Massive Connectedness: Formal Structures Emerge to Take on Cyberthreats

Adam Stone | October 3, 2016

Even as Texas' chief information security officer (CISO), with the full weight of the state's IT apparatus at his disposal, Edward Block has a limited range of vision when it comes to cybersecurity.

"We don't see everything that is out there. We see a lot of stuff, and we tend to see things pretty early in their evolution. But we don't see everything. So collaboration is really critical," he said. To succeed in cyber, the state's 160 distinct agencies have to pool their resources. "The bad actors out there are happy to share information with each other all day long. If we don't do the same, we are letting them have a distinct advantage."

Given the unheralded complexity and severity of the threat, some say cyber is going to have to be a team effort. "There may be times when assets or authorities from one agency are needed to help another work its way through cyberproblems. And indicators of compromise in one system may indicate or presage indicators of compromise in other systems," said Martin Libicki, a RAND senior management scientist who works extensively on government issues.

This way of thinking increasingly typifies the government approach to cybersecurity — and necessarily so, said Steve Spano, president and chief operating officer of the

Center for Internet Security, which operates the Multi-State Information Sharing and Analysis Center on behalf of the U.S. Department of Homeland Security.

This way of thinking increasingly typifies the government approach to cybersecurity — and necessarily so, said Steve Spano, president and chief operating officer of the Center for Internet Security, which operates the Multi-State Information Sharing and Analysis Center on behalf of the U.S. Department of Homeland Security.

In response to this emerging landscape, government IT executives, emergency planners, security agencies and other key players across the nation are forming alliances. They're putting in place formal structures to ensure that when new cyberthreats emerge, all relevant players can be prepared to act.

Connected Networks

In Georgia an executive order in mid-2015 established the State Government Systems Cybersecurity Review Board to be headed up by the state CIO, with members to include the adjutant general of Georgia and the leader of the Georgia National Guard, the commissioner of the Department of Administrative Services, and Jim Butterworth, director of the Georgia Emergency Management Agency/Homeland Security.

"With everything going more and more to the cloud, it is quickly becoming obvious that any network that is connected to other state networks could be vulnerable," Butterworth said. "That means we need to create the security across the entire infrastructure."

The group's first act was to request a self-assessment from agencies. Based on a December report, the state Legislature approved $3 million over the next three years to fund a deeper study of Georgia's cybersituation. "That is going to get us out of the gate and get us some good data that shows us exactly where we are," Butterworth said. "It is definitely a good push to get us started."

The effort is already having a direct practical impact. State agency IT leaders have been emboldened to get more aggressive on cyber, knowing they have a larger body backing them. Take the ransomware attacks, for instance. "Because of some of these conversations and because we have empowered these agency CIOs, they are beginning to back up systems more and more, so when these ransomware demands pop up — and they have been — we don't give in," said Butterworth. "We don't pay, and so far, we have been able to successfully stop those efforts."

The actual mechanics of collaboration are still a work in progress. Everyone says they want to work together; no one wants to be told what to do, and not everyone likes to make it known when a problem has impacted their systems. These early days require finesse.

"We have to make it clear that we are not beating them over the head: 'We have the clout of the governor's office and we are throwing this in your face.' So we say up front that if an agency comes up red in some area, we aren't going to publish the name of that agency. This is not a punitive effort," said Butterworth. "Our philosophy is that a rising tide raises all ships. We are simply here to empower them in what they are already trying to do."

While the state CIO and security chiefs make an obvious fit on the board, some might wonder why Administrative Services is at the table. Simply put: These are the folks who ultimately purchase the systems. If there are going to be security concerns around IT purchases, best bring them in early. “They have the control to say yes to this system and no to that system. If they are in the conversation, we can help them understand the needs for certain protections,” Butterworth said.

Taking Center Stage

“The thing about cyber is, it is truly worldwide and it is instantaneous. So it requires massive connectedness to combat it.”

That’s Victor Chakravarty, an enterprise architect in the Maine Office of Information Technology. Like Georgia, Maine has in place a formal body designed to take cyber out of the IT closet and put it smack in the center of the room. The Maine State Information Protection Working Group is chaired by the state CIO and includes the Office of Information Technology, Maine Emergency Management Agency, Maine Information and Analysis Center (MIAC, or the fusion center), Maine National Guard, U.S. Department of Homeland Security, the University of Maine, and IT directors of the cities of Auburn and Bangor.

Different players bring different expertise. Some on the team look at cyber as a law enforcement or national security issue. Chakravarty just wants to be sure he can keep the lights on — like last year, when hacking group Vikingdom struck state and local agencies in 27 states with a denial-of-service attack. “My job is service restoration,” he said. “The most important thing I care about is that the state of Maine services remain up and my customers’ services are not affected. But when you look at the fusion center, they are focused on public safety, so they are more interested in the forensics and the prosecution.”

Having that plurality of interests at the table works to everyone’s benefit. “That is what makes it a rich, symbiotic relationship,” said Chakravarty. “I personally do not have the wherewithal to do forensics and prosecution, but there are others who do. Because we meet and spend time together we have evolved these patterns of information sharing that play off of each other’s skills, and that is something that can only come through a long partnership.”

In practical terms, the relationship is very much about responding to immediate threats. “If new ransomware hits the state of Maine, I consider it my sacred duty to inform the fusion center, and they then up-channel it to DHS and FBI,” Chakravarty said. “If the university sees some variant in the malware, or if we see something in the state networks, we all consider it our immediate responsibility to share that. It is in my best interests to contribute to that sum total of community wisdom.”

At the same time, the group takes a bigger-picture approach. Members share best practices among one another, and they are building cyber-recommendations to help guide the governor’s office, the Cabinet and Legislature. “Part of our mission is to educate them,” he said. “And we also would like to up the profile of cybersecurity, so that potentially they can help us overcome burdens we ourselves cannot overcome.”

‘Body Armor’

Mike Sena literally helped write the book on cybercollaboration. As executive director of the Northern California Regional Intelligence Center (NCRIC) he helped develop a toolkit on the topic, the Bureau of Justice Assistance Guide: Cyber Integration for Fusion Centers from the U.S. Department of Justice.

With Silicon Valley in the region, it is perhaps not surprising that the NCRIC fusion center has become a hub of cyberactivity. Partners in the effort range across the state and federal gamut: The highway patrol and state justice department stand shoulder to shoulder with representatives of DHS, DEA, FBI and local law enforcement.

The primary mission is defensive, with planners utilizing FireEye software to continuously monitor participating networks. “When one group is being attacked by an actor, and that attack fails, that actor is likely to go on to the next person. So the goal is to be able to collect and share that information in real time, to create the body armor as best we can for disparate networks,” Sena said.

NCRIC does outreach too, engaging state agencies in cybertraining and readiness activities. Sena’s team has gone spearfishing among critical infrastructure stakeholders, sending out bogus messages to ensnare sloppy users in a mock security breach, and they usually get a bite. “The last time we did this, 7 percent of the folks clicked on the link,” he said. “My advice to the organization is you only need one person.”

Sena is angling to position the 80-person NCRIC as the go-to source for government IT when cybertrouble occurs. To that end, in addition to sending out a steady stream of warnings and updates, the center also has produced a mobile optimized application to help people report incidents and threats. It also mounts a 24/7 response team.

When an incident or threat is reported, “we have the ability to reach out to that agency, to reach out to law enforcement, to reach out to the IT folks. From there we can send a team out, to have a human body out there working with them,” said Sena. “We don’t have enough bodies to send someone every time, but if it is a priority issue we will have somebody on the ground.”

Why the pressing need for collaboration? Because, as Sena puts it, cyber is not like other threats.

“We come together on a unified message for physical threats. ‘If X happens you do Y.’ But when we get to cyber it isn’t the same,” he said. “With cyber, if A happens, you can either do B, F-l, M or 3. That’s not the best thing. We need to be able to say, ‘This is the way we handle cyberevents in America. This is the way we handle cyberinvestigations.’ We are not there yet.”

The Virtual Threat

Mike Geraghty joins with Sena and others in government in wanting to change that status quo. As director of the New Jersey Cybersecurity and Communications Integration Cell, he oversees a collaborative effort intended to forge a common front against the cyberfoe.

“No one agency has all the answers or is even capable of keeping up with information security on the necessary scale,” he said. “When you have a threat that is physical and local, you can protect against that. But this is a threat that is virtual, that can happen anywhere against anything, and the only way to protect against that is cooperatively.”
To get at it, the cell embraces a broad mandate. “We want to be the one-stop shop for cybersecurity,” Geraghty said. “That may be information on current threats, it may be best practices to implement cybersecurity, or the current state of cyber. We are also doing a lot of analysis, looking to see what a viable threat is and making sure we can articulate the nature of that threat and why it is important.”
That’s a lot to bite off. Automation helps: A security information and event management system deployed across state networks records up to 2 billion events a day. Operations and analysis teams track that feed; communications professionals get the word out to more than 1,500 members.

Mike Geraghty wants the New Jersey Cybersecurity and Communications Integration Cell to be a one-stop shop for the state’s cyberefforts. Photo by Donnelly Marks.
The cell gets regular alerts from outside sources like DHS and FBI. The art here lies in taking all that information and lining it up against what’s happening internally. “Others can receive the same sorts of external information from the same sources. Our secret sauce is in comparing that to what we see on our network,” he said. “We vet that information so that what we provide our members with what is most relevant. We strip out the noise. Otherwise you are just opening a fire hose.”

While agencies are generally cooperative, Geraghty admits encountering the occasional "reticence to disclose" — IT leaders shy about lifting the covers on their systems' vulnerabilities. His promise: Tell us your troubles, and we'll keep it anonymous. "Even if you don't strip it out and sanitize it before you give it to us, we will do that on our end so that when we do make use of that information, we will not disclose anything about you or your systems," he said.

In the drive toward cybercollaboration, this appears to be the big looming hurdle: the need to drive cultural change in an IT environment that tends to play security issues close to the vest.

In Texas, agencies are required to report cyberincidents to CISO Block, "but they are really uncomfortable doing so, because they don't know where that information is going to go. Will it go to the people who manage their budget? Will it go to the Legislature? Will it end up in a report that is available to the public?"

Texas law says everything is public knowledge unless specifically exempted. Block will go to bat to shield agency IT leaders from the spotlight, but only to some extent. "If it is just something embarrassing, if it is just the news of a breach, that is not something I would try to protect" from disclosure, he said. "But how it happened? If showing that would put that system or another in jeopardy, that is something I would try to protect."

Experts across government say IT leaders will need to find a way to walk this fine line. With collaboration virtually the inevitable next step in government cyber, they will have to construct not just the technical mechanisms to anonymize breach reports, but also the trust and relationships that will make it possible for all players to feel secure in putting their cards on the table.

http://www.govtech.com/security/Massive-Connectedness-Formal-Structures-Emerge-to-Take-on-Cyberthreats.html