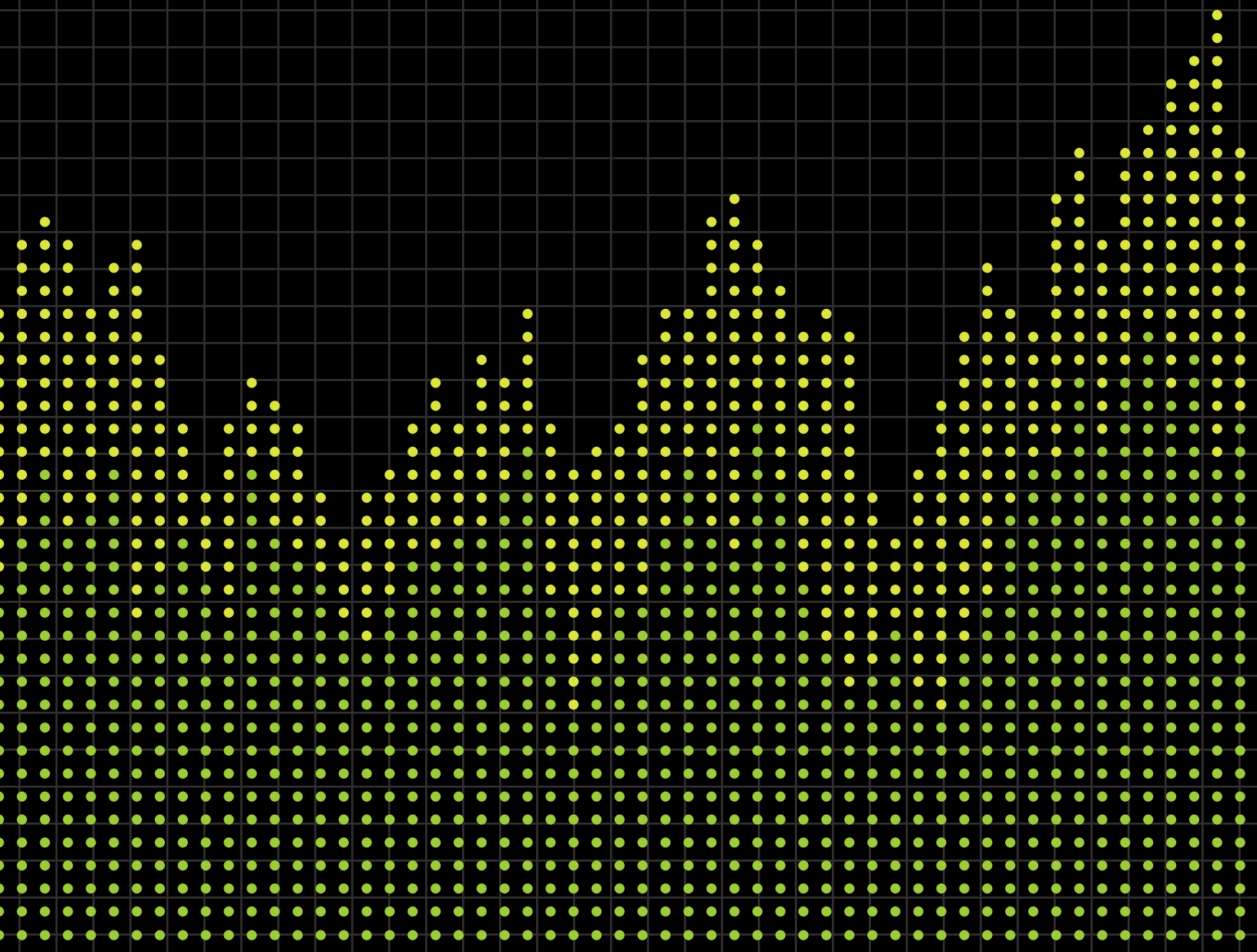
CyberBay

SURVEY REPORT

2025



Executive Summary

We stand at a pivotal moment. AI is accelerating the depth and breadth of connectivity and technological integration in every private sector, government, and academic organization - while at the same time, adoption of forward-looking cybersecurity practices and solutions are lagging. We are, in effect, creating more entry points for bad actors without the safeguards necessary to secure information. Reliable cyber defense is key to protecting our digital infrastructure, and it should be ubiquitous across sectors, from small businesses to multinational enterprises.

We launched the inaugural CyberBay Survey to learn more about where the gaps are and why stronger cyber defense has not yet been prioritized.

We launched the inaugural CyberBay Survey to learn more about where the gaps are and why stronger cyber defense has not yet been prioritized. We gathered insights from organizations on the most significant challenges they face in cybersecurity; the results show a unified acknowledgement that better, more cost-effective tools and training are needed. Alongside technological concerns, the survey examined nontechnical factors such as policies, education, workplace culture, and organizational processes, which are crucial to the success or failure of security measures. Participants included 203 IT and cybersecurity professionals from Small and Medium-Sized Businesses (SMBs) and public-sector entities.

Previous studies show that SMBs face the same cyber threats as larger enterprises but often lack the resources, expertise, and capacity to defend themselves effectively. This makes them more vulnerable, particularly given their central role in the global economy, where SMBs account for more than 90 percent of businesses and around 60 percent of global employment (Junior et al., 2023). Despite their importance, these organizations are frequently overlooked in cybersecurity initiatives and encounter persistent challenges in adopting protective measures.

The 2025 CyberBay survey shows us that both the need for improved cybersecurity education and implementation is clear, as are the obstacles to implementation.

As the hub of the evolving protective ecosystem, the CyberBay movement brings together stakeholders from across the cybersecurity arena in an effort to prioritize practical, scalable, and human-centered strategies that integrate affordable tools with robust policies, education, and workforce development programs.

The time for change is now. CyberBay is leading the charge.

UNIVERSITY of SOUTH FLORIDA

BELLINI CAPITAL

CYBER FLORIDA AT THE UNIVERSITY OF SOUTH FLORIDA

Key Findings

- **High Cost of Solutions:** A significant 80.2% of respondents agree that the majority of existing cybersecurity technology solutions are too expensive, with public-sector organizations feeling this even more emphatically.
- **Integration Challenges:** 71.9% believe that most cybersecurity solutions address specific, isolated problems and are not well integrated with other necessary solutions, a sentiment particularly strong in the public sector.
- **Difficulty of Use:** 63.7% find that existing cybersecurity solutions are too difficult to use or require too much time for users to become proficient, with public sector organizations again expressing this concern more acutely.
- **Organizational Vulnerabilities:** An overwhelming 81.3% agree that many organizations in similar sectors lack appropriate policies, processes, employee behaviors, and culture essential for maintaining a secure IT environment.
- **Cybersecurity Talent Gap:** 80.1% agree there are not enough skilled cybersecurity professionals to meet growing organizational needs, with managed service providers (MSPs) and public-sector organizations feeling this most acutely.
- **Hiring Impediments:** Internal budget restrictions (41.2%) and the lack of skilled talent supply (24.7%) are identified as the most significant impediments to hiring cybersecurity professionals.
- **Education Deficiencies:** A substantial 74.5% believe that the existing undergraduate cybersecurity curriculum is missing important elements, a problem felt more acutely by MSPs. Similarly, 62.9% feel that professional education options for current professionals are also lacking, with MSPs once again highlighting this as a greater issue.
- **Perceived Attack Likelihood:** 70.2% disagree with the notion that their organization is unlikely to be a victim of a cyber attack causing serious harm, indicating a strong awareness of cyber threats. So the idea that their organization should take cybersecurity seriously is well understood and permeated across all sectors.
- **Top Risks from a Breach:** Financial loss is a major concern across all sectors, while customer/member loss and brand reputation loss are also highly ranked, especially by MSPs.
- **Primary Attack Concerns:** Social engineering is the most concerning potential cyber attack for all sectors, followed by infrastructure vulnerabilities and supply chain vulnerabilities.

Audience and Methodology

The CyberBay Survey was designed to explore the varied perspectives organizations hold on a range of cybersecurity issues, specifically focusing on non-technical factors crucial for organizational success or failure.

- **Target Audience:** The survey targeted IT and cybersecurity professionals from both the private and public sectors, explicitly focusing on small and medium-sized businesses (SMBs) in contrast to large enterprise accounts. This emphasis is supported by findings indicating that SMBs face unique cybersecurity challenges. *The Search for the Cyber Unicorn* (see page 8) study has demonstrated that smaller teams and limited budgets restrict the capacity to hire and train inexperienced staff, which increases the demand for improved cybersecurity knowledge and workforce capabilities (Burley et al., 2025). Additionally, recent research shows that SMBs may be more vulnerable to cyber threats due to limited resources, a smaller pool of specialized personnel, and reduced access to advanced security infrastructure.

Methodology

- **Sample:** The study obtained completed surveys from 203 participants.
- **Eligibility:** The study pre-screened respondents to ensure they met the specified targeting criteria.
- **Data Collection:** The study collected survey responses by telephone and an online form.
- **Study Design:** The study used a mixed-methods design integrating quantitative (closed-ended) and qualitative (open-ended) data.
- **Data Analysis:**
  - **Quantitative:** The study applied descriptive statistics (frequencies and percentages).
  - The study conducted a thematic synthesis of open-ended responses to identify recurring patterns and notable insights, analyzing responses verbatim (word for word).
  - **Integration:** The study used qualitative themes to contextualize and illuminate the quantitative findings.
- **Confidence and Error:** The study targeted an 85% confidence level with a 5% margin of error.
- **Areas of Inquiry:** The general areas explored in the survey included:
  - Understanding the audience's experience with cybersecurity solutions.
  - Issues related to talent and culture.
  - Their perspective on cybersecurity education.
  - Their sense of the potential impact of a cybersecurity attack.
  - Access to relevant resources.

Note: See Appendix for metrics on respondent distribution by Size of Organization, Industry Sector, and Job Responsibility.

Key Findings

The following summarizes the major findings shared by the research participants:

Finding 1: Solution Experience

Respondents were asked to agree or disagree with statements regarding cybersecurity solutions. In this report, "cybersecurity solutions" refers broadly to the commercial products and service offerings organizations rely on to secure their operations–including licensed security software, integrated technology platforms, and newer tools with advanced capabilities such as AI.

Expense of Cybersecurity Solutions:

- A significant 80.2% of respondents (63.9% Somewhat Agree, 16.3% Strongly Agree) believe that the majority of existing cybersecurity technology solutions are too expensive.

  This sentiment is even stronger within the public sector, where 68.8% Somewhat Agree and 18.8% Strongly Agree.

80.2% of respondents believe that the majority of existing cybersecurity technology solutions are too expensive.

This finding aligns with existing studies, which highlight that high solution costs and limited budgets are among the most significant challenges for small and medium-sized organizations, particularly in the public sector (Hossain et al., 2025; Manzoor et al., 2024). Financial constraints can restrict SMBs' ability to replace outdated infrastructure, upgrade systems, or invest in advanced cybersecurity tools such as AI. The literature further emphasizes that resource scarcity leaves SMBs more vulnerable, as inadequate financial support makes it difficult to address evolving cyber threats and keep pace with rapidly changing technologies (Chidukwani et al., 2022).

Integration of Cybersecurity Solutions:

- 71.9% of respondents (62.2% Somewhat Agree, 9.7% Strongly Agree) agree that the majority of existing cybersecurity solutions treat specific/isolated problems and are not well integrated with other necessary cybersecurity solutions.

  In the public sector, the overall sentiment is similar relative to Agreement, but the emphasis shifts toward Strongly Agree, with 46.7% Somewhat Agree and 26.7% Strongly Agree.

A Center for Strategic and International Studies report indicates that organizations typically use an average of 47 tools from various vendors, leading to significant interoperability issues and decreased overall effectiveness (Crumpler & Lewis, 2020). Additionally, a Fortinet survey of SMB leaders reveals that 35% consider the lack of end-to-end integration to be a major cybersecurity challenge, with smaller firms particularly noting complexity as a significant factor. The report suggests that SMBs may achieve improved results by implementing integrated security architectures instead of relying on isolated point products (Fortinet, 2020).

Difficulty of Use and Proficiency with Cybersecurity Solutions:

- 63.7% of respondents (52.8% Somewhat Agree, 10.9% Strongly Agree) agree that the majority of existing cybersecurity solutions are too difficult to use and/or take too long to become proficient in their use.

  This sentiment is notably higher in the public sector, where 65.3% Somewhat Agree and 16.3% Strongly Agree.

The concerns raised in our survey are consistent with recent academic and industry studies. Di Nocera, Tempestini, and Orsini (2023) reviewed 55 studies on "usable security" and found a recurring issue: as security systems become more advanced, they often become harder for people to use, leading to steep learning curves and user frustration. NIST's Haney (2023) in *Users Are Not Stupid* highlights similar problems, showing how tools designed without considering usability often fail to gain user adoption. On the practitioner side, the *KPMG Security Operations Center Survey 2024* found that the lack of skills, expertise, and reliable measurement tools remains among the top obstacles in managing cybersecurity solutions. The *Fortra 2025* State of Cybersecurity Survey also shows that organizations continue to struggle with tool and vendor complexity when trying to execute their strategies. Similarly, *The Search for the Cyber Unicorn* study revealed that even "entry-level" positions often come with unrealistic requirements, with hiring managers prioritizing experience over education and certifications, which adds another layer of difficulty for new professionals trying to gain proficiency (Burley et al., 2025). Taken together, these studies reinforce what our respondents told us: many cybersecurity solutions remain too difficult to use or take too long for professionals to become proficient.

Finding 2: Talent and Culture

The survey explored prevailing opinions and challenges related to talent and organizational culture.

Lack of Appropriate Policies, Processes, Employee Behaviors, and Culture:

- A significant 81.3% of respondents (53.4% Somewhat Agree, 27.9% Strongly Agree) concur that many organizations, similar to theirs, lack the necessary policies, processes, employee behaviors, and culture for a secure IT, Application, and Data environment.

  There was no strong distinction in responses across Commercial, MSP, and Public Sector.

Participant Perspectives on Gaps and Challenges:
Participants offered in-depth qualitative insights that provide deeper context to these findings. Common challenges included:

- Many MSPs are perceived to be lacking sufficient backup sets (which should be immutable, local, and cloud-based, with 24/7/365 SOC/NOC monitoring and remediation) despite having firewalls, antivirus, and MDR/EDR.
- Small companies often underestimate their vulnerability to attacks.
- Users sometimes bypass or circumvent standards and procedures for what they believe is correct, rendering policies ineffective when exceptions become commonplace.

- Understaffing, lack of time to develop policies, an overwhelming amount of information, and a scarcity of skilled workers.
- Many organizations are seen as reactive rather than proactive, only developing policies after an incident occurs.
- Some organizations don't understand the "bigger picture" like cyber liability and compliance requirements.
- Employees often do not follow, know, or understand policies because they don't see them as relevant to their specific jobs.
- Leadership buy-in is often minimal, and end-users are often unwilling to learn or adapt to change.
- Many businesses, especially SMBs, lack resources, know-how, or the desire to adhere to compliance needs.
- Employee inattention and lack of vigilance are considered major weaknesses.
- Budget constraints, cuts, and staff wearing "many hats" also contribute to these issues.

Participant Perspectives on Positive Practices

Despite these challenges, participants shared examples of effective practices that contribute to significant cybersecurity outcomes:

- Some organizations place a strong focus on security awareness training and have robust policies with compliant staff and a strong security culture.
- Regulatory requirements, particularly in the public sector, dictate a strong emphasis on cybersecurity policies and processes.

Research at both national and international levels supports this perception. Bishop (2025) stresses that policies, procedures, and compliance are fundamental to building a resilient cybersecurity culture, as they set the standards that guide both technical practices and employee behavior. Similarly, Paananen et al. (2020) show that many organizations continue to struggle with implementing and enforcing effective information security policies (ISPs) and frameworks, leaving gaps that undermine both technology and training efforts. Without clear, enforceable policies, even the best tools and awareness programs are unlikely to achieve lasting impact. *The Cyber Transformation* study (PwC, 2025) reinforces this point, finding that the absence of formal security policies, inadequate risk assessments, and undefined responsibilities are among the most frequent and significant challenges identified in small and medium businesses, making policy and governance gaps among the top recurring challenges.

The *2025 SANS/GIAC Cybersecurity Workforce Research Report* reinforces our findings by showing that workplace culture is central to cybersecurity team success. Notably, 34 percent of respondents identified "working well within a team" as the most important cultural value when hiring for cybersecurity roles. This aligns with our survey results, which reveal that many organizations still lack the cultural foundations needed to attract, retain, and sustain cybersecurity talent effectively.

Lack of Skilled Cybersecurity Professionals:

- 80.1% of respondents (50.6% Somewhat Agree, 29.5% Strongly Agree) agree that there are not enough skilled cybersecurity professionals to meet the growing needs of organizations.

  85% of MSPs and almost 90% of public sector organizations perceive the talent shortage as even greater.

National data reinforces these perceptions. CyberSeek (2025) reports more than 514,359 open cybersecurity positions across the United States, with approximately 1.3 million employed professionals, reflecting a supply-to-demand ratio of just 74 percent. This persistent mismatch highlights the significant gap between the number of available workers and the demand for cybersecurity talent.

In 2025, Cyber Florida published the *Search for the Cyber Unicorn* study (Burley et al., 2025), which draws on interviews with HR professionals and cybersecurity managers to show that the shortage is not only a matter of numbers but also of hiring practices. Many so-called "entry-level" positions are described with unrealistic requirements, demanding multiple certifications, degrees, and years of prior experience that few candidates possess. Furthermore, small teams, budget constraints, lack of trust, and the pressure for new employees to "hit the ground running" often lead employers to prioritize experience over education or credentials. As a result, hiring pipelines are constricted, time-to-hire is prolonged, and qualified candidates are frequently overlooked.

According to the *2025 SANS/GIAC Cybersecurity Workforce Research Report*, many organizations are starting to revise their job descriptions for early-career roles to reduce unrealistic skill expectations and place more weight on aptitude, hands-on skills, and potential rather than rigid credential requirements. *The Fortinet 2024 Skills Gap* report further confirms that traditional requirements remain a significant barrier, particularly in smaller organizations that cannot afford to demand both high credentials and extensive experience.

Cybersecurity Talent Shortage: Is Your Organization Affected?

Somewhat Agree	Strongly Agree	Somewhat Disagree	Strongly Disagree
50.6%	29.5%	17.7%	2.2%

Significant Impediments to Hiring Cybersecurity Professionals:
Participants identified several barriers to effective hiring, with little differentiation among sectors, including the following:

- Internal budget restrictions: 41.2%
- Lack of supply of skilled cybersecurity talent: 24.7%
- Threat landscape changing too fast: 17.3%
- Waiting to see what impact AI and automation will have: 12.8%
- No significant impediments: 4%

Burley et al. (2025) provide further context, noting that many cybersecurity managers in small and medium organizations turn first to internal candidates, often from IT roles such as the Help Desk, because they are perceived as faster to trust and quicker to onboard. This approach helps small teams with limited financial and structural resources reduce the time-to-value challenge, whereas hiring an external candidate is often viewed as a slower and riskier process. Ramezan et al. (2023) and Nkongolo et al. (2023) add that unrealistic hiring requirements for new entrants, such as multiple certifications or years of prior experience, often prolong the hiring process and discourage otherwise qualified applicants. *The (ISC)² Cybersecurity Workforce Study* (2023) likewise found that many organizations hesitate to hire early-career workers due to concerns about how long it will take them to reach full proficiency. Taken together, these studies confirm our finding that organizational expectations for new hires are often misaligned with realistic learning curves, which both narrows the external pipeline and slows the overall hiring process.

Finding 3: Perspective on Cybersecurity Education

The survey explored prevailing opinions and challenges related to talent and organizational culture.

Undergraduate Education Curriculum is Missing Important Elements:

- 74.5% of respondents (55.3% Somewhat Agree, 19.2% Strongly Agree) agree that the existing undergraduate education curriculum for future cybersecurity professionals is missing important elements, with real-world experiences and hands-on with industry tools a general theme.

  MSPs experience this as an even bigger problem, with 56.8% responding Somewhat Agree and 31.8% Strongly Agree.

These findings are consistent with recent research highlighting systemic challenges in workforce readiness. Junior et al. (2023) describe how small and medium-sized enterprises remain "unaware, unfunded, and uneducated" in cybersecurity, pointing to both limited employee literacy and the misalignment between higher education curricula and industry requirements (p. 12). Burley et al. (2025) likewise emphasize that employers frequently encounter difficulties in recruiting "job-ready" entry-level candidates who can quickly adapt to organizational needs. A growing body of scholarship further highlights that a holistic and multidisciplinary approach to cybersecurity education–integrating technical foundations with hands-on training, professional skills, and ethical awareness–is essential. Without such approaches, graduates are likely to remain underprepared for the realities of cybersecurity work, particularly as the rise of artificial

intelligence and other emerging technologies accelerates the pace of change in the field (Blair et al., 2020; Towhidi & Pridmore, 2023; Mukherjee et al., 2024; Payne et al., 2021; Wei-Kocsis et al., 2023).

- Reflecting these concerns, participants in the *CyberBay Survey* pointed to a number of specific areas where undergraduate programs could improve. Their recommendations included:
  - Need for more practice and real-life situations, moving beyond "book knowledge" that doesn't translate to real-world practice.
  - Emphasis on hands-on experience and internships is crucial, ideally in year one of college.
  - Inclusion of soft skills (social, communication) and ethical decision-making.
  - Teaching different frameworks like NIST 2.0 and CIS controls.
  - Curriculum needs to adapt to rapidly changing technology, including AI components and current threats.
  - Focus on threat detection and response, as well as real-world scenarios for data breaches and incident management.
  - Fundamental knowledge of networking and system administration is required.
  - Suggestions for earlier introduction of cybersecurity concepts (elementary/high school).
  - More practical problems with effective solutions, and collaboration between universities and local businesses.

Professional Education Options Missing Important Elements:

- 62.9% of respondents (55.1% Somewhat Agree, 7.8% Strongly Agree) agree that the existing professional education options for maintaining cybersecurity professionals' proficiency are missing important elements.

  Again, MSPs experience this as an even bigger problem, with 58.8% Somewhat Agree and 27.1% Strongly Agree.

Suggestions for Improvement

- In their open-ended responses, participants offered a range of recommendations for strengthening professional cybersecurity education. The most common suggestions included:
  - Need for collaboration and sharing of knowledge to democratize skills, rather than professionals building data silos.
  - Professional education must keep up with the fast-changing threat landscape and new technologies, including AI.
  - More real-world training, simulations, practical application, case studies, and hands-on experience.
  - Focus on how cyber criminals think and being proactive rather than reactive.
  - Emphasis on the "human firewall" and motivating people to protect themselves.
  - Continuous education in short segments, rather than periodic, long courses.
  - Affordability of training and professional development.
  - More technical, specific solution training.

Helpful Professional Education Resources/Practices

Participants who did not perceive major gaps in professional education pointed to several resources and approaches they considered particularly effective in preparing cybersecurity professionals. These included:

- Online resources like YouTube, LinkedIn Learning, Udemy, and various web tools.
- Universities like the University of West Florida, University of South Florida, University of Florida, Georgia Tech
- Certifications and certification bodies such as SANS, CompTIA (Security+), ISC2 (CISSP), ISACA, EC-Council, Palo Alto.
- On-the-job hands-on experience.
- Cybersecurity solution providers offering ongoing education webinars.
- Big Tech companies (Google, Microsoft, Amazon) that promote security-first approaches.
- Organizations like MITRE and RangeForce.

Participants highlighted the University of South Florida as one of the universities effectively preparing the next generation of cybersecurity professionals.

Finding 4: Perspective On Impact of an Attack

Respondents shared their views on the likelihood and potential consequences of cyber attacks.

Likelihood of Harmful Cyber Attack:

- 70.2% of respondents (48.1% Somewhat Disagree, 22.1% Strongly Disagree) disagree with the statement that their organization is unlikely to be the victim of a cyber attack that causes serious harm.

  This indicates a strong awareness and concern across all industry sectors regarding the potential for serious cyber incidents, with 70% to 75% disagreeing with the notion of being unlikely victims.

The *CyberBay Survey* results indicate that SMBs recognize their vulnerability to cyberattacks; however, research shows that awareness does not always translate into preparedness. For example, ConnectWise (2024) reported that 94% of SMBs have experienced at least one cyberattack, a sharp increase from 64% in 2019. Similarly, Arroyabe et al. (2024), in a survey of 232 SMBs, found that although many organizations express significant concern about cybercrime, these concerns rarely lead to comprehensive protective measures. To close this gap, studies recommend that SMBs adopt dynamic risk assessments, invest in employee education and training that goes beyond basic cybersecurity awareness, and foster a robust cybersecurity culture. In addition, active collaboration within the wider cyber ecosystem - through threat intelligence sharing and adoption of best practices - has been identified as a critical step toward building resilience.

- **Biggest Business Risks Associated with a Successful Cybersecurity Breach** (Rated 1-5, 5 being highest risk):

Financial loss is a major concern across all sectors, while customer/member loss and brand reputation hit are also highly ranked, especially by MSPs and Public Sector.

Impact / Sector	Commercial	MSP	Public Sector
Financial Loss	4.13	3.84	3.06
Brand Reputation Hit	3.68	3.93	3.56
Customer/Member Loss	3.53	4.3	2.81
Inability to Grow	2.97	2.98	2.31

The concerns raised in the *CyberBay Survey* align with challenges that many SMBs face nationally and internationally regarding cybersecurity breaches. Research indicates that SMBs frequently identify financial loss, reputational damage, and customer attrition as significant risks, which can have serious implications for their operations. For example, a study by Okta (2024) found that nearly two-thirds of U.S. SMBs prioritize financial and reputational consequences as their primary concerns. Additionally, ConnectWise (2024) reported that 78% of SMBs believe that a major cyberattack could jeopardize their sustainability, long-term stability, and resilience. VikingCloud's 2025 Threat Landscape Report enhances the urgency of these findings, noting that one in five SMBs might be compelled to close if a cyberattack resulted in damages of as little as $10,000, and that reputational damage often extends beyond the technical resolution of an incident. Collectively, these insights suggest that the concerns of CyberBay participants are consistent with broader trends observed for SMBs and highlight the importance of enhancing not only technical defenses but also strategies for financial, reputational, and customer-trust resilience.

- **Most Expected Sources of Cyberattacks** (Rated 1-5, 5 being most expected):

Organized Cyber Crime tended to top the list with a shift toward nation-state attacks for public-sector organizations.

Source / Sector	Commercial	MSP	Public Sector
Organized Cyber Crime	3.87	3.91	3.5
Nation-State Attacks	3.5	3.44	3.69
Lone-Wolf Hackers	3.2	3	3.38
Internal Staff	2.95	3.21	3.25
Consulting / Contracting Staff	2.74	2.79	2.81

- **Most Concerning Types of Potential Cyber Attacks** (Rated 1-5, 5 being most expected):

Social engineering was the top concern, followed by infrastructure vulnerabilities and then the supply chain for all sectors.

Type / Sector	Commercial	MSP	Public Sector
Social Engineering	4.26	4.3	4.25
Infrastructure Vulnerabilities	3.66	3.74	4
Supply-Chain Vulnerabilities	3.38	3.53	3.25

The *CyberBay Survey* indicates that respondents across all sectors are most concerned about human-driven threats, particularly social engineering. This concern is amplified by advancements in artificial intelligence, which are enabling more sophisticated phishing campaigns, scalable exploitation of vulnerabilities, and automation of various forms of cybercrime. Recent research highlights that AI-driven phishing attempts are not only more frequent but also more convincing (*Harvard Business Review,* 2024). Industry analyses further suggest that small and medium-sized businesses (SMBs) are especially vulnerable as AI continues to expand the threat landscape (Okta, 2024).

Finding 5: Access to Resources

Respondents rated how well their organization is served when augmenting existing resources in solutions, talent, or expertise (Rated 1-5, with 5 being the best-served).

Overall, organizations feel best served in Solutions/Technology and Services, particularly MSPs. However, areas like Upskilling Existing Talent and Talent Availability are rated significantly lower, indicating **persistent challenges in augmenting human capital resources across all sectors.**

Resource / Sector	Commercial	MSP	Public Sector
Solutions / Technology	3.76	4	3.63
Services	3.56	3.84	3.63
Best-Practice Approaches	3.46	3.47	3.44
Peer Insight	3.44	3.44	3.5
Upskilling Existing Talent	3.3	3.3	3.13
Talent Availability	3.14	3.05	3.19

The findings of the *CyberBay Survey* indicate that gaps in talent development and availability remain significant obstacles to cybersecurity resilience. Industry studies highlight the scale of this challenge: the *ISACA State of Cybersecurity 2024* report finds that 57% of organizations consider their cybersecurity teams understaffed–43% somewhat understaffed and 14% significantly understaffed. Similarly, the *(ISC)² Cybersecurity Workforce Study (2024)* reports a global shortfall of approximately 4.76 million cybersecurity professionals, reflecting a 19.1% year-over-year increase. Small and medium-sized businesses (SMBs) are particularly impacted, as limited budgets and competition with larger enterprises hinder their ability to attract and retain skilled professionals. According to the *Ponemon Institute (2023),* while many SMBs rely on managed service providers to address these gaps, such reliance is not a substitute for long-term investments in workforce development and organizational learning.

Conclusion

The *CyberBay Survey* highlights that small and medium-sized businesses (SMBs) encounter the same evolving cyber threats as larger enterprises but often lack the resources to respond effectively. Persistent challenges such as high costs, limited integration, complex tools, skills shortages, and weak organizational cultures continue to hinder their efforts. Nonetheless, the survey indicates that leaders are acutely aware of these risks and are keen to bridge the gap between awareness and preparedness.

To enhance cybersecurity for SMBs—and all the organizations that make up our nation's economy and well-being—we must move beyond mere compliance checklists and costly point solutions.

In short, our digital borders are under siege. Cyberattacks have evolved into a relentless assault on our nation's infrastructure, economy, and security.

The solution requires more than siloed academic programs or new software. Urgent, systemic change is needed – change that builds upon an ecosystem in which education, innovation, private capital, and national security operations converge. Creating this kind of environment means engaging universities, defense agencies, the private sector, and investors that can fuel the engine for innovation and scale. To dominate the cybersecurity battlefield, academia must train the next generation while military command centers advance state-of-the-art solutions. Startups bring speed, flexibility, and cutting-edge thinking and enterprises bring deployment infrastructure and reach.

The CyberBay movement is at the heart of this change. Our work has just begun, and we are committed to serving as the catalyst for a safer world.

References

Andres, J. & Crumpler (2020) .Cybersecurity and the problem of interoperability. ***https://www.csis.org/analysis/cybersecurity-and-problem-interoperability***

Arroyabe, M. F., Arranz, C. F., De Arroyabe, I. F., & de Arroyabe, J. C. F. (2024). Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. *Computers & security, 141*, 103826.

Bishop, G. (2025). *Cybersecurity Culture*. CRC Press.

Blair, J. R., Hall, A. O., & Sobiesk, E. (2020). Holistic cyber education. In *Cyber Security Education* (pp. 160-172). Routledge.

Burley, D.; O'Connell; S.; Angelo-Rocha, M. (2025). *The Search for the Cyber Unicorn: Perspectives from HR on Filling Entry-Level Cybersecurity Positions*. ***https://cyberflorida.org/the-search-for-the-cyber-unicorn/***

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations. *IEEe Access, 10*, 85701-85719.

ConnectWise. (2024). *SMB cybersecurity survey report*. ConnectWise. ***https://www.connectwise.com/company/press/releases/connectwise-research-finds-78-of-smbs-concerned-a-cyber-attack-could-put-their-organizations-out-of-business***

CyberSeek. (2025). Cybersecurity Supply/Demand Heat Map. ***https://www.cyberseek.org/heatmap.html***

Di Nocera, F., Tempestini, G., & Orsini, M. (2023). Usable security: A systematic literature review. *Information*, 14(12), 641.

El-Hajj, M., & Mirza, Z. A. (2024). Protecting Small and Medium Enterprises: A specialized cybersecurity risk assessment framework and tool. *Electronics*, 13(19), 3910.

Fortinet. (2024). 2024 cybersecurity skills gap global research report. Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/reports/2024-cybersecurity-skills-gap-report.pdf Fortinet. (2024). *2024 cybersecurity skills gap global research report*. Fortinet. ***https://www.fortinet.com/content/dam/fortinet/assets/reports/2024-cybersecurity-skills-gap-report.pdf***

Fortinet.(2020). Small and midsize businesses and cybersecurity: current priorities and challenges. ***https://www.exclusive-networks.com/usa/wp-content/uploads/sites/35/2020/12/US-VR-Fortinet-White-Paper-SMB-A-Report-on-Current-Priorities-and-challenges.pdf***

Fortra. (2025). *State of Cybersecurity Survey Results*. Fortra. ***https://www.fortra.com/resources/guides/fortra-state-cybersecurity-survey-results***

Haney, J. (2023), Users Are Not Stupid: Six Cyber Security Pitfalls Overturned, Cyber Security: A Peer-Reviewed Journal, [online], ***https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=935795***

Haney, J. , Cunningham, C. and Furman, S. (2024), Towards Integrating Human-Centered Cybersecurity Research Into Practice: A Practitioner Survey. ***https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=957088***

Harvard Business Review. (2024, May). *AI will increase the quantity — and quality — of phishing scams*. ***https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams***

(ISC)^2. (2024). *Cybersecurity workforce study*. ***https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study#KeyFindings***

ISACA. (2024). *State of cybersecurity 2023: Global update on workforce efforts, resources and cyberoperations*. ***https://www.isaca.org/resources/reports/state-of-cybersecurity-2024***

Junior, C. R., Becker, I., & Johnson, S. (2023). Unaware, unfunded and uneducated: a systematic review of SME cybersecurity. *arXiv preprint arXiv:2309.17186*.

KPMG. (2024). *Time to Transform Now: Security Operations Center Survey*. KPMG International. ***https://kpmg.com/us/en/articles/2024/transform-soc-now.html***

Manzoor, J., Waleed, A., Jamali, A. F., & Masood, A. (2024). Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. *Plos one, 19*(3), e0301183.

Mukherjee, M., Le, N. T., Chow, Y. W., & Susilo, W. (2024). Strategic approaches to cybersecurity learning: A study of educational models and outcomes. *Information, 15*(2), 117.

Nkongolo, M., Mennega, N., & van Zyl, I. (2023). Cybersecurity career requirements: A literature review. *arXiv preprint arXiv:2306.09599*.

Okta. (2024). *How AI impacts the SMB threat landscape*. ***https://www.okta.com/blog/ai/how-ai-impacts-the-smb-threat-landscape/***

Okta. (2024). *Okta SMB cybersecurity report 2024*. ***https://www.okta.com/newsroom/press-releases/north-american-smb-face-significant-cyberattack-challenges/***

Paananen, H., Lapke, M., & Siponen, M. (2020). State of the art in information security policy development. *Computers & Security, 88*, 101608.

Payne, B. K., Mayes, L., Paredes, T., Smith, E., Wu, H., & Xin, C. (2021). Applying high impact practices in an interdisciplinary cybersecurity program. *Journal of Cybersecurity Education, Research and Practice, 2020*(2), 4.

Ponemon Institute. (2023). The 2023 global study on the state of cybersecurity in SMBs. Ponemon Institute. ***https://www.hpe.com/psnow/doc/a00130892enw***

PwC. (2025). Cyber Transformation Methodology and Roadmap Analysis. ***https://www.pwc.com/ee/en/press-room/news-and-articles/CyberTransformationMethodologyandRoadmapsanalysishasbeencompleted.html***

Ramezan, C. A. (2023). Examining the cyber skills gap: An analysis of cybersecurity positions by sub-field. *Journal of Information Systems Education, 34*(1), 94-105.

SANS Institute & GIAC. (2025). *2025 cybersecurity workforce research report*. SANS Institute.***https://www.sans.org/mlp/2025-attract-hire-retain-cybersecurity-roles***

Tahsin, H. S., Tan Yigitcanlar, K. N., & Xu, Y. (2025). Cybersecurity in local governments: A systematic review and framework of key challenges. *Urban Governance*.

Towhidi, G., & Pridmore, J. (2023). Aligning cybersecurity in higher education with industry needs. *Journal of Information Systems Education, 34*(1), 70-83.

VikingCloud. (2025). *SMB threat landscape report: Small- and medium-sized businesses, big cybersecurity risks*. ***https://www.vikingcloud.com/resources/vikingclouds-2025-smb-threat-landscape-report-small--and-medium-sized-businesses-big-cybersecurity-risks***

Wei-Kocsis, J., Sabounchi, M., Mendis, G. J., Fernando, P., Yang, B., & Zhang, T. (2023). Cybersecurity education in the age of artificial intelligence: A novel proactive and collaborative learning paradigm. *IEEE transactions on education, 67*(3), 395-404.

Appendix

Respondent Attributes

- Data Types: The survey captured both quantitative data and qualitative data (verbatims) to provide a comprehensive understanding of the issues.

The survey collected responses from 203 individuals.

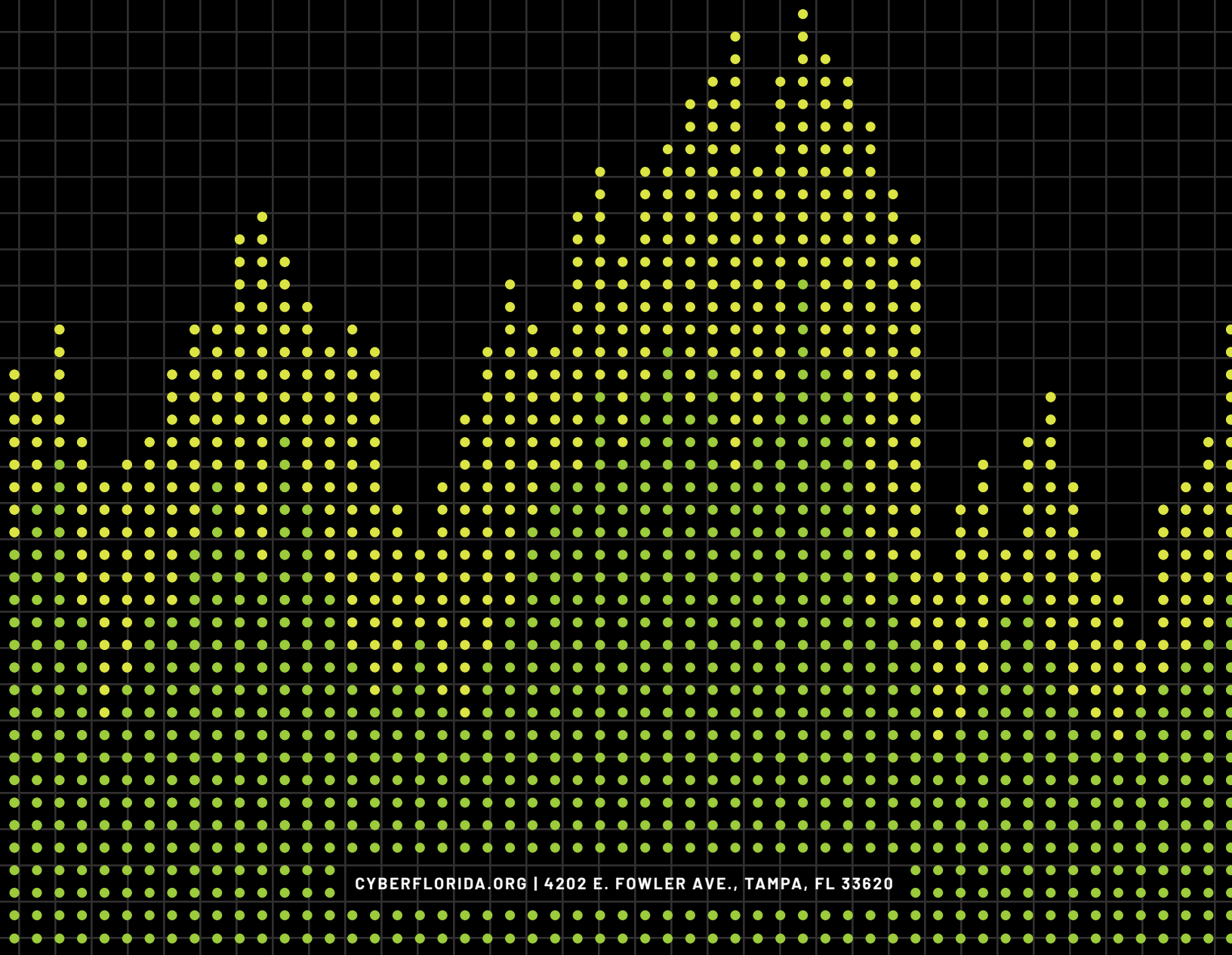
- **Size of Organization Distribution:**
  - Under 50 employees: 21.6%
  - 50 - 100 employees: 12.5%
  - 100 - 250 employees: 16.4%
  - 250 - 500 employees: 19.7%
  - 500 - 1000 employees: 27.4%
  - 1000+ employees: 2.4%

- **Industry Distribution:**
  - Commercial: 71.2%
  - Managed Service Provider (MSP): 20.7%
  - Public Sector: 7.7%

- **Job Responsibilities:**
  - IT Technical Analyst: 26%
  - IT Manager or Team Lead: 27%
  - IT Director or Department Head: 26%
  - Security Analyst: 3%
  - Security Manager or Team Lead: 10%
  - Security Director or Department Head: 8%

CyberBay

UNIVERSITY OF SOUTH FLORIDA / CYBER FLORIDA / BELLINI CAPITAL



CYBERFLORIDA.ORG | 4202 E. FOWLER AVE., TAMPA, FL 33620