Resiliency and Recovery after a Cyber-attack

HOW QUICKLY AND COMPLETELY CAN WE GET TO NORMAL AFTER AN ATTACK

BY NELSON SANTINI

In late 2017 three hurricanes wreaked havoc on the U.S. mainland and territories. Our social media and news feeds were flooded with headlines and snippets about three million U.S. citizens in Puerto Rico who had been sent to the middle ages overnight, and would remain there for months until the island's power grid could be restored. Still six months after Hurricane Maria's landfall, over 50% of the island, affecting some two million citizens, was without reliable power; and as of this writing, no end was in sight for full restoration.

Politics and sensationalism aside, at least two facts are known. FEMA responded to all of these natural disasters; and said responses were hampered by lack of available and working infrastructure. Note that the hurricane(s) here is the instigator or cause; but the aftermath toil is weather independent, purely a function of the recovery's success.

Hurricane Season comes every year at the same time. Watching the predictions for the season are almost like watching the NFL or NBA draft.

How many category four/five hurricanes will we have this season? How many, and where, will they make landfall? Computer models vary and broadcasters use them to compete for audiences who have prepared, to varying degrees, for years to mitigate damage and recover from the hurricanes' effect. And still, recoveries are simply "a beast".

Imagine now, for a moment, that without warning and out of the blue, instead of three million citizens on a faraway island, or 250,000 displaced citizens in Houston that all 300,000,000+ Americans INCONUS lose power in the blink of an eye after a rogue or enemy sanctioned entity unleashes a cyber-attack on our country. The attack is persistent and its effect felt for weeks or months. Now what? No power, no Internet, no communications, and truly challenging logistics at a large scale.

The Department of Homeland Security (DHS) is responsible for responses to Federal level cyberattacks. The Department of Defense (DoD) against military force. The National Guard (NG) is

Resiliency and Recovery after a Cyber-attack

HOW QUICKLY AND COMPLETELY CAN WE GET TO NORMAL AFTER AN ATTACK

responsible for State level responses to cyber attacks. The Federal Emergency Management Agency (FEMA) responds to “disasters” (natural only?). Who would be in charge? What would be the protocol and Chain of Command? Who would coordinate? How could each agency possibly communicate without common access to telecom resources?

Not being a pessimist or preying on fear here, but if we don’t have a well-rehearsed and tested plan we will test Hollywood’s best dystopian plots of the last 5 years.
A multi-agency response of this magnitude is unprecedented and its execution as infinitely complex in its logistics as “Overlord” was in WWII or landing Apollo XI on the moon. Yet we accomplished those feats through preparation, ingenuity and heart.

In the age of the Internet of Things (IoT) cyber-security readiness is critical on all fronts. Business continuity plans must be adjusted and tailored to include the cyber domains. Agency plans must be dovetailed on paper, and through practice, to ensure that the fastest possible recovery from what seems to be inevitable, if not in its full breadth, a partial manifestation of an attack.

Being ready goes far beyond having a plan. It involves rehearsal, preparation and a trusted network of expert partners ready to collaborate in restoring the infrastructure to its full operational capacity. Prepare. Do so now. Not a leaf on a tree will indicate the storm has arrived, and when it does arrive, there will be no time to discuss what we should have done today.

Remember, “the more we sweat in peace…”

ENVISTACOM

6 Concourse Pkwy • Atlanta, GA 30328
Phone: (470) 255-2500 • Web: www.envistacom.com