CYBER UPDATE

White House Briefing on Cyber Incident Coordination

In August 2016, Bruce de'Medici, Director of Legal & Cyber Security for Uledger, Inc. attended a briefing with The White House Cybersecurity Coordinator on Presidential Policy Directive 41.

The Directive sets forth principles governing the federal government's response to cyber incidents. The pillars of the Directive are to enhance security, take the fight to the bad guys, and improve reaction and recovery. The Directive establishes lead federal agencies to respond to cyber incidents and an architecture for coordinating the response.

The response is to include:

- shared responsibility between the private sector and governmental agencies;
- calibration of response to the assessment of risk;
- safeguards for the incident details, privacy, civil liberties, and private sector information;
- deference to the affected parties in notifying other affected parties and the public; and
- unity of effort by governmental agencies.

The response is to be conducted in a manner to facilitate restoration and recovery of affected parties, while balancing investigative/security requirements, public health and safety, and the need to restore normalcy. In responding to any cyber incident, federal agencies are to undertake:

- threat response activities (such as law enforcement investigative activity, collection of evidence, attribution, linkage to related incidents, identification of additional affected entities, identification of threat pursuit and disruption opportunities, mitigation, and information sharing);
- construction of situational threat awareness, threat trends, knowledge gaps, and the ability to degrade or mitigate adversary threat capabilities.

An affected federal agency shall have primary responsibility for management of cyber incident impact, by maintaining business or operational continuity, addressing adverse financial impacts, managing liability risks, complying with legal and regulatory requirements, and dealing with media and congressional inquiries.

When a cyber incident affects a private entity, the federal government will not typically play a role in the lines of effort, but will remain cognizant of the affected entity's response activities and will do so in coordination with the private entity. Private entities want to be cognizant of their organization concerning cybersecurity and incentive for preparing against cyber incidents, including accounting for personnel interaction with technology.

Cybersecurity threats possess the capacity to negatively impact operational capacity, create civil liability, and impair investor value. Cybersecurity is not merely delegable to a department or employee. Effective cybersecurity depends upon integration of awareness of risk and remedial architecture throughout an organization, with a keen eye to legal and regulatory requirements. Effective safeguards require security architecture, operational integration, and ongoing implementation. Anything short of this can create risk that cannot be fully projected.