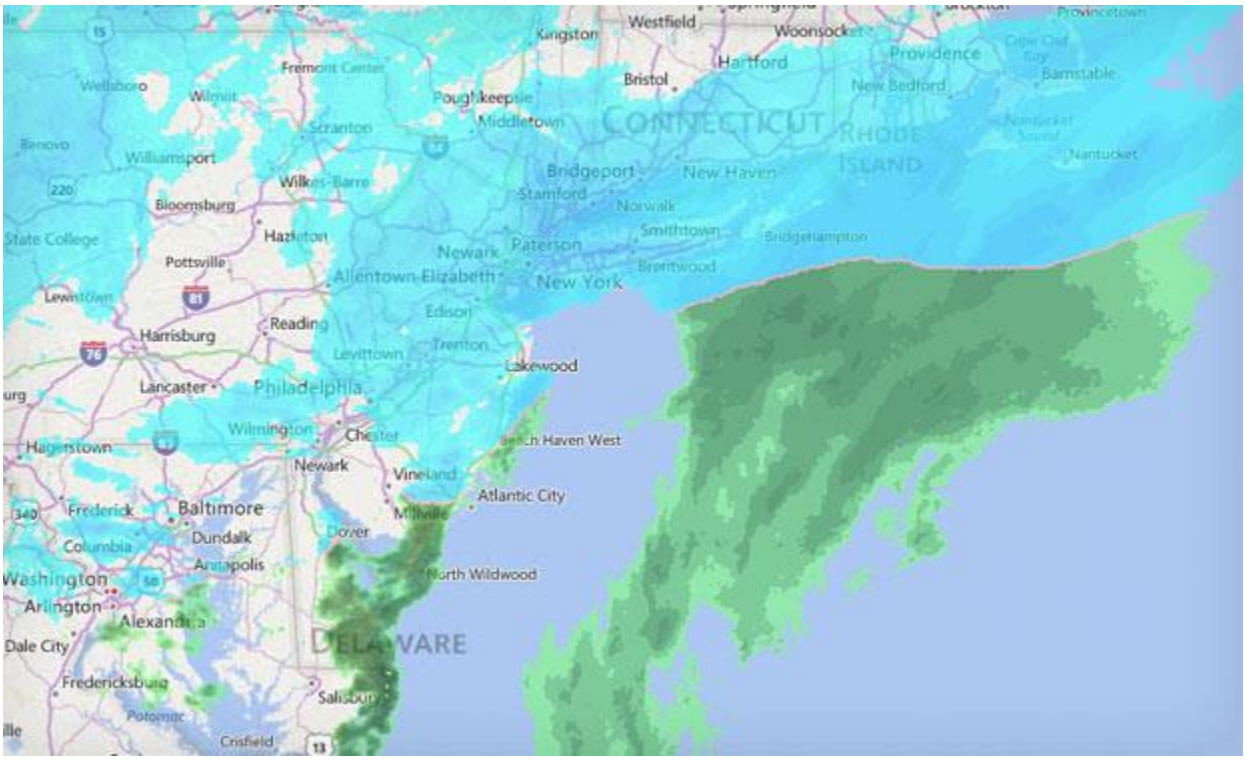
Blizzard 2015: Business Continuity Tips

Organizations Should Be Reviewing, Activating Plans

By Jeffrey Roman, January 26, 2015.



As the East Coast braces for a massive blizzard, dubbed Winter Storm Juno, security experts say organizations in the path of the storm should be reviewing and preparing to launch their **business continuity** plans.

See Also: Mobile Deposits & Fraud: Managing the Risk

First and foremost, disaster recovery plans should already have determined which processes and workers are essential during a crisis, says **Kate Borten**, a privacy and security consultant at The Marblehead Group, which is based in Massachusetts.

Other priorities for businesses include reviewing their backup processes and accounting for personnel during the storm, experts say.

Personnel Issues

A key issue over the next few days will be dealing with personnel issues, says **Alan Berman** of the Disaster Recovery Institute. "There are major corporations who block out hotel rooms so that they can have their employees close by," he says. "[Many] will have employees staying at the office."

But if those plans weren't developed ahead of time, it may be too late for such options, Berman notes.

For those employees working remotely, a concern will be securing communications over home or public networks, he says. "[But] we're seeing more biometrics and token access," he says. "All of the newer PCs and iPads are doing fingerprint recognition."

Reviewing Backup Processes

Organizations should be reviewing their backup processes, such as redundant power options in the case of an outage, especially if systems are hosted locally, Borten says. The status of backups and plans for alternative sites, if appropriate, should also be reviewed, she says.

It's also important to determine what the potential security impact of emergency failover processes will be. "For example, are your carriers going to send traffic over the Internet unencrypted and without notifying you?" Borten asks. Those issues must be considered and accounted for before activating the business continuity plan, she says.

Maintaining Priorities

The first priority at healthcare organizations should be the safety of their patients, Borten says. "Then, the primary IT issue is keeping critical systems, such as EHRs [electronic health records] up and running for patient care."

At financial institutions, it's important to ensure lines of communication with customers remain open during the storm. For example, when Hurricane Sandy hit in 2012, North Jersey Community Bank in Englewood Cliffs, N.J. - now ConnectOne Bank - took the appropriate steps to ensure the continuity of its business (see: ***Post-Sandy: Lessons Learned***). The bank's plan included duplicate operation centers and telecommunication systems, as well as multiple avenues for communications, including redundant phone systems and social media.

Yet communications is usually one of the biggest challenges during a storm, says Christopher Paidhrin, a security administration and integrity manager in the compliance division of PeaceHealth, a healthcare delivery system in the Pacific Northwest. "Who can reach whom, when the cell towers and phone lines go down?" he asks. "Do you have a short-wave backup [or] microwave option? Do key stakeholders have emergency call trees - and know what to do when calls can't or don't get through? That is the test of an always-on service. Are you prepared for your primary and secondary systems to fail in a crisis?"

After the storm, organizations should take the opportunity to review and improve their disaster recovery plans, Borten stresses. "Those plans should be living documents that are continually refined to make the next disaster a bit less disastrous," she says.

Source: http://www.bankinfosecurity.com/blizzard-2015-business-continuity-tips-a-7837