Bond Case Briefs

Municipal Finance Law Since 1971

Every Government Needs a Plan for the Worst-Case Cyber Scenario.

Relying on a one-off cybersecurity plan is no viable way for governments to defend their systems. Leadership changes, budgets and new technologies must be continually considered for long term success.

A colleague asked me last week if I could chat about refreshing her government organization's cybersecurity strategic plan, and the very next day the California Department of Technology and its Office of Information Security published "CAL-SECURE," described as the state's "multi-year information security maturity roadmap." Talk about coincidence: It's an issue that couldn't be more timely and worthy of discussion both inside the cybersecurity community and throughout government leadership.

The CAL-SECURE plan is one of the best I've seen, and when I asked California's chief information security officer, Vitaliy Panych, about it, he told me that "planning a roadmap that is applicable to all public-sector entities requires a community-driven approach where input from across the public and private sector is considered." The CAL-SECURE road map, he added, "consists of multiple people, process, and technology initiatives to continuously increase privacy and security for the benefit of all residents of California."

I have written or co-written several cybersecurity strategic plans over the years, and I think California's approach is right on target. As I thought about how I could help my CISO colleague with her strategic-plan refresh, I focused on some of the common mistakes and what I believe are the critical and essential elements of an exceptional plan.

A proper cybersecurity plan should be viewed through the lens of CAL-SECURE — as a road map that sets the stage for the future, and in government that means preparing for the people, processes and technology resources to carry out the mission. It also means calibrating with the CIO's goals to ensure that the cybersecurity road map is in alignment with the jurisdiction's digital transformation initiatives and the delivery of citizen-facing services.

I found a number of state government cybersecurity strategic plans online and also discovered the National Governors Association's "Meet the Threat" memo on state cybersecurity strategies that, while a few years old, uncovered some incredibly consistent data across 18 state strategic plans. The NGA's Resource Center for State Cybersecurity is another goldmine for tools and recommendations to develop cybersecurity policies and practices.

One of the significant differences between private- and public-sector strategic planning is the dynamic nature of executive branch leadership over the course of election cycles. There is almost certain to be an election between the time a plan is published and the plan's time horizon, and priorities are often dramatically adjusted between administrations. A solid strategic plan helps keep long-term cybersecurity initiatives in focus and on target.

"It is especially important for government organizations to plan ahead because of the way budgets

work," said Mike Lettman, who served as state CISO in both Arizona and Wisconsin. "Government entities are often asked to determine their risk and recommend a technology to fill it, but the funding doesn't happen until a year later and implementation until a year after that. Because technology innovation happens so quickly compared to the pace of government, both the risk and the technology will have undoubtedly changed by the time you get the funding or are ready to implement the technology."

One of my soapbox issues that I believe should be mandatory in any cybersecurity strategic plan is how the organization is planning for the growing and potentially calamitous cybersecurity workforce deficiencies. The just-released (ISC)2 Cybersecurity Workforce Study highlights that in the United States alone there are more than 350,000 vacancies in the cybersecurity workforce. Security executives everywhere should take the opportunity to read through this report, because while it highlights the challenges we face in hiring qualified people it also suggests a number of interesting and innovative approaches to address the development and retention of existing staff and provides key takeaways for managers seeking to hire people into cybersecurity roles.

While there are a number of fundamental components in a good strategic plan, I think there are three critical ones that hold the keys to success:

- Make success measures actionable and quantitative. A strategic plan is not the time to be solely aspirational. Putting stakes in the ground with measurable goals that clearly identify success and will survive the test of time encourages organizations to take ownership and be accountable.
- Get input from every organization with a role in the success of the strategic plan. Nothing sours a plan quicker and creates more animosity than being held accountable to a plan you didn't have a role in developing.
- A strategic plan is the beginning, not the end. Far too many state government cybersecurity plans are simply check-in-the-box exercises and begin to gather dust the moment they are signed. A strategic plan should be viewed as a living document, and because the cybersecurity threat and vulnerability environment change so rapidly, it should be reviewed at least annually to make sure the things you planned for last year are still valid. A strategic plan that hasn't been updated in two or three years is almost certainly worthless.

"Updated strategic plans were always vital to our enterprise success," said Dan Lohrmann, former chief technology officer and chief security officer for the state of Michigan. "Articulating a clear vision as well as an actionable road map to delivering expected results meant that everyone stayed on the same page from the governor's office all the way to the frontline workers. Strategic plans guide enterprise priorities, funding, project initiatives, resource gaps and much more."

Dan has it right: Cybersecurity has become a fundamental organizational component of all government organizations, and solid strategic planning is the least we can do for the citizens who support us.

Governing

November 04, 2021 • Mark Weatherford