Cyber Exercises – Preparing for Cyber Incident Response.

Jonathan Storment[1]
[1]*Northrop Grumman*

Cyber incident response differs from responding to natural disasters or other hazards. In most cases there is ample warning, if not, there is a standardized response. Additionally, there is an understanding of what recovery looks like, power restored, business reopened, etc. This is not the case when responding to cyber incidents.

Responding to the wide variety of cyber threats is more difficult and there is no real standardized response, there are methods to streamline the response and recovery process. Having an incident response plan is the first step in ensuring a prompt response and return to steady state. Validating that plan and training against it is the second step and likely the most important.

Conducting exercises to validate your plan and train personnel is widely overlooked and the benefits underestimated. Discussion and operations based exercises are valuable methods to ensure your incident response team, leadership, public affairs, and other employees all understand their roles when responding to a cyber incident. It is much better to rehearse when to activate your response team, notify leadership, share information with other agencies, notify the public, and when to notify law enforcement prior to an incident. Once a breach occurs, it is too late.