ITI Promoting Innovation Worldwide

Testimony for the Record
The Information Technology Industry Council

"Growing the National Cybersecurity Talent Pipeline"

Before the

United States House of Representatives Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection

June 22, 2023

The Information Technology Industry Council (ITI) appreciates the opportunity to provide written testimony to the Subcommittee on growing the national cybersecurity talent pipeline. ITI is the premier advocate for the technology sector, representing the world's most innovative companies. We promote public policies and industry standards that advance competition and innovation worldwide. Our diverse membership and expert staff provide policymakers with the broadest perspective and thought leadership from technology, hardware, software, services, and related industries.

Recruiting, training, and educating a diverse cybersecurity workforce is a top priority for ITI and its member companies. The ongoing shortage of cybersecurity professionals profoundly impacts ITI's membership. We welcome the Committee's attention to this pressing national issue for both the government and private sector. While ITI member companies take a range of actions to invest in and develop their cybersecurity professionals, we would like to focus our attention on the role that Artificial Intelligence (AI) must play in reducing the security workload and empowering cybersecurity professionals.

ITI recently launched our AI Futures Initiative, which crafts action-oriented AI policy recommendations to address emerging AI questions in the U.S. and globally. Led by a task force of technical and policy experts and serving as a convener for a diverse set of stakeholders ranging from industry to academia to civil society, the AI Futures Initiative will explore topics relevant to AI policy discussions, from transparency and accountability to AI's societal impacts. The AI Futures Initiative will feature a robust exploration of the foundational models that underpin Large Language Models (LLM – such as OpenAI's ChatGPT or Google's Bard) and how generative AI more broadly will impact cybersecurity.

It is important to note that the cybersecurity industry benefits from a workforce that reflects a variety of backgrounds, perspectives, and experiences. As part of the tech sector's efforts to engage with educational institutions to prepare a diverse and ready workforce, ITI established the National Initiative to Increase Diversity in Tech, in partnership with Morehouse College, one of the most pre-eminent Historically Black Colleges and Universities (HBCU) in the United States. This initiative connects ITI's member companies with Morehouse leadership and educators to develop innovative programs that provide both the private sector and other professional fields—including the federal government—with a skilled workforce that understands the technology sector's cybersecurity needs.

The Cybersecurity Challenge

The US Government (USG) or other large organizations have three primary challenges when developing and maintaining effective cybersecurity – finding the true signal in the noise of logged data, a constantly evolving threat landscape, and an insufficiently skilled workforce. Each of these areas requires dedicated attention and policy solutions to address and improve the resilience and security of the IT ecosystem. As illustrated by these three challenges, the modern cybersecurity reality is that even the most-skilled security operators are aways playing catch up with security risks.

The volume of data being created and shared continues to grow exponentially minute-by-minute; the threat landscape continues to evolve with the pace of technology; and at best we are providing only small-scale increases in the IT security workforce. The USG and their private sector partners need to change the game to improve the calculus for cyber operators. Advances in technology, especially AI, can be leveraged to empower a skilled workforce to focus on the most complex problems and keep pace with the most sophisticated threats.

AI, when used properly, can find the few actual threat events among the billions of logged activities any large system deals with on a daily basis. According to a recent threat intelligence survey, 84% of global business and IT leaders, are concerned that their organization is missing threats or incidents due to the high volume of alerts and data that they need to analyze.[1] AI-powered analytical tools can help identify the new and novel tactics, techniques, and behaviors of sophisticated and well-resourced adversaries. This is an especially important security use case as we must assume that malicious cyber actors will train their own AI systems to look for and exploit vulnerabilities in our defenses.

Finally, properly applying AI systems, services, and capabilities can help solve one of the biggest challenges facing the security operations workforce – the amount of time and energy that must be put into simply collecting and organizing data. The continued use of legacy systems across the USG, and other large organizations, means that the workforce in a security operations center (SOC) spends much of their time simply trying to integrate data from different, often outdated, and outmoded, systems. The repeatable and time-intensive activities of aggregating and enriching data from multiple sources adds no direct cybersecurity value, yet are essential for the operations of the SOC, and consume much of the workforce's time.[2]

AI and the Cybersecurity Workforce

Due to these three challenges, cybersecurity is no longer a human-scale problem. Advances in AI, machine learning, and other automated processes are revolutionizing how cybersecurity practitioners identify and resolve vulnerabilities and manage increasingly sophisticated threat actors.

[1] Google Cloud Blog, "Why AI: Can new tech help security solve toil, threat overload, and the talent gap," posted on Apr. 26, 2023 available at https://cloud.google.com/blog/transform/why-ai-can-new-tech-help-security-solve-toil-threat-overload-and-talent-gap. (last viewed on Jun 20, 2023)

[2] *See e.g.* blog post "Expanding our Security AI ecosystem at Security Summit 2023, posted on June 12, 2023 available at https://cloud.google.com/blog/products/identity-security/expanding-our-security-ai-ecosystem-at-security-summit-2023?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axioscodebook&stream=top. (last viewed on Jun 19, 2023)

AI-powered tools, capabilities, and services enable the analysis of massive quantities of risk data to speed response times and focus skilled security operators on the highest risk activities; thereby improving outcomes and reducing strain on the workforce. A recent Wall Street Journal article found that 75% of chief information security officers in the U.S. are experiencing burn out.[3] There is also a global cybersecurity workforce shortage of nearly 3.4 million – an all-time high.[4] Cyberattacks are being launched faster than companies can recruit and train the skilled security professionals necessary to combat these increasingly sophisticated threats.

AI technologies do not offer a silver bullet solution to cybersecurity challenges and cannot replace the value of human analysis and decision making when it comes to security operations. Rather AI technologies augment the abilities of the security workforce whose time and resources are limited. ITI member companies have identified, and currently employ, a range of AI-enabled tools to address key challenges and improve overall effectiveness of cyber solutions:

1. **Detection & Prevention**: Cybersecurity systems that leverage AI can better provide real-time analysis and prevention compared to cybersecurity systems that do not incorporate the latest technologies. Leveraging AI means detecting anomalous activity becomes faster and more accurate, improving the proactive steps that network defenders can take to identify and mitigate threats. One ITI member company takes in 36 billion security events per day and requires only 8 of those to be manually analyzed.[5] In those security events, an organization could face millions of potential Indicators of Compromise (IOC) per day, which requires security teams to have contextual awareness and visibility from across their entire environments to put their time and resources where it will have the greatest impact.

2. **Advanced Threat Response**: AI-powered capabilities allow for the automation of security recommendations and responses, streamlining security operations and allowing for human expertise to focus on the highest-risk threats. Sophisticated cyber attackers require specific responses to their unique behaviors and tactics, and AI-enabled technologies can help defenders adapt by identifying new patterns that correlate to known malicious activity.

3. **Scaling Productivity of Security Specialists**: When combined with cloud services, AI-delivered security capabilities can also help scale security efforts through continuous learning, make best-in-class security tools available to small and medium-size organizations, and keep on top of the latest vulnerability mitigations. These efficiency gains broaden the impact of security experts and operations to identify intrusions more quickly and empower network defenders to act to mitigate potential harm, without specialized domain knowledge or deep tool expertise.[6]

4. **Cost Effectiveness:** ITI member companies have identified a strong correlation between deploying AI in cybersecurity with reduced costs. One ITI member found that fully deployed security AI and

[3] Catherine Stupp, Cybersecurity Leaders Suffer Burnout as Pressures of the Job Intensify, WSJ (May 17, 2023) available at https://wsj.com/articles/cybersecurity-leaders-suffer-burnout-as-pressures-of-the-job-intensify-b0609ef1#:~:text=Seventy-three%20percent%20of%20CISOs,burnout%20in%20the%20past%20year.
[4] https://securityintelligence.com/articles/bridging-workforce-gap-cybersecurity/
[5] Palo Alto Networks, Qurater 3 Fiscal Year 2023 Earnings Call (May 23, 2023) available at https://investors.paloaltonetworks.com/static-files/70379c02-346b-493b-81c0-69ef1498b730.
[6] Google blog, Jun 13.

automation was associated with average breach costs that were $3.05 million lower than with no security AI and automation deployed, a difference of 65.2%, the largest cost savings in the study."[7] These are cost savings that can be used to address the workforce capacity issues facing both the government and large organizations.

Recommendations on AI Adoption and the Cyber Workforce

Given the beneficial impact of AI tools, capabilities, and services on an already strained cyber workforce, the following recommendations provided to the Committee will help accelerate the use and implementation of AI to improve cybersecurity outcomes.

- Consider how to leverage technology like generative AI to supplement and improve security practitioners' skills, including data analysis, in cases where automation is not helpful or appropriate.

- CISA and other federal cybersecurity policymakers should support the use of AI for cybersecurity purposes and incorporate AI systems into threat modeling and security risk management. To the extent practicable, we urge the Committee to leverage existing U.S. frameworks for assessing and mitigating AI-related risks, such as NIST's AI Risk Management and Cybersecurity Frameworks, rather than tasking the Office of Management and Budget (OMB) or other federal agencies with creating new and potentially duplicative or conflicting risk models.

- CISA should increase access to government sources of publicly available data, as appropriate, in machine-readable formats to enable access by AI tools and services. Data is fundamental to innovation in AI, and cybersecurity is no different. As network security becomes more automated, and AI manages repeatable tasks, AI will be more able to assist the human network defenders.

- Prioritize federal procurement of AI-based technologies and applications. In particular, it will be increasingly important to invest in security solutions that are aimed at countering adversarial AI attacks.

- CISA and other federal agencies should also explore funding research and development of AI systems that are resilient to manipulation by adversaries. Malicious actors use machine learning models to misinterpret inputs into the system and behave in a way that is favorable to the attacker. To produce the unexpected behavior, attackers create adversarial examples that often resemble normal inputs, but instead are meticulously optimized to break the model's performance.

- ITI member companies encourage the Committee to consider "The National Community College Cybersecurity Challenge Act," which creates a funding stream for eligible state applicants to grow and develop cybersecurity programs at community colleges, as well as to assist states in promoting educational advancement for the in-demand jobs of the cybersecurity workforce.

[7] Cost of a Data Breach Report 2022, conducted by Ponemon Institute, sponsored, and analyzed by IBM (2022) available at https://www.ibm.com/security/artificial-intelligence?mhsrc=ibmsearch_a&mhq=cybersecurity%20ai%20for%20dummies

Conclusion

We commend the Committee's focus on addressing the cybersecurity workforce and skills gap. In the constantly evolving and fast-moving technology ecosystem, the expanded use of AI will benefit both attackers and defenders. Last year, Rob Strayer, ITI's Executive Vice President of Policy, testified before this Subcommittee that, "As innovation in Artificial Intelligence (AI) continues and the technology itself evolves, it is important for policymakers to consider how to harness the benefits of AI while simultaneously addressing societal or other challenges that may emerge."[8] It is incumbent on governments and the private sector to realize and invest in AI-enabled cybersecurity services and tools to raise the cost of conducting cyberattacks and ease the workload on security professionals.

[8] Rob Strayer Executive Vice President of Policy Information Technology Industry Council (ITI) before the U.S. House Committee on Homeland Security Subcommittee on Cyber, Infrastructure Protection & Innovation on June 22, 2022 on a hearing entitled, "Securing the Future: Harnessing the Potential of Emerging Technologies while Mitigating Security Risks." Available at https://www.itic.org/documents/cybersecurity/20220622ITIHouseHomelandCmteTestimonyonEmergingTechandCyber.pdf