Famous Last Words: "Disasters Only Happen to Other Businesses"

Don't gamble your entire practice on the belief that a disaster won't happen.

arevtech
Managing Technology | Enabling Success

Think a Disaster Won't Happen to Your Practice?

Don't gamble your entire practice on the belief that it won't happen.

With 24-hour access to immediate news from around the globe, we have almost constant reminders of the potential for major disasters. While nobody wants to live in fear, it is also important to not be complacent. You've invested too much in your practice to leave it vulnerable to disaster.

Disaster can strike even in the absence of a major hurricane or earthquake. It can result from nothing more than a single lightning strike, a simple pipe burst, or a short in your electrical wiring. There's also negligence, employee sabotage, computer viruses, or simple human error. The bottom line is: disaster strikes thousands of businesses every year.

Over 90% of businesses fail within two years after being struck by a disaster.
(per the US Small Business Administration).

Natural disasters

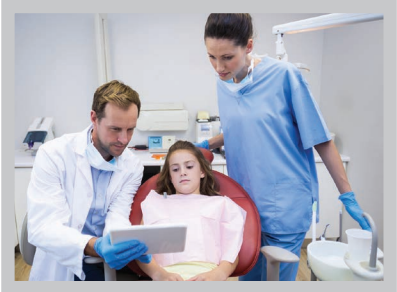
"With road, communication infrastructure, and building damage common after sizable disasters, it's not uncommon for local businesses to be shut down for some time after the aftershocks settle."

–"Financial Effects of Natural Disasters" (Jonas Elmerraji), Forbes.com, March 15, 2011

Even prior to the disastrous hurricanes and floods of 2017, estimated losses from earthquakes, tsunamis, cyclones, hurricanes, and flooding were up to $300 billion per year.[1]

If you haven't had to close your practice due to a natural disaster, you're fortunate. According to the National Small Business Poll conducted by the National Federation of Independent Businesses, 30% of small businesses surveyed had to close for 24 hours or more at least once within a three-year period due to one or more natural disasters. The natural disasters that most impacted their business included blizzards and ice storms, extreme cold, tornados, hurricanes and typhoons, high winds, hail storms, and floods. Other disasters that shattered businesses included power outages and fires.[2]

You may think your practice is safe because it's located in a geographical region (or a stormproof building) that is not prone to typical natural disasters. But it is wrong to assume your practice isn't susceptible. When the tsunami destroyed miles of buildings in eastern Japan in March of 2011, a vehicle manufacturer located in the U.S. was forced to cut its production numbers due to parts shortages.[3] A shortage of computer storage drives caused their prices to soar here in the U.S. for several months. So, while you may not be located in a region prone to natural disasters, it's very possible that your key suppliers are. And if your practice can't get critical supplies—or those supply costs soar due to shortages—your business will be negatively impacted.



Human-made disasters

While natural disasters typically receive more widespread media attention, most business outages aren't the result of natural disasters. In fact, 95% of businesses have experienced outages unrelated to natural disasters.[4]

A 2015 Zetta survey of IT professionals indicated that the most common causes of IT downtime were power outages and hardware errors. But it's also important to note that one in three of those businesses surveyed indicated that they had been hit by a virus or malware attack.[5]

In addition, sabotage and human error can lead to breaches in your patient information and other critical data. An annual study by ID Experts and Ponemon Institute on the privacy and security of healthcare data has revealed some alarming statistics. In 2016, nearly 90% of healthcare organizations surveyed had experienced a data breach within the previous two years. Almost 79% had had two or more data breaches in that timeframe. That's an increase of almost 20% since the first study in 2010. The cost of those breaches is estimated at $6.2 billion.[6]

To make matters worse, the healthcare industry is more susceptible to data breaches than other industries. According to a 2015 annual report by Symantec, almost 40% of all data breaches took place within the health services subsector. And 36% of all data breaches (across all industries) included medical records.[7] In addition, a 2016 study by the Identity Theft Resource Center (ITRC) found that healthcare organizations were hit hardest by hacking, skimming, and phishing attacks—and had the most records exposed by employee error or negligence.[8]

The high cost of business downtime

The statistics on the likeliness and cost of business downtime are sobering. A full 54% of businesses report that they have experienced a downtime incident lasting at least eight hours in the past five years, and 67% of these businesses estimate that a site outage would cost them, on average, more than $20,000 per day.[5]

In another study, just one hour of downtime was found to cost an average of $8000 for small business, $74,000 for mid-sized businesses, and $800,000 for enterprise businesses .[4]

According to the Federal Emergency Management Agency (FEMA), more than 40% of businesses never reopen after a disaster. Of those that do reopen, 71% are out of business in just two years. Those that lose their information technology for nine days or more after a disaster are bankrupt within one year.[9]

Consider what just a few hours of downtime could mean to your practice: notifying patients and rescheduling appointments, the inability to access patient files, your staff unable to do their jobs. The costs go beyond financial when patients grow frustrated and dissatisfied with your practice.

Disaster recovery should be part of your IT plan

Reducing the risks of downtime starts with a solid, documented disaster recovery plan. If you don't have a well-designed, up-to-date disaster recovery plan, you're not alone. The Zetta 2015 survey of IT professionals indicated that 40% of organizations do not have a formally documented disaster recovery plan to guide them in the event of an outage. Of those that do have a formal plan, many do not test that plan regularly.[5]

Without a well-designed disaster recovery plan and support personnel dedicated to reviewing and testing your plan regularly, you're not doing what you should to protect your practice and your patient's data.

Don't worry. There's help. And it's called Arevtech.

If the business risks and costs of disaster are making you nervous, that's normal. The good news is that there's professional help available with proven data protection and disaster recovery expertise, and solutions designed specifically for dental and medical practices. And that's Arevtech.

At Arevtech, we have years of experience delivering IT solutions and services that protect practices from disasters. We can also help to ensure you're compliant (and audit-ready) with critical regulations such as PCI-DSS and HIPAA. We can develop and implement a well-designed disaster recovery plan and perform regularly scheduled security assessments of your IT systems. Our goal is to help you build a successful, healthy practice and ensure that it's truly compliant, safe, secure, and protected from a data breach.

Peace of mind—and more

In addition to safeguarding your practice and ensuring regulatory compliance, we offer 24/7 network monitoring. That means we're always on the job, keeping your critical systems and network up and running, securing your vital data, and addressing IT issues before they become real problems. This also means peace of mind for you.

arevtech
Managing Technology | Enabling Success

Contact Us Today

Contact us today to learn more about how Arevtech's team of experts provides friendly, knowledgeable IT service to help you build and grow a streamlined, productive practice while enabling you to stay focused on providing top quality patient care.

714.256.1500 Talk to one of our Dental Practice IT experts, or visit us at **www.arevtech.com/Dental**

NOTES:

[1] UNISDR Global Assessment Report 2015 ~~as~~ referenced by PreventionWeb: **http://www.preventionweb.net/risk/direct-indirect-losses** Accessed September 22, 2017.

[2] William J. Dennis, Jr., NFIB Research Foundation "National Small Business Poll," Volume 4, Issue 5, 2004 As seen: h**ttp://www.411sbfacts.com/sbpoll-about.php?POLLID=0023** Accessed September 22, 2017.

[3] Mike Seemuth, Miami Herald. August 10, 2014. **http://www.miamiherald.com/news/business/biz-monday/article1979104.html** Accessed September 22, 2017.

[4] Infrascale, "The Future of Disaster Recovery," 2015. As seen: **https://www.infrascale.com/25-disaster-recovery-statistics-for-2015-infographic/** Accessed September 22, 2017.

[5] Zetta State of Disaster Recovery, 2016. **http://www.zetta.net/resource/state-disaster-recovery-2016** Accessed September 22, 2017.

[6] ID Experts, **"Six Years Later, Patient Data Still at Risk for Data Breach,"** June 2016. Accessed June 30, 2017.

[7] Symantec, **"ISTR Insights: Cyber Threats and the Healthcare Industry,"** June 2016. Accessed July 6, 2017.

[8] Healthcare Informatics, **"Report: Healthcare Sector Hit Hard in 2016 by Data Breaches,"** January 2017. Accessed June 30, 2017.

[9] Federal Emergency Management Agency (FEMA), as reported by Forbes.com, 2014. **https://www.forbes.com/sites/causeintegration/2014/09/04/will-your-business-recover-from-disaster/#27d35418295c** Accessed September 22, 2017.