

Deepening dependency on technology raises risk of breakdowns

July 9 2015, by Michael Liedtke And Barbara Ortutay



Traders work on the floor at the New York Stock Exchange in New York, Wednesday, July 8, 2015. Hong Kong's main stock index plummeted as much as 8.5 percent on Wednesday as a sell-off in mainland Chinese shares accelerated despite new measures to support the market; U.S. stocks were poised to open lower. (AP Photo/Seth Wenig)

When technology breaks down now, people's lives go haywire, too.

Wednesday's confounding confluence of computer outages at United Airlines, the New York Stock Exchange and The Wall Street Journal delivered a jolting reminder about our deepening dependence on interconnected networks to get through each day.

For the most part, technology has worked smoothly while hatching innovations and conveniences that have made our lives easier and our jobs more productive. Computers, though, could bring more frequent headaches as they link together with billions of other electronic devices and household appliances— a phenomenon that has become known as the "Internet of things."

This technological daisy chain will increase the complexity of the systems and raise the risks of massive breakdowns, either through an inadvertent glitch or a malicious attack.

"The problem is humans can't keep up with all the technology they have created," said Avivah Litan, an analyst at Gartner. "It's becoming unmanageable by the human brain. Our best hope may be that computers eventually will become smart enough to maintain themselves."

Technology already is controlling critical systems such as airline routes, electricity grids, financial markets, military weapons, commuter trains, street traffic lights and our lines of communications.

Now, computers are taking other aspects of our lives as we depend on smartphones to wake us up in the morning before an app turns on the coffee pot in the kitchen for a caffeine fix that can be enjoyed in the comfort of a home kept at an ideal temperature by an Internet-connected thermostat designed to learn the occupant's preferences.

Within the next few years, we may even be unlocking our doors with high-tech watches after being chauffeured home in robotic cars.

Technology's relentless march demands better security measures to prevent hackers from breaking into system and more rigid programming standards to reduce the chances of crippling outages, said Lillian Ablon, a technology researcher for the Rand Corp.

"Instead of just letting the technology rush ahead of us and then trying to catch up in terms of privacy and security, we should be baking those things into the systems from the start," she said. "We need to be a little smarter on how we are coding things."

The sequence of Wednesday's outages appears to have been a fluke. Sabotage isn't suspected, FBI Director James Comey said during an appearance before Congress.

But a domino effect may have contributed to The Wall Street Journal's outage. Comey believes the newspaper's website buckled after the New York Stock Exchange's problems caused alarmed investors looking for information to swamp the Journal's website.

The length of Wednesday's outages also is disconcerting, Gartner's Litan said.

It took the New York Stock Exchange more than three-and-half hours to resume trading, slowing Wall Street's usually furious pace. A "router issue" at United Airlines grounded its plane's for nearly two hours, leading to 800 flight delays and 60 cancellations.

"Everyone needs to assume technology is going to go down sometimes, but you should be resilient enough to quickly recover from the outage within a half hour, if not a few minutes," Litan said.

Wednesday's breakdowns were minor inconveniences compared to what might happen if better security measures aren't imposed to keep out intruders bent on wreaking havoc, said Jeff Williams, [chief technology officer](#) for Contrast Security.

Too often, the [technology](#) industry's focus is on creating something cool and worrying about security later, Williams said. He said the lackadaisical attitude breeds a mindset like this: "Oh, we'll just put your blender on the Internet, there are no security issues there. And hackers figure out a way to turn on your blender in the middle of the night and set your house fire."

Computers may get smarter through a combination of better programming, machine learning and more sophisticated chips. If computers can reach the still far-off goal of becoming artificially intelligent, they could be better equipped to prevent problems and fend off unauthorized users. Self-reliant and self-aware computers would still confront humans with a scary question, Litan said: "Are the computers going to be nice to us or are they going to take us out?"

© 2015 The Associated Press. All rights reserved.

Citation: Deepening dependency on technology raises risk of breakdowns (2015, July 9) retrieved 26 April 2024 from <https://phys.org/news/2015-07-deepening-technology-breakdowns.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--