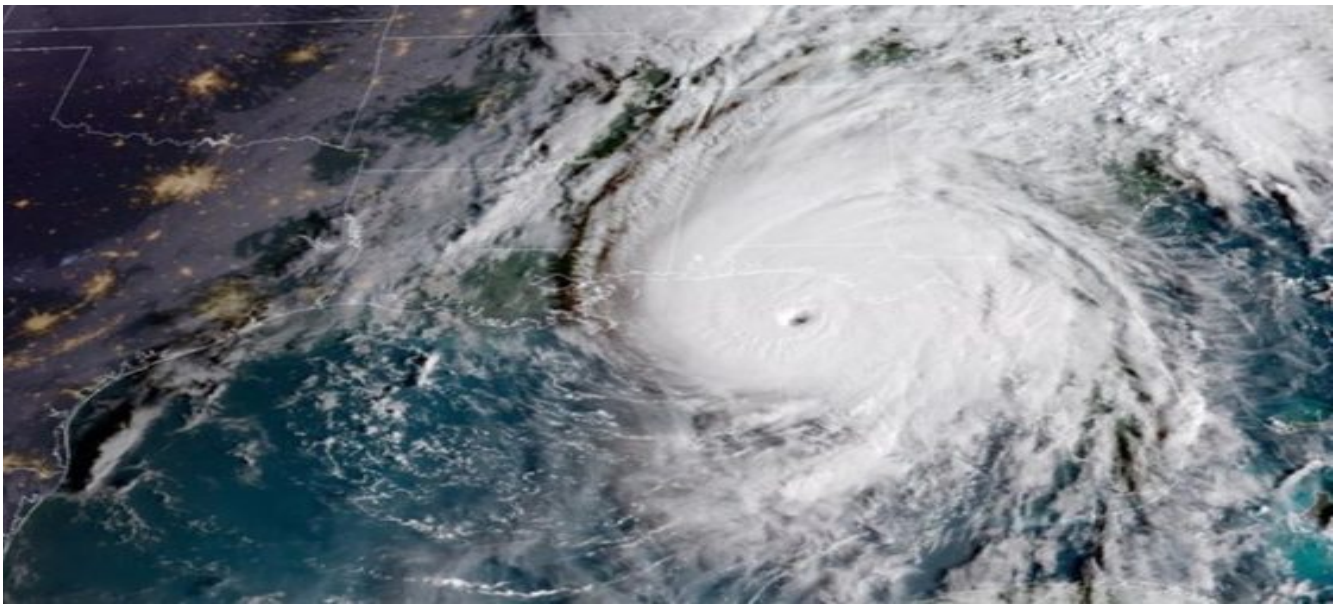
Postlethwaite & Netterville



# Including Technology in Your Disaster Recovery Plan

*by Michael Richmond*

Every summer, households and businesses along the Gulf Coast wonder if this will be the year disaster strikes. But what exactly is a disaster? You might think of a hurricane, flood, or other natural disaster. Those situations definitely require planning ahead in order to get through safely, but when it comes to your organization; a disaster can be anything that interrupts your ability to do business. Disasters aren't tied to a specific season, and can strike any time.

Business-related disasters include loss of electricity (whether from a storm or an accident that takes out power lines), interruption in your internet access, or even a ransomware attack that locks you out of your systems and files. With highly-disruptive cybersecurity threats like ransomware becoming more wide-reaching and difficult to thwart, it's crucial to reconsider how your organization envisions disaster recovery and business continuity.

Just like preparing your household for disaster ahead of time can minimize the impact on your family, creating a complete and functioning IT disaster recovery plan long before business-related disaster strikes, and ensuring that it stays up to date, can minimize the impact on your organization. Most businesses generate and update large amounts of data throughout a single workday. If that data is lost, stolen, or inaccessible, business is disrupted for whatever length of time it takes to restore what you can.

Having an IT disaster recovery plan in place can get your systems up and running with minimal loss of time and data. Getting caught in an IT disaster without a plan can make recovery costlier, and less complete.

## Planning Ahead for Data Backup

| | |
|---|---|
| 3-2-1 Backup Rule | Maintain at least 3 total copies of your data. Two copies are local but on different devices, and at least one copy is saved off-site. |
| Recovery Time Objective (RTO) | How long can your organization tolerate a system disruption before it must be restored? |
| Recovery Point Objective (RPO) | How much data can your organization lose without affecting business performance? |

Data backup is a crucial component of any IT disaster recovery plan. To get started, consider the tools, support, and processes you may need in order to recover in the event of a successful cyber attack or network disruption, as well as more traditional forms of disaster.

- Select and implement backup procedures, and any necessary software and hardware
- Schedule backups at an interval appropriate for your business needs
- Periodically confirm that backups are working as intended
- Make sure to follow the 3-2-1 rule for backups
- Review and update your organization's full data backup and recovery plan at least annually

A solid backup strategy is a foundational element for any disaster recovery plan, but will require other aspects as dictated by the type of disaster and business processes affected. Don't ignore the importance of other components that enable your business to function, such as reliance on third-party vendors, manual processes, HR issues, facilities, etc. These must be included in the overall disaster planning process.

If your organization lacks the IT staff or knowledge to implement and monitor your disaster recovery plan, you're not alone. Consider outsourcing some or all of the above. P&N professionals can assess your business' needs and help you with planning, implementation, and monitoring.

**My Files Are Encrypted by Ransomware, Now What?**

P&N has helped other organizations quickly and effectively recover from ransomware attacks. Whether you are a current client or just need help fast, contact us for help creating a disaster recovery plan or recovering from an in-progress attack.