AI for Cybersecurity

Ensuring Cyber Defenders Can Leverage AI to Protect Customers and Citizens

Cybersecurity helps businesses and government agencies serve customers and citizens securely, and artificial intelligence (AI) for cybersecurity makes this more effective and efficient. Governments around the world are focused on developing AI policies that mitigate risks and maximize benefits of AI. Using AI tools for cybersecurity should be a top priority for policymakers.

Malicious Actors Are on the March

Malicious actors are increasing the frequency and impact of their attacks. Consensus among experts is that this trend may continue as they use AI systems to enhance their attacks. For example, malicious actors are already using AI to:

- Improve social engineering attacks (for example, by enabling voice synthesis to simulate the voice of a person trusted by the malicious actor's target);
- Generate fake data or alter existing data (for example, by creating fake social media accounts or generating fake video or audio);
- Evade security measures (for example, by varying behavior to make it harder for security systems to detect anomalies);
- Create more effective malware (for example, by automating malware generation, vulnerability identification, and exploitation; building in detection evasion techniques; and automating propagation); and
- Improve brute-force attacks (for example, by automating the process of guessing passwords).

Enabling cyber defenders to use AI for cybersecurity can defend against these attacks.

Cyber Defenders Need AI for Cybersecurity

Enterprise software companies are increasingly investing in AI solutions for cybersecurity.

These companies are already using AI for cybersecurity, including to:

- **Develop more secure code.** Companies use AI to improve both static and dynamic analysis tools to detect potentially vulnerable code during development.
- **Detect threats and respond.** Companies use AI to quickly identify anomalies across their networks, endpoints, and cloud environments to help defenders detect and respond to malicious activity.
- **Protect against malware.** Companies use AI to detect and block known and unknown malware. AI-powered systems can analyze file attributes, system, and user behaviors, and use cloud-based threat intelligence to block known and emerging threats.
- **Detect and prioritize vulnerabilities.** Companies use AI to automate vulnerability assessments and prioritize remediation activities, helping security teams remediate the most critical vulnerabilities first.

Policymakers should promote using AI to bolster cybersecurity, which can be done while ensuring appropriate regulation around its high-risk uses.

- **Protect against email-based threats.** Companies use AI to enhance email security by analyzing emails, attachments, and user behavior to block phishing attempts, malicious links, and other email-based threats.
- **Improve identity management.** Companies use AI to strengthen identity and access management systems by, for example, detecting suspicious sign-in attempts or compromised user accounts. They also use AI to improve authentication solutions like facial recognition and other biometric solutions.
- **Analyze user behavior.** Companies use AI to create profiles that establish a baseline of normal activity. This helps defenders identify deviations that suggest an account may be compromised or that an insider threat may exist.
- **Generate threat intelligence.** Companies use AI to process vast amounts of unstructured data, including research papers, security reports, and news articles, to help prepare for emerging threats and provide context and insights to enable more informed decision making.
- **Ease the cyber workforce gap.** Companies use AI, including generative AI, to provide contextual insights and recommendations to defenders.

Policymakers should proactively promote using AI, and the innovative technologies it depends on such as cloud computing, to bolster cybersecurity, which can be done without compromising efforts to protect citizens from potential risks.

Policymakers Can Both Protect Citizens and Improve Cybersecurity

Policymakers should promote using AI to bolster cybersecurity, which can be done while ensuring appropriate regulation around its high-risk uses. As the importance of AI for cybersecurity increases, it is also critical that laws and policies improve security, and security is not used as a justification for other political or protectionist objectives.

BSA SUPPORTS LAWS AND POLICIES THAT:

Use Risk-Based Frameworks

Policymakers should require developers and deployers of AI intended for high-risk uses to establish risk management programs and conduct impact assessments to mitigate those risks.

Enable Cybersecurity Innovation

Policymakers should promote using AI as a key cyber defense tool.

Protect Data Transfers

Policymakers should enable data flows needed to analyze normal behavior and detect malicious behavior. The ability for data to move across borders helps to deliver the best cybersecurity outcomes.

Harmonize Laws and Policies

Policymakers should work with like-minded countries in a globally coordinated effort to ensure laws and policies advance the ability for cyber defenders to use AI for cybersecurity. This coordination should aim to harmonize rules across policy domains, such as cybersecurity and privacy, and leverage or develop internationally recognized standards where appropriate.

We Can Create a More Secure World With AI for Cybersecurity

We are still writing the story of how AI, with appropriate safeguards, will improve the lives of individuals and communities. Citizens, industry, and governments undertake this work while malicious actors continue to use AI—like other tools—for nefarious purposes.

We must address challenges associated with high-risk uses of AI systems while promoting AI for cybersecurity.