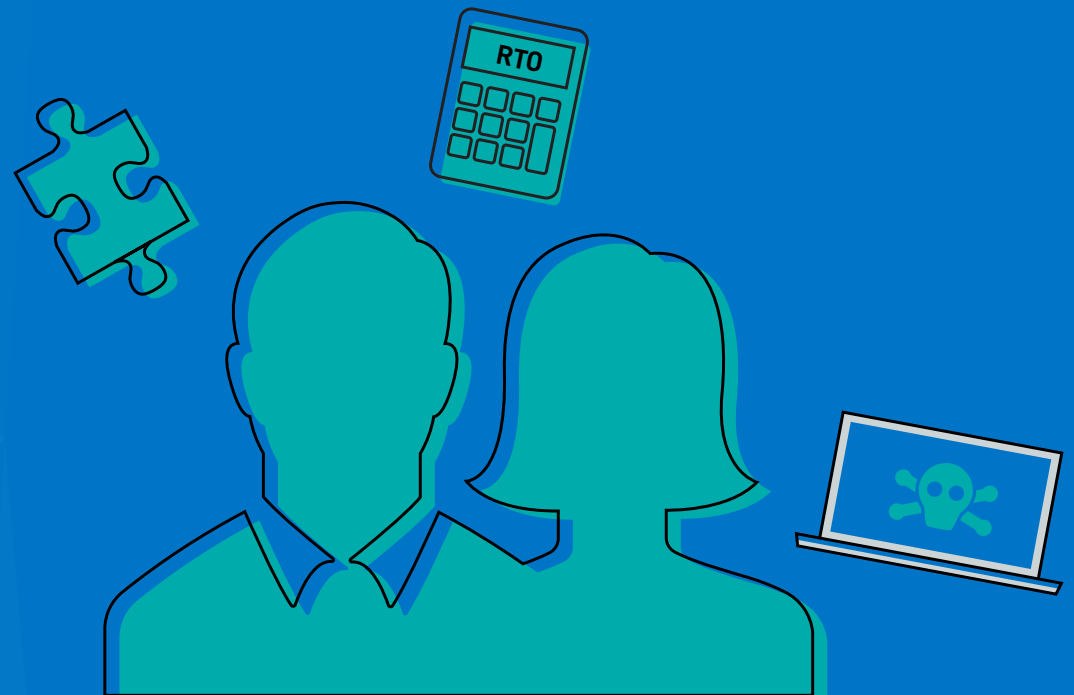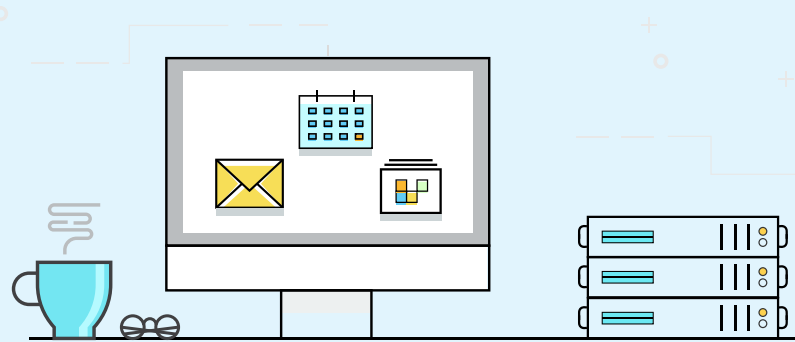pch technologies

CEO? HERE'S WHY YOU CARE ABOUT BUSINESS CONTINUITY AND DISASTER RECOVERY
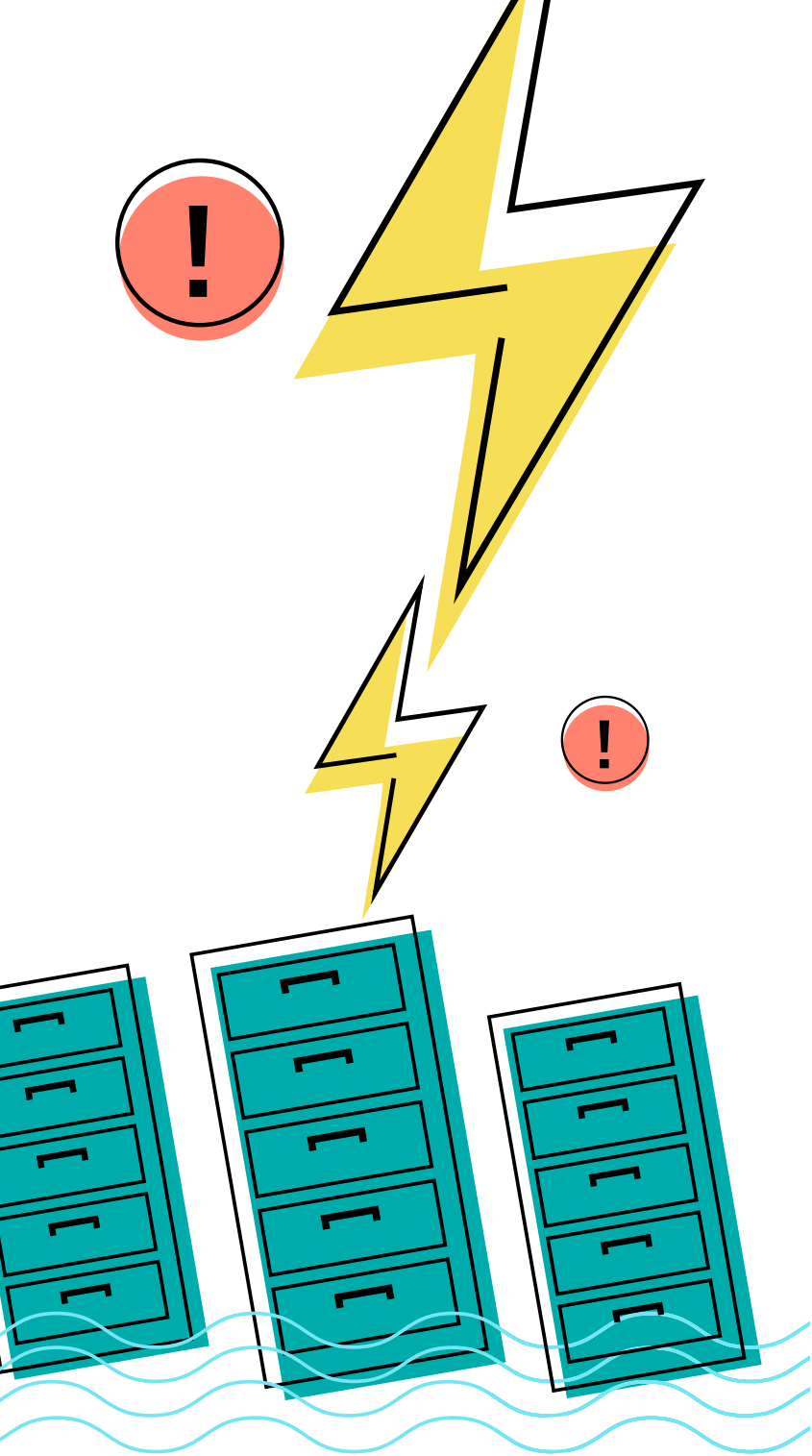
4 Undeniable Reasons to Care about BCDR

As a proactive CEO, you know that implementing a solid business continuity and disaster recovery plan, also referred to as BCDR, is essential for your business. After all, why would anyone in your esteemed position ever put a business at risk to downtime or data loss when prevention is so easy?

While some negligent CEOs fail to give BCDR the proper attention it deserves, we're not worried about you. But if anyone asks, here are four critical reasons that you, the CEO, care about business continuity and disaster recovery.

YOU CARE BECAUSE DOWNTIME IS EXPENSIVE

If your employees or customers lose access to business-critical applications and data, there will be a direct impact on productivity and revenue. While this sounds obvious, many organizations do not consider the actual costs of downtime. To better understand this cost, consider the following example using Datto's RTO calculator. Let's say your business has 100 employees, average hourly revenue is $1,500 and the backup data set amounts to 2 TB. Given these parameters, a full restore from a local backup would take over 8 hours. The associated downtime cost would amount to $34,000 in lost revenue. Some modern BCDR products offer the ability to run applications from backup instances of virtual servers. This allows users to continue operations while primary application servers are restored. Choosing a BCDR solution aimed at reducing downtime makes good business sense.
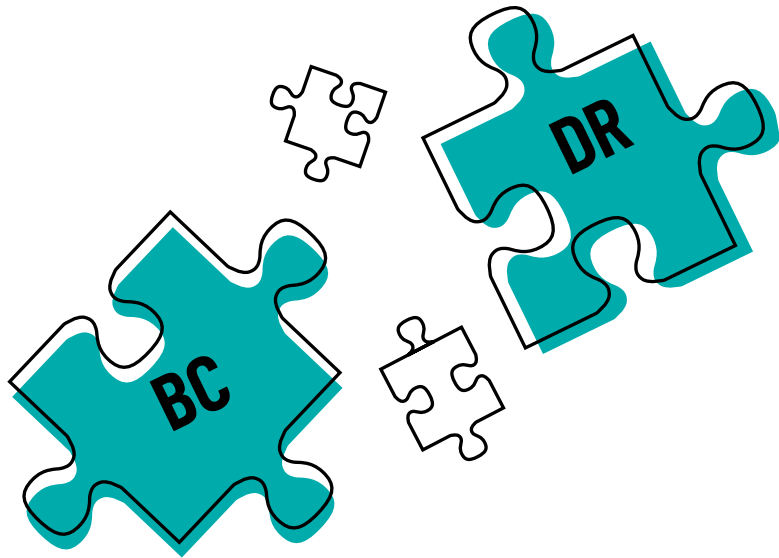
YOU CARE BECAUSE BACKUP ALONE IS NOT ENOUGH

You'd be hard pressed to find a business today that doesn't conduct some form of data backup. But, what happens if a flood wipes out your primary and backup servers? Sending a copy of data offsite for disaster recovery should also be considered essential. Historically, this meant sending tapes to a secondary location or tape vault. As previously mentioned, modern BCDR products can run applications from backup instances of virtual servers, and some can extend this capability to the cloud. This approach is frequently called cloud DR or disaster recovery as a service (DRaaS). The ability to run applications in the cloud while onsite infrastructure is restored is widely considered to be a game changer for disaster recovery. As CEO, you don't want yesterday's backup technology. Backup and business continuity are not one in the same. Your business needs both.

YOU CARE BECAUSE OF THE RISK OF DISASTERS

Not every disaster is broadcasted on news and weather channels. Most IT downtime is a result of common, every day actions like accidental (or intentional) data deletion, damage to computer hardware and poor security habits. For example, a recent CompTIA study found that 94% of respondents routinely log into public wifi, in spite of security risks. And, 69% of this group accesses work-related data over public wifi. A ransomware attack or virus can halt operations just as easily as a tornado or a power surge. These "lower-case d" disasters are typically a result of human error, which in unpreventable. Having technology in place that allows your business to continue operations following these "hurricane humanity" disasters is equally if not more important than protecting against a hurricane that may or may not strike your business.

YOU CARE BECAUSE BUSINESS CONTINUITY IS EVERYONE'S CONCERN

Data is essential for all types of organizations today, so ensuring access to applications and data following a disaster is critical. But it's just one piece of the BCDR puzzle. Evaluating your business' ability to restore IT operations can be a good starting point for company-wide business continuity efforts. Good BCDR planning should look at the business as a whole, and the goal should be to develop business resilience. In fact, many BCDR planning efforts start by conducting a business impact analysis or risk assessment—these studies can reveal weaknesses in your business' ability to continue operations that go far beyond IT. You know a disaster (natural or otherwise) is coming at some point and in the company you lead, everyone has a stake in BCDR.

CONCLUSION

It's so refreshing that you've acknowledged business continuity and disaster recovery as a company-wide responsibility. After all, failure to protect your business from human error, hardware failure and/or natural disasters can be detrimental and impact every single stakeholder. Now that you've implemented a BCDR solid plan, I bet you sleep much more soundly at night knowing you're fully prepared for any potential disaster that might come your way.

For more information please contact:
Timothy Guim | President
Phone: 856-754-7500
Email: tguim@pchtechnologies.com
PCH Technologies | pchtechnologies.com
11 Enterprise Court, Suite 100 Sewell, NJ, 08080