VISION by protiviti

In Focus

July 23,
2024

Will CrowdStrike serve as a reboot on tech resiliency?

By Kim Bozzella

Managing Director and Global Leader, Technology Consulting, Protiviti

Global IT systems are still in reboot and recovery after a software update by cybersecurity vendor CrowdStrike caused a massive worldwide outage of Windows computers. Global businesses, governments and organizations were impacted across several industries, including airlines, banks, telecommunications, and healthcare. While the dust settles on the specifics of the how and the why of the global meltdown, one thing that is certain is some bad code in a CrowdStrike content update has served as massive wake up call to the world about our collective technology vulnerability.

Why it matters

According to a blog post by Microsoft, less than 1% — more than 8.5 million — of all Windows machines were affected. However, the consequences of CrowdStrike's flawed patch were significant. Experts have put the economic impact in the billions for what may be the most significant IT outage in history.

For his part, CrowdStrike CEO George Kurtz stated that it may take weeks to fully recover the over 8.5 million Windows devices that were affected by the software update. Technology experts have long warned that the interconnected nature of the underlying systems supporting essential services across several industries could result in more global outages. In the immediate aftermath, business leaders should:

- **Focus on resumption of 'business as usual' activities.** As most organizations are still in the process of formal response to the incident, the primary focus should be on addressing known issues and resumption of normal business services, deploying workarounds where necessary.
- **Communicate across the enterprise to increase transparency on known issues.** As ad hoc technical fixes became available, end users may have taken steps to remediate that do not align with enterprise practices and may result in unintended issues.

- **Understand impact to key supporting vendors.** Directly engage with your critical third parties to understand if there may be downstream impacts to your organization in the services/efforts they provide. Implement remediation strategies to address potential vendor impacts.
- **Communicate with your customers.** Provide clear and concise communications to customers about the extent of the impact and state of recovery to increase customer confidence that the issue is being managed.
- **Be on the lookout for phishing e-mails.** Communicate to the enterprise the importance of following communication and support protocols when resolving this issue and be alert for phishing e-mails masquerading as solutions to this issue.

What they say

Thomas Vartanian, Executive Director, Financial Technology & Cybersecurity Center

"Imagine if you couldn't find or access your money? That day could be coming sooner than we think, and it is up to us to act. Businesses should take the lead and work with governments to finally, once and for all, secure our virtual world. Over the last 25 years, if democratic nations had reconfigured cyberspace according to some commonsense rules that incorporated the same authentication, governance, enforcement standards and responsibilities that we employ in the analog world, virtual vulnerabilities and the chances of global shutdowns would've been greatly reduced."

What we say

Unfortunately, this could become the new normal as we move further into an interconnected IT future. Tactically, business leaders should assess other third-party agents, tools and products that share similar characteristics to CrowdStrike, which may pose a similar threat going forward. Establish action plans to mitigate these threats. Business leaders should integrate a 'CrowdStrike-type incident' into existing scenario libraries. Meanwhile, reviewing third-party risk management practices and taking steps to better identify and monitor those with similar characteristics to CrowdStrike.

Strategically, organizations should continue to invest in a thoughtful — and tested — framework with which to make informed business decisions during an adverse event. The one certainty is that the next outage will be different than the last one. Organizations that prepare for responsive and responsible reaction and recovery will be better suited in the future.

The bottom line

A CrowdStrike-like event will almost certainly happen again. Business leaders should use this incident as an opportunity to reboot tech resiliency. Companies that stay vigilant and have the proper protocols and plans in place will be most prepared to minimize widespread damage, keeping in mind their organizations may experience downstream secondary impacts that may not surface for days or weeks. These impacts include compliance related activities, data integrity issues, shadow IT activities performed from end user devices that experience disruption or disruption of recurring activities that have not completed a cycle.

Business leaders should continue to focus on practical changes the organization could make, such as ensuring the software supply chain is as fully automated as possible to minimize risk related to human error, to better prepare for the next widespread tech outage.

Protiviti's Sameer Ansari, Samir Datt and Andrew Retrum contributed to this report.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach, and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, digital, legal, HR, governance, risk, and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2024 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with smaller, growing companies, including those looking to go public, and with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

About VISION by Protiviti

VISION by Protiviti is a global content resource exploring big, transformational topics that will alter business over the next decade and beyond. Written for the C-suite and boardroom executives worldwide, *VISION by Protiviti* examines the impacts of disruptive forces shaping the world today and in the future. Through a variety of voices and a diversity of thought, *VISION by Protiviti* provides perspectives on what business will look like in a decade and beyond.

protiviti®