RANSOMWARE PROTECTED BACKUPS AND BUSINESS CONTINUITY

Do you have an independently verified and validated business continuity plan ready for when critical incidents occur? Do you have complete, independent and secure verified backups that not only recover data; but also detect and self-heal from cyber-attacks?

Data loss can be the result of many things, from computer viruses, ransomware, hardware failures to file corruption, flood, fire or theft. If you are responsible for your business's data, a loss may involve a substantial impact on financial, customer, and company data and to your reputation. Having reliable data backup is often not enough. A well-developed Business Continuity Plan that has been independently verified to address modern, constantly evolving cyber threats is critical. This will minimize disruption to the health of your company's financial and operational stability, as well as to its reputation from today's devastating cyber impacts.

Are you required to keep records for an extended period of time for tax and regulatory purposes? Companies that only have localized backups of their data put themselves at considerable risk. Cloud backups have significant risks as well.

A modernized business continuity strategy, designed and tailored for your organization by cybersecurity experts, protects against organized criminals and nation-state actors. In fact, cyber attacks that target backups are detectable through modernized backups and controls. These attacks are often mitigated through advanced warnings of malicious activity which attempt to poison backups rapidly or incrementally over a prolonged period of time. The IRS and regulatory commissions are not concerned if you have suffered a disaster or have been the victim of a cyberattack. To them, it means you are not compliant.

WITHUM'S CYBER ENCRYPTED BACKUP AND BUSINESS CONTINUITY SOLUTION OFFERS TRUE DEFENSE IN-DEPTH SECURITY PROTECTION

1. Data Protection and 24/7/365 recovery of your critical data by certified experts.
2. Incident Response notifications to identify stealthy cyber attacks with integrated intelligent self-healing systems to mitigate major business impacts.
3. Data integrity and business continuity assurance.

HLB WE ARE AN INDEPENDENT MEMBER OF THE GLOBAL ADVISORY AND ACCOUNTING NETWORK

Matthew Ferrante
Partner, Market Leader, Cyber and Information Security
T (212) 537 9397
wcyber.info@withum.com

Eric Jackson
Senior Manager, Advisory
T (973) 867 7432

withum

A comprehensive Backup and Business Continuity Plan should have the ability to retrieve vital data quickly and revive critical business operations as soon as required. Withum's Encrypted Backup and Business Continuity Solution will minimize risk and create the best environment for full restoration after a disruption.

STATS AND FACTS

- Cyber Criminals specifically target business backups.
- Approximately 75% of backups fail after a cyber attack or other business critical event.
- 2020 was a bad year for ransomware attacks. 2021 will be worse with damages expected to rise to $20 billion, nearly doubling.
- An organization falls victim to ransomware every 11 seconds.
- New Rules: Businesses can be fined up to $20 million USD if they pay ransomware criminals, regardless if the fine was paid by your business or via a third party. Cyber insurers are starting to decline to pay.

WITHUM'S INTELLIGENT BACKUPS

Identify Cyber Attacks
Self-Heal
Mitigate Major Business Impacts

Set up your comprehensive Backups and Business Continuity Plan today by contacting one of Withum's Cybersecurity Specialists.

☎ **NEED MORE INFORMATION?** Contact us at 1 (800) 470 0988 or (212) 537 9397, email us at wcyber.info@withum.com or visit withum.com to learn more.