ARCTIC WOLF

BRIEF

Securing Digital Transformation in Local Government

Are Local Governments Protecting Citizen Data?

44%

The percentage of local governments that said they experience cyberattacks on a daily basis.

40%

The percentage of local governments that have no idea if or when they've been breached

71%

The percentage of local governments that don't provide cybersecurity awareness training

— 2016 Survey by the International City/County Management Association

Today's news is filled with stories on the latest major corporations and federal bureaucracies that have suffered data breaches. But while big-name companies and organizations are the ones that get all the headlines, cyberattacks are an everyday occurrence for local governments around the country. In fact, according to a survey by the International City/County Management Association, 44% of local governments said that they experience cyberattacks on a daily basis.

From the largest state and county departments to the smallest local jurisdictions, local government systems contain the valuable citizen data they need to provide necessary services. Such data includes tax information, social security numbers, passwords, and credit card numbers.

In addition, the strained resources of local governments often means that their cybersecurity investments fall woefully behind those of similar-sized private businesses. Siloed departments, a bureaucratic structure, and departmental sprawl all make it challenging to provide adequate protection.

As digital transformation drives local governments to deliver more services online through hyper-connected, cloud-based internal systems, this increases their threat exposure. Combine a valuable target, relatively weak defenses, and an ever-increasing amount of entry points to attack, and it's not hard to see why local governments are in the crosshairs. Whether the goal is to steal information, stage a ransomware attack, or just cause chaos, hackers view local governments as an easy target.

The Need to Understand Risk

While some local governments recognize the cyber risk they face, they often struggle to gather the information they need to form an effective response when called upon. According to the survey, more than 50% of local governments don't track how often their systems are targeted for attack, while 40% don't even track how often they are breached. In addition, 58% of local governments said they lack the ability to determine what types of attackers are going after their systems.

Without knowing who is attacking, if the attacks are successful, and how they themselves respond, many local governments simply lack the ability to formulate and execute an effective cybersecurity strategy required to protect citizen data.

> Governments say they lack the cybersecurity expertise on staff to adequately defend cyberthreats.
>
> — 2016 Survey by the International City/County Management Association

A Lack of Cybersecurity Expertise

Local governments experience the same cybersecurity skills gap that even the largest enterprises struggle to overcome. While there's a growing threat of cyberattacks in both the private and public sector, there just aren't enough cybersecurity experts to go around.

What's more, there are many constraints that limit the ability of local governments to effectively compete for top cybersecurity talent, and most of them have to do with money. The local governments surveyed listed the inability to pay competitive salaries (58%), an insufficient number of staff (53%), a lack of funds (52%), and a lack of adequately trained personnel (31%) as the top reasons why they can't practice better cybersecurity.

This lack of funding reflects a lack of priorities from decision-making officials. More than two-thirds of elected officials aren't sufficiently aware of the need for cybersecurity, while a lack of support from top elected and appointed officials is cited by more than three-quarters of respondents to explain why their local governments don't practice better cybersecurity. Since these are the people who control the purse strings and the agenda, cybersecurity initiatives invariably fall to the bottom of the list when compared to more visible needs like education, road repair, and emergency services.

And if you think the citizenry is going to spark change, think again: 71% of local governments surveyed don't provide cybersecurity awareness training for their constituents. Without voter awareness, local government officials often only make a commitment to cybersecurity after an attack is reported and all over the local news.

How Can Local Governments Regain Control?

Local government officials and their IT staffs need to work together if they want to avoid becoming the next Atlanta, Allentown, Colorado DOT, or Baltimore. Since digital transformation means more and more devices and services will be connected in coming years, employees, administrators, elected officials, and even citizens and local media need to ensure that cybersecurity is a foundation of their government's digital planning instead of something only considered an obligatory burden.

To get ahead of future cybersecurity threats, local governments need to execute a three-pronged approach:

1. Outsource expertise

Local governments can overcome a lack of internal know-how by working with third-party providers who provide cybersecurity services. These vendors work with organizations of all sizes, and can bring best practices to the table more easily than the internal, under-trained and overwhelmed IT staffs that make up most local government offices.

2. Prioritize knowledge

Local governments must improve their ability to monitor, detect and respond to attacks. The more information they have about their risk, the more it will become a priority for relevant decision makers.

3. Take advantage of a SOC-as-a-service

A local government can achieve the same cybersecurity protection as even the most sophisticated businesses by using a managed security operations center (SOC) that combines the best of these first two approaches. A cybersecurity strategy augmented with SOC-as-a-service can be just what your local government needs to protect its systems and citizens from attack. Arctic Wolf's SOC-as-a-service combines the human expertise of security engineers and analysts with machine intelligence to extend and augment the capabilities of your local government's IT team.

Download our guide to SOC-as-a-service to learn how it can help you implement the most essential elements of modern security.

ARCTIC WOLF

arcticwolf.com

©2019 Arctic Wolf Networks, Inc. All rights reserved. Arctic Wolf Networks, AWN and the Arctic Wolf Networks logo are trademarks of Arctic Wolf Networks, Inc. in the United States and/or other jurisdictions. Other names used in this document are for identification purposes only and may be trademarks of their respective owners.

Contact Us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com