New opportunities to **modernize security**

IT modernization is opening up innovative ways to tackle cyberthreats

Jon Ramsey
CTO, Secureworks

A **KEY OBJECTIVE OF IT MODERNIZATION** is to build systems that are resilient to hardware and software faults. However, agencies must also build systems that are resilient to cyberthreats, which often represent a more dynamic risk.

Adversaries take advantage of the fact that a complex array of multi-vendor systems presents a huge challenge to administrators; it's difficult to stay abreast of how all the elements interoperate. Therefore, a critical part of modernization involves simplifying IT systems and keeping them up to date.

A modernized architecture should also enable network micro-segmentation. Instead of allowing every machine to talk to every other machine on the network, agencies can use a default deny policy and allow only certain machines and services on those machines to communicate with one another, thereby reducing the attack aperture.

That approach can go a long way toward preventing the ransomware attacks that have targeted state and local governments in particular. Such attackers scan the internet looking for misconfigured or open systems that allow extensive access to the infrastructure. At the very least, agencies should make sure that their data is backed up regularly in an immutable or unmodifiable way so that if they are hit with a ransomware attack, they could recover their data.

Mitigating risks more quickly and effectively

No agency can ever assume it is 100% protected. Instead, however, agencies can take several preemptive measures to ensure they are taking all measures to protect their data and information before there's an actual breach.

As they modernize, agencies must think about security in terms of measured risk and making the most of their resources. This simply means that they identify all the potential information or data an adversary might want to steal from your agency and how they would go about doing that. Once they think through those possibilities, IT administrators can embed capabilities that effectively reduce the risk. Modern systems based on software-defined data centers are better at mitigating risk because they can respond more quickly to cyber incidents than traditional IT systems can.

Furthermore, agencies can be prepared for a potential breach by encrypting data when it's in transit, in storage and being processed in memory.

Finally, despite all the technology precautions we take, cyberattacks can still target the human factor. Therefore, agencies should train employees to recognize and avoid social engineering schemes.

> As they modernize, **agencies must think about security in terms of measured risk** and making the most of their resources.

Boosting the ability to respond to a crisis

During the coronavirus pandemic, technology has allowed us to stay connected while being socially distant and to participate in the economy without going to restaurants or retailers. It has also highlighted the need for agencies to deliver critical services even when government offices are closed to the public.

Furthermore, technology has an essential role to play in helping leaders make decisions about how to manage a pandemic. With a modern IT infrastructure, the government can boost its ability to correlate data and gain critical insights into understanding who is at higher risk of contracting the disease, the most likely means of pathogen transmission, the best containment and mitigation practices, and the most effective way to do contact tracing, for example.

A modern IT infrastructure is an essential tool in enabling the government to respond to current and future challenges. When it comes to securing those systems and the digital services that agencies provide, the government needs technology that is specifically built for protecting modern IT systems, efficient and effective processes, and the help of qualified security experts.

Ultimately, even the most sophisticated IT system needs people, process and technology to stay secure. ■

Jon Ramsey is CTO at Secureworks.

We're Revolutionizing Cybersecurity.

Secureworks combines machine learning with human intelligence to detect faster, respond smarter, and predict and prevent more threats altogether.

4,100	300+	20+
Customers in 50+ Countries	Expert Security Analysts, Researchers and Responders	Years of Attack and Threat Actor Group Data

Request a demo. Learn more at secureworks.com

Secureworks®