U. S. Department of Homeland Security
National Cyber Security Division (NCSD)
Cyber Exercise Program (CEP)

Lessons Learned Information Sharing
LLIS.gov

TREND ANALYSIS

Cyber Exercise Trends: Key Observations, Good Practices, and Challenges

INTRODUCTION

The Department of Homeland Security (DHS), Cyber Exercise Program (CEP) provides support to Federal, state, local, international, and private sector stakeholders in their design, development, execution, and evaluation of discussion-based and operations-based cyber exercises. CEP helps stakeholders leverage cyber exercises to enhance their cyber preparedness and strengthen the overall security and resilience of the Nation's cyber systems. CEP's support to stakeholders includes exercise planning and facilitation, scenario and injects development, after-action analysis, and overall cyber exercise design consultation.

VALUE OF CYBER EXERCISES

Cyber exercises are an essential tool for organizations to evaluate their cyber incident preparation, mitigation, response, and recovery capabilities. The exercise environment allows stakeholders to simulate real-world situations, to improve communications and coordination, and to increase the effectiveness of broad-based critical infrastructure protection capabilities – all absent the consequences of real cyber event. Throughout the course of CEP's engagement in cyber exercises with the preparedness community, a number of key observations, good practices, and persistent challenges have emerged across several fundamental categories of cyber security objectives. Four primary categories include:

- Cyber Information Sharing;
- Cyber Incident Command and Control;
- Internal/External Collaboration/Communications; and
- Cybersecurity Training and Education.

About This Trend Analysis
DHS CEP continuously monitors the latest cyber trends, threats, and vulnerabilities. CEP reviewed exercise and incident AARs and other documents to develop this Trend Analysis. If you would like to contact CEP, please email CEP@hq.dhs.gov.

Key Cyber Exercise Findings

The following list highlights several of CEP's key findings within each broad objective area and provides a brief description of each finding to serve as a foundation for additional research and analysis.

Objective Area 1: Cyber Information Sharing

An organization's information technology (IT) team should serve as the primary clearinghouse for cyber threat, vulnerability, and incident information across an organization. However, information received by IT departments is not always effectively communicated to the broader response elements of an organization, particularly senior management. IT staff must be able to effectively communicate cyber risk, realized/potential impacts of a cyber event, and recommended courses of action to senior leadership in

understandable (non-technical) terms. This communication must be ongoing during a cyber incident and occur at regular established intervals as part of an organization's incident response "battle rhythm."

Objective Area 2: Cyber Incident Command and Control

Organizations, both public and private, typically implement adequate command and control mechanisms for addressing cyber incidents internally. However, when involving external entities in a cyber incident response (e.g., law enforcement, state/government agencies, other sector partners, and third-party security vendors) command and control can often become overly complex and lack clear definition. Organizations must strive to clearly define the incident command roles and responsibilities associated with small, medium, and large-scale cyber attacks and work with outside entities on a regular basis (perhaps through exercises) to clarify how incident command roles and responsibilities may shift as a cyber incident evolves/escalates.

Objective Area 3: Internal/External Collaboration/Communications

Organizations, both public and private, face challenges in clearly defining the cyber incident roles and responsibilities of IT staff and crisis managers. Such roles and responsibilities must complement one another during a cyber crisis in order to fully support the execution of robust cyber incident response capabilities. Further, organizational IT and continuity managers often do not collaborate closely with one another on a regular basis, resulting in an uninformed perception of the other's roles and available resources that can be leveraged during a cyber incident. To address this issue, cyber exercises are an effective mechanism for both defining the joint response roles of IT and continuity managers as well as providing a forum for increased collaboration between IT and continuity departments during a simulated cyber event.

To assist stakeholders with their exercise development needs, CEP maintains a variety of resources on the *LLIS.gov* DHS National Cyber Security Division (NCSD) – Cyber Exercise Program (CEP) page.

Organizations also face challenges in establishing clear communications channels between IT staff and external affairs during a cyber incident. These channels are necessary to ensure customer messaging is timely, accurate, and intelligible. Likewise, establishing mutual awareness between IT and legal departments regarding any potential legal implications/restrictions involved in cyber incident response is imperative (e.g., hiring a third-party vendor to help support incident response or providing an infected client server to law enforcement for forensics).

Objective Area 4: Cybersecurity Training and Education

One of the biggest cybersecurity challenges that many organizations face is a lack of user awareness and cyber education. While many organizations do conduct some form of cyber awareness training for their employees, this training is often infrequent (i.e., only for "new-hires" or on an ad-hoc basis), lacks current/relevant material, and is often non-mandatory, resulting in poor user retention of information or general lack of cyber security awareness among employees. Cyber exercises are an effective tool for educating staff on different cyber attack strategies/vectors employed by bad actors, the potential impacts of a cyber event, and the mechanisms for sharing observed suspicious information/cyber activity within an organization.

If an organization does conduct regular cyber exercises, such exercises are typically wholly technical in nature, primarily involve IT staff, and are mainly "exercises of validation" – i.e., exercises used to assess the effectiveness of existing plans, procedures, and protocols. Organizations must continue to conduct such exercises in addition to "exercises of discovery", which seek to involve the broader response elements of an organization (e.g., external affairs, senior leadership, human resources, legal, business continuity) in order to address not only the technical mitigation of a cyber attack but also key internal and external communications processes. Exercises of discovery also forge vital response relationships;

establish clear communications channels across an organization; help define incident response roles; identify capability gaps and areas for improvement; and inform strategic planning and security investment.

Where many organizations succeed in implementing the technical solutions necessary to mitigate the effects of a cyber incident (e.g., patching systems, conducting forensics, analyzing malware, and updating anti-virus software) some fail to appropriately manage the "whole organization" response to a cyber event, which requires close collaboration and information sharing between IT staff and the broader response elements of an organization.

SOURCE

Bulava, Adam. *Ensuring a "Whole Company" Response: Strengthening Corporate Cyber Incident Response Relationships through Exercises*. Industrial Control Systems Joint Working Group, Quarterly Newsletter, June 2012, pgs. 15-16.
https://llis.dhs.gov/docdetails/details.do?contentID=56402 or
http://www.us-cert.gov/control_systems/pdf/ICSJWG-Newsletter-2012-06.pdf

DISCLAIMER