



## FOR IMMEDIATE RELEASE

### **CyberBay 2025 Report: Securing the Future Together**

*Survey reveals cost, complexity, talent shortages are leaving SMBs and public sector organizations dangerously under-protected*

**Tampa Bay, FL — September 25, 2025** — Cyber threats are escalating in scale and sophistication. Yet our defenses remain siloed, expensive, and out of reach for a wide range of organizations. The newly released 2025 CyberBay Report, based on insights from hundreds of IT and cybersecurity professionals, sounds the alarm and issues an urgent call to action for the private sector, educators, and cyber defenders to step forward and lead.

Download the 2025 CyberBay Report at <https://cyberbay.org/survey/>

As artificial intelligence accelerates digital integration, the risks to and both private- and public-sector organizations are intensifying. Small- and medium-sized businesses (SMBs), which serve as the backbone of the economy, are left with tools they can't afford, talent they can't find, and systems that can't keep up.

### **A System Under Siege**

The CyberBay Report found that:

- **80.1%** report a shortage of skilled professionals
- **81.3%** cite organizational gaps in policy, behavior, and security culture
- **74.5%** say undergraduate curricula are missing essential job-ready content
- **80.2%** say cybersecurity tools are too expensive
- **71.9%** find tools fragmented and poorly integrated
- **62.9%** say professional training programs fall short of evolving demands

The results provide a strategic blueprint for filling gaps in the cybersecurity ecosystem. To protect our infrastructure, economy, and future, we must shift from isolated fixes to system-level transformation.

### **1. Democratize Cybersecurity Solutions**

Affordability and usability are no longer optional. We must build scalable, AI-augmented defenses that even the smallest organizations can deploy.

## **2. Prioritize Cyber Defense as a Business Imperative**

The private sector must lead—not with gated solutions, but with open collaboration, public-private partnerships, and investment in real-world resilience.

## **3. Elevate Education as a Strategic Asset**

Cybersecurity education must evolve from theory-heavy programs to hands-on, threat-ready training that begins early and mirrors real-world challenges. Certification bodies, continuing education platforms, and vocational pipelines must align with the pace of escalating risk.

## **4. Activate a Culture of Readiness**

Cybersecurity requires both the right toolset and the right mindset. Every organization needs policies, leadership buy-in, and cultural norms that reinforce vigilance. Readiness must replace awareness as the new standard.

### **CyberBay: The Movement Begins in Tampa**

CyberBay, the Tampa-based cybersecurity collaborative, is proactively addressing the issue. By unifying private, public, and government sectors, CyberBay is democratizing cyber defense, prioritizing readiness over awareness, and training the next generation to meet the moment.

The inaugural [CyberBay 2025 Summit](#) will bring this mission to life. From October 13–15 in Tampa, FL, cybersecurity leaders, educators, technologists, and public sector champions will gather to build the future of cyber defense.

Register now at [CyberBay.org](https://CyberBay.org) and be part of the transformation.

Media Contacts:

Jennifer Kleman  
Cyber Florida  
[jennifer437@cyberflorida.org](mailto:jennifer437@cyberflorida.org)

Christina Pandapas  
Longview Strategies  
[cpandapas@longviewstrategies.com](mailto:cpandapas@longviewstrategies.com)