PUBLIC
TECHNOLOGY
INSTITUTE
A DIVISION OF FUSION LEARNING PARTNERS

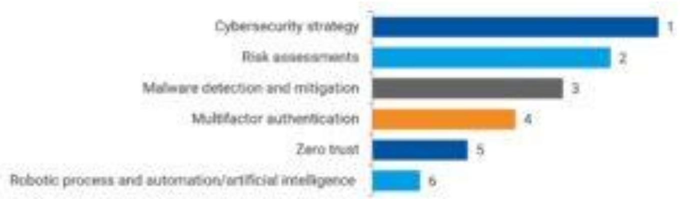
Best Practice Brief:

HOW AI CAN ASSIST CITIES AND COUNTIES WITH CYBERSECURITY

The Public Technology Institute's *2023 Local Government Cybersecurity National Survey* was just released. Based on past years results, there were few surprises but continued reassurance that cybersecurity continues to remain the top focus of all local governments. The survey asked about financial support, where 64 percent reported that cyber budgets were inadequate. Only 36 percent felt their cybersecurity budgets were adequate.

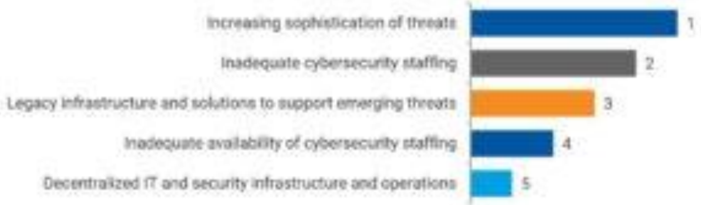
The good news is that 55 percent reported an increase over last year, but a disturbing 7 percent reported financial support for cyber went down. Of the following activities, respondents were asked to rank the priority initiatives for the next twelve months.

Of the following activities, please rank the priority initiatives for the next 12 months.



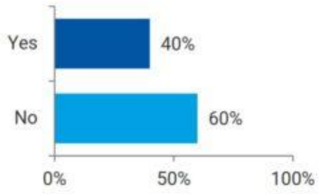
When it comes to the obstacles local governments face when it comes to cybersecurity, one can see a clear picture of the headwinds they face.

Of the following, please rank the barriers that you believe your organization faces to address cybersecurity challenges.



This year a new question was added, “Are you turning more to vendors that utilize AI solutions for cybersecurity support?” While AI has been around for many years, it appears interest in AI and cybersecurity has reached renewed and heightened interest, 40 percent responded with a “yes.”

Are you turning more to vendors that utilize AI solutions for cybersecurity support?



Of course, like all entities of government, much of any pivot to AI cybersecurity tools are wholly dependent on the vendor and managed service provider community offerings. So, when one considers the many challenges of sustainable cybersecurity budgets, staff training, retention and recruitment, automation becomes increasingly important.

AI certainly holds great promise when one considers that AI systems are 24/7, they never sleep or go on vacation, AI is superior at finding patterns and anomalies in milliseconds as opposed to days or weeks. Despite the noted advantages many local government tech leaders remain uncertain about what is either possible or even available. So, the timely question of the day is, how can AI assist in cybersecurity operations aimed at protecting our cities and counties? Realistically, local governments can use AI in cybersecurity to enhance or supplement their ability to protect sensitive data, infrastructure, and systems from cyber threats. So exactly how can AI assist local governments? Here are several ways in which AI can be leveraged for cybersecurity in the context of local governments:

1. Threat detection and analysis

AI can analyze network traffic patterns and detect anomalies that may indicate unauthorized access or suspicious activities.

2. Behavioral analytics

AI can monitor user and system behavior to identify deviations from normal patterns, helping to detect insider threats and advanced persistent threats (APTs).

3. Malware detection

AI-powered antivirus solutions can recognize and quarantine malware, including new and previously unknown variants.

4. Predictive analytics

AI can analyze historical data to predict potential future cyber threats and vulnerabilities, allowing local governments to proactively address security weaknesses.

5. Vulnerability assessment

AI can automate vulnerability scanning and assessment, identifying weaknesses in software, systems and configurations that need to be patched or updated.

6. Threat intelligence

AI can gather and analyze threat intelligence from various sources to provide local governments with real-time information about emerging threats and vulnerabilities.

7. Security automation and orchestration

AI-driven automation can streamline incident response by automatically containing and mitigating threats, reducing the workload on cybersecurity teams.

8. User and entity behavior analytics (UEBA)

AI can analyze user and entity behavior to detect anomalies that may indicate compromised accounts or insider threats.

9. Phishing detection

AI can help identify phishing emails and malicious links, reducing the risk of employees falling victim to phishing attacks

10. Security monitoring and alerts

AI can continuously monitor logs, events and network traffic to provide real-time alerts and notifications when suspicious activities are detected.

11. Threat hunting

AI can assist in threat hunting by identifying hidden threats within an organization’s network and data.

12. Incident response

AI can aid in incident response by providing recommendations on how to contain and mitigate security incidents more effectively.

13. Access control and identity management

AI can enhance access control mechanisms by analyzing user behavior and adjusting access privileges accordingly.

14. Compliance monitoring

AI can help local governments ensure compliance with cybersecurity regulations and standards by continuously monitoring and reporting on security posture.

15. Security awareness training

AI-driven tools can help provide personalized and interactive cybersecurity training to local government employees, improving their ability to recognize and respond to threats.

While it's important for local governments to consider the specific needs, resources and regulatory requirements of their jurisdiction, it becomes more challenging when it comes to AI and cybersecurity. Experts agree that in considering AI in any application, strong data privacy and ethical considerations must be considered to ensure responsible and secure AI implementation. And as appealing as many of the AI applications are, many worry about the potential for over dependency on automation—AI in particular. Hopefully, AI adoption in cybersecurity programs and services will be viewed as supplemental and at the same time emphasizing the importance of human leadership as being ultimately responsible and in control.

As local governments battle the likes of cyber-criminals and nation-states, there is a growing concern that AI can also be used *against* each of the tools governments use in cyber protection. Not only must humans remain actively in-charge, they must also be ready to continuously upgrade their digital infrastructure and seek new tools as weapons against any cyber-attacks. It is easy to foresee the greater sophistication of attacks, let alone their frequency. As has been said many times, local government must get it right all the time—but the bad guys only need to succeed once.

Dr. Alan R. Shark is the executive director for the Public Technology Institute (PTI), a division of Fusion Learning Partners; and associate professor for the Schar School of Policy and Government, George Mason University, where he is an affiliate faculty member at the Center for Advancing Human-Machine Partnership (CAHMP). Shark is a fellow of the National Academy of Public Administration and co-chair of the Standing Panel on Technology Leadership. Shark also hosts the bi-monthly podcast Sharkbytes.net. Dr. Shark acknowledges collaboration with generative AI in developing some articles. This first appeared on americancityandcounty.com in November 2023