JAMA Health Forum™

Viewpoint

Promoting the Resilience of Health Care Information Systems —The Day Hospitals Stood Still

Daniel B. Kramer, MD, MPH; Kevin Fu, PhD

Author affiliations and article information are listed at the end of this article.

On Friday, July 19, 2024, health care workers woke to emails declaring systemwide information technology (IT) emergencies. Many hospital IT personnel had already been awake for hours. Crowdstrike, a US technology firm that automatically protects enterprises from advanced cybersecurity threats, had issued an errant software update affecting Microsoft Windows.[1] Because Crowdstrike had access to the most sensitive core parts of the Windows operating system, the automated process caused an immediate global outage of computer systems using the Crowdstrike Falcon product, which is embedded in many computer systems at health care organizations.

The resulting chaos disrupted critical infrastructure and service industries, including government agencies, airlines, financial services, and health care systems worldwide. Responses varied widely. In Boston, Massachusetts, some major academic centers cancelled all elective procedures and many outpatient clinics, while others delayed normal operations for several hours before resuming activities under crisis management conditions.[2] In some cases, restoring normalcy required solutions ranging from climbing ladders to reach computers in ceilings to restoring individual hospital computers with preloaded USB (ie, universal serial bus) sticks.

The harms to patients and institutions wrought by this sudden but largely transient shockwave may be difficult to quantify. Weary from the prolonged and far-reaching crisis of the COVID-19 pandemic, regulatory authorities, health care administrators, and the public might have let this episode pass without deeper consideration. But, the Crowdstrike event was an important reminder to health care practitioners, consumers, and regulators about critical weaknesses in the nation's health IT infrastructure, with urgent lessons for making this infrastructure more resilient.

How This Happened

Twenty years ago, a system crash at 1 academic hospital foreshadowed the growing reliance on IT for daily operations.[3] Features still in early dissemination then—electronic health records and pharmacy systems—are now ubiquitous. How was it possible for a private firm to have such a broad and direct reach into so many health care institutions' critical systems?

While Microsoft has claimed that the European Union antitrust regulatory climate led them to give companies access to modify the function of Microsoft Windows' core components,[4,5] there appeared to be no required verification process that third-party software would not harm the Windows operating system before global deployment. Because of the large number of cybersecurity threats ranging from ransomware to phishing attacks, health care delivery organizations seek commercial solutions to manage the cybersecurity risk. Crowdstrike has a history of successfully defending against cybersecurity threats and has been extremely effective at deploying the product widely across the health care sector.[6]

In this case, initial analysis pointed to inadequate testing and verification processes, exacerbated by distributing the software update to all customers simultaneously rather than a more cautious, phased rollout.[7,8] Importantly, because the Crowdstrike software changed the most inner parts of the Microsoft Windows operating system, this initial malfunction disabled subsequent automated remediation. This also explains why the fix, once characterized, could not be simply and

swiftly pushed out using the same pathway as the initial problem. While the failure was automated, the manual remediation process required physical access to computers that often were "headless," without a keyboard or mouse.

Promoting Health Care IT Resilience

Unfortunately, patients and health care practitioners can do little beyond advocating through their congressional representatives to push the industry beyond self-regulation. Despite many advantages of an increasingly digitized and connected health care ecosystem, digital systems can fail in ways that are more sudden and catastrophic than can older analog systems.

The burden for preventing the next "benign" IT meltdown and fortifying systems even further against malicious attacks[9] falls on health care systems and their regulators. First, US health care institutions must shift from a culture of cybersecurity to a culture of resilience. Cybersecurity tools are necessary because of the endemic threats of ransomware and phishing attacks, but no cybersecurity tool should threaten clinical workflows. Contracts between health care delivery organizations and cybersecurity service providers should have consequences for damages if a software update causes a major interruption to clinical workflow, and there should be more universal use of the cybersecurity procurement language developed by the Health Sector Coordinating Council as a consensus of the health care community.[10]

Second, recognizing market forces alone to be inadequate, the US government should leverage existing offices and organizations for health care cybersecurity to create a national technical means to simulate and emulate the behavior of medical devices and IT equipment in clinical environments. Health care organizations and software manufacturers can then test the impact of their products on clinical workflow and hospital operations before deployment. A number of agencies within the US Department of Health and Human Services (HHS) and the Department of Homeland Security have the congressional remit to prepare for cybersecurity threats to health care critical infrastructure. The HHS Assistant Secretary for Preparedness and Response (ASPR) and the Department of Homeland Security Cybersecurity & Infrastructure Security Agency (CISA) already partner to respond to health care cybersecurity incidents, but they have not provided preparedness measures beyond guidance documents and success metrics. If they partner with the US Food and Drug Administration and the Health Sector Coordinating Council, the government could leverage the HHS Advanced Research Projects Agency to simulate hospital outages due to cyberattacks or software failures.

This simulation could help catch problems, such as Crowdstrike-induced outages, by requiring vendors to practice in a safe simulation before deploying in sensitive clinical environments. Individual manufacturers do not have these capabilities other than simulation of their own medical devices, and what is lacking is the whole-hospital simulation for cybersecurity threats. These complex and expensive investments are needed to prevent incalculable harm to patients from preventing and delaying care while avoiding enormous losses across health care and other critical sectors in the US economy. Rather than beta testing potentially defective software on a live hospital network, as occurred in the Crowdstrike event, government investments and mandates can partner with the IT industry to create a virtual proving ground to verify resilience of computer systems before distributing new software widely to hospitals.

One key challenge for both industry action and government oversight includes scaling clinical computer system emulation platforms and patching without interrupting clinical workflow. For instance, testing one infusion pump will not necessarily help to emulate a different manufacturer's device. Important or idiosyncratic differences across manufacturers can complicate emergency and routine clinical care but also may interfere with independent cybersecurity testing, thereby lowering standards for all. Moreover, testing in a different clinical environment (large hospital vs rural clinic) would require significant system engineering to meaningfully emulate the new context.

As of this writing, 2 months have passed since hospitals and clinics briefly stood still, and daily operations appear predominantly restored. Going forward, quasi-experimental methods may help to quantify the patient harm wrought by the natural experiment of a largely random Friday with surgeries and clinic appointments cancelled, diagnostic tests deferred, and clinicians' workflows disrupted. These analyses may miss the impact on patients and families forced to recalibrate, reschedule, and revise treatment plans ranging from preventive visits to urgent procedures. Rather than accept this event as inherent to a complex, digitized, and wired health care ecosystem, we urge the US Congress, health care regulators, and the public to insist on proactive preventive methods to avoid future IT catastrophic events rather than simply waiting for the next disruptive crisis requiring an emergent response.

ARTICLE INFORMATION

Published: November 27, 2024. doi:10.1001/jamahealthforum.2024.3968

Corresponding Author: Daniel B. Kramer, MD, MPH, Beth Israel Deaconess Medical Center, 375 Longwood Ave, Boston, MA 02215 (dkramer@bidmc.harvard.edu).

Author Affiliations: Section on Electrophysiology and Digital Health, Richard A. and Susan F. Smith Center for Outcomes Research, Beth Israel Deaconess Medical Center, Boston, Massachusetts (Kramer); Harvard Medical School, Boston, Massachusetts (Kramer); Department of Bioengineering, Department of Electrical & Computer Engineering, and Khoury College of Computing, Northeastern University, Boston, Massachusetts (Fu); Archimedes Center for Health Care and Medical Device Cybersecurity, Boston, Massachusetts (Fu).

Conflict of Interest Disclosures: Dr Kramer reported receiving grants from the National Institutes of Health and personal fees for consulting from HeartCor Solutions, Peterson Health Technology Institute, and Whoop, Inc outside the submitted work. Dr Fu reported being director of the Archimedes Center for Healthcare and Medical Device Security during the conduct of the study; being a shareholder in Virta Labs LLC and receiving personal fees from Brillient Corporation for being a consultant to the US Food and Drug Administration to run seminar series and from MITRE Corporation for being a consultant for defense science advising outside the submitted work; and serving on the White House President's Council of Advisors on Science and Technology Working Group on Cyberphysical Resilience. No other disclosures were reported.

REFERENCES

1. Allyn B, Mann B, Chappell B, Al-Kassab F. What we know about the computer update glitch disrupting systems around the world. National Public Radio. Accessed July 26, 2024. https://www.npr.org/2024/07/19/g-s1-12222/microsoft-outage-banks-airlines-broadcasters

2. Toole M, Rex K. Microsoft outage forces Mass General Brigham to cancel non-urgent surgeries, hospital visits. WBZ/CBS News. Accessed September 18, 2024. https://www.cbsnews.com/boston/news/microsoft-outage-crowdstrike-mass-general-brigham-hospitals-boston/

3. Kilbridge P. Computer crash–lessons from a system failure. *N Engl J Med*. 2003;348(10):881-882. doi:10.1056/NEJMp030010

4. Bethan J. EU pushes back on claim regulation played role in CrowdStrike outages. Lexology. July 23, 2024. Accessed July 26, 2024. https://www.lexology.com/pro/content/eu-pushes-back-on-claim-regulation-played-role-in-crowdstrike-outages

5. Phelan D. CrowdStrike outage: Microsoft blames EU while Macs remain immune. Forbes Magazine. July 22, 2024. Accessed July 26, 2024. https://www.forbes.com/sites/davidphelan/2024/07/22/crowdstrike-outage-microsoft-blames-eu-while-macs-remain-immune/

6. Crowdstrike listed on the S&P 500. Business Wire. Accessed September 18, 2024. https://www.businesswire.com/news/home/20240623781335/en/CrowdStrike-Listed-on-the-SP-500#:~:text=AUSTIN%2C%20Texas%2D%2D(BUSINESS%20WIRE,protect%20customers%20and%20stop%20breaches

7. Remediation and Guidance Hub. Crowdstrike, Inc. Accessed September 18, 2024. https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/

8. Bott E. What caused the great CrowdStrike-Windows meltdown of 2024? history has the answer. ZDNet.com. Accessed September 18, 2024. https://www.zdnet.com/article/what-caused-the-great-crowdstrike-windows-meltdown-of-2024-history-has-the-answer/

9. Neprash HT, McGlave CC, Cross DA, et al. Trends in ransomware attacks on US Hospitals, clinics, and other health care delivery organizations, 2016-2021. *JAMA Health Forum*. 2022;3(12):e224873. doi:10.1001/jamahealthforum.2022.4873

10. Health industry cybersecurity—model contract-language for Medtech Cybersecurity. Healthcare & Public Health Sector Coordinating Councils. March 2022. Accessed July 26, 2024. https://healthsectorcouncil.org/wp-content/uploads/2022/03/HSCC-Model-Contract-language-for-Medtech-Cybersecurity-2022.pdf