ISSUES TO WATCH

Deb Snyder: Six Ways to Enhance Cybersecurity in a Post-Pandemic World

Deborah Snyder joined the New York State Office of Information Technology Services as deputy CISO in 2012, a position she held until being promoted to the state's top cybersecurity job in June 2017. As New York State's CISO, Snyder was responsible for setting policies for data security, vulnerability monitoring and cyber hygiene across one of the biggest state government organizations in the country. She retired from her state position in November 2019.

Snyder recently shared her thoughts on key steps state and local government agencies can take to improve cybersecurity in a post-pandemic environment.

1 Focus on immediate, actionable efforts to bolster security and assure resiliency. First, secure critical operational needs, including the mass shift to telecommuting and remote access. Then review and tighten security controls.

"Organizations that rushed to get people connected and working have told me security was relaxed or sidelined during that time," says Snyder. "Now is the time to revisit the security of those solutions. Go back and put the right controls in place and affirm you are protecting sensitive information in all places."

2 Reexamine and reevaluate. The technologies organizations put in place quickly during the pandemic might not be the technologies that will serve them best in the future.

"Look at your cyber strategy or strategic plans with new eyes. The lessons we learned from the pandemic response experience and challenges shouldn't be wasted. Ask tough questions about priorities and planned investments, and recalibrate those plans now to add value and address current and future risks and workplace realities," says Snyder.

3 Take advantage of new tools. The pandemic forced government leaders to think differently about how they work and how they secure their environments. Snyder recommends security leaders ask their teams and partners how to take advantage of new technologies to achieve long-term benefits and efficiencies, reduce operational costs and improve security.

"Think about the future workplace and focus on technologies that can improve security in that environment, including zero-trust strategies that restrict access or integrated solutions that enable better productivity," says Snyder. "Then, make sure you have essential end-to-end defensive measures in place. Automation is key. Leverage technologies that enable automated blocking, detection and response, and address advanced threats."

4 Consider new partnerships. Don't automatically rely on your old allies, recommends Snyder. Greater creativity and innovation are two positive outcomes of the pandemic. Look for forward-thinking partnerships that can help you address new challenges and gaps.

5 Plan with the new normal in mind. Consider remote work scenarios as the expected norm going forward. The workforce and the workplace may never go back to what they were. Most organizations don't have contingency plans that fully reflect critical operational processes, requirements and alternatives. Examine your organization's business continuity and disaster recovery plans to make sure they work and are scalable and sustainable in this new environment.

"That includes everything from updating emergency contacts to testing realistic scenarios so you can understand where even the best thought-out plans might run aground," says Snyder.

6 Reconsider cyber insurance. Cyber insurance is designed to protect organizations from risk and is worth consideration. But before securing a cyber insurance policy, think carefully and holistically about your coverage and your organization's needs.

"No one size fits all," says Snyder. "All cyber insurance policies have deductibles, exclusions and exemptions. Be cautious and make sure your cyber insurance policy addresses your organizations' specific needs and that it will support you during a network security incident, a data breach or a pandemic."