

Manufacturer?

Protect Your Company by Adding Business Continuity to the Assembly Line



As a manufacturer, you're producing real, tangible products each and every day. Your company's ability to produce high volumes at low costs can determine where you fall among your competitors.

In the age of technology, your equipment relies heavily on the computers configuring their behavior. What would happen if those systems become compromised? How long could you afford to halt production?

In the Manufacturing industry, downtime comes with costs from all directions. If production stops, you'll likely be paying a lot of employees who are standing around, waiting for a solution. The inability to fill quotas can impact sales. This can also damage your reputation as customers are unable to place orders. Like any other business, manufacturers are vulnerable to fire, flood, severe weather, power outages and any other calamity that could take systems offline and/or wipe out valuable data. Additionally, there's the risk of human error that comes into play, which is when your own employees make mistakes or take malicious actions. For manufacturers specifically, the loss of intellectual property data can greatly hamper a business.

In the manufacturing industry, downtime comes with costs from all directions.



A False Sense of Security

While you may be taking some precautions, such as securing and backing up your sensitive data, sometimes that's not enough. **There is a common misconception that data is safe if backed up once a day, but this outdated practice is no longer sufficient for several reasons:**

- If you forget to perform the backup or the backup process fails, you're not protected.
- If you only back up your files once a day, you're left vulnerable to the loss of an entire day's work.
- If you don't properly validate your backup files, you could be in for an unpleasant surprise when you actually try to use those files to restore your company's operations.
- If you only back up your files on-site, you could lose them too—leaving you with no way to restore production.
- If you only back up your raw data, rather than all your application and server configuration files, it could take several days to restore your business — because you will also have to rebuild your servers, operating systems, applications, etc.

Some manufacturers are turning to business interruption insurance to cover the costs to rebuild, restore, or regain lost income. However, while an insurance provider may write you a check for the cost of a server that gets damaged because of a broken pipe, it won't shield you from damaged or lost client relationships. Ultimately, your reputation isn't something for which you can easily be compensated.

How Vulnerable Are You?

If your company identifies as a business that doesn't have the IT resources to effectively recover from a major outage, make sure you're weighing all of the factors around the costs of downtime. Here are the facts:

- US businesses lose \$12 billion annually due to data loss.¹
- 93% of companies that lose their data center for 10+ days file for bankruptcy within one year.²

Best Practices For Manufacturers

In a survey by Kaspersky Lab, manufacturers reported: "Internal Operational Information" and "Intellectual Property" as data they would most fear losing³. Among the causes of recent data loss, malware was the most common. Following malware, software vulnerabilities, network intrusion, and targeted attacks were all mentioned. Here are some tips to help your business avoid costly downtime:

- Outsource your company's IT needs to an expert who has experience in the manufacturing industry.
- Don't sacrifice quality to save money when purchasing hardware. It will benefit you (and your bottom line) to have strong technology in the long-run.
- Perform timely hardware and software updates, maintenance and backups.
- Establish, review and maintain system security of all company technology.



US businesses lose \$12 billion annually due to data loss.¹

A true business continuity solution will protect data on-premises in physical and virtual servers and in the cloud.



For more information please contact:

Phone: +44 131 202 0777

Email: help@brightridge.co.uk

Brightridge | www.brightridge.co.uk

6 Nasmyth Court, Housoun Industrial Estate,
Livingston, EH54 5EG

Any company that has not recently re-assessed its backup and disaster recovery procedures should, therefore, do so in order to conform to these industry-standard best practices.

The Better Way: Business Continuity

Business continuity describes a complete solution for backup and disaster recovery. **A true business continuity solution will protect data on-premises in physical and virtual servers and in the cloud.** Whether data is on servers or in SaaS applications, it needs to be backed up. Business continuity goes a step further and offers you the ability to restore your data, which we call disaster recovery.

Whether a business is faced with a natural disaster or one man-made, a strong solution will have you up and running in minutes. Solutions that leverage the hybrid cloud can guarantee a quicker restore time as well. Why? Local backups are great to keep data stored on local devices, but if something happens to that device, then what? A hybrid cloud backup solution takes an initial backup on a local device and then replicates the backup to a cloud server. Cloud-only solutions are not as reliable on their own due to bandwidth issues. A hybrid model works to alleviate the vulnerabilities by implementing both processes to fill in the gaps. That's intelligent business continuity.

Sources

¹ Beyond Technology

² National Archives & Records Administration

³ Kaspersky Lab