No Website Contingency Plan? Seven Steps Can Save Your Business!

By Catherine Goodrum, Principal

On the morning of October 21, I was sitting among dozens of conference-goers in a New Orleans meeting room, listening to a speaker. Just minutes after the session concluded, the room was buzzing – not about what we had heard from the podium, but about what we saw on our smart phones: *Nothing.*

No email, no Twitter, no online calendar to steer us to our next business meeting. As the news spread, we heard that across wide swaths of the United States, people were reporting problems connecting to multiple websites, including Twitter, Spotify, PayPal and *The New York Times,* amid others.

The culprit, as we all now know, was a coordinated DDoS (distributed denial of service) attack perpetrated on Dyn, a DNS (domain name service) provider. If you've never heard of a DDoS, you're not alone. As WIRED writer Lily Hay Newman explained, "A DDoS attack overwhelms a DNS server with lookup requests, rendering it incapable of completing any." In short, if your clients are trying to reach you, they are stalled for the duration of the attack.

What does this mean for our businesses? Right now, all that is known for sure is that an attack of this type can limit a company's ability to communicate with, and receive communications from, others. At the very least, this could result in impatient customers; at the worst, it could sow seeds of doubt about a company's integrity or even its viability. And, as Kyle York, Dyn's chief strategist, observed in a *New York Times* interview: "The number and types of attacks, the duration of attacks and the complexity of these attacks are all on the rise."

So, following the wisdom of "the best offense is defense," this may be a good time to create or update your company's contingency plan in the event of a disruption to your website. For a good overview of this topic, take a look at this document, "Contingency Planning Guide for Federal Information Systems," published by the National Institute of Standards and Technology in 2010. The Guide's seven-step contingency plan, excerpted below, can be adapted to IT departments of any size.

1. Develop the contingency planning policy statement. A formal policy provides the authority and guidance necessary to develop an effective contingency plan.
2. Conduct the business impact analysis (BIA). The BIA helps identify and prioritize information systems and components critical to supporting the organization's mission/business processes. A template for developing the BIA is provided to assist the user.
3. Identify preventive controls. Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs.
4. Create contingency strategies. Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.

5. Develop an information system contingency plan. The contingency plan should contain detailed guidance and procedures for restoring a damaged system unique to the system's security impact level and recovery requirements.
6. Ensure plan testing, training, and exercises. Testing validates recovery capabilities, whereas training prepares recovery personnel for plan activation and exercising the plan identifies planning gaps; combined, the activities improve plan effectiveness and overall organization preparedness.
7. Ensure plan maintenance. The plan should be a living document that is updated regularly to remain current with system enhancements and organizational changes.

If you are still on the fence about a full-blown contingency plan, at the very least consider what your company's vulnerabilities could be in the event of a breach, what it would take to mitigate the damage and whether your company can withstand the outcome.

The Trilogy Group is a leading provider of independent support services to organizations specializing in Global Mobility. Trilogy's client base comprises the U.S. government, industry trade organizations, multi-national companies and corporations.

www.TheTrilogyGroup.com

tel 703-391-2744
email info@thetrilogygroup.com

URLs for the NIST pubs:

Guide: [http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf]

Steps: [http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf#page=13]