Fortune: What CIOs and CTOs plan to do differently after CrowdStrike's massive tech outage

NEWSLETTERS· CIO INTELLIGENCE

What CIOs and CTOs plan to do differently after CrowdStrike's massive tech outage

BY JOHN KELL
July 24, 2024 at 2:15 PM EDT

(From left to right) CNH chief digital and information officer Marc Kermisch, Akamai CIO Kate Prouty, Cockroach Labs CTO Peter Mattis.
COURTESY OF COCKROACH LABS, AKAMAI, AND CNH

Prakash Kota, chief information officer at business software firm Autodesk, was fortunate enough to experience an uneventful flight home on Thursday evening to the San Francisco Bay Area after attending a leadership team meeting in Montreal.

By Friday morning, Kota and others awoke to the largest IT outage in history. A software update pushed out by cybersecurity company CrowdStrike caused millions of Windows based computer systems to crash, upending air travel, banking, retail transactions, hospitals, and railways across the globe. Many CIOs are still dealing with the aftermath.

And while nearly all of Autodesk's employees were back online by Friday morning, Kota says the episode shows that IT leaders must create more protections in an era when software on corporate devices is often updated by external partners. "I would say it almost gives a wakeup call to some of these vendors that want to be agile, but certain things have to be tested," Kota said.

One change Kota is strongly considering at Autodesk is more oversight of automatic software updates from vendors before they're accepted. "Is there a way where we can restrict some of the changes before they get deployed broadly?" Kota asks.

At cloud company Akamai Technologies, the CrowdStrike outage had no direct impact on operations due to a prior decision to prevent vendors from pushing through automatic updates. Instead, the company's IT department must approve them before they're downloaded.

"That's a lesson: Have faith in your providers, but you can't trust them wholesale," says Akamai CIO Kate Prouty. "You need to do your own testing."

While unscathed this time around, Akamai learned a few lessons from the CrowdStrike debacle. It realized that the existing encryption on the company's devices adds an extra layer of complexity if and when staff needs to decrypt those machines remotely to resolve a problem. Akamai is now considering automating the process to get those devices back online quickly following a mass outage rather than having to unlock them one at a time.

Prouty said she's also thinking through how to ensure employee communications if the company's internal messaging system became inaccessible due to a tech disruption.

Peter Mattis, chief technology officer at database startup Cockroach Labs, says CrowdStrike isn't solely responsible for the outages that impacted so many businesses. Its customers, he argues, also deserve some blame. "Why weren't they mandating that they had more control over what's being deployed to their critical infrastructure? They are essentially turning it over into the hands of this vendor," Mattis says.

When companies sign deals with new vendors, they often require those companies to complete a questionnaire to attest to the security of their systems. Some of these questions focus on "system resiliency," details that would reveal how CrowdStrike and other vendors think through data protection, disaster recovery, business continuity planning, and how they stage software updates.

“I’m already asking our procurement people to do a little scrutiny to [determine] should we be asking more incisive questions about their resiliency,” says Mattis.

Tom Parker, CTO of security company NetSPI, says the outage exposed significant industrywide “gaps in our ability to react and respond” to CrowdStrike-like threats**.** But he remains a fan of CrowdStrike and the security industry as a whole. “There’s definitely a tendency to have a knee-jerk reaction,” says Parker.

CrowdStrike customers should perform a deep analysis of what happened inside their companies during the crisis, he adds, and perform tabletop scenarios, or simulated IT emergencies that help train employees and expose weaknesses.

At CNH, a manufacturer of agriculture and construction equipment, 8,500 employees were confronted with the “blue screen of death” on Friday that made their devices unusable. By mid-day Saturday, 100 IT professionals were able to get some operations up and running, and after 72 hours, the company was fully operational.

Marc Kermisch, CNH’s chief digital and information officer, says his optimistic view of the outage is that it gave many companies an opportunity to put their disaster recovery plans to work.

“We really got a chance to exercise that and it was a great learning moment,” he says. And while relieved CNH had a plan to execute against, he adds, “I hope to never have to do that one again.”