27 Dec 2018 | 15:49 GMT

The Biggest IT Failures of 2018

Technical mishaps occurred in trains, planes, automobiles, and many more places

By **Robert N. Charette**

Illustration: iStockphoto

This year proved once again that IT-related failures "are universally unprejudiced: they happen in every country; to large companies and small; in commercial, nonprofit, and governmental organizations; and without regard to status or reputation." Below is a review that just scratches the surface of the sundry failures, glitches, and other IT hiccups that made the news in 2018.

- Airlines
- Automakers
- Communications
- Cybercrime
- Financial Institutions and Markets
- Government IT
- Health IT
- Policing
- Rail Transport
- Retail

Airlines: Many Delays, But Fewer Than Previous Years

This year saw a slight reduction in the number of flight cancellations and delays due to computer-related problems as compared with the past three years, especially in the United States. Still, some significant incidents occurred.

PSA Airlines, a wholly owned subsidiary of American Airlines, experienced a problem with its crew scheduling and tracking system that led to nearly 3,000 flights being cancelled over seven days in June, and cost the airline an estimated US $35 million. American had brief outages of its own in July and again in November, both blamed on connectivity issues.

Spirit Airlines had multiple IT issues in 2018, including problems in February and March, as well as a system-wide two-hour problem with its dispatching system in August, which delayed dozens of flights. A Southwest Airlines computer problem with its gate and lobby check-in systems at LAX in January lasted more than three hours, causing hundreds of flight delays across its system. Delta Airlines had a three-hour "physical device issue" in September, causing a system-wide ground stop for more than an hour and the delay of some 600 flights.

Air Canada experienced two network-related failures in February and March. British Airways suffered a world-wide computer system problem in July and another computer issue at London Heathrow Terminal Five in September, while Pakistan International Airlines experienced operational issues with its new reservation system, also in September.

An air traffic control computer failure at the Eurocontrol centre in Brussels delayed an estimated 14,000 European flights in April, while over New Year's —and for a second year in a row—the U.S. Customs and Border Protection computer systems experienced an outage, leaving thousands of international passengers across the country in long queues waiting to clear customs. Hopefully, this New Year's won't be a three-peat.

Finally, the recent Lion Air crash off Jakarta may show that the automation paradox is back at work.

Automakers: Another Bumpy Year

According to a study [PDF] by AlixPartners, the number of recalls required to fix defects in vehicle electronic/electrical systems has grown 30 percent per year for the past several years. The problems with vehicle electronics continued unabated throughout 2018.

Fiat Chrysler recalled 5.3 million multiple car models for a cruise control issue, while GM recalled one million pickups and SUVs to fix a steering problem. Toyota recalled 2.8 million hybrids, Subaru recalled 640,000 of its vehicles, and Fiat Chrysler recalled 154,000 minivans, each for stalling-related problems. Software fixes were announced as remedies for all of them.

In addition, a coding error with the spot-welding robots at Subaru's Indiana Automotive plant in Lafayette, Ind., meant 293 of its new Subaru Ascents had to be sent to the car crusher. A similar problem is suspected as the reason behind the welding problems affecting the steering on Fiat Chrysler Jeep Wranglers.

Further, studies are showing that the cost of repair of new auto safety technologies is skyrocketing, which is not good news if vehicle electronic reliability continues to be problematic.

Communications: I Can't Hear You Now

There were sporadic communication problems reported throughout 2018. Australia's telco Telstra suffered a software problem in May that took down its 3G and 4G services nationwide for millions of its customers. Telstra's mobile customers experienced another outage in June, while a network outage crippled Eftpos machines and ATMS across the country in November.

In July, cuts in fiber optic cables disrupted service for 29 million Comcast and Xfinity TV, Internet, and phone customers across the United States.

Telco supplier Ericsson's expired software certificate took down networks in 11 countries in December for nearly a day, causing major headaches for 30 million Softbank mobile customers in Japan and 25 million U.K. O2 mobile customers. Ericsson is likely to pay tens of millions of pounds in compensation.

And the first test of the U.S. presidential emergency alert system took place in October, not without some reported problems.

Cybercrime: Another Banner Year for Attacks

In January, I asked whether U.S. corporations would ever take cybersecurity seriously, and the answer during 2018 still seems to be no.

There have been numerous data breaches and ransomware attacks reported this year, including of airline systems (British Airways, Cathay Pacific), government systems (Atlanta, Matanuska-Susitna, Alaska), healthcare systems (Allscripts, Labcorp, SingHealth), hotel systems (Huazhu, Marriott), and maritime systems (Ports of Barcelona and San Diego, Cosco Shipping). Infrastructure and defense systems continue to be at risk of cyberattacks, too.

Google and Facebook had security and privacy issues this year, as well. Google decided in October to close its Google Plus social network because of a security flaw. Facebook acknowledged in April that 87 million users had their personal data improperly accessed by now-defunct data mining company Cambridge Analytica, and later admitted in September to a "security issue" that exposed 50 million accounts to cybercriminals. In December, Facebook announced that a "bug" allowed possible unauthorized access to 6.8 million users' photos.

A December report [PDF] released by the U.S. House Oversight and Government Reform Committee into Equifax's massive 2017 data breach stated that the breach was "entirely preventable" if the company had followed basic IT security practices. However, the report said, Equifax didn't follow those procedures because the company had little understanding of its own IT systems or the security threat to them. This is a characterization that could fit too many organizations today, unfortunately.

Financial Institutions and Markets: A Year to Forget

This year wasn't kind to financial institutions' IT systems. A botched migration to a new software platform in April at TSB bank in the United Kingdom caused major disruptions for weeks, angered the bank's 5 million customers, and eventually led to the resignation of its CEO.

Recurring IT failures at TSB as well as at other U.K. banks like HSBC and Barclays sparked such a level of public outrage that a parliamentary inquiry was initiated to examine their causes.

The year also hasn't been kind to stock markets. Samsung Securities experienced a $105 billion fat-finger share error in April that was exploited by some of its employees, behavior that helped trigger a Japanese regulatory inquiry into brokerage companies.

There were also IT problems at the Vietnam Stock Exchange (January), Toronto Stock Exchange (April), India's National Stock Exchange and the Multi Commodity Exchange Ltd (May), the New Zealand Stock Exchange (August), and Tokyo's Stock Exchange (October).

Government IT: Protracted Pernicious Pain

Government IT problems were plentiful in 2018, too, although many were just continuations of problems that began years ago. Canada's federal Phoenix payroll system that was disastrously introduced in February 2016 continues to be an "incomprehensible failure" with no replacement in sight. Minnesota's multi-year effort to deliver a fully functional vehicle and driver services system continues to have annoying problems, while Germany's long attempt to deliver a new high-tech frigate is not doing much better.

There were also numerous new IT operational hiccups. Florida's effort to upgrade a major roadway vehicle tolling system in June is still trying to correct numerous billing problems six months later. The U.S. Department of Veterans Affairs so thoroughly mangled the planned year-long computer implementation of the new 2017 veteran education benefits law that the VA admits it will have to start over and take yet another year to implement the law.

The U.S. Internal Revenue Service suffered a major April tax day outage, while Australia's taxation commissioner told businesses to quit whining about the agency's multiple tax system outages since they were "a fact of modern life." The commissioner also told businesses to expect more outages in the future.

New government IT privacy policies also came into effect in 2018. The European General Data Protection Regulation (GDPR) began in May which significantly increases an EU citizen's data privacy rights, while in December, the Australian government moved in the opposite direction by passing legislation [PDF] permitting intelligence and law enforcement agencies to demand companies to disable user encryption protections. How the two laws clash should be interesting to watch in 2019.

Health IT: Running a High Temperature

IT issues plagued healthcare this year, especially concerning U.S. military-related electronic health systems. The U.S. Coast Guard finally admitted defeat after spending $67 million in its mismanaged attempt to develop an electronic health record.

The Department of Defense's $4.3 billion new MHS Genesis electronic health record was characterized as "operational unsuitable" in initial tests by independent reviewers, while the Veterans Department's new $15.8 billion EHR development was already running $300 million over budget less than six months after awarding a contract.

In the U.K., a debate raged over whether the military's decade-old EHR system was putting British service personnel at risk. And some 450,000 women were said to have missed their breast cancer screenings due to an "algorithm failure," but upon further review, this number has been reduced to a maximum of 67,000—and more likely—only 5,000 women.

In Australia, the government has changed the date to opt out from having a government-mandated electronic MyHealth Record to 1 January 2019 from 15 October 2018 after public outcry over the security and privacy of the EHR, as well as its efficacy. At least 1.15 million Australians have so far chosen to opt out.

Finally, studies in the United States indicate some physicians are deciding not to practice medicine because of the administrative burden placed on them by electronic health records. It has gotten so bad, that the American Medical Association has called for an end to electronic health record "abuse" of physicians.

Policing: AI Not Yet to the Rescue

Law enforcement agencies across the world, especially in China, the United States, and the United Kingdom, are increasingly looking to AI to improve their effectiveness and increase efficiencies. However, some experts have expressed concerns that the underlying algorithms are biased, or just don't work very well, as in the case of automated face recognition. These setbacks are not deterring police forces, especially in the United Kingdom, where the Norfolk Constabulary has been deciding whether it should investigate a burglary based on an algorithmic assessment.

In addition, the U.K. government announced in December £1 million in funding for a new AI "hate lab" at Cardiff University which will be used to help predict outbreaks of terror and hate crimes in the country. The thought is that there will be a spike in hate crimes in the United Kingdom following Brexit.

Rail Transport: Code Derailments

IT problems also hit the rail transportation sector this year. Sydney's trains suffered several computer signal failures in August, causing chaos for tens of thousands of passengers over the course of a week. October signal failures also caused havoc on England's South Western Railway as well as on Hong Kong's Mass Transit Railway.

BHP Billiton, the Australian natural-resources company, used rail signals and points in a creative way in November to derail ones of its train. The train, consisting of four locomotives and 268 rail cars filled with iron ore, traveled 57 miles at 110km/h, but without its driver. The cause of the runaway train was attributed to a combination of brake failure, and incorrect operating procedures by the driver.

Retail: The Chickens That Didn't Cross the Road

The retail sector did not go unscathed from IT-related failures, either. German supermarket company Lidl decided in July to scrap an ineffective three-year old merchandise management system after spending more than $565 million on it.

Amazon suffered glitches for several hours in July when demand exceeded expectations on Prime Day, while several retailers had problems over Black Friday sales days. Australian retailer Woolworths also suffered a major outage in April that took down its cash registers across the country.

Demand also couldn't be met by KFC in the United Kingdom after the failure of the logistics management system at its new supplier caused it to shut down 470 stores for several days because of a lack of chicken to fry. KFC's clever public apology help diffuse customers' angst over missing their fried poultry.

This listing of dozens of incidents just scratches the surface of IT-related failures, problems, and issues that occurred this year, and we didn't even begin to explore the plethora of hardware-related or operating system problems reported, as well.

However, all of them serve to remind us how ubiquitous IT is in our daily lives, as well as how consequential it can be when something goes wrong, either by accident or on purpose. Let's hope 2019 sees fewer IT problems, but if past is prologue, I wouldn't bet much money on that happening.