International Center for Enterprise Preparedness (InterCEP)

Vital Strategies and Approaches to Integrating Cyber-Security with Disaster Recovery and Business Continuity

Web Forum

October 18, 2016, **Nader Mehravari, PhD**, Chief Scientist at **Axio**, led a discussion about cyber risks and business continuity titled "Response and Recovery Considerations in Face of Disruptive and Destructive Cyber Events." As summarized below, his presentation addressed the nature of the cyber threat, potential impacts for an organization, and how different responses may be warranted depending on the specific circumstances of a cyber-attack.

Cyber Intrusions and Breaches

Cyber intrusions and data breaches have impacted many organizations, including high profile multi-national corporations and government agencies. Some examples in recent history discussed in the media include Yahoo!, eBay, Sony Pictures, MedStar Health, The Home Depot, the U.S. Postal Service, the U.S. State Department, Saudi Aramco, and many others.

Cyber-attacks can be damaging to an organization, and some significant impacts include:

- Disclosing operationally sensitive information
- Disclosing privately identifiable information (PII)
- Stealing intellectual property (IP)
- Stealing user access credentials
- Losing credit card information
- Disclosing classified information
- Revealing company proprietary information
- Exposing corporate email messages
- Leaking trade secrets
- Hacktivism – take-over of Facebook and Twitter accounts
- Hacktivism – defacing of websites

The impacts to an organization may also include physical damage and data loss. In 2009, the Stuxnet malware was used at a Uranium Facility in Iran to overtake the industrial control system and change the speed of centrifuges. As a result about a thousand centrifuges were damaged.

In August, 2012, Saudi Aramco experienced a cyberattack whereby an insider deployed the Shamoon wiper malware. As a result, data were destroyed on 30,000 computers, which were rendered inoperable. The recovery lasted 10 days. Similarly, in 2014, Sony Pictures experienced a malware attack that damaged information technology infrastructure and destroyed data.

Cyberattacks can also impact the provision of critical infrastructure services. In 2015, SCADA systems at several utilities in Ukraine experienced cyber intrusions as part of a coordinated attack. The attacks had multiple impacts, including "Blinded" power dispatchers and damaged SCADA system hosts, which resulted in blackouts that affected 80,000 customers.

Adversaries are becoming increasingly interested in using cyber intrusion to:

- Delete and destroy data
- Cause operational havoc
- Cause physical harm to people
- Cause physical damage to infrastructure
- Destroy physical goods
- Damage critical infrastructure
- Stop the delivery of products and services
- Shut down day-to-day business operations
- Prevent access to data
- Affect health and safety

Response and Recovery Following a Cyberattack

As a result of this growing threat, business continuity (BC) plans, COOP plans, contingency plans, and IT disaster recovery plans are more likely now to have to be executed following cyber-induced business disruptions. Moreover, cybersecurity professionals are being increasingly called upon to partner with their business continuity and IT disaster recovery colleagues.

These kinds of attacks may be hard for organizations to detect. Oftentimes an organization may not find out until an external entity informs them there has been a breach. And the time frame for identifying a cyber intrusion may also be lengthy, with many organization not realizing they have experienced an attack several months after the start of the attack.

A key decision that an organization that has experienced a cyber intrusion will face is whether to deal with the adversary (e.g., corner him, get him out the organization's environment, etc.) before starting recovery and restoration activities. The answer depends on a number of factors and the specific circumstances of the attack. Some key factors to consider include:

- Is there a chance that the adversary may try to do major damage if it notices that the organization is trying to corner it or kick it out?
- How long will it take the organization to get the adversary out? What are the organization's stated Recovery Time Objectives?
- How will an organization be sure that the adversary is no longer around?
- Are the organization's common enterprise systems (e.g., email, Internet access, file shares, printers, PBX, VoIP) available? If they are, the adversary is probably monitoring every move the organization makes.
- While rebuilding damaged/destroyed/corrupted systems, how would an organization ensure that the adversary won't get into these newly built infrastructures while building them on their currently (infected) environment?

As a result of the increasing risks of cyber intrusions and data breaches, as well as the potential costs of these attacks, operational risk management activities must explicitly incorporate matters related to cybersecurity risk, cyberattacks, and cyber-enhanced incidents into their planning, testing, and execution phases. These operational risk management activities include:

- IT Disaster Recovery
- Business Continuity
- Continuity of Operations
- Emergency Management
- Incident Response
- Crisis Communications
- Workforce Continuity

Recommendations and Guidance

Some recommendations for organizations to improve preparedness when faced with a cyberattack include:

- Start, continue or enhance cybersecurity training for BC, DR, and incident management teams
- Start or continue interaction and communication between information security teams and Business Continuity and IT Disaster Recovery teams
- Update preparedness planning frameworks and strategies to incorporate risks associated with cyberattacks, and include new scenarios centered around cyberattacks and cyber-enhanced disruptions

- Update and/or expand contingency plans (DR, BC, contingency plans) to account for execution in an environment that has been affected (e.g., penetrated, damaged, destroyed) by a cyberattack

Additional Resources:

- Axio: http://www.axio.com/cyber-risk-landscape
- CERT Insider Threat Center at Carnegie Mellon University's Software Engineering Institute: http://cert.org/insider-threat/cert-insider-threat-center.cfm
- NYU Cybersecurity Center: http://cyber.nyu.edu/
- U.S. Department of Homeland Security: https://www.dhs.gov/topic/cybersecurity
- Institute for Information Infrastructure Protection (I3P): http://www.thei3p.org/
- Sandia National Laboratories – Cybersecurity: http://www.sandia.gov/missions/defense_systems/cybersecurity.html