Intelligent, Ubiquitous Security

Protecting endpoints and personally identifiable information across the enterprise is no longer a job for siloed devices and cybersecurity staff working alone. ***Tony Lee,*** *vice president of global services technical operations for Blackberry, explains how AI-enabled security and automation will help state and local governments address the cybersecurity challenges of today and tomorrow.*

What cybersecurity challenges do you see as government organizations move forward on remote work?

Before the pandemic, most organizations had some understanding of their organizational boundary and the footprint of their remote workforce. Now, the increased need for "work from anywhere" and "bring your own anything" across a larger set of roles has blurred the traditional organizational boundary. Suddenly we need to secure a larger variety of devices located farther away from IT staff — while still ensuring operational excellence. As organizations expand work-from-home options, the IT department must support a flexible, virtual, and secure workforce.

What should governments keep in mind about cybersecurity strategy?

While individuals can control what companies they reward with their business, they have little control over which government agencies receive their personal information. The public is tired of government and private sector organizations compromising their personal information. It takes years to build a sterling reputation and a few unfortunate clicks to tarnish it. The largest U.S. government data breaches have affected millions of people — this is unacceptable.

How can organizations secure end users, devices and other endpoints regardless of their location?

Organizations need prevention and visibility on the endpoints themselves because these devices are in varying risk environments and will eventually be connected to the network, if they aren't already. Very few sizable breaches occur without accessing or compromising an endpoint. Organizations should focus on prevention first and then visibility because the value of visibility lessens if you don't have the resources to act on what you see. Preventing an attack early is far less expensive and time-consuming than stopping it later. Organizations need to apply a uniform Zero Trust defense strategy across all devices — mobile included — and personnel.

Discuss the role of AI and ML in keeping up with evolving threats.

AI and ML need to be treated as force multipliers that compensate for a cyber-security skills shortage. This technology augments our human workforce and takes over an increasing number of tasks as the models become smarter. AI-based defenses are becoming more predictive as the models witness and train on a wide variety of attacks. Unless extremely novel attacks occur, the models should be able to recognize an attack and know how to act without specifically being told. This AI augmentation frees up personnel to focus on strategic security initiatives designed to defend against more advanced threat actors and targeted novel attacks.

How can organizations evaluate their security practices, adjust course and plan for sustainability?

Enlist the help of expert consultants. Although there's an upfront cost, their expertise in performing these tasks day in and day out should help achieve security goals faster. Start high-level with overall structure and architecture and then dig into the details. For example, start with security technology or program gap assessments to determine what may be missing or duplicated, and then improve coverage and efficiency in those areas. Both offensive testing and defensive readiness matter. Use offensive testing, such as penetration testing and red teaming, to validate security controls. Defensive readiness includes endpoint protection and visibility, threat hunting, threat intelligence, 24/7 monitoring and incident response readiness — whether in-house or via an incident response retainer. Develop an incident response readiness plan, and then drill and test the plan so you are ready in the unfortunate event of a breach.

Where do you see device and user protection going in the next three to five years?

Both device and user protection will rely more heavily on AI and ML. Device protection has already grown tremendously in this area, with more vendors and organizations investing in this technology. We're also seeing advances in continuous user authentication based on passive biometrics such as keyboard and mouse patterns. Being able to learn and uniquely identify the user helps enable a Zero Trust architecture, which moves us beyond the need for user names and passwords.

Learn more at **Carah.io/GT-Dec-Blackberry**