Finally, Cybersecurity Gets the Attention It Deserves

A confluence of factors push the issue into the executive suite

Cybersecurity reached a tipping point in 2021. Although protecting data and systems from cyber threats is a long-running concern for IT leaders — the issue has ranked at the top of CIO priority lists for years — executive attention and resources devoted to cybersecurity rarely have matched the scale of the problem. That’s changing now, thanks to a convergence of factors.

One big driver is a wave of disruptive attacks — some targeting critical infrastructure and important supply chains — that has put a national spotlight on this long-simmering issue. In May, a ransomware attack on the Colonial Pipeline crippled fuel delivery to much of the southeastern United States, touching off panic buying and long lines at gas stations. Before that came the SolarWinds attack, where hackers compromised a supplier of IT management software that’s widely used by governments and private companies, enabling the hackers to distribute malicious code to the company’s customers through regular software updates.

These attacks — and others like them — are a wake-up call to elected officials and line-of-business leaders regarding the risk presented by growing cybercriminal activity. That call has gone all the way to the Oval Office, where the Biden Administration issued an executive order aimed at shoring up the nation’s cybersecurity through better sharing of threat information, greater adoption of Zero Trust security architectures and secure cloud services, and other measures.

The COVID-19 pandemic has been another important driver, turning up the heat on modernizing security approaches and tools in state and local government.

“The pandemic was the pivot point,” says Deb Snyder, former CISO for New York State, who is now a Center for Digital Government (CDG) senior fellow. “The sudden adoption of remote work, the dramatic escalation of COVID-themed ransomware attacks, the need to deliver services to constituents online — it all forced government agencies to address security measures that in many cases should have already been in place.”

As a result, many agencies have stopped deferring critical investments in replacing outdated security technologies and tools. Now they’re looking to beef up proactive threat monitoring and visibility, intrusion detection and response, and other sophisticated capabilities.

Another critical factor: There’s new money available for cybersecurity modernization — and a lot more is on the way. Federal relief programs like the CARES Act and the American Rescue Plan Act include funds for cybersecurity improvements. And the Biden Administration’s newly passed Infrastructure Investment and Jobs Act offers almost $2 billion for cybersecurity funding, more than half of which is set aside for state, local and tribal governments.

All this points toward cybersecurity having a long overdue moment. Snyder suggests it’s also an opportune time for state and local agencies to reassess security plans and approaches before they make their next move.

“Agencies should look at the solutions they deployed fast and furious and under duress during the pandemic to see if they need to tighten security around them,” she says. “It’s also a good time for agencies to review interim solutions they deployed, as these solutions may not align or be sustainable from a cost or maintenance perspective. It’s okay to pause and pivot rather than invest further in a path that won’t take the organization where it needs to go to support this new way of doing business.”

Snyder offers this advice for agencies as they move forward on security modernization in 2022:

Prioritize cloud security: One big impact of the pandemic has been rapid adoption...
of cloud-based platforms and applications — and this trend will continue as state and local agencies prioritize the modernization of legacy systems. But as they migrate more systems and workloads to the cloud, they’ll need processes, governance structures, tools and staff skills for managing security in the cloud.

This evolution includes integrating cloud security services into your overall security planning, Snyder adds. “Most cloud providers include built-in security services for data protection, regulatory compliance, privacy and access control. You shouldn’t rely on them exclusively — but you should use them.”

**Embrace Zero Trust:** This approach eliminates the concept of trusted users. Instead, it continuously authenticates and validates users whenever they try to access applications or data — even if they’re already logged into a network. “It’s not one technology,” says Snyder. “It’s a philosophy, design architecture and network access strategy built for the way organizations work and deliver services today. It moves your defenses from static network-based perimeters to perimeter-less security controls.”

For most organizations, enterprise-wide adoption of Zero Trust will be an incremental process. Snyder recommends working with an expert partner to identify a suitable framework and set priorities. “You can leverage resources you already have that align with your strategy and drop things that don’t,” she says.

**Strengthen digital identities:** Strong digital identities will be foundational for sustaining remote work and expanding digital service delivery. “Identity validation ensures trust,” says Snyder, “and trust is really the underpinning of all these digital transactions we want to provide to employees and the public.”

**Harness artificial intelligence (AI) and automation:** Intelligent security tools are increasingly important for strengthening cybersecurity. AI-powered tools can augment human security staff by automating high-volume tasks like evaluating security alerts. They can also speed up response to potential security incidents.

Fortunately, greater adoption of AI for security is already underway. “I think 2020 was the year that security teams finally embraced automation to improve their capacity to deal with the sheer volume of alerts and incidents,” Snyder says.

**Invest in training:** Upskilling internal staff will be critical as agencies seek to safely grow their use of cloud, manage complex hybrid computing environments, implement secure software development approaches and make other improvements.

“Organizations must take the time to assess their training and education needs, and then build those needs into their budgets to avoid gaps in critical skills and reduce the risk of losing talent,” Snyder says. “That’s non-negotiable; it should be viewed as an investment, not an expense. It makes your human factor a strength, not a liability.”

**Gear up for new funding:** Finally, with millions of dollars in new cybersecurity funding on the horizon, now is the time to prepare. Agencies should perform security assessments, update strategic plans and identify priorities in anticipation of capturing those dollars.

“Get your prioritized initiatives in order and your grant folks working on developing sound proposals now,” Snyder says, “so you’re ready to take advantage of those funds when they become available.”

---

### Modernizing Key Security Tools

<table>
<thead>
<tr>
<th></th>
<th>Cities</th>
<th>Counties</th>
<th>States</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI / Machine learning</td>
<td><img src="image" alt="23%" /> <img src="image" alt="23%" /> <img src="image" alt="23%" /></td>
<td><img src="image" alt="20%" /> <img src="image" alt="32%" /> <img src="image" alt="29%" /></td>
<td><img src="image" alt="28%" /> <img src="image" alt="28%" /> <img src="image" alt="25%" /></td>
</tr>
<tr>
<td>Cloud security</td>
<td><img src="image" alt="10%" /> <img src="image" alt="32%" /> <img src="image" alt="48%" /></td>
<td><img src="image" alt="10%" /> <img src="image" alt="43%" /> <img src="image" alt="42%" /></td>
<td><img src="image" alt="17%" /> <img src="image" alt="39%" /> <img src="image" alt="44%" /></td>
</tr>
<tr>
<td>Identity and access management</td>
<td><img src="image" alt="5%" /> <img src="image" alt="38%" /> <img src="image" alt="56%" /></td>
<td><img src="image" alt="8%" /> <img src="image" alt="43%" /> <img src="image" alt="48%" /></td>
<td><img src="image" alt="2%" /> <img src="image" alt="27%" /> <img src="image" alt="68%" /></td>
</tr>
</tbody>
</table>

Source: Center for Digital Government Digital Cities, Counties and States Surveys