Managing Cyber Exposure in Law Enforcement

As IT plays an increasingly critical role in crime-fighting and public safety, law enforcement agencies are facing new cybersecurity challenges. ***Michael Rothschild,*** *Senior Director of Marketing for Tenable, shares advice for protecting data and resources even as the cybercrime landscape expands and evolves.*

What trends are you seeing around threats and vulnerabilities within law enforcement agencies?

We are seeing more ransomware attacks, where hackers use an unaddressed vulnerability to gain entry and then lock law enforcement files until payment is made. These demanded payments are cleverly set at an amount that makes the attack worthwhile for the hacker but cost-effective enough that the municipality will agree to pay to get its data back.

What are the biggest cybersecurity challenges for law enforcement agencies?

A law enforcement agency can face a variety of issues. It may need to address issues related to who has access to what information based on their role. It may need to segment its network — for example, to separate CJIS lookups from other areas that are open to the public. Law enforcement organizations may also be connected to other municipal departments such as the Department of Public Works or even other departments outside the municipality. Addressing these potential attack vectors requires security expertise, which in many cases is not on the agency's priority list or in its budget. As a result, these agencies become even more susceptible to attack.

What is cyber exposure management and how can it help law enforcement agencies protect their systems and data?

Whether it is CJIS, digital fingerprinting, NCIC lookups, e-tickets or e-reports, paper is a thing of the past. Technology is making these departments more efficient and effective in carrying out their missions, but it can also add exposure from a cyber risk perspective. Therefore, it is important that law enforcement agencies roll out their new technology with security built in instead of adding it as an afterthought. It is also important to regularly assess security policies and technologies to detect vulnerabilities and threats before an attack occurs. Doing so will help ensure successful alignment with the agency's core mission without introducing potential threats and attack vectors.

How can organizations best protect data that is accessed or shared from mobile devices?

There is much in the way of security technology that helps accomplish this. Some of the base systems are spelled out in compliance regulations. The technologies include encryption, access control, physical security and more. Agencies should work with partners that have expertise in both technology and law enforcement to ensure they are compliant, secured and compatible with new regulations and threats both now and in the future.

What best practices do you recommend in terms of risk and vulnerability management?

Because the security environment is in constant flux and new vulnerabilities regularly arise, we recommend ongoing assessments that can find new weak points before they are exploited. We also recommend a "triaged" approach to deal with these alarms or concerns, because it is impossible to meaningfully handle multiple alarms at the same time. Taking a risk-based view and having the system assign a vulnerability priority rating (VPR) score that is specific to the threat in your unique environment will help you meaningfully address threats in an appropriate order to keep your agency safe.

With looming budget cuts, how can law enforcement agencies invest strategically to transform cybersecurity?

No single product can definitively and magically deliver security. Instead, security requires different best-in-class products to deliver solutions to specific challenges. As mentioned before, these solutions include encryption, vulnerability management, access control and more. The magic happens when these products work together to deliver a security-in-depth solution where the combined and fully integrated solution working together delivers more than the sum of its parts. This yields a strong security posture with a compelling ROI that moves the needle without bankrupting the budget.