AFTER DISASTER

November 29th, 2017 • WDI Magazine • Kevin Beasley

When a disaster strikes, businesses have many concerns including protecting employees and property and supporting customers. However, a business's information and technology assets are also at risk and if destroyed, the loss can devastate businesses. According to FEMA, 40 percent of businesses never reopen their doors following a disaster.

Going beyond natural disasters, cyberattacks are at an all-time high, and in today's IoT driven workplace, a case of malware can easily compromise an entire business. Having a disaster recovery plan can save businesses, and when it comes to warehouses and distribution centers, there are countless assets that need protection.

Write it Down

All warehouses and distribution centers should have a written operations response and recovery plan. Copies of this plan should be made both in paper form and in a computer database, so no matter the disaster you can have a copy of the plan on hand. A written disaster recovery plan should include all of the information needed to continue operating in the wake of a disaster or how to move operations elsewhere. It should also include emergency response and recovery in the event of damage.

As a key part of the supply chain, disasters that affect warehouses and distribution centers will inevitably affect other operations in the supply chain, so a disaster recovery plan is of the utmost importance. Having an effective recovery plan can minimize downtime or loss of data, therefore minimizing the impact to the rest of the supply chain and helping customers and vendors maintain trust in your business if a disaster strikes. It's far less expensive to create a disaster recovery plan than it is to re-acquire lost customers after a disaster occurs.

So what goes into a disaster recovery plan, and where should you start? The first step is perhaps one of the simplest, yet one of the most crucial components. A complete inventory of all devices and applications, as well as a list of jobs and vendor technical support information must be listed out. This list should be sorted and ranked, with critical assets your business absolutely cannot operate without specifically noted or marked with a star. Natural disasters, fires, broken water pipes, malware and other disasters can cause significant outages and costs, and knowing exactly what your critical assets and jobs are helps ensure they are made priority when disaster strikes.

Alongside your list of critical assets and jobs should be a list of any and all potential disasters that could affect the distribution center. Based on this list, a protection plan for each critical asset should be made for each potential disaster. While this is the most time-consuming part of the disaster recovery plan, when a disaster strikes, you'll be thoroughly prepared to maintain operations as best as possible with the most critical assets covered.

All disaster recovery plans should take note of employees involved with the plan, with clearly defined roles and responsibilities assigned. When disaster strikes, there is hardly time to assign key jobs and explain to employees what the plan is and what their role is right then and there. It is essential to also communicate those roles and the entire disaster recovery plan as soon as it is developed and each time it is updated.

Back it Up

One of the most critical parts of an effective disaster recovery plan is a back-up plan for systems and data. Particularly in distribution centers where data is a key aspect of systems and workflow, this information will need to be protected, maintained and accessed during and after a disaster. Data should always be stored and backed up in multiple places, whether it is in a public or private cloud, data center, hard drive or elsewhere.

Finally, while you can plan for disaster extensively, you never truly know how effective it will be unless you test your plan. Backup applications may fail and a critical employee may be unavailable, thus making task cross-training an imperative part of the plan, and many other hiccups can hinder a plan from being effective. Testing the plan several times a year can ensure that the plan is running smoothly. Similarly, the disaster recovery plan must be updated on an on-going basis as new assets or applications are added. This will ensure no asset gets left behind when disaster strikes.

No one likes to think that a disaster could strike their business. However, no business is immune to disaster, and it is a question of when a disaster will come, not if. Being prepared with a recovery plan is the difference between having the ability to support your customers and be operational or a business ruined. By establishing a disaster recovery plan and keeping it updated and tested, businesses can be one step ahead.