

# Cybersecurity Lost Its Natural Language And Why Upskilling Is the Only Way to Bridge the Gap

January 21, 2026

12 min read



**Author:**  
**Paula Januszkiewicz**

CEO of CQURE & CQURE Academy,  
Cybersecurity Expert, MVP & RD, MCT

## Intro

Cybersecurity used to have a relatively shared vocabulary. Firewalls. Antivirus. Patching. Perimeter defense. These concepts once formed a common language understood not only by security teams, but also by IT, leadership, and even non-technical stakeholders. Security discussions were simpler, threat models were narrower, and defensive responsibilities were more clearly defined.

Today, that language no longer exists in a simple or unified form.

Modern cybersecurity has evolved into a highly fragmented, deeply specialized, and fast-moving discipline that spans cloud architectures, identity-centric security, AI-driven threats, supply-chain exposure, regulatory pressure, and advanced incident response. The result is paradoxical: even cybersecurity specialists struggle to stay fully up to date.

This is not a failure of individuals. It is a structural shift in the industry.

And it has profound consequences for how organizations must think about talent, training, and resilience.

## Before We Talk About Cybersecurity, Answer This

Before diving into market dynamics or strategic direction, take a moment to stop and ask yourself – honestly:

- 1. Do you feel that today your own, or your team's, cybersecurity skills are truly up to date?**
- 2. When you look at current cybersecurity challenges and long-term security strategy, do you genuinely feel that you "have this under control"?**

From my perspective, more and more often across our enterprise and SMB clients, I hear significant hesitation. There used to be more confidence when this language was simpler, even though confidence does not always equal readiness, and familiarity does not guarantee fluency. The industry has changed faster than most organizations realize – not only in terms of threats and technologies, but in the very language used to describe, detect, and defend against them.

## The Language of Cybersecurity Has Changed – And Most Organizations Can't Speak It

Cybersecurity isn't what it used to be. Today, even experienced cybersecurity professionals struggle to stay current with the breadth and pace of change. It almost feels that if you do not keep yourself intensively up to date, you are not only downgrading yourself from the skills perspective but also it's hard to think about ideas, while we are not familiarized with new terms. How can we grow then, if we get stuck in language? This is not a matter of perception – the data ((ISC)<sup>2</sup> Cybersecurity Workforce Study 2025) clearly shows an industry at a turning point, where cybersecurity talent is scarce and increasingly difficult to develop without deliberate internal investment.

In 2026, organizations will not be just short of cybersecurity professionals – they will be short of professionals with the right skills.

From the aforementioned global workforce research, in 2025 one trend is unmistakably clear: while cybersecurity workforce evolving threat landscape.

The research shows that nearly 60% of organizations report critical or significant cybersecurity skills shortages, while over 90% identify at least one key skills gap within their security teams. Importantly, many organizations acknowledge that filling open roles alone does not eliminate operational risk, as newly hired professionals often require substantial upskilling before they can function effectively in modern security environments.

This is truly a significant issue. To defend current threats we need to understand each other more than ever. How can we do that, as we keep using language that we may not always understand or even worse – speak through different definitions of concepts in cybersecurity.

Let me share with you common example that almost on a weekly basis I happen to encounter: we all speak about testing LLM models. Do we really know how to approach this and what is the expected outcome?

In my opinion, the implications of this skills gap extend far beyond staffing challenges.

This is, in fact, huge operational risk that will hit us from behind if we do not address it today.

Crucially, IBM's analysis (IBM: Cost of a Data Breach Report 2025) demonstrates that organizations experiencing significant cybersecurity skills shortages incur markedly higher breach costs, often millions of dollars more per incident than organizations with mature, well-trained security teams. This establishes a direct and measurable link between skills gaps and financial exposure, confirming that workforce capability is not a soft issue, but a core risk factor.

Broader breach investigations conducted at CQURE in 2025 reinforce this conclusion. Across sectors, human-driven factors – including misconfigurations, phishing attacks, and credential misuse – continue to rank among the most common root causes of security incidents. These findings highlight a critical reality: effective cybersecurity defense depends not only on advanced technology, but on people who can correctly interpret signals, understand modern attack patterns, and act decisively under pressure.

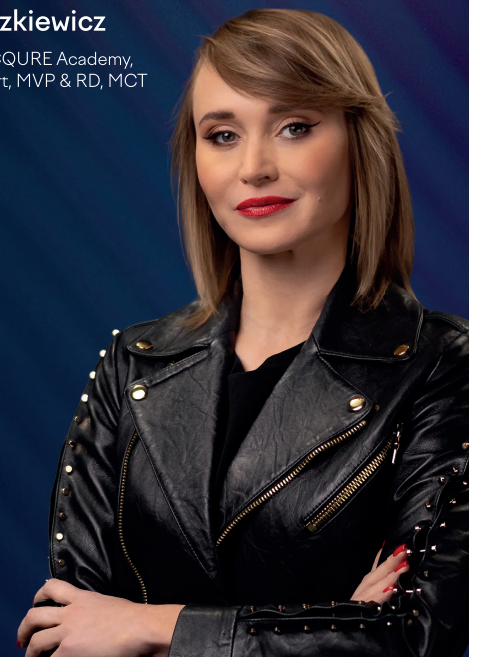
Taken together, the evidence points to a clear conclusion:

**When organizations lack professionals who speak the language of modern cybersecurity, the cost is paid repeatedly – in financial loss, operational disruption, reputational damage, and erosion of strategic trust in partnerships.**

**“When organizations lack professionals who speak the language of modern cybersecurity, the cost is paid repeatedly – in financial loss, operational disruption, and erosion of strategic trust”**

**Paula Januszkiewicz**

CEO of CQURE & CQURE Academy,  
Cybersecurity Expert, MVP & RD, MCT



## From One Discipline to Many: Why Cybersecurity Became So Hard to “Speak”

Cybersecurity didn't suddenly become complex – it accumulated complexity over time.

In 2025, a single security role may be expected to understand:

- Cloud-native infrastructure and misconfiguration risk
- Identity and access management across hybrid environments
- AI-assisted attacks and AI governance risks
- DevSecOps pipelines and software supply-chain threats
- Detection engineering, threat-hunting, and automation
- Regulatory obligations such as NIS2, DORA, or sector-specific frameworks

Each of these areas evolves independently – often faster than traditional education, certification, or hiring models can keep up. What was once a linear career path has become a multidimensional challenge requiring constant recalibration.

Conclusions are direct and clear:

- Skills shortages are now considered a larger risk than headcount shortages
- Nearly all organizations report missing critical, modern cybersecurity capabilities
- The gap is no longer “how many people we have” – but whether they understand today's threat language

This explains a reality many CISOs quietly acknowledge: Teams are staffed, but not fully fluent. Sounds familiar?

## The Modern Reality: Complexity Meets Scarcity

Research from (ISC)<sup>2</sup> estimates the global cybersecurity workforce gap may exceed **~4–4.8 million unfilled roles in 2025**, even as hiring budgets compress and economic pressures rise.

This gap isn't just numerical – it's semantic and cognitive.

Roles today require fluency across multiple domains (e.g., cloud security, identity management, AI governance, incident response automation, threat intel pipelines, DevSecOps integration). Many professionals struggle to keep pace with

emerging attack surfaces (like Shadow AI) and the complex defensive measures needed to counter them.

As a result, organizations increasingly find themselves in a paradoxical situation: security teams exist, tools are deployed, but understanding is fragmented.

## Why the Market Cannot Simply “Hire Its Way Out” of the Problem

The natural reaction to skills shortages is hiring. In cybersecurity, this approach is no longer sufficient.

### 1. Talent Is Scarce – and Competition Is Global

In 2025, millions of cybersecurity roles remain unfilled worldwide. Even when budgets exist, organizations compete for the same limited pool of specialists – often losing them to global players, consultancies, or vendors.

### 2. Experience ≠ Currency

Years in cybersecurity do not automatically translate into readiness for:

- Cloud identity attacks
- AI-enabled social engineering

- Modern breach response work flows
- Detection-driven security operations

Without continuous upskilling, even strong professionals fall behind.

### 3. Budget Pressure Limits External Hiring

Economic uncertainty and cost optimization mean many organizations cannot endlessly expand security teams. Instead, they must extract more value – and more capability – from the people they already have.

This is why internal development is no longer “nice to have.” **It is the only scalable option.**

### When Teams Don’t Speak the Language, Costs Skyrocket

The business consequences of this linguistic divide are measurable and severe.

According to IBM’s 2025 Cost of a Data Breach Report, the global average cost of a data breach in 2025 reached USD 4.44 million. While this represents a modest decrease from previous record highs, it remains a substantial financial

burden for organizations of all sizes. In the United States, breach costs escalated further, reaching an average of USD 10.22 million per incident – the highest level recorded to date. With the current trend, this is likely to worsen, as we step into a false sense of security in a smaller or bigger scale. Critically, breaches in organizations with significant security skills shortages cost much more (often millions higher) than in organizations with better -resourced security teams – a direct indicator that talent and skills gaps translate into financial risk.

Data from wider industry analyses also show that human factors – including misconfigurations and phishing – remain major drivers of incidents, underscoring that both technical and human language fluency matters in defense.

The takeaway? When your team can't understand and respond to modern attack vectors or technologies, your organization pays – in dollars, disruption, reputation, and strategic trust.

## **Training From Within: The Only Way Forward**

If cybersecurity has a language, organizations must do two things:

### **1. Invest in Internal Skill Development**

Training current staff – rather than just relying on external hiring – is now a strategic imperative.

Structured, continuous learning programs help teams stay current with evolving domains such as cloud security, threat intelligence frameworks, identity-first security, and AI risk governance. Skills development isn't a one-off event: it's an ongoing commitment that must evolve as fast as the threats themselves. An organization's capacity to learn often becomes the differentiator between resilience and vulnerability.

### **2. Ensure Fluency in the Latest Cybersecurity Concepts**

Today's security professionals must be literate not only in technical tools but in the language of current threats and defenses. This includes:

- AI-driven attacks and adversarial models
- Cloud and hybrid infrastructure risk models
- Secure software development lifecycles (DevSecOps)
- Identity-driven access and zero-trust frameworks
- Incident response automation and orchestration

Organizations that don't cultivate this fluency internally are left with teams that can maintain legacy controls but cannot lead strategic defense.

## Conclusion: Reclaiming the Language of Cybersecurity

Cybersecurity didn't become complex because we wanted it to; it evolved because threats, technologies, and enterprises became more capable – and more vulnerable.

The reality in 2026 is undeniable:

- Cyber risks remain massive and growing – measured in trillions of dollars annually
- Breach costs remain multi-million dollar events with substantial operational fallout
- Skills gaps and talent shortages are fundamental risk multipliers

The solution isn't just more hiring – it's training, fluency, and lifelong learning within the organization.

To secure the digital enterprise of today and tomorrow, organizations must embrace internal talent development as a strategic defense, and ensure that their teams speak the language of modern cybersecurity – not yesterday's vocabulary.

**Cybersecurity didn't lose its language by accident. The question is whether organizations are willing to relearn it – together.**

Thank you for your time and reading this article! We would like to thank you by giving you a 25% **Discount Code: 25DISCOUNT**, to be used at the checkout for a training program that addresses that skills gap. Coupons can't be applied to products already on sale.

**Join the top 1% of experts who thrive in the world's most complex environments**

From IT Specialist to Cybersecurity Master in **12 months** with the Master Annual Program

Amr Thabet, Damian Widera, Marcin Krawczyk, Peter Kloep, Ronald Harmsen, Sami Laiho, Paula Januszkiewicz, Artur Kalinowski, Norbert Krzepicki

...and more, including Guest Speakers!

**CQURE**  
ACADEMY

## Why the Cybersecurity Master Annual Program from CQURE Exists and how to address this gap?

We have done our homework to respond to the shifting market and we have created a fully customizable up to a year-long program that allows us to address the skills and language gap. We have called it Cybersecurity Master Annual Program, where you can attend 16 important classes throughout the year or pick ones that fit you and your Team.

This exact industry problem is why the Cybersecurity Master Annual Program (CMAP) was created by CQURE. CMAP was not designed as a single course. It was designed as a living program that evolves with the cybersecurity landscape. CMAP is not a single course. It is a living program that evolves with the cybersecurity landscape.

## How CMAP Directly Addresses the Skills & Language Gap

Let me explain it, but first check out information about our training here: **LINK** and in case of questions reach out to us at: [training@cquireacademy.com](mailto:training@cquireacademy.com).

## 1. Continuous Learning Instead of One-Time Training

CMAP runs throughout the year, ensuring participants stay aligned with:

- Current attack techniques
- Evolving defensive strategies
- Real-world incident response practices
- Emerging technologies and regulations

This directly reflects how cybersecurity actually changes – continuously.

## 2. A Unified Cybersecurity Language

Rather than teaching isolated silos, CMAP connects:

- Identity, cloud, endpoints, and detection
- Offensive and defensive perspectives
- Strategy, operations, and execution

Participants don't just "know more" – they think in modern cybersecurity terms.

### 3. Built for Working Professionals

The program is designed for professionals who:

- Cannot step away from work for long periods
- Need practical, applicable knowledge
- Want depth without losing strategic perspective

This makes CMAP ideal for internal talent development inside organizations.

### Accessible by Design: Subscription & Financing Options

Recognizing that budgets and personal situations differ, CMAP offers:

- Multiple subscription models
- Flexible payment options
- Financing possibilities for those who cannot pay the full amount upfront

This ensures that access to modern cybersecurity education is not limited by cash-flow timing.

---

### Sources (2025)

(ISC)<sup>2</sup> – Cybersecurity Workforce Study 2025

IBM Security – Cost of a Data Breach Report 2025

Verizon – Data Breach Investigations Report (DBIR) 2025

WEF - <https://www.weforum.org/stories/2024/04/cybersecurity-industry-talent-shortage-new-report/>

#### Author:

Paula Januszkiewicz, CEO of CQURE & CQURE Academy, Cybersecurity Expert, MVP & RD, MCT

Want to know more?

[Subscribe to our Newsletter](#)