A CENTER FOR DIGITAL GOVERNMENT ISSUE BRIEF

CENTER FOR
DIGITAL
GOVERNMENT

How Local Governments Can **Get Ahead** of Their Threat Opponents

Agencies of all sizes, in every discipline, and at all levels of government have at least one thing in common: they're facing a large and growing cybersecurity threat landscape. Government entities are vulnerable to a multitude of attacks, including hacking, ransomware and distributed denial-of-service.

Many agencies are simply unprepared to defend themselves against these assaults on their own. There are two important questions organizations need to address: How do they know when they need help, and how can they determine the best cybersecurity partner? Once agencies have selected a partner, a key to success is knowing how to measure the value added from such a relationship.

Organizations are Under Attack

The cybersecurity attack surface has grown considerably in recent years, and government agencies are among the biggest targets of bad actors.

Many employees continue to work from home at least part of the time, as the hybrid work model becomes more common. Oftentimes workers use their own devices rather than those sanctioned by the IT department. The lack of visibility and sufficient security on devices or network connections gives attackers new opportunities to penetrate systems.

Incidents such as ransomware and distributed denial-of-service are on the rise. Workers and managers are also increasingly vulnerable to phishing and malware attacks. Furthermore, the shift to cloud services can give cybercriminals additional opportunities to gain access to systems and data.

"Information could be leaked that is proprietary or sensitive, involves financial information or contains content that a threat actor could use for identity theft," says Rex Johnson, director and practice leader of cybersecurity consulting services at Computer Aid Inc. (CAI). "That's a large area of risk for an agency to mitigate."

Defenses are Lacking

Even as they face this array of threats, a lot of government agencies that operate with limited budgets and resources are simply not prepared to defend themselves against increasingly sophisticated attacks.

Many public sector organizations at the local level do not have the budget to create sufficient security teams and invest in the latest tools to detect and stop attacks. Agencies must compete for cybersecurity talent against private sector businesses that in many cases have more resources.

Government entities are vulnerable to a multitude of attacks, including hacking, ransomware and distributed denial-of-service.

Organizations can’t just assume a security partner will deliver on all its promises and provide the expected value from the relationship.

“With over 300,000 open cybersecurity jobs nationwide, many smaller agencies do not have mature cybersecurity programs in place,” says Frank Ury, senior client executive at CAI and a director of the Santa Margarita Water District Board in Rancho Santa Margarita, Calif. “Bad actors recognize these agencies’ vulnerability, and therefore are likely to make them targets for attack.”

What’s particularly concerning is attackers can be present within agency systems for a substantial amount of time before they are detected. This gives them the opportunity to learn about vulnerabilities and enables them to gain access to and steal more data.

Even among agencies with adequate security programs, there is oftentimes a sense of complacency about security.

“But every agency is vulnerable, regardless of the financial resources,” Ury says.

How to Know When Help is Needed

Agencies need to conduct an honest assessment of their existing security programs and be on the alert for signs they need to bring in outside expertise to bolster their defenses.

One of the best ways to determine if an organization needs help to address cyber risk is to conduct a readiness or current-state assessment, Johnson says. With such an assessment, a government agency can identify what it is doing well and where it needs help.

“Make sure it’s an objective assessment from someone who’s qualified to understand their business and how government works,” Johnson says.

Aside from an assessment, a sure-fire way to know that assistance is needed is a steady increase in the frequency of attacks such as ransomware. This is a clear sign that the current security program — tools as well as procedures — may be failing to protect systems and data.

The lack of a coherent incident response plan or procedures for dealing with breaches is another indicator of a need for improvement.

Choosing the Right Partner

Once a government organization determines that it needs outside expertise for help with securing its infrastructure, it must decide which partner is the best fit.

One important attribute of a service provider is extensive experience, not only in cybersecurity but in the particular areas in which the agency is focused. For example, if a government entity is involved in healthcare services, the partner should have knowledge of healthcare issues, regulations, threats, etc.

The ability to customize services is also vital. An agency needs a partner that can provide exactly what it needs in the way of protection. This includes understanding the specific systems the agency has in place and the potential security issues and vulnerabilities.

“Even though there are security frameworks, there really is no cookie-cutter approach to cybersecurity,” Johnson says. “Organizations need to consider their operational needs and how to protect their most critical information and assets. It is not the same for everyone.”

Of course, the partner also needs to meet the budget requirements of the agency. This is especially important for small, local agencies with limited resources.

Getting the Most Value from a Partnership

Organizations can’t just assume a security partner will deliver on all its promises and provide the expected value from the relationship.

A partner should be willing and able to sit down with agency leadership, as well as IT and security executives, and discuss security strategy and how to build a roadmap to carry out the strategy over a given time period, Ury says.

Priorities should be set, so the most pressing risks are addressed first and less important issues are dealt with at a later time. This way, agencies can deal with and mitigate the truly urgent risks right away rather than use up resources on multiple projects at the same time.

An agency and its partner should create and implement a cybersecurity strategy within the context of the budget requirements of the agency. If all goes well with a security partnership, the agency should be able to significantly increase its level of cybersecurity maturity over time.

This paper was written and produced by the Center for Digital Government, with information and input from CAI.

CLICK HERE to arrange a meeting with CAI cybersecurity experts. Or, you can reach Rex via email at Rex.Johnson@cai.io.

Produced by: CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com**.

For: CAI

About Rex Johnson, Director and Practice Leader — Cybersecurity
Rex has over 30 years of senior level management experience encompassing IT, cybersecurity, privacy, digital forensics and analysis, and enterprise risk management. He is a frequent speaker on cybersecurity addressing national and international audiences with Gartner, Secure World, and the Information Systems Audit and Control Association.

About CAI
CAI is a leading business technology services firm committed to helping private and public organizations drive value, improve productivity, and enhance customer experience. The firm specializes in digital transformation services, including application management, strategy and consulting, intelligent automation, contingent workforce solutions, IT service management and business analytics. **CLICK HERE** to learn more about CAI.

IMAGE PROVIDED BY SHUTTERSTOCK.COM