The way in which businesses develop software has changed remarkably over the past decade. Software testing, however, has not experienced this same level of change. Software testing methodologies and tooling have been slow to transform to the needs and demands of enterprises undergoing digital transformation. Until recently, the ideas and tools that could make a difference were only fringe players. That dynamic is changing.

Analyst reports like the Gartner Magic Quadrant for Test Automation make it clear that legacy tools can no longer keep pace with software development. A new era is upon us: one that requires us to rethink our software testing strategies, tool stacks, and priorities, and reimagine what we can accomplish in the software industry.

Reports like the Software Fail Watch provide a much-needed “reality check” for those of us in the testing world. Today, software plays a larger part in consumer and business interactions than ever before, and, yet, the number of news stories of reports of bugs being released into production only continues to grow. However, with the right strategies, approaches to automation, and better alignment with the business, I am confident that trend will change.
SOFTWARE FAIL WATCH:
WHY IT MATTERS

Software has afforded humanity a significant level of convenience, so much so that it’s hard to imagine living without it in much of our professional and personal lives. When was the last time you walked into a bank to transfer funds or cash a check? When was the last time you purchased a plane ticket at an airport counter? How long has it been since you drove to a video rental store and browsed available selections by walking down the aisles? Thanks to software, all of these consumer processes can be done from your own home, and on a mobile device.

Software has become so convenient that when it fails, our life is highly disrupted. And this isn’t just personal convenience that disappears; there are dramatic business implications to software failures and outages. The implications can range from travelers being stranded at airports for days, to highly sensitive data being stolen and made public, and impacts to stock prices that can quickly climb into billions of dollars of lost revenue.

We measure and analyze the year’s biggest headlines in this report because, as our dependency on software grows, so does the social, business, and financial impacts when it fails. How can organizations reverse this trend?

While many have modernized the ways they develop and deploy software in order to release digital services faster, the modernization of software testing has lagged behind. Legacy software testing tools that were developed two decades ago—some which are still heavily in use today—were never intended to support high levels of quality in today’s rapid release cycles. It’s time for a change.
2017'S SOFTWARE FAIL WATCH TOTALS

SOFTWARE FAILS STORIES COMPANIES
To find the total amount of people affected, we added all the numbers we had pulled: i.e., cars recalled, mobile phones with malware, paychecks undelivered, accounts hacked, etc. and assumed that each item directly affected one person.

That means that in reality, our end sum is on the conservative side. It is far more likely that for every car recalled, a larger total number of people were affected, with further implications that rippled outwards in a software “butterfly effect”.

Statistically, there is a very good chance that you have been personally impacted by a software failure this year – perhaps even in the last quarter, or week.
SOFTWARE FAIL STORIES BY MONTH
2017
LO$$E$ FROM SOFTWARE FAILURES (USD)

1,715,430,778,504

ONETRILLIONSEVENHUNDREDFIFTEENBILLIONFOURHUNDREDTHIRTYMILLIONSEVENHUNDREDSEVENTY-EIGHTTHOUSANDFIVEHUNDREDFOUR
Every CIO I’ve ever known has had large, board-visible projects where a defect discovered at the release date is so critical that it requires a major redesign of the project that leads to tens, if not hundreds of millions of dollars in costs, massive delays, and a huge loss of credibility.

TODD PIERCE
Healthcare and Life Sciences Board Member and Executive
ACCUMULATED TIME LOST

46 MINUTES
8 HOURS
3 DAYS
2 WEEKS
8 MONTHS
268 YEARS
What industries top the software failure headlines? In previous years, software failures tied to Public Services and Healthcare got the most news coverage, with an average of 15 bug-related stories per month. This year however, Retail and Consumer Tech has taken the lead with 19 stories per month - in large part thanks to buggy smartphone updates and the exploits of security researchers or hackers.

Other numbers indicate a change in the trends we had observed in past editions of the Software Fail Watch. Between July and August of 2017, the average total of software failure stories increased by 25% over previous months, and stayed high for the remainder of the year. While this jump is most remarkably reflected in the Consumer Tech and Retail industries, each industry's failures reach its yearly high point between August and October of 2017.
SOFTWARE FAILURE STORIES BY MONTH

304 stories picked up by multiple news outlets
There are far more software bugs in the world than we will likely ever know about.
Comparing 2017’s data against previous years paints an interesting picture. While the overall total number of software failure stories in the news has grown, several industries were reported on far less than in previous years. Failures in Services and Utilities, and the Entertainment industries, saw a three-year low in media coverage against their 2015 and 2016 rankings. Transportation industry bug stories dipped slightly, while Finance remained roughly even with previous years.

Which industry saw the biggest drop in media coverage? Public Services and Healthcare. Once the highest reported on by far, this year’s numbers are approximately 30% lower than 2016’s all-time high of 187 media stories. And, on the flipside, Retail and Consumer Tech industry clocked in with 197 software failure stories, which was a staggering near-80% increase from 2016.

In spite of the decrease of bugs covered by the media within certain industries however, the overall total number of software bugs reported has grown. While the hard numbers gleaned from 2017 indicates that the total of people affected by software bugs decreased in 2017, adding in the year’s security vulnerabilities and hacks, would suggest otherwise. Hacks and vulnerabilities aren’t always “bugs” but many are certainly detectable and even preventable. These attacks carry an even greater risk of media coverage that can quickly lead to brand erosion, financial loss, and even greater media coverage.
“Embedded” includes all software that is built into a device or piece of hardware. If a casino’s slot machine experienced a software glitch, or a car’s airbag sensor malfunctioned, it was placed into this category. Transportation makes up the majority of this category, with 41 of 113 stories. This is unsurprising given that most Transportation software fails stem from a problem programmed in the vehicle itself, be it car, plane, or train.

“Mobile/Cloud” encompasses all web or app-based software. If a website crashed due to a software fail, it went into this category. While each industry was well represented (showing how even industries that traditionally run legacy software have jumped on the mobile boat), Retail and Consumer Tech predictably took the lead with 125 stories. Of those 125 stories, 72 featured hardware and smart phone manufacturers such as Apple, Alphabet, or Samsung.

“Enterprise Apps” encompasses all software that requires installation in a specific location. If an organization’s internal system, such as an ERP (Enterprise Resource Planning) or accounting software crashed, it went into this category. Enterprise Apps software exists within every industry. However Public Services and Healthcare overwhelmingly dominates this list, making up 42% of the stories in this category.
The software fail stories we record are split into one of three categories: software bugs, security vulnerabilities, and usability glitches. The first, and most common, is a software bug: an instance in which a software application fails to work as intended. The second type is a security vulnerability: a flaw that attackers can exploit to alter a system's behavior or steal data. The third and final is a usability glitch: a software design flaw that decreases the product or application's "ease of use" – in many cases, rendering the product unusable.
TYPE OF FAIL BY INDUSTRY

ENTERTAINMENT
- Security Vulnerability: 20
- Usability Glitch: 4
- Software Bug: 8

FINANCE
- Security Vulnerability: 30
- Usability Glitch: 10
- Software Bug: 8

PUBLIC SERVICE AND HEALTHCARE
- Security Vulnerability: 27
- Usability Glitch: 22
- Software Bug: 11

RETAIL AND CONSUMER TECH
- Security Vulnerability: 109
- Usability Glitch: 5
- Software Bug: 4

SERVICE AND UTILITIES
- Security Vulnerability: 27
- Usability Glitch: 13
- Software Bug: 4

TRANSPORTATION
- Security Vulnerability: 21
- Usability Glitch: 13
- Software Bug: 9
Approximately 274 of the companies mentioned in software fail headlines in 2017 were public companies. While it is not always possible to trace the effects of a software fail in the rise and fall of a company's stock prices, there are times when the correlation is unmistakable.

In August 2017, Provident Financial, a UK-based sub-prime loan company, lost £1.7 billion of its market value in just one day. The crash happened after the CEO of Provident Financial announced that the implementation of a new appointment scheduling application had malfunctioned so badly that only 57% of loan debts had been collected on time.

The buggy software, which had been part of a £21.6 million department overhaul, ultimately costing the company £120 million in profit loss over the course of 2017. Following the announcement, the CEO of Provident Financial resigned. The stock value crash is believed to be the largest one-day share price plummet in the history of the blue chip FTSE 100 index history.
Digital transformation offers great opportunities for improving software quality. Specifically, continuous testing can improve the UX through added user acceptance testing (UAT), by reducing risk and by bolstering security to prevent a failure that rapidly erodes brand trust and loyalty.

MANISH MATHURIA

CTO and Co-founder, Infostretch
Power Surge causes system failure
Back-up System fails to engage

Booking system: British Airways forced to rebook 50,000 people on 30 other airlines; RyanAir sees surge in last minute bookings

Arriving Airplanes: Thousands of people forced to wait for hours on tarmac to disembark

Check in desks: No computerized check-in possible; Airport staff has to use whiteboards to display flight information

Mobile phone apps: No mobile check-in possible; British Airways has to reimburse premium phone charges

Baggage handling: “Tens of thousands” of passenger bags left sitting in warehouses

Arriving Airplanes: Over 1000 flights canceled over 3 days

Booking system: Over 75,000 people affected

British Airways: Estimated compensation bill of over $200 million

British Airways: Share price dropped by over $220 million

THE ANATOMY OF A SOFTWARE FAIL
BRITISH AIRWAYS, MAY 27, 2017
Software failures within the Public Services and Healthcare industries dominated the media’s coverage of other industries. While we saw 30% fewer stories about Public Services and Healthcare in 2017 than in the previous year, the failures and vulnerabilities that made it onto the media’s radar this year were more than troubling. We saw countless stories of hacking and tampering with international election processes, WiFi vulnerabilities that exposed the data of billions of people, IT issues that caused tens of thousands of letters that went unsent to patients and doctors, millions of dollars in overpaid medical billing — the list goes on and on.

A government organization contracts a software development company to customize software that can fulfill complex operations and process massive amounts of data. Implementation of the finished software doesn’t go as planned however, compounded by the fact that many of the end users working with the software on a daily basis are not adequately trained on the new interface.

Though several bugs surface during and shortly after implementation, decision makers are pressured to move ahead since they already invested large amounts of public funds into the project. The bugs eventually come to light however, when a glitch affects the public. A small scandal is kicked up over the cost of the new software, and the organization moves to either fix the bugs with the contractor, or takes legal action to break the contract.

Many people, especially those directly affected by these types of errors, read these stories and wonder, “How in the world did they let this happen?” Though the causes of these failures and vulnerabilities are multifaceted, the chain of events tends to go something like this:

# OF FAILS IN 2017 PER BRANCH

- **15** ELECTIONS
- **23** TAXATION
- **26** PUBLIC SUBSIDIES
- **24** GOVERNMENT ADMINISTRATION
- **33** HEALTHCARE
- **37** SAFETY & DEFENSE
The Entertainment category encompasses stories ranging from video and game app failures, to media company hacks and bugs in social media platforms. Some of the biggest stories in this category include the arrest of a Pakistani man, when Facebook incorrectly translated his “good morning” to a threat, the leak of unaired HBO Game of Thrones episodes, and an Instagram API hack that stole the private data of many celebrity users. As more and more of our entertainment options turn 100% digital, the likelihood and resulting damage of an app being unable to handle the load increases dramatically. Perhaps the most vivid example in 2017 was Niantic’s epic Pokemon Go Fest failure. Following the rampant success of Pokemon Go, Niantic organized a sold-out festival in Chicago, promising that several rare Pokemon would be available to catch. 20,000 Pokemon Go players flooded the festival grounds, only to find that both the game and the cellular service networks were continually crashing under the load. The day spiraled into a PR nightmare as attendees grew increasingly angry, the festival was deemed a catastrophe, and lawsuits have sprung up in its aftermath.

Source: www.gamerant.com/pokemon-go-fest-niantic-hanke-letter
While vehicle recalls are the most ubiquitous of the Transportation industry-related software fails, the bugs that create the biggest uproar are certainly airline outages. While only 14 of the reported transportation stories pertained to air travel, the rage that these types of bugs elicit ensures broad media coverage and palpable brand damage. British Airways took one of the biggest hits, with 6 outages within 2017 – 3 of which took place in the span of 1 month. An outage in May 2017 spawned global chaos over the course of 2 weeks, causing a total loss of $200 Million and as much as a 4% percent drop in stock price that erased hundreds of millions from the company’s value.

2017 also saw a surprising increase in train-related software bugs, 4 of which, oddly enough, took place in Denver, Colorado. The biggest train bug of the year took place in Singapore. A software safety mechanism failed, causing two metro trains at Joo Koon station to crash into each other. 38 people were injured, and the scheduled maintenance to fix the bug will impair train operations for over 6 months.

These types of bugs often occur as a result of routine software updates, a fact which underscores the necessity of end-to-end testing. This is particularly true within highly-complex system landscapes like transportation logistics, when the lives of customers—not just financials—are at stake.

Source:
www.telegraph.co.uk/business/2017/05/31/shares-british-airways-owner-iag-skid-failure-chaos
It's been less than a decade since the smartphone took off and became a public mainstay. Now, the devices are so embedded in our daily lives that they have influenced everything from banking to parenting philosophy.

The Internet of Things has solidified the role that consumer tech plays in retail and in our lives. All of this means that as companies race to be on the “bleeding edge” of innovation, the “small” bugs we consumers encounter can quickly escalate into full-blown product disasters.

Take, for example, Apple’s spate of autocorrect bugs in 2017. The release of iOS 11 revealed a typing bug that would autocorrect the word “I” to “A□”. While the bug is, functionally speaking, a mere nuisance, the situation was aggravated by two factors. First, there are currently more than 700 million iPhones in use worldwide. Second, 6 billion SMS messages are sent per day – and that’s just in the United States! The global estimate falls at 8.6 trillion messages per year.

With so many consumers encountering the same “nuisance” of a bug upwards of 50 times a day, it is no wonder that something as simple as an autocorrect glitch can become one of the most talked-about bugs of 2017.

Source: www.fortune.com/2017/03/06/apple-iphone-use-worldwide
wwwedition.cnn.com/2012/12/03/tech/mobile/sms-text-message-20
Some failures can be fixed with a rapid rollback, however, we've had critical systems go down for as many as seven days, and had to revert to manual processes. This 'solution' created frustration for our customers, sales and employees—the impact to our downstream processes was huge.

CIO
Major US Retailer
The Service and Utilities category covers stories ranging from hotel booking bugs to internet and power outages. These industries play a significant, though quiet, role in our daily lives. Whether it’s through travel, electricity, or the internet, the work of a service-oriented company often provides crucial support to the work of government organizations, retail, and healthcare. Without the services these companies provide, many other companies simply cannot function.

Take, for example, the late February disruption of Amazon’s cloud storage service, AWS. Though the service was only down for a few hours, it is estimated to have knocked out over 100,000 websites including Github, Slack, and Expedia. Internet of Things devices were also affected, prompting one Twitter user to share that they had lost control of their TV, lights, and front gate, all as a result of the outage.

---

Source: www.seattletimes.com/business/amazon/outage-in-aws-storage-service-causing-online-disruptions
As shown in each year of this report, software failures in the finance industry rarely hit the headlines. This is not because the industry does not have software fails – rather, it is because of two reasons. One, major financial institutions often have powerful crisis control teams that quickly draw attention away from negative news, and, two, much of a financial institution’s software lies behind the scenes, away from the public eye.

This makes it easier for bugs to be patched quickly, before their repercussions can snowball into a major news story. The finance-related bugs that do come to light either take place in public view (such as in the stock market, online banking, or ATM withdrawals), or feature bugs so catastrophic that the story cannot be buried.

It is also possible that the Finance industry has more incentive to be vigilant in their fight against software bugs. Massive legal fines and possible lawsuits await any organization that is seen as having mishandled money or data. It would also appear that financial institutions are more scrupulous about maintaining their public image than companies in other industries. Many people are already wary of trusting their hard-earned money to a bank. A proliferation of software bugs, blocking them from accessing their accounts, would only confirm their fears.
“Although not distinctly measured, testing is one of the last components of our process that we invest in—which is common in this industry. To date, it's been hard to justify continuing to increase the funding around our current testing strategy, because our quality just isn't increasing accordingly.”

CIO
US Commercial Bank
Brand damage and erosion is one of the primary side-effects of the public announcement and media coverage of software bugs, failures, hacks, and vulnerabilities. Quantifying the extent of that damage however, is not an easy task. Stocks are simple enough to track, but how do you measure the damage to a brand’s reputation amongst their customers, or even amongst those considering becoming one of their customers? And is there an industry that is especially prone to damage when a software fail is exposed?

To answer these questions, we created a Brand Erosion Index. We started by sampling a random selection of stories from each industry, ensuring to select stories from diverse points throughout the year and covering a variety of topics. We then started researching the keywords from each story, noting down the number of relevant news hits we found. Finally, we averaged the numbers from each story together into an industry ranking – the higher the number of stories published on a specific software bug, the greater the level of damage done to a company’s brand.

The industry that came out on top, with the highest level of media-driven brand damage per bug, is Consumer Tech. This was a somewhat surprising find, given that the software fails around Healthcare, Finance, and Public Services tend to threaten health and well-being – a far more serious situation than a botched smartphone update.

The truth, perhaps, lies in our choices as consumers. If you are unhappy enough with your smartphone, it is relatively easy to change to another company. This is not the case however, with a government contractor, where the choice of service or software provider lies entirely out of the consumer’s hand. This fact raises the tolerance level for bugs beyond anything consumers would stand for in a retail company. Another factor is the speed at which companies within the consumer tech industry are forced to innovate and release products. The race to lead the market can result in the quick release of poorly tested software – a story we have seen repeated over and over (and over) in 2017.

With the speed at which those in the media can get stories online, and the far faster speed that consumers can share their feelings via blogs, comments, GIFs, emojis, petitions and demands, brand erosion can quickly spread from social media to stock prices.
Transforming testing is emerging as a stealth strategy to take your digital transformation initiatives to the next level. Many organizations are quietly transforming their testing process to deliver instant insight into the business risks of each release candidate.

TERRY MILHOLLAND
Former CIO Internal Revenue Service
SCARIEST
Noida fire: Automatic doors trapped six persons, says Fire dept
Six people tragically died in an office fire after being trapped between sets of automatic doors. The doors were not built with a manual fail-safe in case of emergencies, so when the electricity cut out, the software shut down—locking the doors and the unfortunate victims inside.

FUNNIEST
Connected sex toys recorded intimate sessions without consent
A Reddit user took to the forums to share his discovery that his Internet of Things connected “adult toy” was recording audio files during usage, and saving them to his phone. The embarrassing discovery was quickly picked up by mainstream media, causing the toy’s maker, Lovense, to scramble their way out of a privacy intrusion and PR nightmare.

BIGGEST WTF
Facebook’s translation software got a man wrongly arrested
A Palestinian man was wrongly arrested by Israeli officials after Facebook mistranslated his post. The construction worker posted a photo of himself by a bulldozer, with the caption “Good morning” written in Arabic. Facebook translated the message to “Attack them” in Hebrew, and “Hurt them” in English. The unfortunate man was arrested by (assumedly) non-Arabic speaking police, and held as a possible terrorist before the mistake was discovered. Facebook offered no explanation as to how the translation mistake occurred.
EQUIFAX HACK STEALS DATA OF OVER 50% OF AMERICANS

Equifax, one of the United States' largest credit reporting agencies, faced a crippling scandal in 2017 after belatedly announcing that up to 143 million of their consumer records, including names and social security numbers, were stolen by hackers. Equifax also reported that 209,000 credit card numbers were stolen, along with the driver's licenses of 700,000 UK citizens and 10 million US citizens. Given that the population of the United States clocks in at 331 million, this means that approximately 50% of Americans could now find themselves in danger of identity theft or worse. Though the hack took place in May 2017, Equifax hid the story until early September, further outraging the public.

WANNACRY ATTACK PARALYZES COMPANIES WORLDWIDE

The WannaCry ransomware attack hit more than 230,000 computers in over 150 countries–making it the largest ransomware attack in history. The virus, which primarily targeted a bug in a common but out-of-date version of Microsoft Windows, locked operating systems, holding the contents for ransom until the users paid a fine. Within less than 24 hours, the British National Health Service (NHS), Germany and Russia’s national railway, Chinese universities, Spanish and Russian phone companies, Brazilian social security agencies, Slovenian factories, and many more had fallen victim. It took 3 days and a 22 year-old British security researcher (now being hailed as a hero) to finally halt the attacks. Global financial damage is estimated to reach upwards of $4 billion.

KRACK VULNERABILITY IN GLOBAL WIFI

The discovery of the security exploit dubbed “Krack” opened up a vulnerability in billions of devices around the world. Virtually any device using WiFi was at risk. The exploit targeted WPA2, an extremely common authentication method used to establish the connection with WiFi and a device. Consumer tech and service providers jumped to address the issue, though the ubiquitous nature of the bug made many efforts to guard against it feel fruitless.

UBER PAYS OFF HACKERS

For the ride-sharing service Uber, 2017 was packed with scandals. The latest came to light in November, when Uber admitted to falling victim to a hack that stole 57 million user records and 600,000 driver’s licenses. The hack, which took place in late 2016, was covered up for over a year by Uber executives, who paid the hackers $100,000 to delete the stolen data. Uber’s failure to disclose the hack potentially violates several state laws, placing the already embattled company in even deeper trouble.

BIGGEST HACKS OF 2017
STATE GLITCH PUTS DATA OF 1.9 MILLION PEOPLE AT RISK

The state of Michigan discovered that the private information of 1.9 million people had been exposed due to a software glitch stemming from a system upgrade, affecting more than two-fifths of the state’s workforce. The situation looked particularly bad as the system in question had recently come under fire for a series of software bugs that had resulted in over 20,000 innocent people being falsely accused of fraud. The government had just settled a federal lawsuit over the matter when the latest damning bug came to light.

detroitnews.com/story/news/local/michigan/2017/02/03/uia-msp/97454924/

SOFTWARE ISSUES CAUSE 22,000 HOSPITAL LETTERS TO GO UNDELIVERED

The Worcestershire Acute Hospitals NHS Trust in the United Kingdom admitted to being aware of an astounding 22,000 patient letters that had gone undelivered over a period of 6 years due to a software bug. At the time of writing, the hospital had reviewed 11,000 of the letters for follow-up, and had 11,000 to go. As shocking as this story may seem, this event was unfortunately only one in a string of hospital correspondence glitches in 2017.
digitalhealth.net/2017/08/it-issues-causes-22000-undelivered-letters-at-worcestershire-acute/

VULNERABILITY COULD ALLOW HACKERS TO CONTROL NUCLEAR POWER PLANTS

A security company uncovered a critical security vulnerability in the software controlling over 200 sensitive Australian government sites. The bug, if exploited, would allow hackers to take over control of highly-secured areas such as Sydney’s nuclear power plant and a Royal Australian Air Force base— all without so much as login access.

3 MONTHS OF CHILD ABUSE TIPS UNREPORTED

The state of Florida discovered that nearly 1500 reported cases of child abuse had been overlooked due to a software glitch. The bug caused the stories to be collected, but never forwarded to the correct jurisdictions for law enforcement follow up. Though the glitch began in early February 2017, it was not discovered until May 2017, putting the safety of 1500 children at risk in the meantime.

tampabay.com/news/child-abuse-tips-silenced-for-months-by-dcf-computer-glitch/2323316

709,000 PIECES OF MEDICAL MAIL UNDELIVERED

The United Kingdom’s National Audit Office discovered that 709,000 pieces of medical mail had never been delivered to the patients or their General Practitioners thanks to a software glitch. The backlog of letters had been stacking up for five years, thrown into boxes and stored in a warehouse. 500,000 of the letters were found to have contained confidential patient data, and 1,700 cases were identified where the missing information could have caused the patient serious bodily harm.

The company charged with delivering the letters had reportedly known about the issue since 2014.
digitalhealth.net/2017/06/10,000-cases-of-potential-harm-from-medical-correspondence-error/

COMPUTER GLITCH EXTEND MAN’S JAIL SENTENCE BY 5 MONTHS

An inmate had his 1-year prison sentence extended by 5 months due to a software glitch that could be affecting hundreds of inmates. Reports claim that the prison facility technicians had been warned of the bug that altered saved changes, causing data to “display incorrectly” unless closely monitored. However, there was no word on whether efforts had been made to fix the $1.5 million software system. Since the story broke, lawsuits have been filed stating that hundreds of other inmates had their sentences unlawfully extended due to the same software bug.
slate.com/blogs/suture-tense/2017/11/3/inmate_had_to_remain_in_prison_for_five_extra_months_likely_due_to_a.html
The Software Fail Watch has grown in popularity with each year’s release. In years past, we’ve kept our focus on which industries had the most bugs, failures, and hacks reported on, and tried to spot trends around whether certain industries were getting better about keeping bugs out of production. However, just because a bug doesn’t make it to the front page of multiple newspapers and websites, doesn’t mean it never existed. There are some industries that are better at keeping these stories under wraps, and there are some industries that media outlets simply may not have the same desire to publish stories about.

What we noticed in this year’s report—in all industries—was really the butterfly effect, and the rapid increase in brand erosion as news coverage and negative social media posts ramp up. All it takes is a single critical bug in the hands of your consumers for the damage to begin. Like the saying goes, “Where’s the worst place to find out about a bug in your software? Twitter.” Once your customers are sharing screenshots of their error message, reporting poor customer service and lost data, one unhappy customer quickly becomes 10. Then a news story comes out and now it’s 100 unhappy customers—after multiple sites curate and republish that original story it’s 500. Soon your support team is inundated with the same complaint for which they don’t have an estimated repair time. Before you know it, you’re being added to next year’s version of the Software Fail Watch.

We don’t publish this report to call out any one particular industry, or bring everyone’s attention back to a failure that’s long since been repaired. Our hope is that by publishing the Software Fail Watch we can only shed some light on just how impactful software failures can be. But, more importantly, this year’s report has shown that even if many organizations have figured out how to develop and release software much more quickly—many continue to struggle with quality. The good news is that as more organizations turn to a modernized, continuous testing strategy that meets the needs of accelerated development of complex software, we may actually decrease the number of failures in this annual report, and in the software we’ve all come to rely upon so heavily.
The Software Fail Watch is an analysis of software bugs found in a year’s worth of English language news articles. To find the stories, we set up a Google account with alerts for phrases such as “software glitch” and “software bug.”

Then we manually sort through each of the alerts, picking out promising headlines, reading the articles for relevance, and noting down any specific details of interest. While reading the articles we ask ourselves questions like: What industry does this story fall into? Does the article say how much the affected software cost to implement? Does it mention how many products were recalled? How long was the system down? Is the associated company public, private, or a government contractor?

You get the idea.

If the article reported a unique software bug, we extract as much information as possible and log it into a detailed Excel sheet. No exact numbers are recorded unless they are explicitly stated in the article itself.

Stories that appear in multiple news alerts and are covered by multiple reputable sources are marked as having a “high level” of brand damage.

In the end, we categorized all the stories into 9 broad industry categories: Public Services, Healthcare, Retail, Consumer Tech, Finance, Utilities, Services, Transportation, and Entertainment.

In the following pages, you will find a breakdown and analysis of the software fails we collected in the last calendar year. While we could never claim to have comprehensively covered every software fail of 2017, the data does undeniably reveal one truth: when software doesn’t work, the world notices.
If you are a tester, it behooves you to ask
»Is whatever I’m doing now advancing the
mission? Am I focused on investigating the
product and finding important problems,
or am I being distracted from that mission?«

In my view, until testers are clear on that
themselves, the organization won’t be clear
on it either.

MICHAEL BOLTON
Principal Consultant, DevelopSense
RESOURCES

WHITEPAPER
Agile is All About Change…Why Does Testing Remain the Same?
www.tricentis.com/resource-assets/agile-testing-continuous-testing/

VIDEO
What CxOs Really Think About Testing, Todd Pierce
youtube.com/watch?v=J_F5ssmvAqI&index=3&list=PLVOwF-9pokc5ZZgw7vhtjc14w1By8pyf

FREE TRIAL – LOAD TESTING
Load Testing with Flood
flood.io/users/sign_up

FREE TRIAL – EXPLORATORY TESTING
Exploratory Testing for Jira
marketplace.atlassian.com/plugins/com.tricentis.jira.plugins.exploratorytesting.jira-plugin/server/overview