6 Real-Life Business Continuity Examples You'll Want to Read

by Tracy Rock | Dec 20, 2018

It's no secret that we believe in the importance of disaster preparedness and business continuity at every organization. But what does that planning actually look like when it's put to the test in a real-world scenario?

Today, we look at 6 business continuity examples to show how organizations have worked to minimize downtime (or not) after critical events.

Back To Top

Business Continuity Examples: The Good, The Bad & The Ugly

1) Ransomware hobbles the city of Atlanta

There has been no shortage of headline-making ransomware attacks over the last few years. But one that stands out (and whose impact was still reverberating at the time of this writing) was the March 2018 SamSam ransomware attack on the City of Atlanta.

The attack devastated the city government's computer systems, disrupting numerous city services, including its police records, courts, utilities, parking services and other programs. Computer systems were shut down for 5 days, forcing many departments to complete essential paperwork by hand. Even as services were slowly brought back online over the following later, the full recovery took months.

Attackers demanded a $52,000 ransom payment. But when all was said and done, the full impact of the attack was projected to cost more than $17 million. Nearly $3 million alone was spent on contracts for emergency IT consultants and crisis management firms.

The Atlanta ransomware attack is a lesson in inadequate business continuity planning. The event revealed that the city's IT was woefully unprepared for the attack. Just two months prior, an audit found 1,500 to 2,000 vulnerabilities in the city's IT systems, which were compounded by "obsolete software and an IT culture driven by 'ad hoc or undocumented' processes," according to StateScoop.

Which vulnerabilities allowed the attack to happen? Weak passwords, most likely. That is a common entry point for SamSam attackers, who use brute-force software to guess thousands of password combinations in a matter of seconds. Frankly, it's an unsophisticated method that could have been prevented with stronger password management protocols.

Despite the business continuity missteps, credit should still be given to the many IT professionals (internal and external) who worked to restore critical city services as quickly as possible. What's clear is that the city did have some

Back To Top

disaster recovery procedures in place that allowed it to restore critical services. If it hadn't, the event likely would have been much worse.

2) Fire torches office of managed services provider (MSP)

Here's an example of well-executed business continuity:

In 2013, lightning struck an office building in Mount Pleasant, South Carolina, causing a fire to break out. The offices were home to Cantey Technology, an IT company that hosts servers for more than 200 clients.

The fire torched Cantey's network infrastructure, melting cables and burning its computer hardware. The equipment was destroyed beyond repair and the office was unusable. For a company whose core service is hosting servers for other companies, the situation looked bleak. Cantey's entire infrastructure was destroyed.

But ultimately, Cantey's clients never knew the difference.

As part of its business continuity plan, Cantey had already moved its client servers to a remote data center, where continual backups were stored. Even though Cantey's staff were forced to move to a temporary office, its clients never experienced any interruption in service.

It was an outcome that could have turned out very differently. Only five years prior, the company had kept all of its client servers on site. But founder Willis Cantey made the right determination that this setup created too many risks. All it would take is one major on-site disruption to wipe out his entire business, as well as his clients' businesses, potentially leaving him exposed to legal liabilities as well.

Cantey thus implemented a more comprehensive business continuity plan and moved his clients' servers off-site. And in doing so, he averted disaster.

Back To Top

3) Computer virus infects UK hospital network

In a recent post, we highlighted one of the worst business continuity examples we saw in 2016. In November, a nasty computer virus infected a network of hospitals in the UK, known as the Northern Lincolnshire and Goole NHS Foundation Trust. The virus crippled its systems and halted operations at three separate hospitals for five days. Patients were literally turned away at the door and sent to other hospitals, even in cases of "major trauma" or childbirth. Only critical emergency patients, such as those suffering from severe accidents, were admitted. In total, more than 2,800 patient procedures and appointments were canceled because of the attack.

A report in Computing.co.uk speculated that there had been no business continuity plan document in place. Even if there had been, clearly there were failings. Disaster scenarios can be truly life-or-death at healthcare facilities. Every healthcare organization must have a clear business continuity plan outline with comprehensive measures for responding to a critical IT systems failure. If there had been in this case, the hospitals could have remained open with little to no disruption.

The hospital system was initially tight-lipped about the attack. But in the year following the incident, it became clear that ransomware was to blame – specifically, the Globe2 variant. Interestingly, however, hospital officials did not say the ransomware infection was due to an infected email being opened (which is what allows most infections to occur). Instead, they said a misconfigured firewall was to blame. (It's unclear then exactly how the ransomware passed through the firewall—it may have come through inboxes after all.) Unfortunately, officials knew about the firewall misconfiguration before the attack occurred. They had plans to fix the problem, but they were too late. The attack occurred "before the necessary work on weakest parts of the system had been completed."

4) Electric company responds to unstable WAN connection

After a major electric company in Georgia experienced failure with one of its data lines, it took several proactive steps to ensuring its critical systems would not experience interruption in the future. The company implemented a FatPipe WARP at its main site, bonding two connections to achieve redundancy, and it

Back To Top

also readied plans for a third data line. Additionally, the company replicated its mission-critical servers off-site, incorporating its own site-failover WARP.

According to Disasterrecovery.org, "Each office has a WARP, which bonds lines from separate ISPs connected by a fiber loop. They effectively established data-line failover at both offices by setting up a single WARP at each location. They also accomplished a total site failover solution by implementing the site failover between the disaster recovery and main office locations."

While the initial WAN problem was minimal, this is a good example of a company that is planning ahead to prevent a worst-case scenario.

5) German telecom giant rapidly restores service after fire

Among the better business continuity examples we've seen, incident management solutions are increasingly playing an important role. Take the case of a German telecom company that discovered a dangerous fire was encroaching on a crucial company facility. The facility was a central switching center, which housed important telecom wiring and equipment that were vital to providing service to millions.

The company uses an incident management system from Simba, which alerted staff to the fire, evaluated the impact of the incident, automatically activated incident management response teams and sent emergency alerts to Simba's 1,600 Germany-based employees. The fire did indeed reach the building, ultimately knocking out the entire switching center. But with an effective incident management system in place, combined with a redundant network design, the company was able to fully restore service within six hours.

6) Internet marketing firm goes mobile in face of Hurricane Harvey

Research shows that 40-60% of small businesses never reopen their doors after a disaster. Here's an example of one small firm that didn't want to become another statistic.

Back To Top

In August 2017, Hurricane Harvey slammed into Southeast Texas, ravaging homes and businesses across the region. Over 4 days, some areas received more than 40 inches of rain. And by the time the storm cleared, it had caused more than $125 billion in damage.

Countless small businesses were devastated by the hurricane. Gaille Media, a small Internet marketing agency, was almost one of them. Despite being located on the second floor of an office building, Gaille's offices were flooded when Lake Houston overflowed. The flooding was so severe, nobody could enter the building for three months. And when Gaille's staff were finally able to enter the space after water levels receded, any hopes for recovering the space were quickly crushed: the office was destroyed, and mold was rampant.

The company never returned. However, its operations were hardly affected.

That's because Gaille kept most of its data stored in the cloud, allowing staff to work remotely through the storm and after. Even with the office shuttered, they never lost access to their critical documents and records. In fact, when it came time to decide where to relocate, the owner ultimately decided to keep the company decentralized, allowing workers to continue working remotely.

Had the company kept all its data stored at the office, the business may never have recovered.

Examples of poor business continuity planning

Some of the real-life business continuity examples above paint a picture of what can go wrong when there are lapses in continuity planning. But what exactly do those lapses look like? What are the specific failures that can increase a company's risk of disaster?

Here are the big ones:

- **No business continuity plan:** Every business needs a BCP that outlines its unique threats, along with protocols for prevention and recovery.

- **No risk assessment:** A major component of your BCP is a risk assessment that should define how your business is at risk of various disaster scenarios. We

Back To Top

list several examples of these risks below.

· **No business impact analysis:** The risk assessment is useless without an analysis of how those threats actually affect the business. Organizations must conduct an impact analysis to understand how various events will disrupt operations and at what cost.

· **No prevention:** Business continuity isn't just about keeping the business running in a disaster. It's about risk mitigation as well. Companies must be proactive about implementing technologies and protocols that will *prevent* disruptive events from occurring in the first place.

· **No recovery plan:** Every disaster scenario needs a clear path to recovery. Without such protocols and systems, recovery will take far longer, if it happens at all.

Examples of threats to your business continuity

It's important to remember that business-threatening disasters can take many forms. It's not always a destructive natural disaster. In fact, it's far more common to experience disaster from "the inside" – events that hurt your productivity or affect your IT infrastructure and are just as disruptive to your operations.

Example threats include:

· Data loss

· Cyberattacks

· Malware and viruses

· Network & internet disruptions

· Hardware/software failure

· Fire

· Natural disasters

Back To Top

- Severe weather
- Flooding (including pipe bursts)
- Terrorist attacks
- Office vandalism/destruction
- Workforce stoppages (transportation blockages, strikes, etc.)

The list goes on and on. Any single one of these threats can disrupt your business, which is why it's so important to take continuity planning seriously.

Business continuity technology

Within IT, data loss is often the primary focus of business continuity and disaster recovery (BC/DR). And for good reason …

Data is the lifeblood of most business operations today, encompassing all the emails, files, software and operating systems that companies depend on every day. A major loss of data, whether caused by ransomware, human error or some other event, can be disastrous for businesses of any size.

Backing up that data is thus a vital component of business continuity planning.

Today's best data backup systems are smarter and more resilient than they were even just a decade ago. Solutions from Datto, for example, are built with numerous features to ensure continuity, including hybrid cloud technology (backups stored both on-site and in the cloud), instant virtualization, ransomware detection and automatic backup verification, just to name a few.

Like other BC initiatives, a data backup solution itself won't prevent data-loss events from occurring. But it does ensure that businesses can rapidly recover data if/when disaster strikes, so that operations are minimally impacted – and that's the whole point of business continuity.

Back To Top

Learn more: request a free demo

For more information on data backup solutions from Datto, request a free demo – or contact our business continuity experts at Invenio IT by calling (646) 395-1170 or by emailing success@invenioIT.com.

> **YOU MIGHT ALSO LIKE: What are the benefits of converged infrastructure?**

Check Out Our Must Read Articles:

1. **11 Questions to Ask about a Small Business Backup Solution**
2. **Barracuda Backup vs. Datto: How to Evaluate Your BC/DR Options**
3. **What is Enterprise Data Backup? (And What It's Absolutely Not)**

Tracy Rock

Tracy Rock is the Director of Marketing at Invenio IT. Tracy is responsible for all media-related initiatives as well as external communications—including, branding, public relations, promotions, advertising and social media. She is one busy lady and we are lucky to have her!

Stay Connected

Facebook

Twitter

YouTube

RSS

Categories

Business Continuity (342)

Cloud & Hosting (54)

Compliance (7)

General Tech (9)

Security (58)

Join over 17,000 who get the weekly free & fresh Business Continuity knowledge

Weekly you'll receive business continuity news, tips & advice to protect your business

Back To Top

First Name*

Type your first name

Last Name*

Type your last name

Work Email*

Please enter your work e

Sign Up Now!

Topics

Backup and Recovery cloud computing Compliance & Regulations Datto

Datto SIRIS Errors Datto SIRIS Settings datto vmdk Network Security Network Support

Our Most Popular Posts

6 Real-Life Business Continuity Examples You'll Want to Read

2,113 views

The 9-Point Checklist for Disaster Recovery Plans

641 views

What's the difference: disaster recovery plan and business continuity plan

616 views

9 Critical Business Continuity Plan Objectives

368 views

Can we break it? 7 business continuity plan testing scenarios

356 views

Services

Business Continuity Services

Data Recovery Services

IT Security Services

Back To Top

Solutions

Compare Datto Products
Book Your FREE Datto Demo
Datto SIRIS 4
Datto ALTO 3
Datto NAS
Datto Backupify
Datto DNA
Datto WiFi
Datto Switches

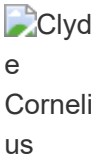
Popular Articles

6 Real-Life Business Continuity Examples You'll Want to Read
The 9-Point Checklist for Disaster Recovery Plans
What's the difference: disaster recovery plan and business continuity plan
9 Critical Business Continuity Plan Objectives
Can we break it? 7 business continuity plan testing scenarios

Invenio IT
5.0 ★★★★★

Paul Gugel
11 months ago
★★★★★ Invenio IT is the backbone for my disaster recovery solution. If I have anything wrong with my backups I am getting a call from Dale. This type of support is awesome especially when backing up 100+ servers.

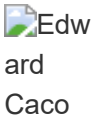
Back To Top



Clyde Cornelius

a year ago

★★★★★ Invenio IT has provided us with an excellent BDR solution in the Datto SIRIS. An enterprise-level solution at a reasonable cost, along with simplicity and ease-of-use, were a few items that helped us move to a Datto SIRIS. The only surprise was the extremely detailed level of service and support we received from Invenio IT. After 20 years of IT experience as a support professional myself, I did not expect to be surprised by the sustained, over-the-top level of support and professionalism that we received from Dale and the Invenio IT team. But I was surprised, and very happily so. Actually, I couldn't be happier!



Edward Caco

a year ago

★★★★★ The Datto Siris product works well and the web portal for management is excellent. My Invenio Rep is attentive, gets in front of issues and monitors the backup service.

Next Reviews

Write a review

Designed by Invenio IT | Powered by Pixi Dust

Back To Top