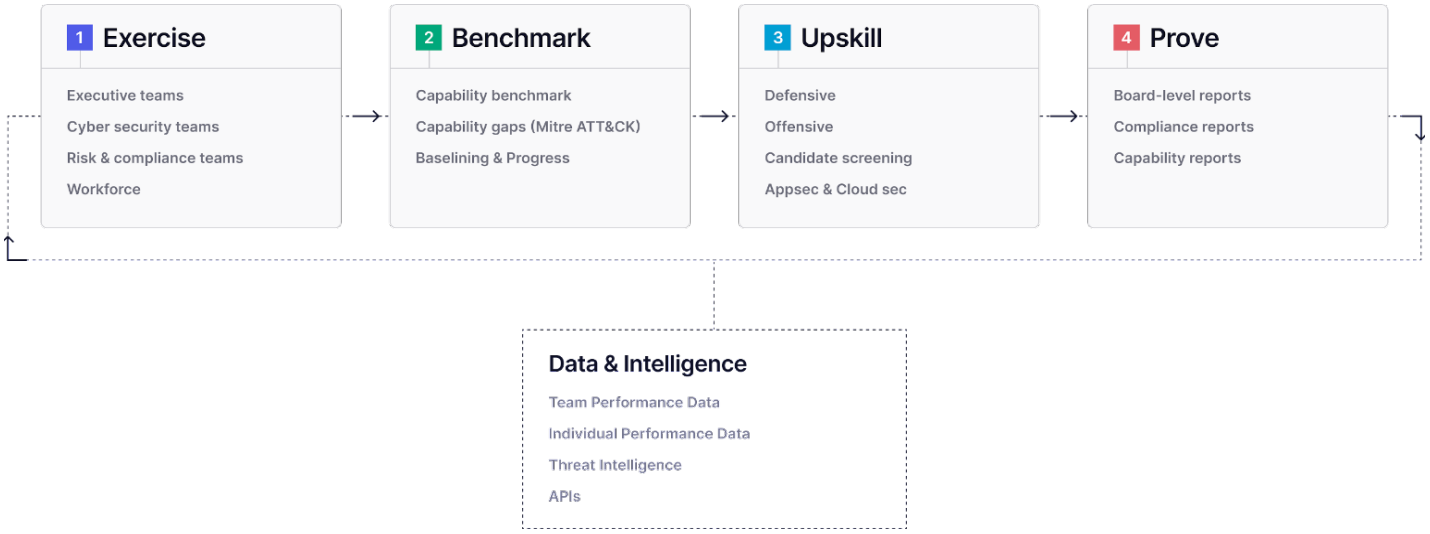
People-centric cybersecurity must be *measurable*. CISOs need to ensure they have the coverage and required acumen across their entire organization. Business and technical leaders need to have confidence in their preparedness across the AppDev, security, IT/cloud operations, legal, communications, and executive teams.

The methodology must be applicable to the individual needs of the many different types of workers involved, from executives to the lowest level of operations. Baselining, benchmarking, and continuous measurement help operational leaders assess and drive overall readiness and program improvement across the organization.

## A Cyber Workforce Resilience Methodology

Leveraging a four-step resilience methodology (see Figure 1), organizations can grow and measure the cyber acumen of every person, regardless of their role. And while cyber acumen is fundamentally about individuals, cyber resilience requires carefully orchestrated interactions between teams and individuals operating within them. This means that as organizations apply the methodology, both exercises and measurement must include personal, team, and inter-team activities, emulating interactions that are needed to handle real-life attack scenarios.

**Figure 1.** The Cyber Workforce Resilience Methodology




*Source: Immersive Labs*

With attack dwell times averaging between 11 and 50 days, depending on company size, before security teams detect them,[4] response actions and times are critical to damage mitigation. Continuous cyber workforce resilience ensures that everyone involved is prepared and knows how to respond in an efficient and coordinated way, leading to remediation and recovery in the shortest possible time.

## Real-life Exercises

Cybersecurity preparedness must be engaging, real world, and have a current focus. The methodology, therefore, begins with a series of engaging, real-life exercises that allow individuals to learn through doing, in advance of actual attacks (see Figure 2).

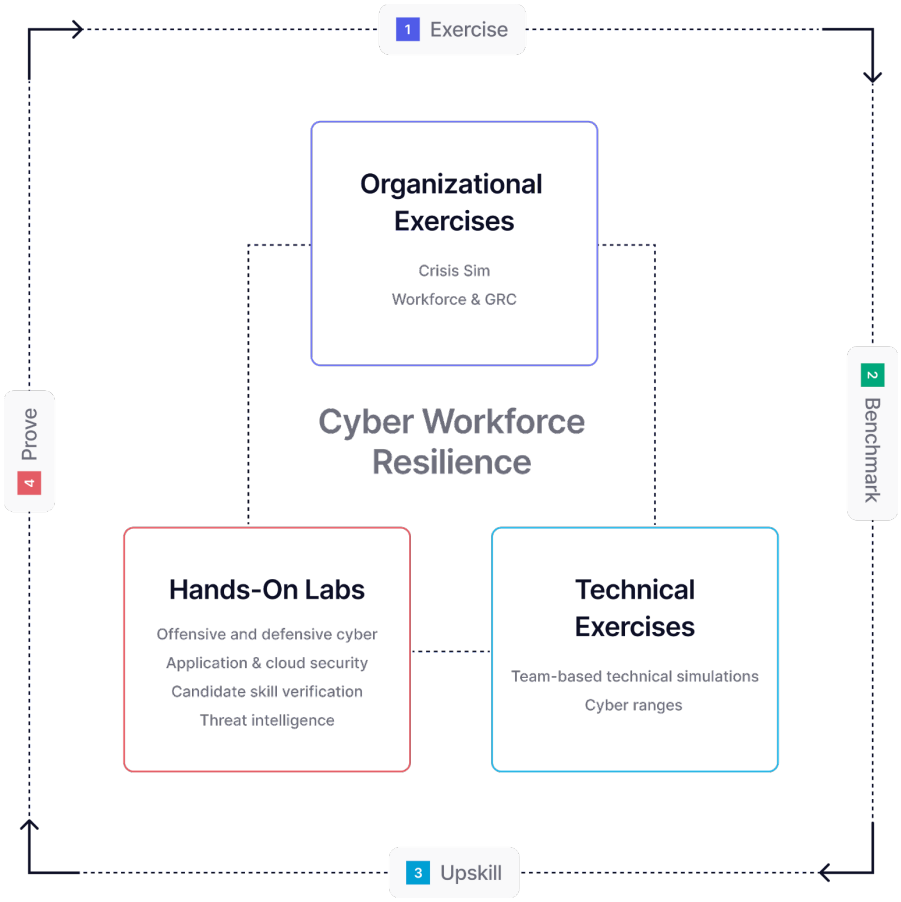
Using highly interactive, realistic simulations and hands-on cybersecurity labs based on real-world scenarios helps evaluate individual and team capabilities and decision making against the latest threats.

Simulated, real-life immersive simulations infuse knowledge of breaking threats, while challenging individual readiness skills and acumen. Specific exercises based on the assessed cyber acumen of each person provide a semi-customized path toward continuous improvement. Exercising orchestrated team activities further improves response, minimizing operational impact.

These exercises fulfill both a learning component and a measurement component, benchmarking capabilities, identifying gaps, and measuring progress toward key objectives. Ongoing exercises are refined to close gaps and sustain knowledge, leading to meeting resilience objectives. Crisis simulations provide a broad assessment of how the entire organization operates in the face of a major attack.

[4] Source: Sophos, *The Active Adversary Playbook 2022*, June 2022.

**Figure 2.** Expanding the Model




*Source: Immersive Labs*

## Benchmarks Enable Program Growth

Benchmarking and measurements are key to understanding readiness and progress. How well are we doing? How do we know? Benchmarking creates a basis for measuring improvement, but also helps compare and assess industry readiness. Benchmarking provides a baseline of cyber resilience, helping security leaders identify and report on key aspects of the operation that require improvement and, potentially, additional focus and investment. Individual organizational capability mapping shows strengths and weaknesses, supporting additional focus on risky functions and areas where increased technical performance is needed. Leveraging industry frameworks like MITRE ATT&CK coverage reporting and NIST incident response provides a common assessment framework that can further guide future security and architecture investments.

## Up-skilling Individuals and Teams

Continuous assessments help security leaders understand where skills are strong—and weak—within each team and adjust the delivery of instant targeted training to address any weaknesses, allowing them to enable retention and rewards based on capability—not tenure. Engaging, continuous training informs and reinforces knowledge and situational awareness. And again, this applies to both individuals and to teams and follows the methodology, providing engaging, real-life exercises that allow individuals to learn through doing, prior to actual attacks.

### Enabling Retention and Rewards Based on Capabilities, Not Tenure

Continuous assessments help security leaders understand where skills are strong—and weak—within each team and adjust the delivery of instant targeted training to address any weaknesses, allowing them to enable retention and rewards based on capability—not tenure.

### Proving Results

Because these measurements are continuous, they support both ongoing operational reporting and reporting for other event-driven requirements, such as for BoD meetings; special, periodic compliance/audit reporting; and M&A activities.

Further, benchmarking can help leaders understand and report on where they stack up against other organizations in similar industries.

## Automating Resilience Delivers Positive Outcomes

Organizations investing in people-centric, cyber-resilience strategies are reducing risk, limiting cyberattack damage, and improving crisis response. Additional benefits include:

1. Increased and continuous improvement in overall organizational cyber-readiness, (execs/decision makers, cybersecurity teams, SecOps analysts/defenders/BlueTeams, RedTeams, IT, AppDevelopers, risk/compliance teams, etc.).
2. Improved ability and agility to respond.
3. Upleveling individual and team skills across the org (defensive, offensive, AppSec, CloudOps, hiring, retention, etc.).
4. Clarity into specific program, capability, and skills gaps.
5. Increased executive/BoD confidence in cyber-readiness and resilience (formalized measurement and reporting).
6. Improved efficacy of cyber-recruitment and staffing (hiring: candidate screening to vet their skills, retention, and advancement).
7. Ease of compliance and regulatory reporting.
8. Reduction of application vulnerabilities across the software development lifecycle.
9. Improvement of operational efficiency in overall cybersecurity preparedness activities.

## Introducing Immersive Labs

Immersive Labs is focused on people-centric cyber resilience. Its solutions provide realistic simulations and hands-on cybersecurity labs to improve and evaluate individual and team capabilities and decision-making against the latest threats. The state of an organization's cyber resilience can be measured and proven by comparing industry benchmarks, building, and assessing team capabilities, and demonstrating measurable risk reduction and compliance with data-backed evidence. These capabilities enable organizations to continuously assess, build, and prove their cyber workforce resilience, from front-line cybersecurity and development teams to Board-level executives.

Immersive Labs solutions are helping grow cyber resilience in large organizations and governments, including organizations such as Citi, Pfizer, Daimler, Humana, HSBC, the UK Ministry of Defence, and the UK National Health Service. The company is funded and backed by Goldman Sachs Asset Management, Summit Partners, Insight Partners, Citi Ventures, Ten Eleven Ventures, and Menlo Ventures.

# Conclusion

Legacy cybersecurity training strategies are failing to prepare the individuals and the teams they operate within for modern, advanced threats, leaving security leaders uncertain and organizations exposed. New strategies capable of increasing and measuring the cyber acumen of all types of people required to mitigate and respond to modern threats, inclusive of line-of-business, IT, security, and senior leadership, are needed. Given this new reality, the growth of cybersecurity acumen takes on an important role in risk mitigation strategies.

Innovative cybersecurity training and preparedness solutions from vendors like Immersive Labs are helping security leaders close readiness gaps while increasing overall cybersecurity acumen across their organizations. Enterprise Strategy Group recommends that security leaders consider people-centric security strategies as a path to risk reduction and readiness in a world of increasing cyber-centric risk.

**About Enterprise Strategy Group**
Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community. © TechTarget 2023.

contact@esg-global.com
www.esg-global.com