PLANNING A CYBER RESILIENCE STRATEGY FOR STATE AND LOCAL GOVERNMENT EMAIL

BY CYBERSCOOP AND STATESCOOP STAFF

Through the right blend of advanced security tactics, archiving, business continuity efforts and end-user empowerment, state and local agencies can and should embrace new strategies to become more resilient against email cyberthreats.

When it comes to the concept of cyber resilience, the consensus among state and local government officials is clear — organizations must be able to deliver services and products while remaining protected against the onslaught of threats to their networks and systems.

Despite this focus, recent research conducted by Vanson Bourne on behalf of Mimecast found that only 30 percent of survey respondents have adopted a complete cyber resilience strategy. Another one-third of respondents were only in the early stages of development or planning.

And while there are many factors to true cyber resilience, the true weakness of any system — and therefore any cyber resilience effort — is email, Fairfax County, Virginia's Chief Information Security Officer Michael Dent said.

"Email is the Achilles' heel of any system," Dent said. "We put money into awareness programs, we preach it day in and day out — don't click on the links."

Jim Edman, South Dakota's chief security officer, agreed, and called employee access to email the "front line" to potential threats coming into a state network or system.

"[Employees] are the ones that are getting the phishing messages, the spoof phishing attempts and other aspects of social engineering," Edman said. "I think there's a lot of components to everybody's cyber strategy, and certainly one of those important components is going to be client education."

Even though the threat facing state and local government entities via email is vast, there are some ways to get ahead of the problem. A new eBook from Mimecast outlines "four pillars" of cyber resilience for email — security, data protection, business continuity and end-user empowerment.

Pain points

As state and local government information security leaders confront the challenge of cyber resilience, officials argue that having a broad cybersecurity strategy — while important — is not enough.

"There's a laundry list of technology aspects to go from desktop protection to network protection to application security," Edman said. "Each one of those rabbit holes in and of itself has a wide variety of areas that need to be kept current."

Indeed, in the era of threats of ransomware and other malicious attacks like WannaCry, a broad strategy might not be enough to cover a state enterprise. Instead, leaders need to focus on unique, targeted approaches to making specific systems and areas under their cybersecurity purview more secure.

For Dent, in Fairfax County — which is just south of Washington, D.C., and has more than 1 million residents — the challenge of security resilience with regards to email comes in two spots: the county's email gateway and the end user.

At the gateway level, Dent said he and his team work hard to keep the state's email gateway configured correctly and up to date. In South Dakota, Edman takes a similar approach.

"It's pretty safe to say about 90 percent of all incoming email is spam of some sort," Edman said. "You've got to get rid of the junk, get rid of as much junk as you can. You have gateways to filter things."

For Dent, the gateway is the key to filtering out potential phishing attempts from foreign adversaries and nation-state hackers. Using Domain Message Authentication Reporting and Conformance protocol, Dent said he can strip down potential spoofed email addresses and match them up with actual, reputable email addresses — especially when the emails come from outside the United States.

"The thing elected officials in government are afraid of is not having contact with their constituent," Dent said. "The beauty of it is DMARC can strip all of that and say it's Gmail, but we noticed the 'from' address doesn't match a Gmail account name — this is suspicious."

But even with the most tightly configured email gateway, email phishing attempts and spam can continue to get through, Dent and Edman said, meaning governments also need to prioritize education.

"It's users clicking on links, it's the fact that those bad emails get to us," Dent said. "We've got to be able to stop that."

In South Dakota, state employee cybersecurity training sessions "are absolutely critical."

"The employees, boy, those people are sitting in front of that computer reading that message, they are absolutely critical," Edman said. "If they give up their credentials, or they click on something that's going to download malware, then you're in a reactive game there."

Finding a solution

Though protocols like DMARC begin to move the needle, Matthew Gardiner, a senior product marketing manager for Mimecast, wrote in March 2017 that DMARC "helps, but doesn't by itself solve the entire problem."

Dent agrees, and said he and his team are looking for a product to take the DMARC standard and automate it, and add layers of awareness, knowledge and previously-collected information on top of it.

"I'm looking to find someone that can help review those email headers before they get to my system," Dent said. "This all could be automated, that's the beauty of it, I don't have to get staff worried about it, I don't get alerts constantly.

When selecting vendors to provide this kind of service, Dent said, government needs to be careful.

“Be leery of the existing email providers and gateways and things that you have,” Dent said. “You need to pull back the covers and make sure they truly can do what they say they can do. I just caution [other government leaders] to make sure you’re paying attention to what you’re looking at.”

While Edman also echoed Dent’s sentiments about being careful selecting security solutions from vendors, Edman also emphasized the main part of cyber resilience truly does center on education.

“The value on the cyber side is trying to be able to get the message across,” Edman said. “Whether it’s employees or upper management. When the rubber hits the road, and when it is impacting their day-to-day operations, you have to go back and remind them and say ‘hey, remember, this is really important.’”

In Mimecast’s latest eBook on resilience, the company agreed. The company released a checklist for cyber resilience that encouraged security leaders to communicate, educate and train their workforce. In addition, the checklist called on leaders to know their resilience posture, define policies and procedures, implement the right technology, review their status regularly and get C-suite buy-in early on.

For Dent, doing some email processing in the cloud is another solution that could help improve the security posture of state and local agencies. Those agencies can use cloud-based cyber resilience platforms to process email subject lines, text and attachments to evaluate their potential for risk, Dent said. The thought of moving those activities to the cloud can often be met with apprehension though, he said.

Looking forward

Both Dent and Edman agreed that the need for cyber resilience is here to stay, but that basic practices rooted in education can weed out a majority of the threats that state and local agencies face on a daily basis.

“Security teams are getting better and better,” Edman said. “If you apply the updates, you keep the patches, you use a desktop protection system and you don’t click on the Prince from Nigeria message saying you just won $8.7 million, that goes a long way in the digital world.”

State and local agencies most of all can’t stay still, Dent said. Despite this cybersecurity technology getting better, agencies can’t rest or get complacent. Instead, they need to keep working to improve and further defend their systems — and sometimes that takes money.

“The one thing you can’t do is you can’t be stagnant,” Dent said. “Having staff that know what they’re doing, and then having the leadership to that, and always investing. That has to be a piece, you cannot not invest anymore. If you don’t invest, you’re going to lose.”

At the federal and state and local level, agencies across the country are working together to share information on threats and ultimately keep each other protected. In the private sector, companies are banding together for the same purpose — to better serve and protect their customers.

To get a little closer to finding a way to address the ongoing and continually developing threat of cyber resilience, Mimecast created a Cyber Resilience Coalition in 2016. The CRC, the company said in a release, is designed to encourage “a fresh and comprehensive look” at those four pillars of cyber resilience. The effort brings together industry leaders — currently PhishMe, ZeroFox and Archive 360 — to deliver more visibility and control to their customers.

This article was produced by SCOOP NEWS GROUP, for and sponsored by mimecast® and distributed via **CyberScoop.com** and **StateScoop.com**.