THE ATLAS

3 Strategies Local Governments Should Implement to Help Create a Comprehensive Cybersecurity Culture in 2023

Presented by: COMCAST BUSINESS

Introduction

Local government IT leaders often face expectations from leadership to create a robust cybersecurity environment. Of course, no local government (or any organization) will ever be 100% risk-free, largely in part to the human element. How can local IT leaders set realistic expectations around reducing the risk profile, while creating a security-first culture in their organizations?

The Atlas hosted a roundtable discussion with nine local government IT leaders to hear about the biggest cybersecurity priorities they faced in 2022, and how those lessons learned are shaping their 2023 strategies to build a more comprehensive culture of cyber-awareness and security in their organizations.

LOOKING BACK

Top Cybersecurity Threats in 2022

1. The Log4j vulnerability - where the Log4j library could accept log events from external sources and potential attackers - set the scene in early 2022 for local governments to patch vulnerabilities and evaluate their risk profiles.

2. The Russia-Ukraine war spurred CISA's **Shields-Up guidance**, driving vulnerability management efforts across all levels of government. Local governments have also been responding to ransomware attacks like BlackCat, Lockbit and Hive. Many organizations leveraged those efforts to shift priorities from bringing on new capabilities to more "tightening the ship" efforts throughout the year.

3. Misconfigured cloud posed another threat to local governments - from IT departments onboarding cloud services from vendors to continuing to secure the cloud amidst the work from home shift. Balancing the capacity to address cloud misconfigurations with other city-wide cyber priorities, (i.e. building city-wide data centers) left many IT teams facing network vulnerabilities. Cloud continues to be a big priority going into 2023, as nearly every attendee in the roundtable discussion cited cloud migration as an ongoing task.

The cyber threats that emerged last year presented multiple opportunities for IT leaders to educate the teams not typically involved in cybersecurity activities. IT departments are continuing to leverage that momentum going into 2023, having identified the ways they can lead their organizations into a security-first culture.

LOOKING AHEAD

Creating the Cybersecurity Culture-Shift

Going into 2023, local government leaders named some notable shifts that they're implementing in order to build a security-first culture in their organizations.

1. Educating End Users

The best way to account for the human element is to educate end users on cybersecurity risks. Many organizations are using phishing test software to run phishing simulations across the organization and use the results to tailor education materials based on specific vulnerabilities that regularly emerge. While these tests are an effective way to identify cyber weaknesses, some end users respond poorly to the "gotcha" nature of the tests. In order to mitigate that, IT departments are fostering a "we're all in this together," culture when it comes to training and cybersecurity awareness. Furthermore, educating staff members on cybersecurity in the workplace teaches them transferable skills when it comes to recognizing cyber threats in their personal lives (i.e. banking, insurance, delivery scams). Creating this kind of comprehensive training environment can help build trust from end users.

When it comes to creating training materials for end user education, pooling resources from other local IT professionals responsible for bringing cybersecurity into their organizations can help. For example, Colorado's **Whole of State** plan accelerates information sharing across jurisdictions and reduces duplicative efforts for training on state-wide goals.

2. Positioning IT as the "Department of Yes" vs. the "Department of No"

A challenge that IT departments know all too well is when other departments buy and onboard new technology without first consulting IT. These types of shadow IT activities often lead to IT saying "no" to seemingly great new technologies and services. To mitigate this, many IT leaders are implementing processes to reposition themselves as a "Department of Yes." This can look like creating checklists with procurement departments to get IT sign-off on any new technologies or products that may seemingly not have any IT element to them. Being involved at the beginning of the procurement processes help IT departments to understand the priorities of different departments across the organization and provides the opportunity to give their expertise ahead of the curve, instead of being consulted retroactively.

3. Building Risk Assessment into Processes

To mitigate ongoing security threats, particularly around ransomware, local governments are coordinating with jurisdictional partners, such as the state, divisions of the Department of Homeland Security, CISA and the FBI to communicate any activity. Even with these communications in place, organizations are still trying to put solutions in place, such as a network detection and response (NDR) and endpoint detection and response (EDR).

Aside from communication processes, local IT departments are prioritizing building risk assessment into processes for onboarding new solutions or products. One state county, for example, developed an IT cybersecurity charter program to work with different stakeholders across the organization and try to align their purchases with IT security initiatives. They not only developed a risk assessment to assess different vendors, but also a technical assessment review that could go in hand with an RFQ, RFP or RFI. The technical assessment allows them to know whether a vendor will be working with certain types of data in order to mitigate risk ahead of time.

Learn more about how Comcast Business is working with communities to foster cultures of cybersecurity.

This resource summarizes a closed roundtable discussion with local government leaders that took place on January 25, 2023. Views expressed by the participants are their own and do not imply an endorsement of the views or of the entity they represent. In addition, reference to any specific solution or entity does not constitute an endorsement or recommendation by Comcast Business.