Informing Cyber Storm V: Lessons Learned from Cyber Storm IV

June 2015

Homeland Security

National Cybersecurity and Communications Integration Center

GENERAL INFORMATION

Report Purpose

This report seeks to inform the development of Cyber Storm V (CS V) and to share lessons learned from Cyber Storm IV (CS IV). This report aggregates the After Action Reports (AAR) from each of the exercises conducted as part of the Department of Homeland Security's (DHS) CS IV Exercise Series. The report also provides a general overview of the series and a discussion of trends observed across the exercises. DHS is using the high-level findings and lessons learned from the series to inform the objectives and direction of CS V.

Cyber Storm Background

Initiated in 2006 with the execution of Cyber Storm I (CS I), the CS Exercise Series serves as a key mechanism to provide cyber security response professionals an opportunity to test and evaluate ever-evolving plans, policies, and procedures. The series is sponsored by DHS, under the National Cybersecurity and Communications Integration Center (NCCIC), NCCIC Operations and Integration (NO&I), and the National Cyber Exercise and Planning Program (NCEPP). DHS designs the CS exercises in cooperation with key stakeholders to improve the capabilities of the cyber incident response community; encourage the advancement of public-private partnerships within the critical infrastructure sectors; and strengthen relationships between the Federal Government and partners at the state, local, and international levels. Cyber Storm exercises are typically biennial, national-level capstone events involving thousands of participants. DHS conducted CS I in 2006, Cyber Storm II (CS II) in 2008, and Cyber Storm III (CS III) in 2010. However, as a result of the Federal Emergency Management Agency (FEMA) decision to focus on cyber-based events for National Level Exercise (NLE) 2012, DHS designed CS IV as a series of 15 smaller-scale, focused exercises addressing cybersecurity preparedness and response capabilities. CS exercises and outcomes informed NLE 12 exercise events and many traditional CS stakeholders participated. In addition, subsequent CS IV exercises addressed outcomes from NLE 12 and continued to provide stakeholders with venues to examine identified issues. The CS IV Exercise Series began in late 2011 and concluded in early 2014.

Objectives

Stakeholders and the exercise planning team developed the CS IV Exercise Series objectives in response to the current cybersecurity landscape, previous exercise experience, DHS priorities, and findings from CS III. CS IV objectives included:

- Identify, exercise, and foster the improvement of processes, procedures, interactions, and information sharing mechanisms that exist, or should exist, under the draft National Cyber Incident Response Plan (NCIRP)
- Examine the role of DHS and its associated components during a global cyber event
- Exercise coordination mechanisms, information sharing efforts, development of shared situational awareness, and decision-making procedures of the cybersecurity community (Federal, state, private-sector, and international) during cyber events

- Maintain awareness of other cyber exercise initiatives

CYBER STORM IV AT A GLANCE

The CS IV Exercise Series included participation from across the traditional CS stakeholder communities including: Federal Departments and Agencies; State, Local, Tribal and Territorial (SLTT) Governments; coordination bodies; private sector; and international partners. Although the 15 exercises conducted throughout CS IV did not include a capstone-level exercise, the events still reached a comparable number of participants to Cyber Storms I-III. For many of these participants, CS IV marked their first time participating in a cyber exercise. Capitalizing on the CS IV experience, these new stakeholders will be integrated into future CS activities, including the CS V planning process. Through CS IV exercise participation, many of these stakeholders strengthened their relationships with DHS, whether through reporting relationships or other offerings. For example DHS provided states with planning and playbook templates to support improvement efforts. Figure 1 shows the breadth of the participant base and the primary CS IV focus areas.

Figure 1: CS IV Participants and Focus

Overview of Exercises

Comprised of 15 separate events conducted between November 2011 and January 2014, the CS IV Exercise Series events ranged from small-scale seminars, to tabletop exercises (TTX) focused on state-level response, to large-scale operations-based exercises. To the extent possible, the exercises considered responses across multiple preparedness mission areas - including Presidential Policy Directive-8 (PPD-8) and its focus on prevention, protection, mitigation, response to, and recovery from an incident. As depicted in Figure 2, the majority of exercises also considered participant response across three phases: initial indicators, attack confirmation, and remediation consideration. As players moved through the phases they considered how attack indicators and warnings would be detected, how their organization would confirm an attack was underway, and what kinds of action needed to be considered in order to remediate the effects and better secure their organizations in the future.

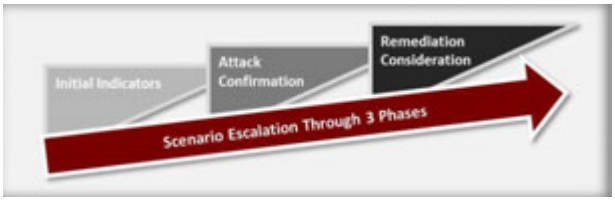

Figure 2: Cyber Exercise Response Phases

Exercise	Date	Summary
National Cyber Incident Response Plan Exercise	November 2011	Large-scale, operations-based exercise; featured two days of distributed play and simulated Unified Coordination Group (UCG) staff and seniors meetings

Exercise	Date	Summary
Cyber Center Directors' Seminar	December 2011	Small-scale, discussion-based seminar; directors reviewed outcomes from a previous centers exercise, relevant standard operating procedures (SOP), and plans moving forward
Public Affairs Tabletop Exercise #1	January 2012	Small-scale, discussion-based exercise centered around the NCIRP External Affairs Annex and supporting SOP
State of Maine Exercise	February 2012	Large-scale, discussion-based TTX for the State of Maine to support state cybersecurity policy advancement and prepare for future CS and cyber exercise participation
State Cyber Coordination Exercise	February 2012	Large-scale, operations-based, distributed exercise for previous CS-participant states and the Multi-State Information Sharing and Analysis Center (MS-ISAC)
Public Affairs Tabletop Exercise #2	March 2012	Small-scale, discussion-based exercise centered around NCIRP External Affairs Annex and supporting SOP
Senate Cybersecurity TTX	March 2012	Discussion-based Principals Exercise that reviewed an attack on the electric grid in light of current legislation
State of Oregon Exercise	May 2012	Large-scale, discussion-based TTX for the State of Oregon to support state cybersecurity policy advancement and prepare for future CS and cyber exercise participation
State of Washington Exercise	August 2012	Large-scale, discussion-based TTX for the State of Washington to support state cybersecurity policy advancement and prepare for future CS and cyber exercise participation
State of Idaho Exercise	October 2012	Large-scale, discussion-based TTX for the State of Idaho to support state cybersecurity policy advancement and prepare for future CS and cyber exercise participation
International Watch and Warning Network (IWWN) Exercise	March 2013	Large-scale, operations-based, distributed exercise; featured two days of distributed play with 11 of 15 IWWN member nations to examine the IWWN's common plans, SOPs, policies, and capabilities
State of Missouri Exercise	June 2013	Large-scale, discussion-based TTX for the State of Missouri to support state cybersecurity policy advancement and prepare for future CS and cyber exercise participation
State of Mississippi Exercise	August 2013	Large-scale, discussion-based TTX for the State of Mississippi to support state cybersecurity policy advancement and prepare for future CS and cyber exercise participation

Exercise	Date	Summary
Evergreen Exercise	November 2013	Large-scale, operations-based, distributed exercise that allowed for observation and evaluation of a simulated cyber-based attack targeting infrastructure at the local level; focused on escalation from internal discovery and communication to national information sharing and remediation considerations
State of Nevada Exercise	January 2014	Large-scale, discussion-based TTX for the State of Nevada to support state cybersecurity policy advancement and prepare for future CS and cyber exercise participation

CYBER STORM IV KEY ACHIEVEMENTS

The Cyber Storm IV Exercise Series:

- Created a forum for participating states, government agencies, international partners, and other organizations and individuals to evaluate cyber incident response capabilities
- Allowed for in-depth examination of specific stakeholder groups, such as individual states and cyber centers, and areas of interest, such as public affairs
- Exercised the escalation of an incident from the local to federal level, identifying issues with cyber emergency escalation, resource allocation procedures, and federal emergency response authorities during a major cyber event
- Introduced cyber exercises to states with little or no previous participation, elevating their cyber awareness and relative capabilities, helping to define a way forward, and integrating these states into NCCIC planning efforts
- Increased awareness of Federal (and other) resources available to coordinate, respond to, and mitigate the effects of cyber incidents
- Integrated new stakeholders into the CS community, providing exposure to cyber response exercises, as well as training and education to a wide range of stakeholders both nationally and internationally
- Exercised response protocols and cyber response plans against the simulated escalation of a cyber incident and identified gaps in communications, response plans, and resources
- Facilitated the development of long-term relationships and improved the partnerships between DHS NCCIC and CS IV stakeholders

CYBER STORM IV TRENDS

Across the CS IV Exercise Series, four main trends emerged that capture core findings from the individual exercises. Outlined below, these trends incorporate perspectives of CS IV participants representing the Federal Government, state and local governments, coordination bodies, the private sector, and international partners. They affect the broad cybersecurity community and represent both areas of progress and areas for future improvement.

Trend 1: Cyber Response and Operating Plans

Cyber response and operating plans are used by both public and private organizations as guiding mechanisms for cyber incident response. Many participating stakeholders used the CS IV Exercise Series to evaluate current or draft plans or to inform future planning efforts. As such, exercise takeaways generally highlighted the need to improve current plans based on exercise outcomes and findings or the need to develop and implement plans where they did not already exist. Participants generally agreed the ability to effectively leverage cyber incident response plans promotes coordination, awareness, and recovery in the event of an enterprise-wide cyber incident. For example, multiple states observed that system dependencies existed across their respective departments. As such, taking systems down, making changes, and ultimately bringing systems back up required an unexpected level of coordination and communication. Players found that defining these dependencies in advance, identifying the critical systems, and capturing the required communication and coordination in planning documents would benefit future response.

As participants discussed insights related to planning and plan components, several common themes emerged. First and foremost, as organizations develop new or update existing plans, they must clearly define roles and responsibilities as well as incident management structures. Operational plans should also include incident response processes and procedures, contingency plans, coordination guidance to address specific incidents, prioritization of mission critical systems, and information sharing protocols. In many cases, planners can leverage concepts in planning documents traditionally used for physical response that adhere to the Incident Command System. DHS NCCIC also has planning resources, such as playbooks and templates, to help inform plan development. Participants recommended that cyber incident response plans be living documents—frequently updated to include both appropriate response measures for emerging cyber threats and relevant lessons learned from real world and exercise events.

Participants also found that training and education efforts must accompany plans—a cyber incident response plan that is not widely socialized or understood across the enterprise is essentially useless. Planners and stakeholders should champion training and education efforts to ensure that plans, and underlying processes and procedures, are widely socialized and understood across the relevant stakeholder set. Regular exercises encourage operational familiarity with cyber incident response duties, roles, and responsibilities. These exercises can range from small-scale seminars or drills to large-scale distributed events.

Trend 2: Information Sharing and Communications

While the Department and the cyber incident response community are improving their respective abilities to share information needed to make decisions during cyber incidents, the issue remains a challenge requiring continued focus. Efforts by public and private stakeholders to develop operational relationships, formalize information sharing procedures, and establish command and control structures prior to an incident contribute to improved information sharing and communication during cyber incident response and enhance the collective ability to respond. Ultimately, the speed and efficiency with which information is shared during incident response directly affects the ability of responders to mitigate and respond to an event.

Although players expressed willingness to share information, they also conveyed uncertainty regarding when to communicate, what to communicate, and with whom to communicate. Communication procedures and thresholds for communication, both internally and externally, are often not well-defined or commonly understood. Organizations with established relationships and experience sharing information during steady state or previous incidents coordinated far more easily during exercise play. These players also had a better understanding of the types of information to provide and the information they may expect to receive. Some exercises highlighted that a comprehensive policy could facilitate the reporting of cyber intrusions into critical infrastructure networks and enhance situational awareness of the threats facing critical infrastructure. Formalized information sharing agreements increase situational awareness among diverse stakeholder groups and lead to more efficient cyber incident response as unclear information lines of flow are frequently a major obstacle during a crisis.

In some cases, questions about legal issues and authorities also challenged interactions between public and private sector players. Several players expressed uncertainty regarding the type of information that could legally be shared among private sector organizations and between public agencies due to unfamiliarity with the authorities and processes established. This unfamiliarity delayed player response. Government players also expressed some uncertainty on the authorities, and accompanying thresholds, that could or should be used to provide assistance to the private sector if requested. Clarification regarding information sharing mechanisms and protocols can benefit both the public and private sectors during cyber incident response. Public and private sector players that leveraged existing operational relationships or bilateral agreements highlighted the benefits of establishing these mechanisms prior to an incident.

Finally, in addition to sharing information among affected entities and relevant stakeholders, participants recognized the importance of effectively communicating with the public during a cyber incident. Established information sharing mechanisms and public communications protocols improved the ability to get the message out. Knowing when, what, and how much information to share publically is an important aspect of communications and cyber incident response as well as involving the correct entities in shaping those messages. Over the course of the CS IV Exercise Series, the willingness and ability of technical staff to coordinate with external affairs personnel and organizational communicators improved significantly.

Trend 3: Resource Identification and Allocation

During a cyber event there are a number of different resources available at the national, state, and local levels—as well as through the private sector. The ability to effectively leverage internal and external resources improves cyber incident response capabilities. Although response capabilities and resources varied widely among participants, CS IV participants expanded their knowledge of available resources and assistance options, as well as how to request and obtain these resources.

Across multiple exercises, participants observed challenges with resource identification and allocation. In many cases the effective use of resources was hampered by affected organizations not knowing what was available or how to access available resources. There are often different requirements; these include prescribed escalation paths, official designations, or associated costs that can be overwhelming to work through during response. In order to develop an accurate picture of available resources – both internally and externally – government agencies, private organizations, and others should catalog available resources and identify related thresholds for outreach – including to the Federal

Government – for additional assistance. At the user level, efforts to identify and understand the available resources prior to an incident will improve response capabilities. Conversely, resource owners should also ensure they are communicating and providing information to a broad spectrum of potential stakeholders.

Trend 4: Cybersecurity Training, Awareness, and Education

The wide range of participants in the CS IV Exercise Series helped demonstrate that cybersecurity is everyone's responsibility and is not limited to the domain of Information Technology (IT) staff. Awareness of cyber threats, attack vectors, and recent incidents can be improved across the cybersecurity stakeholder spectrum. Training and education through seminars, exercises, and other events contributes to staff preparedness and improved response capabilities. In addition, collaboration across organizations, through coordinating bodies such as ISACs, or within working groups, serves to raise common understanding and familiarity with the current cybersecurity landscape.

The CS IV Exercise Series highlighted the urgency of implementing comprehensive cybersecurity and awareness campaigns on the threats posed by cyber attacks. While exercises can increase player awareness of cyber-based threats, attack vectors, and potential attack impacts, more consistent familiarity and exposure is needed. Issues such as employee turnover and the constantly-evolving nature of cyber attacks mean that ongoing training is needed to keep staff knowledge levels consummate with the threat level.

CONCLUSION

Since their inception, CS exercises have served to enhance cyber incident response capabilities, promote public awareness, and reduce cyber risk. Continuing that legacy, CS IV provided the cyber incident response community with the opportunity to conduct focused exercises that evaluated specific capabilities. By addressing CS IV exercise findings and implementation items, participants across the cyber incident response community will continue to improve their capabilities and response processes, bolstering the Nation's cyber resilience.

CS IV exercises also benefitted DHS and the NCCIC due to the focus on the role of DHS and its associated components during a cyber event. The exercises helped to develop new and strengthen existing operational relationships between DHS and CS IV stakeholders. DHS addressed priority areas across multiple exercises – including SLTT relations and NCCIC operational coordination activities, such as Cyber Unified Coordination Group (UCG) standup. Following the precedent of CS I-III, CS IV exercise outcomes, findings, and areas for improvement will continue to be addressed by DHS and will be used to inform future efforts.

The CS Exercise Series is a continuous learning and evaluation process with each exercise informing subsequent CS efforts. As such, DHS is using CS IV (as well as NLE 2012) outcomes and findings in order to shape CS V. For instance, six new states participated in a CS event for the first time during CS IV. These states are leveraging their experience to participate operationally in CS V, providing an opportunity to evaluate the actions they implemented in response to CS IV lessons learned. In addition, CS IV focus areas, such as federal assistance to state and local entities, and federal emergency response authorities, are being considered for further evaluation. For CS V, DHS is returning to the traditional capstone exercise model, exercising thousands of stakeholders in a distributed, operational setting over the course of a week.

Homeland Security

National Cybersecurity and Communications Integration Center