“As cyber threats grow in scale and complexity in this rapidly evolving digital ecosystem, youth engagement is indispensable – not merely in supporting cyber security, but also in shaping it

Youth are at the heart of cyber resilience

by **Alessia Balsamo**

In recent years, the global cyber threat landscape has transformed dramatically. Early on, well-known threats such as malware, ransomware and phishing campaigns were commonplace. Today that old landscape is being changed by far more sophisticated and intelligent tools, capable of deceiving even the most skilled cybersecurity experts.

Bolstering cyber resilience, however, requires more than technical expertise and solutions. This new digital landscape demands the active engagement of everyone – in particular young people who, having grown up inside this environment, are uniquely positioned to be co-creators, educators and defenders. As cyber threats grow in scale and complexity in this rapidly evolving digital ecosystem, youth engagement is indispensable – not merely in supporting cyber security, but also in shaping it.

Companies today face significant and converging challenges: geopolitical tensions that intensify their global risk exposure; unpredictable cyber attack patterns that complicate their planning and response; and their rapid adoption of emerging technologies that create previously unknown vulnerabilities.[1]

Compounding these global challenges is a widening cybersecurity skills gap.

> **"In 2025, nearly half (49 per cent) of public-sector organizations cited a lack of skilled personnel as a barrier to meeting their security objectives"**

an increase of 33 per cent from the previous year.[2] This is not merely a perception; the data confirm it as a worsening trend: from 2020 to 2024, 56 per cent of all major cyber incidents recorded since 2011 occurred in those five years alone.

[1] World Economic Forum. Global Cybersecurity Outlook 2025. Geneva: World Economic Forum, 2025.

[2] *Ibid.*

More striking, in comparison to 2019 – prior to wide spread remote work and the emergence of pervasive artificial intelligence (AI) – major incidents have increased by 112 per cent with a monthly average that rose from 139 incidents in 2019 to 295 in 2024.[3] A shortage of skilled personnel coupled with a staggering increase in the number of cyber attacks remains an obstacle to effective cybersecurity.

Cyber attacks inflict substantial economic, legal, reputational and technological damage, and know no geographical bounds. In 2024, 65 per cent of worldwide incidents targeted Europe and the Americas, a large number that may in part be due to strong disclosure obligations under the European Union's General Data Protection Regulation, the Network and Information Security Directives, and the Digital Operational Resilience Act. Nevertheless, within that geographic area, Europe alone still recorded a 67 per cent surge. Considering Oceania, that region saw a 228 per cent increase in the number of cyber attacks, largely attributed to newly enforced cybersecurity disclosure policies.[4]

In terms of the types of attacks in 2024, cybercrime remains dominant, accounting for 86 per cent of global incidents. Cyber criminals have adopted the so-called as-a-service model – where criminal tools are rented – which has made cybercrime more profitable and accessible, especially to individuals with minimal technical skills.

"Traditional organized crime now reinvests proceeds from offline operations into cyber activities, increasing their threat capacity."

[3] Clusit. Rapporto Clusit 2025 sulla sicurezza ICT in Italia e nel mondo. Milan: Clusit, 2025

[4] *Ibid.*

Outside of cybercrime, hacktivism and information warfare nearly doubled in 2024, while espionage and sabotage declined.[5]

The social and economic impacts of cybercrime cannot be underestimated. A much-cited example is the 2024 CrowdStrike incident in which a software update crashed 8.5 million Windows systems globally, resulting in significant disruption to airports, hospitals, financial institutions, and businesses. In that cyber incident alone, companies experienced more than USD $5 billion in direct losses.[6]

As cyber threats grow in scope and complexity, there is a rising demand for new perspectives from law, psychology, communication, and other non-technical fields. These disciplines will inform the social, behavioural, and strategic dimensions of cybersecurity. Intensifying this need is workforce strain. By the end of 2025, nearly half of global cybersecurity leaders were projected to leave their roles due to burnout. Beyond that, 66 per cent of Chief Information Security Officers reported that expectations were excessive. In fact, over half of them had experienced burnout in the previous year. Workforce burnout remains a troubling concern in the present digital ecosystem.

Amid the demand for new perspectives in a diminished workface, it is not surprising that the gap in talent is widening. In fact, two in three organizations report a critical shortage of cybersecurity professionals; only 14 per cent express confidence in their current capabilities.[7]

Youth engagement presents a viable solution to current cyber challenges. Yet bridging this talent gap requires a broader, more inclusive approach to talent development – one that empowers young people from all backgrounds to contribute fully to cyber resilience.

5 Clusit. Rapporto Clusit 2025 sulla sicurezza ICT in Italia e nel mondo. Milan: Clusit, 2025
6 CNN. CrowdStrike outage: cause and cost CNN Business, 24 July 2024.
7 World Economic Forum. Global Cybersecurity Outlook 2025.

Young people grew up in digital environments; they have never known anything else. With ease, they navigate informal channels and emerging platforms both of which are increasingly targeted by cyber threats, such as identity theft, phishing, and AI-generated deepfakes.

> **“Fluency in digital culture, creative tools, and online social dynamics are the reasons why youth are well equipped to strengthen cyber resilience from the inside.”**

Yet, being embedded in this digital space, while essential, is not enough – youth engagement must extend beyond technical skills alone.

Young people today live in a hyper-connected world, which does not in itself produce the critical awareness or understanding needed to navigate this digital space. Cyber awareness remains an essential skill not to be underestimated. To help young people understand the implications of their online actions and the value of their personal data, new approaches are needed. Those actions include: digital peer education that enables youth to serve as content creators within their communities; regional learning hubs that offer AI and cybersecurity training; and mentorship in collaboration with youth organizations and global platforms that strengthen and share the knowledge of the tools used daily.[8]

Today’s cyber threat landscape is fast-moving, AI-driven, and increasingly complex, leaving no sector or region untouched. Traditional, purely technical responses, can no longer keep pace with the speed and sophistication of modern cyber attacks. So what is the solution?

Investing in early cyber awareness, fostering capacity-building before workforce entry, and opening inclusive career pathways for individuals from diverse backgrounds, young people can benefit from their status moving from passive digital consumers into proactive defenders. Closing the skills gap, countering burnout, and building resilience will require a generational shift, one that fully embraces youth as active partners in cybersecurity.

About the Author

Alessia Balsamo is a cybersecurity professional specialized in IT risk with 7 years of experience in Security for Financial Services. Her academic background includes a law degree with a focus on international criminal law from the Milano Bicocca University during which she had the opportunity to study also in Lithuania (Erasmus) and Spain (Summer School). In 2025, she represented Italy in the official Youth engagement Group of the G7 (Y7) for AI and Digital Technology and in October she began the Master of Laws (LL.M.) in Cybercrime, Cybersecurity and International Law organized by UNICRI.

[8] Youth 7. Y7 Summit Communiqué 2025. Rome: Youth 7, 2025.


“
Youth engagement presents a viable solution to current cyber challenges