An Inflection Point for Cybersecurity

Now is the time to reassess security policies and strategies.

For security professionals, the COVID-19 pandemic represents something of a perfect storm.

First, the risk landscape exploded in a matter of days. State and local agencies — many with little telework experience or established policies — rapidly sent thousands of employees home to work remotely. Due to equipment shortages, these workers often used poorly secured personal devices and home networks to continue delivering vital government services. To connect remote employees to enterprise resources, agencies expanded their use of virtual private networks, increasing the chances of inappropriate network access or theft of access credentials.

The urgency of responding to the pandemic also pushed government organizations toward cloud-based solutions that could be quickly deployed to support remote meetings and collaboration, handle spiking unemployment claims, collect and analyze virus-related data, and provide other important functions. But, again, many of the agencies adopting emergency cloud solutions had little experience with the nuances of cloud security.

The bad guys, of course, weren't sitting on their hands. Sensing opportunity, hackers quickly shifted to COVID-related phishing schemes — impersonating agency leadership, health officials and other authority figures to play on users' fears and anxieties.

Midyear reports from several security providers confirmed an alarming rise in cyberattack activity. Skybox Security found ransomware attacks had grown by 72 percent during the first half of 2020.[1] And Check Point Security said COVID-themed phishing attacks jumped from 5,000 per week in February to 200,000 a week in late April.[2]

Regaining Security Focus

As all this happened, security personnel and resources were stretched exceedingly thin. Many security teams were redeployed from operational tasks to urgent projects such as standing up new online services to help citizens apply for unemployment insurance benefits and other safety net programs.

"There was an awful lot of shifting of resources, which I think really depleted the energy of security teams," says Deb Snyder, who was CISO for New York State until January of this year. "COVID didn't completely change the game. Instead, it expanded the preexisting threat surface exponentially at a time when we were already dealing with significant risk."

Snyder and other security professionals say now is the time to reevaluate security tools, processes and strategies in light of these massive COVID-driven changes. Immediate steps include understanding and addressing situations where users may be storing sensitive data on insecure home computing devices, as well as dialing back remote access privileges to reduce the risk of inappropriate access or stolen user credentials.

"We know we deployed solutions without normal security planning considerations and took steps to get things up and running that were risky," Snyder says. "So, take steps now to review and strengthen security controls."

Moving Forward

Over the longer term, agencies must develop better monitoring capabilities that help them spot threat activity and potentially risky user behaviors. Most government agencies don't have the visibility they need into network traffic patterns and user habits. With many agencies planning to continue remote work options and expand digital services post-pandemic, gaining these capabilities is crucial for securing a new way of operating.

"Without this sort of visibility, you're flying blind — you can't make informed decisions,"

says Snyder. “In this new reality of virtual work and workplaces, we really need to study system activity and network traffic to develop a baseline. Then we can act flexibly and with agility when we see changes.”

Government organizations also must increase their sophistication around securing cloud services. Cloud solutions aren’t necessarily secure out of the box, she says. Agencies need to understand the security capabilities of cloud providers, as well as their own responsibilities around data protection and security configurations for cloud-based tools. And as governments rely more heavily on cloud, they’ll need to invest in cloud access broker services to manage and enforce security policies across multiple clouds.

Automation is the Answer

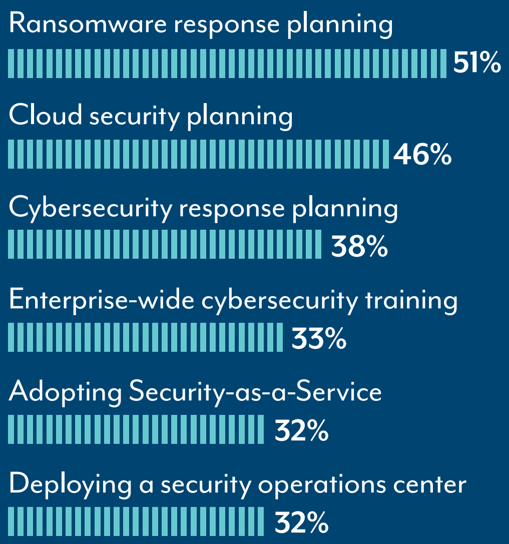
Finally, smart automation will be crucial to augment overwhelmed security staffs as they contend with a greatly expanded threat surface and cyber attacks that are growing more numerous and sophisticated.

Movement toward implementing smarter cybersecurity tools already is underway, according to the Center for Digital Government’s annual Digital Cities and Counties surveys. Fifty-eight percent of cities and 69 percent of counties responding to the 2019 surveys said they already use some form of artificial intelligence (AI) for cybersecurity. Another 37 percent of cities and 26 percent of counties said they plan to implement AI-powered cybersecurity tools in the future.

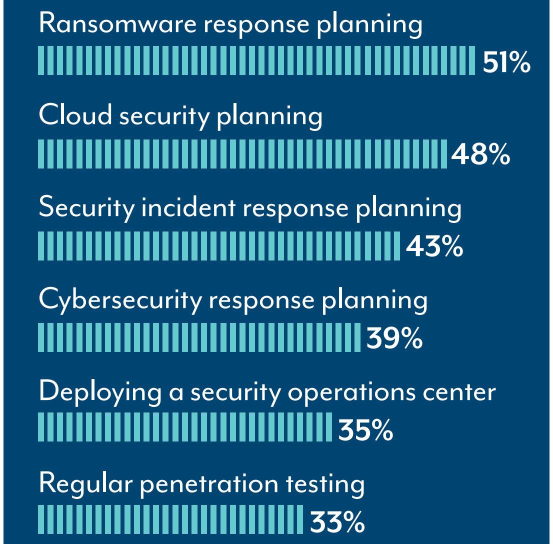
But Snyder argues more work needs to be done around automating government’s response to cyber threats.

“I believe this crisis is really a wake-up call for so many organizations that haven’t embraced the benefits of AI and automation tools that detect and process threat intelligence,” Snyder says. “Security teams need effective tools that reduce the noise, increase efficiency and apply contextualized threat information. In this environment, we need to automate threat detection and incident response as much as possible.”

Cybersecurity Priorities for Cities



Cybersecurity Priorities for Counties



Source: 2019 Digital Cities and Counties Surveys

[1] COVID-19 pandemic sparks 72% ransomware growth, mobile vulnerabilities grow 50%. *Security Magazine*. https://www.securitymagazine.com/articles/92886-covid-19-pandemic-sparks-72-ransomware-growth-mobile-vulnerabilities-grow-50

[2] COVID-19 Has Given Hackers an Unfair Advantage, Experts Say. Govtech.com. https://www.govtech.com/security/COVID-19-Has-Given-Hackers-an-Unfair-Advantage-Experts-Say.html