FEDInsider

Municipalities Are Making Identity the New Security Perimeter

Inside a California city's shift from reactive defense to zero trust resilience after a major cyber incident

In today's public sector environment, a cybersecurity incident is no longer just a technical disruption; it's a defining moment for organizational resilience and public trust. That's why municipalities are beginning to treat identity as the new perimeter. During a recent FedInsider webinar, government and industry leaders explored how municipalities can move beyond reactive defense toward a more proactive, identity-centered security strategy.

Using the City of Fullerton, California, as a real-world case study, the discussion highlighted how one local government navigated a significant security event and used it as a catalyst to modernize its entire IT environment, and how Fullerton's experience offers a practical roadmap for moving forward. By prioritizing identity, investing in zero trust principles, and aligning technology with people and processes, the city transformed its posture from recovery to resilience.

The Attack and its Impact

In 2019, the City of Fullerton, California, experienced an "unintended disclosure" by way of a ransomware attack. "It was big enough that it got really everyone's attention, and it was made public," said Marty Miller, CIO and vice president of professional services at Glass Box Technology.

After identifying and addressing the immediate threat, leaders in the city — including the city council, mayor, city manager and chief of police — began investigating the attack and analyzing the systems and processes that ultimately failed.

The security review revealed identity was an issue, and prevention going forward was key. The city turned to Glass Box Technology in November 2019 for further assessment and future planning. Shortly after, the COVID-19 pandemic hit, and the standard IT and network model changed. People weren't just accessing data and applications on-site with a single device; they were accessing them at home with multiple devices.

By that point, the city was already implementing the security platform Okta for workforce identity, which was a critical step. "We previously had less than one dozen people who had VPN access, and now we had 500 who needed to have remote access," Miller said. Okta helped with this, especially as the city realized the value of a zero trust framework.

The city also determined that phone-based verification and simple password resets would no longer provide the type of assurance it needed. Considering the number of employees and contractors employed by the city, and the number of devices connecting to its network remotely, having identity locked in for those actively working for the city was crucial.

Still, this wasn't a single implementation solution fix. In response to the breach, big changes happened in a very short time, said Aaron Fry, CTO of managed services for Glass Box Technology and CTO for the City of Fullerton — but these are ongoing solutions.

"The threat landscape evolves, and how we run the department and run the environment has to evolve with it," Fry said. The city had to remain consistent and implement to scale. "Identity is part of the core foundation, not something that was bolted on or added on, but part of the foundation that has been part of the growth journey," Fry said.

Featured Experts:

- **Eddie Manfro**
  City Manager,
  Fullerton, California

- **Aaron Fry**
  CTO, Managed Services,
  Glass Box Technologies
  & CTO, City of Fullerton

- **Marty Miller**
  CIO & Vice President, Professional Services,
  Glass Box Technology

- **Morgan Reed**
  Field CTO,
  Okta

carahsoft | GLASS BOX TECHNOLOGY | okta

Recovering and Scaling

At the core of the city's response was going back to IT basics: people, processes and technology. When a tool finds an anomaly and generates an alert, the right people must be able to identify and respond to it. Similarly, identifying the risk is only useful if there is a clear process to regularly review the discovered vulnerabilities, prioritize them and actively resolve them. "The partnership with Glass Box and Okta made that possible as the organization continued to grow and their security continued to improve," Fry said.

The city implemented adaptive multi-factor authentication and MSA to seamlessly identify and confirm trusted devices on the network, making security as transparent for the user as possible. Over 170 applications have also been integrated into the city's new identity platform, establishing a framework of assurance so the right people have access only to the systems they need, on-site or remotely.

"Having those things in place improves visibility, shrinks the attack surface and supports faster decision-making and response for the overall process when something does come up," Fry said.

The city also integrated a physical access system for human resources to make onboarding and offboarding more accurate and efficient, which was initially a challenge. Eddie Manfro, city manager for the City of Fullerton, said he helped employees with their hesitancy to embrace new technology and ways of doing business while leveraging Glass Box Technology after the attack.

"The city is kind of a collection of dissimilar organizations," Manfro said. "You have all of these organizational silos." The city had several independent IT systems loosely connected to central IT, and connecting security to the HR process was necessary to enroll employees and contractors in those new identity tools.

"Now, when we have someone go out on a leave of absence, they are immediately disconnected from the city because we have centralized the process through HR with IT integration," Manfro said.

Defense and Prevention

Establishing strong identity security and adopting a zero trust framework are some of the ways the City of Fullerton is strengthening its security posture for the future, especially by managing device access and connectivity through Okta.

"It really helps to whittle down the number of opportunities for threat actors to work against your environment and breach it," Miller said.

Moving forward, the city is aligning with NIST frameworks and focusing on refinement and automation to make security both stronger and easier to implement. Scaling the HR-driven workflow processes from full-time employees to all types of staff or contractors, for example, is in the works.

And according to Fry, the city is also exploring biometrics as an authentication option. Other initiatives currently in the pilot phase include business email compromise protection and implementing a data loss prevention strategy.

Municipalities Are Shifting From Disaster Recovery to Business Continuity

As proven by the City of Fullerton, technology isn't the only piece at play – people and leadership have a major role in security. "Technology works, but getting the people aspect right is critical," said Morgan Reed, distinguished strategic advisor for state and local governments at Okta.

Since the incident in Fullerton, Reed has noticed a shift in organizations from reactive, IT-centric approaches to a proactive, organizational approach. "Five years ago, cybersecurity was an IT department problem focused on defending against basic threats. And today, it is understood as a core leadership responsibility for maintaining continuity of public services and the trust of citizens," Reed said.

The threat landscape is highly sophisticated, and threat actors can shut down a city's infrastructure, so thinking about citizen trust and transitioning from defense to resilience is key. Preventing the breach isn't enough – organizations must have the processes and solutions in place to recover quickly and continue serving the public when an incident occurs.

Responsibility for digital security is no longer reserved for the CIO or the IT team; it is a shared responsibility from the mayor's office down to every single municipal employee.

"The path forward is cultural, and most successful cities are now fostering a culture of security," Reed said. "That includes continuous employee training, adopting modern security principles like zero trust, being transparent with the public and building up and maintaining trust."

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016
(202) 237-0300
Info@FedInsider.com
FedInsider.com
Facebook.com/FedInsiderNews
Linkedin.com/company/FedInsider
@FedInsider

Carahsoft
11493 Sunset Hills Road, Suite 100
Reston, VA 20190
(703) 871-8500
Oktasled@Carahsoft.com
Carahsoft.com
Facebook.com/Carahsoft
Linkedin.com/company/Carahsoft
@Carahsoft

GlassBox Technology
2855 Camino Serbal
Carlsbad, CA 92009
Contact: **Katherine Karampour**
(949) 771-4109
Info@GBoxTech.com
GBoxTech.com
Linkedin.com/company/GlassBoxTechnology

Okta
100 First Street, 6th Floor
San Francisco, CA 94105
(800) 588-1656
Oktasled@Carahsoft.com
Okta.com
Facebook.com/Okta
Linkedin.com/company/Okta
@Okta