TLP: WHITE

Cyber Storm VIII: After-Action Report

August 2022
Cybersecurity and Infrastructure Security Agency

TLP: WHITE

Table of Contents

EXECUTIVE SUMMARY

Introduction

The Cyber Storm (CS) exercise series provides a venue for the federal government, state and local government, the private sector, and international partners to simulate response to a large-scale, coordinated, significant cyber incident impacting the nation's critical infrastructure. Cyber Storm VIII (CS VIII), held in March 2022, allowed over 2,000 participants to exercise their cyber incident response plans and identify opportunities for coordination and information sharing. Building on the success and momentum of Cyber Storm 2020 and lessons learned from real-world events, CS VIII prepared participants to respond to emerging and evolving threats. Additionally, CS VIII was the first iteration of the exercise to be designated as the National Cyber Exercise per the requirements of Section 1744 of the Fiscal Year 2021 National Defense Authorization Act (Public Law 116-283, enacted January 1, 2021).

As an operations-based functional exercise, CS VIII allowed participants to simulate their response to multiple concurrent cyber incidents. The exercise assessed cybersecurity preparedness; examined incident response processes, procedures, and information sharing; and identified areas for improvement. While players worked to resolve the cyberattacks targeting their own organizations, they exercised their capacity to share information and coordinate incident response externally. Participants found that the exercise scenario and mechanics generated robust play and learning relevant to real-world incident response.

Exercise Background

From March 7-10, 2022, the Cybersecurity and Infrastructure Security Agency (CISA) conducted CS VIII, the eighth iteration of the national capstone cyber exercise that brings together the public and private sectors to simulate response to a cyber crisis impacting the nation's critical infrastructure. CISA sponsors the CS exercise series to improve capabilities of the cyber incident response community, encourage the advancement of public-private partnerships within the critical infrastructure sectors, and strengthen the relationship between the federal government and its government partners at the state, local, and international levels. The exercise findings contribute to safeguarding the nation's security and cyber infrastructure by identifying ways to strengthen coordinated incident response along the whole-of-nation approach outlined in the National Cyber Incident Response Plan (NCIRP).

Exercise Goal & Objectives

Goal: Strengthen cybersecurity preparedness and response capabilities by exercising policies, processes, and procedures for identifying and responding to a multi-sector significant cyber incident impacting critical infrastructure.

Objective 1: Examine the effectiveness of national cybersecurity plans and policies.
Objective 2: Explore the roles and responsibilities during a cyber incident with potential or actual physical impacts.
Objective 3: Strengthen information sharing and coordination mechanisms used during a cyber incident.
Objective 4: Foster public and private partnerships and improve their ability to share relevant and timely information across partners.

Scenario & Adversary

CS VIII utilized a realistic scenario to reflect the current operating environment. As the United States (U.S.) has adjusted to the "new normal" professional landscape of a hybrid work environment, the attack vectors have grown, and the paths and levels of trust are increasingly being tested. As a result, attackers are now better able

to exploit organizations.

In an attempt to disrupt U.S. infrastructure components, an attacker named Network Controller (NC) developed a zero-day exploit called DVER. This exploit was designed to provide an opening in networks that allowed adversaries to execute remote commands, move laterally across corporate and industrial networks, and elevate privileges for attackers.

Initially, DVER was written to exploit shared services, allowing attackers to craft specialized packages to gain remote control. Once the attackers gained initial access, they contacted a command and control (C2) server that was set up as a staging device for additional tools and ransomware.

As a result of heightened security measures, internet-facing applications were not prevalent in some organizations. In these instances, the attackers modified the code to allow for socially engineered delivery. Some organizations received phishing emails while others fell victim to watering hole attacks. In all instances, the adversaries exploited an attack vector created by the victim.

As the storyline progressed, the adversaries gained access, connected to the initial C2 or staging server, executed commands, and then employed known tools and vulnerabilities to perform reconnaissance and conduct exploitation.

The core scenario for CS VIII included attacks against industrial control systems/operational technology (ICS/OT) and attacks against traditional enterprise networks. These had their own nuances, but the core attack methodology was consistent across target environments.

Key Achievements

CS VIII built upon preceding iterations to provide a venue for learning and advancement. Through the exercise planning process and execution, CS VIII:

- Strengthened cybersecurity preparedness and response capabilities by exercising policies, processes, and procedures for identifying and responding to a multi-sector significant cyber incident impacting critical infrastructure;
- Integrated new stakeholders into a CS national capstone exercise, including one new sector, Water and Wastewater Systems, expanding their exposure to large-scale cyber exercises, supporting relationship-building, and providing a foundation for future exercise and improvement efforts;
- Provided a multifaceted attack vector based on common core scenario conditions that provided a mechanism for increased participation within and across participating organizations while also enabling a record number of veteran organizations to participate;
- Raised awareness of the rapidly expanding cyberattack surface and the nuances of response to incidents impacting ICS/OT and enterprise information technology (IT) networks;
- Drove government stakeholders to convene the Cyber Unified Coordination Group (UCG) based on procedures contained in the NCIRP. Once formed, Cyber UCG members conducted several daily conference calls, signifying unity of effort in coordination and information sharing, along with the production and dissemination of multiple intelligence and information reports to private and public organizations;
- Supported classified planning and execution efforts in coordination with the Intelligence Community Security Coordination Center (IC SCC) for ICE STORM 2022, a classified companion exercise. During execution, players successfully exercised tear-line processes to share contextual information at the unclassified level with CS VIII participants. This information enabled government and private sector

coordination and response activities in CS VIII;

- Emphasized information sharing and communication as International Watch and Warning Network (IWWN) partner nations worked toward improving their incident response communications (in terms of frequency, mechanism, and type of information shared). In addition, during the planning phase, the collaborative scenario and inject development process led to increased coordination and information sharing during exercise execution, specifically between United Kingdom (UK) and Canadian players in response to a simulated multinational company with operations in both countries affected by the scenario;
- Created a multilayered scenario that provided participants the opportunity to stress a whole-of-organization response to an incident, involving organizations' technical experts, public affairs representatives, legal affairs representatives, and organizational leadership. Participating organizations engaged their senior leadership in discussions and decision-making, considering how incident response plans and process aligned to strategic priorities and governance principles;
- Integrated a simulated and dynamically-updated traditional and social media platform to replicate the customer and general public components of an incident and provided a no-fault learning environment to practice strategies that support this aspect of response;
- Allowed participating states to closely examine the associated roles and responsibilities of supporting agencies within their cyber incident response frameworks. Moreover, CISA examined the unity of effort between states and federal agencies during a significant cyber incident exhibiting physical impacts; and
- Achieved the development and dissemination of an in-exercise joint Cybersecurity Advisory (CSA) for the first time in a CS exercise. This joint CSA was authored by CISA, the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA), as well as Canada's Communication Security Establishment (CSEC), Australia's Cyber Security Centre (ACSC), the United Kingdom's National Cyber Security Center (NCSC-UK), and New Zealand's National Cyber Security Centre (NCSC-NZ). During the CS VIII Sector Coordination Call, CISA briefed stakeholders on the joint CSA, giving actionable steps to aid in response efforts. The creation of the in-exercise joint CSA highlights the ongoing, real-world collaboration and coordination between federal law enforcement partners, the intelligence community, and DoD. This continued cooperative effort allows partners to seamlessly produce a joint CSA and other products that detail real-world threats. A month after CS VIII, the Department of Energy (DOE), CISA, NSA, and FBI released a real-world joint CSA, warning certain advanced persistent threat (APT) actors have exhibited the capability to gain full system access to ICS/supervisory control and data acquisition (SCADA) devices.

Key Findings

Finding 1: CS VIII highlighted the need to review and update national plans and policies, such as the NCIRP, to reflect the current cyber threat environment.

During the exercise, national plans and policies as written and discussed had limited impact or influence on private sector response. With a constantly evolving cyber landscape, the public and private sectors must maintain a comprehensive understanding and awareness of national plans, policies, statutes, and other implemented guidance that can shape an organization's response and impact operations. In addition, IT standards, governance, and related policies must be included in respective incident response plans, contracts, and daily operations to ensure compliance from an organizational or legal perspective and promote a whole-of-organization response approach.

Finding 2: The exercise continued to examine public and private sector information sharing, collaboration, and

coordination during a cyber incident and identified ongoing challenges that exist within the cyber response community.

Though substantial strides in specific escalation processes and coordination have been made in recent years, the exercise exposed continuing challenges that exist in information sharing, collaboration, and coordination at all levels of incident response.

Finding 3: CS VIII emphasized the need for organizations to review and be trained appropriately on their cyber incident response plans.

Organizations can more quickly and effectively respond to a cyberattack when their cyber incident response plan is fully understood across the organization. Periodically reviewing and testing cyber incident response plans and procedures ensures roles and responsibilities are clear, that plans can address emerging threats, and proper resources are readily available.

Finding 4: In the event of a cyberattack that affects IT and ICS/OT networks, a coordinated response within an organization is paramount to a consistent and well-informed response.

The exercise highlighted the potential for a cyber incident to impact or put at risk both IT and ICS/OT networks. Though the technologies, systems, and functions; associated response and recovery considerations; and required subject matter experts (SME) can be distinct, the exercise demonstrated the importance of coordinated organizational response.

Finding 5: CS VIII highlighted the value of proactive and responsive public affairs engagement to address customer and stakeholder concerns in the event of a cyberattack.

External affairs play during the exercise demonstrated the importance of cyber response beyond the technical sphere. Victim organizations were confronted with simulated criticism on social media and exposure on traditional media that potentially threatened their brand reputation, financial stature, and customer base. In CS VIII, organizations with proactive public affairs engagement addressed customer and stakeholder concerns and could shape the narrative around their cyberattack. This emphasizes the importance of a whole-of-organization response during a cyber incident.

Conclusion

Over three days of live distributed exercise play, CS VIII provided stakeholders with a realistic environment to stress their cyber incident response capabilities through a multi-sector cyberattack targeting critical infrastructure. Players examined national-level cybersecurity plans and policies while sharing information and coordinating across the cyber response community. Public and private entities were able to foster relationships through exercise planning and execution which led to an improvement in their ability to share relevant and timely information. In addition, the exercise's simulated platform provided a realistic, dynamic environment to safely engage non-technical entities within participating organizations and exercise the communications aspects of their cyber incident response plans.

Building on previous CS iterations, CS VIII continued to allow for significant examination of processes and procedures throughout the cyber incident response community. The exercise enabled planners to identify strengths and weaknesses within their respective organizations, while also providing the opportunity to analyze trends across the entire exercise participant set, yielding a set of findings that highlight the progress made through participating in cyber-focused exercises, evaluating real world events, and increasing cybersecurity preparedness activities. The findings in this report stress potential areas to improve the nation's cyber resilience and response capabilities, and all participating organizations are encouraged to leverage these findings to improve their own preparedness posture.

EXERCISE OVERVIEW

After Action Report Purpose

The Cyber Storm VIII (CS VIII) After Action Report (AAR) provides an overview of the exercise's design, development, and execution, and details the findings identified from the evaluation phase of the exercise lifecycle. These findings are derived from observations made during the planning and execution of the exercise and are intended to inform the Cybersecurity and Infrastructure Security Agency (CISA) and stakeholder improvement activities.

Cyber Storm Series Overview

The Cyber Storm (CS) exercise series has evolved over time in step with the dynamic nature of cyber threats and the maturation of cyber incident response plans and policies. Cyber Storm I marked the first time the cyber response community came together to examine the national response to cyber incidents. Cyber Storm IV included 15 building block exercises to help communities and states exercise cyber response capabilities for escalating incidents. Cyber Storm 2020 (CS 2020) involved more than 2,000 distributed players from approximately 210 organizations across critical infrastructure sectors who exercised incident response procedures in a remote environment. CS 2020 raised awareness of long-standing and ongoing vulnerabilities in the core infrastructure of the Internet.

CS VIII was built on lessons learned from all previous CS exercises to challenge participants with a sophisticated scenario rooted in the evolving nature of today's cyber threats and increasingly connected world.

This exercise demonstrates CISA's commitment to training the nation's critical infrastructure stakeholders to continuously evaluate incident response capabilities and improve the nation's cyber resilience.

Acknowledging its importance, CISA conducted the exercise while preparing for and responding to real-world issues in a heightened threat environment. Participants across the globe came together to respond to a simulated cyberattack impacting critical infrastructure. Outcomes from the exercise include actionable lessons learned related to cyber incident response plans and improved cyber hygiene, as well as the value of building new and strengthening existing relationships between public and private sector peers.

Exercises are critical to our nation's cyber preparedness and resilience – bringing together the cybersecurity community to learn from each other in a safe environment. CISA is committed to providing the nation with access to a range of cybersecurity resources and exercises, to include CS, designated as the National Cyber Exercise.

EXERCISE GOAL & OBJECTIVES

Goal: Strengthen cybersecurity preparedness and response capabilities by exercising policies, processes, and procedures for identifying and responding to a multi-sector significant cyber incident impacting critical infrastructure.

Objective 1: Examine the effectiveness of national cybersecurity plans and policies.
Objective 2: Explore the roles and responsibilities during a cyber incident with potential or actual physical impacts.
Objective 3: Strengthen information sharing and coordination mechanisms used during a cyber incident.
Objective 4: Foster public and private partnerships and improve their ability to share relevant and timely information across partners.

PARTICIPATION

CS VIII included participants from federal, state, and private sector organizations, as well as international partners. Within key communities of interest:

- More than 100 private sector companies represented a diverse cross-section of industry and spanned 10 critical infrastructure sectors.
- Thirty-three federal departments and agencies included organizations responsible for threat response, asset response, intelligence support, private sector coordination, and public services.
- Nine participating states included components of law enforcement, administrative, and public-service organizations.
- Fifteen partner nations from the International Watch and Warning Network (IWWN) joined the United States (U.S.) in exercising their information sharing and incident response coordination.

Within organizations, CS VIII players spanned from operational shop floor and front-line customer care staff, to security and technical responders, incident response teams, legal affairs specialists, public affairs specialists, and senior leaders.

KEY ACHIEVEMENTS

CS VIII built upon preceding iterations of the exercise to provide a venue for learning and advancement. Through the exercise planning and execution process, CS VIII:

- Strengthened cybersecurity preparedness and response capabilities by exercising policies, processes, and procedures for identifying and responding to a multi-sector significant cyber incident impacting critical infrastructure;
- Integrated new stakeholders into a CS national-level capstone exercise, including one new sector, Water and Wastewater Systems, expanding their exposure to large-scale cyber exercises, supporting relationship-building, and providing a foundation for future exercise and improvement efforts;
- Provided a multifaceted attack vector based on common core scenario conditions that provided a mechanism for increased participation within and across participating organizations while also enabling a record number of veteran organizations to participate;
- Raised awareness of the rapidly expanding cyberattack surface and the nuances of response to incidents impacting industrial control systems/operational technology (ICS/OT) and enterprise information technology (IT) networks;
- Drove government stakeholders to convene the Cyber Unified Coordination Group (UCG) based on procedures contained in the National Cyber Incident Response Plan (NCIRP). Once formed, Cyber UCG members conducted several daily conference calls, signifying unity of effort coordination and information sharing, along with the production and dissemination of multiple intelligence and information reports to private and public organizations;
- Supported classified planning and execution efforts in coordination with the Intelligence Community Security Coordination Center (IC SCC) for ICE STORM 2022, a classified companion exercise. During execution, players successfully exercised tear-line processes to share contextual information at the unclassified level with CS VIII participants. This information enabled government and private sector coordination and response activities in CS VIII;
- Emphasized information sharing and communication as International Watch and Warning Network (IWWN) partner nations worked toward improving their incident response communications (in terms of frequency, mechanism, and type of information shared). In addition, during the planning phase, the collaborative scenario and inject development process led to increased coordination and information sharing during exercise execution, specifically between United Kingdom (UK) and Canadian players in response to a simulated multinational company with operations in both countries that were affected by the scenario;
- Created a multilayered, realistic scenario that provided participants the opportunity to stress a whole-of-organization response to an incident, involving organizations' technical experts, public affairs representatives, legal affairs representatives, and organizational leadership. Participating organizations engaged their senior leadership in discussions and decision-making, considering how incident response plans and processes aligned to strategic priorities and governance principles;
- Integrated a simulated and dynamically-updated traditional and social media platform to replicate the customer and general public components of an incident and provided a no-fault learning environment to practice strategies that support this aspect of response;
- Allowed participating states to closely examine the associated roles and responsibilities of supporting

agencies within their cyber incident response frameworks. Moreover, CISA examined the unity of effort between states and federal agencies during a significant cyber incident exhibiting physical impacts; and

- Achieved the development and dissemination of an in-exercise joint Cybersecurity Advisory (CSA) for the first time in a CS exercise. This joint CSA was authored by CISA, the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA), as well as Canada's Communication Security Establishment (CSEC), Australia Cyber Security Centre (ACSC), the United Kingdom's National Cyber Security Center (NCSC-UK), and New Zealand's National Cyber Security Centre (NCSC-NZ). During the CS VIII Sector Coordination Call, CISA briefed stakeholders on the joint CSA, giving actionable steps to aid in response efforts. The creation of the in-exercise joint CSA highlights the ongoing, real-world collaboration and coordination between federal law enforcement partners, the intelligence community, and DoD. This continued cooperative effort allows partners to seamlessly produce a joint CSA and other products that detail real-world threats. A month after CS VIII, the Department of Energy (DOE), CISA, NSA, and FBI released a joint CSA warning certain advanced persistent threat (APT) actors have exhibited the capability to gain full system access to ICS/supervisory control and data acquisition (SCADA) devices.

SCENARIO & ADVERSARIES

Core Scenario Overview

CS VIII utilized a realistic scenario to reflect the current operating environment. As the U.S. has adjusted to the "new normal" professional landscape of a hybrid work environment, the attack surface has expanded. As organizations struggle to balance requirements for both remote access and security, attackers have increasingly diverse methods to penetrate and exploit organizations.

In an attempt to broadly compromise and disrupt U.S. infrastructure components, an attacker named Network Controller (NC) developed a zero-day exploit called DVER. This exploit was designed to provide an opening in networks that allowed adversaries to execute remote commands, move laterally across corporate and industrial networks, and elevate privileges for attackers. NC wrote DVER to exploit shared services, allowing attackers to craft specialized packages to gain remote control. Once the attackers gained initial access, they reached out to a command and control (C2) server that served as a staging device for additional tools and ransomware.

As a result of heightened security measures or segregated environments (e.g., ICS/OT), some organizations prohibited or severely limited their internet-facing applications. In these instances, the attackers modified the code to allow for socially engineered delivery. Some organizations received phishing emails while others fell victim to watering hole attacks.

As the storyline progressed, the adversaries gained access, connected to the initial C2 or staging server, executed commands, and then employed known tools (e.g., Cobalt Strike) and vulnerabilities (e.g., CVE-2021-41379) to perform reconnaissance and conduct exploitation. The core scenario for CS VIII included attacks against ICS/OT and attacks against traditional enterprise networks. These had their own nuances, but the core attack methodology was consistent across target environments.

Industrial Control Systems/Operational Technology

ICS/OT have unique and often disparate implementations. NC planned for this eventuality and DVER and the ransomware variant, EpiCrypt, had multiple attack paths to infect these networks. If the attackers could connect to the ICS/OT network through remote execution, they used the C2 server to download tools and ransomware to the vulnerable networks. This attack was more complex and harder to eradicate from the network. If the ICS/OT networks were considered air-gapped, the attackers, under direction of NC, used socially engineered attacks to install malicious code on an engineer's laptop or on a portable flash memory device. The ransomware was coded to detonate at a designated date and time, allowing the ransomware to worm its way through the network. As

the scenario unfolded, organizations experienced impacts such as taking essential systems offline, manufacturing and robotics malfunctions, production delays, fulfillment center delays, supply chain disruptions, plant closures, water quality issues, and rail and bus service disruptions. Customers and employees reacted to details about the impacts on OT systems as they appeared on social and traditional media. Victim organizations concluded the exercise by regaining control of their OT systems through coordination efforts and/or independent mitigation strategies.

Enterprise Information Technology

An unforeseen consequence of the "work from home first policy," seen across the country, is expansion of the attack surface. While many companies require a secure connection to access their virtual private network (VPN), most "every day" users do not employ strict cyber hygiene practices at home.

In the scenario, attackers attempted to gain initial entry points into companies' networks through their public-facing Internet. Specifically, the attackers targeted employees at companies of interest, attacked their home networks, and used these as a pivot point to then move into the company network's VPN by piggybacking off the valid connection. The Enterprise IT scenario component paralleled the ICS/OT scenario and allowed participants to examine their responses to ransomware, data exfiltration, or a combination of both. As the attacks unfolded, organizations reported impacts such as data leaks to the dark web, communications challenges, IT service disruptions, degraded consumer experience while processing financial transactions, and human resource systems disruptions. Customers and employees reacted to details about the impacts to business systems, and their possible financial implications, as they appeared on social and traditional media. In the end, the exercise saw the Enterprise IT scenario victim organizations regain control of their enterprise systems through similar efforts as the ICS/OT scenario, coordinating across the cyber response community and implementing independent mitigation strategies.

EXERCISE FINDINGS

CS VIII allowed for examination and stress-testing of policies, procedures, and incident response protocols in order to identify gaps and areas of improvement across the incident response community. The Exercise Planning Team analyzed participant surveys, collected stakeholder lessons learned, and reviewed observations recorded during CS VIII execution to incorporate experiences and feedback from across the federal government, state and local government, coordination bodies, the private sector, and the international community. The following section contains five high-level exercise findings impacting the cybersecurity community, supported by observations drawn from exercise play. Stakeholder recommendations are included to improve the coordinated cyber incident response process.

Finding 1: CS VIII highlighted the need to review and update national plans and policies, such as the NCIRP, to reflect the current cyber threat environment.

During the exercise, national plans and policies as written and discussed had limited impact or influence on private sector response. With a cyber landscape that is constantly evolving, it is imperative for the public and private sectors to maintain a comprehensive understanding and awareness of national plans, policies, statutes, and other guidance being implemented that can shape an organization's response and impact operations. In addition, IT standards, governance, and related policies, must be included in respective incident response plans, contracts, and daily operations to ensure compliance from an organizational or legal perspective and promote a whole-of-organization response approach.

Observations

1. As the exercise unfolded, private sector organizations used current national plans and policies in a limited capacity. These organizations noted that the NCIRP preceded CISA's formation, and therefore it does not include all relevant stakeholders or the latest policies. In addition, participants expressed that the NCIRP does not fully outline the division of responsibilities between CISA and the FBI when establishing unified coordination or distributing information. CS VIII validated the National Defense Authorization Act (NDAA) for Fiscal Year 2022 (FY22) that directs CISA to update the NCIRP every two years to reflect current directives and initiatives. As part of the revision process, engagement with the private sector will allow for greater buy-in and awareness from the cyber response community.
2. Many participating state governments used the NCIRP's framework as a basis for developing organization-specific incident response plans and annexes, incorporating elements of the Cyber Incident Severity Schema to illustrate the impacts of a cyber incident affecting state agencies and critical infrastructure partners. As they developed their own plans and tested them in CS VIII, state agencies agreed that the NCIRP lacks detail regarding the type of support state, local, tribal, and territorial governments could receive during a significant cyber incident. This information would assist state governments with future cyber incident response planning efforts and coordination. In addition, ensuring state plans are consistent with evolving federal policies and guidelines, such as the NCIRP, will help states mitigate future cyberattacks in an ever-evolving threat landscape.
3. Private sector organizations noted that CS VIII underscored the importance of having familiarity with relevant national plans, policies, and statutes before an incident. However, due to the volume of these documents, publications that are not directly related to vulnerabilities or the incident are not immediately helpful during an active cyberattack.
4. National policies and procedures can help guide and augment an organization's internal cyber incident response, reinforcing best practices, and enumerating access to resources. Participants highlighted that larger organizations, possessing mature cybersecurity response capabilities may have unique insights

that smaller organizations or organizations that want to improve their internal cyber readiness and resilience can leverage.

Stakeholder-Derived Recommendations:

- As part of the NCIRP revision process, CISA should incorporate input from public and private sector partners to ensure the plan is relevant to all members of the cyber response community.
- As physical impacts resulting from cyber incidents become increasingly prevalent, further education and awareness of NCIRP-identified roles and responsibilities in future plans and policies will be necessary. Once these national-level resources are updated and developed, CISA and partner organizations (Sector Risk Management Agencies [SRMAs], sector-specific Information Sharing and Analysis Centers [ISACs] and Information Sharing and Analysis Organizations [ISAOs]) should coordinate distribution to public and private sector stakeholders so they can update and align their own plans and procedures as needed. SRMAs should also examine their Sector-Specific Plans to confirm they reflect the latest information and policy guidance.
- Public and private sector partners should consider collaborating on the development of internal "quick start guides" that outline relevant points of contact and communications channels for use during a cyberattack.

Finding 2: The exercise continued to examine public and private sector information sharing, collaboration, and coordination during a cyber incident and identified ongoing challenges that exist within the cyber response community.

Though recent years have seen substantial strides in specific escalation processes and coordination, the exercise exposed continuing challenges that exist in information sharing, collaboration, and coordination at all levels of incident response.

Observations

1. For the first time in the Cyber Storm exercise series, a Cyber UCG activated organically, based on exercise scenario escalation of the cyber incidents. This allowed the organizations assigned to the Cyber UCG, either by the NCIRP, Presidential Policy Directives, or the Cyber Response Group (CRG) to coordinate and synchronize resources in response to a significant cyber incident. On the final day of the exercise, the Cyber UCG provided an operational exercise update to the real-world CRG.
2. During CS VIII, an active UCG was tracking and coordinating responses to real-world issues. It highlighted the potential for multiple active UCGs, requiring mechanisms for joint awareness and coordination. While CS VIII did not ultimately exercise coordination between active UCGs, it highlighted the need to understand how a Cyber UCG coordinates with other active UCGs.
3. Coordination between CISA and key interagency and international partners during the exercise resulted in drafting and releasing a comprehensive Joint Cybersecurity Advisory which aided the exercise community in response efforts, such as identifiying indicators of compromise (IOCs). The production and dissemination of this advisory proved that the process to develop and approve joint, actionable reporting matured since CS 2020.
4. The exercise enabled participants to recognize the resources and steps necessary to protect information systems and critical infrastructure. As response and recovery efforts were underway, CISA convened a

stakeholder conference call to provide insight on the Joint Cybersecurity Advisory, emphasizing specific mitigation actions stakeholders should take. The call provided a valuable opportunity for stakeholders, who may not have participated in a real-world call held by CISA, to learn about CISA's key role in sharing information as rapidly and broadly as possible.

5. In previous iterations, Law Enforcement/Intelligence/Department of Defense (LE/I/DoD) participants expressed the need to increase collaboration between both the unclassified and classified components of the exercise and have robust Intelligence Community participation. In CS VIII, the Intelligence Community successfully engaged at appropriate levels to inject multiple products and tearline reports that enabled government and private sector coordination in the exercise. While law enforcement, intelligence, and DoD partners took the necessary declassification steps to disseminate the appropriate information to private sector partners, players noted that challenges remain in declassifying pertinent and actionable information in a timely manner.
6. During a large-scale cyberattack targeting multiple critical infrastructure sectors, cross-sector engagement led by sector coordination groups, ISACs, and ISAOs can contribute to situational awareness and enable sharing response information and strategies. During CS VIII, the National Council of ISACs (NCI) initiated coordination between cross-sector member ISAC analysts. Though the exercise reached thresholds to coordinate national response bodies and other mechanisms, undefined thresholds limited NCI leadership coordination calls with CISA or other federal strategic partners. Due to exercise timing, the normal battle rhythm of working problems internally and then expanding collaboration with federal partners could not be achieved in real time. As such, NCI senior leadership engagement with public sector partners could not be fully explored or tested.
7. As the scope of cyberattacks continues to expand and impact a more diverse range of organizations, stakeholders noted the importance of maintaining a common operating picture (COP). As the incident widened, they found that they were often unaware of the tactical scope and details and partially filled this void by monitoring simulated social media.
8. Federal partners highlighted the challenge of communicating with federal incident responders and coordinating response efforts in a virtual environment, where responders are working together across multiple work sites and locations. During the exercise, some federal groups utilized internal chat functions to report their actions, provide updates, and share information. They noted the advantage of establishing a cyber-specific group chat and considered implementing a similar process for real life incidents.

Stakeholder-Derived Recommendations:

- Although challenges remain, federal partners should increase collaboration across agencies to continue streamlining the declassification process for relevant and timely information sharing.
- CISA should continue to dedicate resources toward stakeholder engagement activities during and after cyber incidents.
- States should consider reviewing and updating their cybersecurity response plans and policies to correspond with federal policies and guidelines that help further mitigate cyberattacks against critical infrastructure and their citizens.
- Public and private sector partners should continue to review and exercise their communication and information sharing protocols in order to maintain a COP in the event of a cyberattack.
- As an incident management best practice, organizations should consider available tactical communication platforms (e.g., an internal, instant messaging application) that can be leveraged during a cyber incident that may impact the confidentiality, integrity, and availability of traditional communication mechanisms (e.g., email).

Finding 3: CS VIII emphasized the need for organizations to review and be trained appropriately on their cyber incident response plans.

Organizations can more quickly and effectively respond to a cyberattack when their cyber incident response plan is fully understood across the organization. Periodically reviewing and testing cyber incident response plans and procedures ensures roles and responsibilities are clear, that plans can address emerging threats, and proper resources are readily available.

Observations

1. Cyber incident response plan review and testing allows organizations to integrate stakeholders from all levels of the organization. For example, the ransomware simulated in CS VIII underscored issues surrounding legal liability and cyber insurance, leading to legal affairs participation. Faced with encrypted backups, some organizations even went through their ransom payment decision matrices with additional participants from legal affairs and finance. Public and private sector organizations acknowledged that ransomware attacks have changed rapidly over the last few years and their previously developed response plans may not address the most recent tactics, techniques and procedures employed by adversary groups (e.g., polymorphic malware, data exfiltration, public shaming, attacker outreach to organization's leaders, customers, partners). Participants highlighted the need to revisit their ransomware response plans and update them to address current threats.
2. Due to real-world incidents, some private sector organizations could not involve senior leadership in incident response discussions in real-time. Organizations developed numerous solutions to overcome this impediment (e.g., pre-scheduling scenario discussions with senior leaders, conducting post exercise discussions, simulating in-exercise response). Despite these challenges, organizations worked through their incident response processes and procedures and tested their chain of command and external communications either with or without their designated leader(s). Participants noted the value and lessons learned from senior leaders, incident response teams, communication teams, and other staff. In some instances, the absence of a senior leader created an opportunity for backup or secondary contacts to train and make decisions.

3. States examined the activation of their various cyber incident response plans and policy mechanisms, including National Guard mobilization and coordination with federal partners. This allowed the state agencies responsible for coordinating statewide cyber response to explore the associated roles and responsibilities of participating state agencies and critical infrastructure partners. Proactive reporting and response coordination helped states mitigate the technical impacts and business repercussions for impacted agencies and critical infrastructure entities. States achieved this by building on standing policies and existing relationships with impacted agencies and critical infrastructure partners, allowing them to refine coordination procedures and improve their incident response plans.

Stakeholder-Derived Recommendations:

- **Public and private sector partners should consider cross-organizational training on cyber incident response plans, policies, and procedures to combat future cyberattacks.**
- **Although real-world incidents take precedent in an exercise environment, organizations should consider designating some members of senior leadership to participate in future exercises. While these roles can be simulated, their active leadership and policy experience is crucial to the response and mitigation of a cyberattack.**

Finding 4: In the event of a cyberattack that affects IT and ICS/OT networks, a coordinated response within an organization is paramount to a consistent and well-informed response.

The exercise highlighted the potential for a cyber incident to impact or put at risk both IT and ICS/OT networks. Though the technologies, systems, and functions; associated response and recovery considerations; and required SMEs can be distinct, the exercise demonstrated the importance of coordinated organizational response.

Observations

1. In many cases, victim organizations saw impacts across both enterprise IT and ICS/OT environments, but managed incidents and response separately due to the nature of their internal playbooks or procedures. Organizations recognized the need to have a coordinated response due to the growing likelihood of an attack that spans or impacts multiple environments. This would enable organizations to refine internal roles and responsibilities, associated decision authorities, and communications paths.
2. Organizations highlighted the intensive coordination needed to respond to cyber incidents impacting IT and OT networks and noted that establishing communications and response procedures with other stakeholders who are not typically involved in cyber incident response is critical to response and recovery efforts. Some organizations considered integrating notifications and other coordination procedures into relevant plans, so it is clear which entity is responsible for responding to and reporting on both IT and physical aspects of the incident.
3. The exercise underscored the importance of securing ICS/OT systems to ensure physical safety of nearby personnel and potentially the general public using products and services that organizations offer. Through the exercise, organizations developed a keen understanding of the safety component of the ICS/OT and cyber nexus. Because of the existing connections between IT and ICS/OT infrastructure, organizations need to fully understand resulting impacts from a potential cyberattack.

Stakeholder-Derived Recommendations:

- Organizations should develop stronger safety protocols, empower and educate ICS/OT operators, and continue the discussion of physical safety during a cyber incident with physical impacts.
- Organizations should consider developing out-of-band communications or back-up communication mechanisms that could alleviate communication gaps in incident response. CISA should assist agencies in developing alternate communication methodology known as Primary, Alternate, Contingent, and Emergency (PACE).
- CISA should consider training and exercising organizations on establishing best practices for out-of-band/back-up communications mechanisms.
- Organizations should consider training/exercises for their respective groups on the impacts of a cyberattack to ICS/OT systems and share best practices to prevent and respond to incidents.
- CISA should verify that agencies are registered users of Government Emergency Telecommunications Service and Wireless Priority Services (GETS/WPS) to ensure that they have the level of priority needed to communicate during incidents. Users can be added to the GETS and WPS program before, during, or after an incident.

Finding 5: CS VIII highlighted the value of proactive and responsive public affairs engagement to address customer and stakeholder concerns in the event of a cyberattack.

External affairs play during the exercise demonstrated the importance of cyber response beyond the technical sphere. Victim organizations were confronted with criticism on social media and exposure on traditional media that potentially threatened their brand reputation, financial stature, and customer base. In CS VIII, organizations with proactive public affairs engagement addressed customer and stakeholder concerns and could shape the narrative around their cyberattack. This emphasizes the importance of a whole-of-organization response during a cyber incident.

Observations

1. During the exercise, the cyberattacks caused a wave of customer complaints and public speculation on social media; traditional media also scrutinized the incidents. Public Information Officers (PIO) and External Affairs Officers understood the importance of monitoring social media forums and news feeds to understand the depth of public concerns. In response, they provided interviews to journalists, released public statements via social media and the press, and engaged directly with customers to manage the message, allay public concern, and manage disinformation.
2. Some participants noted that the media attention around the widespread incident garnered attention from senior leaders within their organizations and played an important role in helping incident responders understand the scale and severity of the attack. They acknowledged that the incident they were addressing internally may not have escalated as quickly to senior leader levels without the awareness that other organizations across sectors were dealing with a similar incident. While organizations rely on threat intelligence and sector-wide information sharing, they noted that the media played a central role in their understanding of the magnitude of the incident.
3. Unlike in past CS iterations, some organizations came into CS VIII with an extensive communications approach based on a broader understanding of their organization's strategy and key messages during a cyber incident. As part of their strategies for addressing the far-reaching impacts of a cyberattack,

many organizations prepared standard language for internal and external communications, established clear guidelines for external engagement when speaking about the incident, and identified specific points of contact to be the face and voice of the institution. These combined steps helped organizations shape public messaging and mitigate reputational risk during the exercise.

4. Effectively monitoring social and traditional media can provide value to incident response and mitigate reputational issues. During the exercise, players could glean information about the adversaries from media reports, security research, activity on the Dark Web, social media activity, and even adversary trolling directed at their own organization. This gave players insights into the attack and helped them confirm the technical incidents were the impacts of malicious cyberattacks. In several instances, players learning of impacts at other organizations through media reporting also prompted information sharing and coordination.

Stakeholder-Derived Recommendations:

- **Organizations should ensure external affairs teams have media action plans and pre-approved messaging to prepare them to address the public impacts of a cyber incident.**
- **CISA should continue to emphasize effective external crisis communications strategies through various service offerings to include briefings, trainings, and future exercises.**

EXERCISE DESIGN SUMMARY

Exercise Planning Construct

Planning Construct Overview

CS VIII leveraged the Homeland Security Exercise and Evaluation Program (HSEEP) principles to inform the exercise planning, conduct, and evaluation processes. The CS VIII planning timeline was divided into five phases that occurred over approximately 15 months, as identified below in Figure 1.

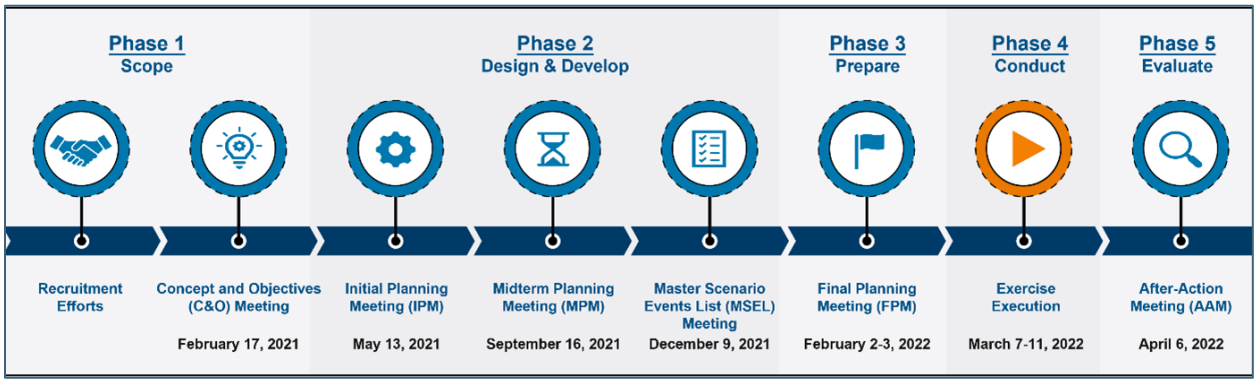

Figure 1: CS VIII Planning Timeline

Scope Phase

In the initial stages of the Scope Phase, the CS VIII Planning Team collaborated with CISA stakeholders to develop an exercise concept. This included identifying the scope, goal and objectives, planning timeline, potential core scenario ideas, and potential primary sectors of participation.

Concept and Objectives Meeting

Overview

On February 17, 2021, CISA hosted the Concept and Objectives (C&O) Meeting. Approximately 100 participants and stakeholders from the government and private sector attended the meeting virtually to review and provide input to the CS VIII concept. The C&O Meeting provided planners with the opportunity to establish consensus on the exercise direction and focus, including the scope, exercise goal and objectives, and the overall planning process, including the planning timeline, scenario ideas for further exploration, and recruitment. During this meeting, the CS VIII planning community refined and finalized the CS VIII objectives.

Following this meeting, the Exercise Planning Team initiated recruitment efforts, reengaged previous participants, and continued to define the overall scope based on feedback from the C&O Meeting.

Outcomes

Critical infrastructure sector selection comprised an important milestone in the Scope Phase. Traditionally, CS exercises include representation from at least two critical infrastructure sectors in addition to traditional IT and Communications Sector participants. Separating from past exercises, CS VIII incorporated private sector participation from across any interested critical infrastructure sector. This change in construct provided the opportunity to offer more flexibility in participation, accommodate robust participation by CS veterans, and the ability to bring in new players.

In terms of exercise design and construct, the Exercise Planning Team retained a community approach to exercise planning. As participants onboarded, the Exercise Planning Team assigned participants to a more

manageable and focused CS Working Group, each with a dedicated Exercise Planning Team Lead. The CS Working Groups created forums to discuss common issues and identify scenario impacts that would challenge their players. The CS VIII Working Groups included Federal, States, International, LE/I/DoD, CISA, and three critical infrastructure sector communities: Critical Infrastructure (CI) I (Communications, Financial Services, IT, and the Commercial Facilities Sector – Retail Subsector), CI II (Chemical, Critical Manufacturing, and Healthcare and Public Health Sector), and CI III (Energy, Water and Wastewater Systems Sector, and the Transportation Systems – Automotive, Pipeline, Postal and Shipping, and Mass Transit Subsectors).

Design and Develop Phase

The Design and Develop Phase comprised most of the planning process and included three of the five major planning meetings. During this phase, the Exercise Planning Team and organizational planners finalized the exercise's goal and objectives, defined boundaries and desired conditions, identified players, developed the scenario and adversary, and applied these to organizational conditions to create scenario injects. In addition, the organizational planners participated in monthly CS VIII Working Group calls, received virtual training on CS VIII, and led all organization-specific aspects of exercise planning.

Initial Planning Meeting

Overview

On May 13, 2021, CISA hosted the Initial Planning Meeting (IPM). Approximately 230 participants and stakeholders from the government and private sector attended the meeting virtually to review and provide input to the CS VIII exercise structure and scenario development. For many of the stakeholders, the IPM was their first chance to gain an understanding of the exercise scope and construct. The plenary sessions informed stakeholders of the timeline, associated milestones, planner responsibilities, and the scenario planning process. CS Working Groups used breakout sessions to scope the participant set, plans and policies, potential attack vectors, and scenario boundaries.

Outcomes

Following the IPM, CS VIII stakeholders identified organization-specific objectives, scenarios of interest, and additional partners and players to recruit for the exercise. A Scenario Team, comprised of key technical and exercise professionals, began to design the exercise core scenario to serve as the technical basis for exercise play. The International Working Group also stood up immediately following the IPM. CS Working Groups held monthly teleconferences throughout the planning process to provide updates and advance community and scenario development. In many cases, CS Working Group Leads also held one-on-one calls with organizations to conduct more focused working sessions on each organization's exercise play.

Midterm Planning Meeting

Overview

On September 16, 2021, CISA hosted the Midterm Planning Meeting (MPM). Approximately 330 participants and stakeholders from the government and private sector attended the meeting virtually to review and provide input to the CS VIII exercise structure and scenario development. At the conclusion of the MPM, the Exercise Planning Team provided information on exercise resources, logistics, the after-action process, and initial public affairs guidance on CS VIII external messaging.

Outcomes

Stakeholder organizations used the time after the MPM to build out their internal scenarios using the core scenario as a baseline. CS Working Group Leads assisted organizations with tying the core scenario baseline to common organizational desired conditions via pre-identified scenario vignettes. Developing these scenario vignettes ensured that the scenarios made logical technical sense and triggered the national level discussions desired by the Exercise Planning Team. They also ensured CS Working Group members experienced similar

conditions to similar systems. Coming out of this process, each organization had a scenario framework established that could be shared with other stakeholders in their working group and be further refined into the observable injects presented to players during the exercise.

Master Scenario Events List Meeting

Overview

On December 9, 2021, CISA hosted the Master Scenario Events List (MSEL) Meeting. Approximately 290 participants and stakeholders from the government and private sector attended the meeting virtually to review and provide input to the CS VIII exercise structure and scenario development. The plenary discussions covered exercise structure, scenario development, timing, and inject development. The working group-focused breakout sessions focused on how the timing of scenario events manifest across the three days of the exercise. During subsequent plenary sessions, all exercise stakeholders discussed the timing of scenarios and cross-working group exercise play. Additional MSEL Meeting briefings provided planners with information on adversary connections, exercise resources and evaluation, public affairs guidance on CS VIII external messaging, and the VIP Program.

Outcomes

Building on the MSEL Meeting, CS Working Groups finalized organization-specific scenario narratives. Using the narratives, planners identified their player observables and developed time-sequenced exercise injects. The sum of the exercise injects for each organization became their MSEL. To be fully prepared for exercise play, planners also identified expected player actions, organizational media play, and simulation requirements for Exercise Control (ExCon). CS Working Group Leads continued to host monthly planning calls as well as individual calls with organizations to update their MSEL in preparation for the Final Planning Meeting (FPM).

Prepare Phase

During the Prepare Phase, the Exercise Planning Team finalized all aspects of the planning process for the CS VIII Working Groups and participants and ensured that all participants received the appropriate training and resources to succeed in the exercise. The Exercise Planning Team's areas of focus during this phase included helping planners to finalize injects, align projected timelines, solidify player rosters, and pre-plan for anticipated information sharing or outreach (e.g., simulated law enforcement or vendors). The team also finalized documentation, prepared for dynamic media and social media play, and developed the adversary website and profiles. Additionally, the Exercise Planning Team focused on the planning, buildout, and testing of the logistical, physical, and IT architecture and exercise environment.

Final Planning Meeting

Overview

CISA hosted the FPM, the fifth and final major planning meeting, on February 2-3, 2022, for approximately 305 stakeholders. The first day consisted of a full-day of plenary discussions focused on exercise scenario events, inject timing, cross-sector interaction, and expected player action. These discussions ensured that the scenario ground truth remained in sync across all working groups. Additional FPM briefings focused on real world and exercise-related public affairs, the VIP Program, logistics, and mechanics to prepare planners for exercise execution.

On the second day of the FPM (an optional day for attendees) the Exercise Planning Team provided training on the exercise website, including information on the registration process and the platform's components and functions. The second day also provided opportunities for voluntary working sessions with CS Working Group Leads. Working Groups reviewed injects and projected timelines and discussed scenario impacts and expected player actions. These sessions allowed planners to delve into injects and timing as they related to the broader

exercise overview from the day prior.

Outcomes

In the final planning phase, CS VIII Working Group Leads coordinated working sessions with members of the Scenario Team and organizational planners to make edits and finalize exercise injects. The Exercise Planning Team supported exercise preparation by providing information on ExCon logistics, assisting with artifact development and contingency inject review, identifying white cell support roles, and finalizing the CS VIII Player Directory. The Exercise Planning Team also provided six virtual CS VIII Controller/Evaluator (C/E) and ExCon Representative Training sessions and 13 sessions of virtual CS VIII Player Training. CS VIII C/E and ExCon Representative sessions provided guidelines for observing exercise play and described roles and responsibilities before, during, and after CS VIII. Player sessions introduced and familiarized players with the exercise and described their role and available resources during the exercise. Both sessions included training on the exercise website and question-and-answer sessions.

Conduct Phase

During the Conduct Phase, the Exercise Planning Team provided comprehensive support for all exercise aspects and to all participants. The key goals included delivering and controlling the scenario, providing participants with the resources they needed to achieve objectives, and capturing insights in AARs that drive improvement.

CS VIII Exercise Execution

Overview

CS VIII executed on March 7-11, 2022, with thousands of participants, representing entities from the public and private sectors within the U.S., as well as internationally. Exercise participants included players, C/Es, and ExCon representatives. CISA hosted approximately 60 representatives at CS VIII ExCon, hosted by the U.S. Secret Service (USSS) in Washington, D.C. Due to continuing COVID-19 travel restrictions at some organizations, some ExCon participants participated from their current work locations, coordinating with ExCon resources, such as CS VIII Working Group Leads, Adversary Team, and Simulation Support virtually. ExCon functions included exercise management; flow control; inject review, development, and release; and simulation support. ExCon representatives included participants from the public sector, private industry, CI sectors, and states. These representatives helped to manage play at their own organizations through interaction with other ExCon members and contact with their offsite C/Es.

The week-long exercise conduct structure is identified in Figure 2 below:

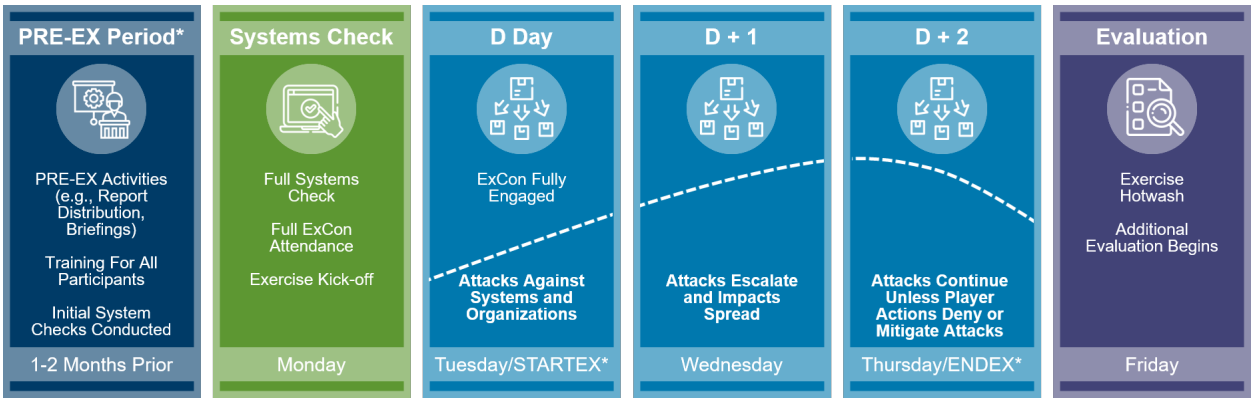

Figure 2: Exercise Execution Schedule

Outcomes

On the first day, ExCon and participants out in the field conducted systems checks, reviewed read-ahead material, and prepared for live exercise play. Live exercise play ran from 0800 Eastern Standard Time (EST) on Tuesday, March 8, until 1600 EST on Thursday, March 10. During this time, ExCon distributed and/or posted on the exercise website more than 2,650 pre-scripted injects. Players received additional ad hoc injects based on player response and exercise play. The CS VIII Exercise Website allowed registered users to access exercise documentation, the CS VIII Player Directory, and simulated social and traditional media. Players accessed adversary sites and blogs through a separate platform. The Exercise Planning Team updated all simulated sites in real time during the exercise based on dynamic play. During exercise play, ExCon also facilitated twice-daily CS VIII C/E and ExCon teleconferences to summarize scenario play, preview upcoming activity, discuss initial observations, and answer questions. On Friday, March 11, 2022, the Exercise Planning Team, ExCon representatives, and distributed C/Es and exercise stakeholders conducted an exercise hotwash. During the hotwash, the Exercise Planning Team reviewed overall exercise play, and all participants discussed exercise outcomes and initial findings. In addition, the team provided information on next steps, the after-action process, and reminded all participants to submit an After-Action Questionnaire (AAQ).

Evaluate Phase

The final phase in the CS process is the Evaluate Phase. The Exercise Planning Team implemented various mechanisms to capture player action, observations, and evaluation input. During CS VIII, planners managed scenario progress, monitored player interaction, and communicated any issues to their CS VIII Working Group Lead. Planners also participated in twice-daily teleconferences to remain in sync and informed of upcoming scenario activity. The Exercise Planning Team encouraged planners to use the CS VIII Evaluation Guide to guide internal tracking and evaluation efforts. After live exercise play concluded, CISA encouraged all participants to complete and submit an AAQ. Two versions of the AAQ existed, a CS VIII Player AAQ and a CS VIII C/E AAQ. Both AAQs included tailored questions that captured feedback on the exercise objectives, the value and effectiveness of the exercise, and lessons learned. CISA hosted several after-action events to discuss and vet potential findings and to solicit stakeholder feedback. Each CS VIII Working Group also hosted a call to discuss working group-specific findings and capture specific observations. The inputs collected during the exercise and during initial after-action events helped to inform the CS VIII Quick Look Report (QLR) that summarized the purpose, structure, and initial findings of the exercise.

After-Action Meeting

Overview

On April 6, 2022, CISA hosted a virtual After-Action Meeting (AAM) for all exercise participants. Approximately 200 virtual stakeholders attended the two-hour meeting. During the meeting, attendees reviewed the initial findings identified in the CS VIII QLR and provided input on supporting observations and recommendations for improvement. Following the AAM, the Exercise Planning Team provided participants with several opportunities to review and provide edits to the after-action documentation.

Outcomes

The AAM provided the Exercise Planning Team the opportunity to evaluate trends across the exercise community, integrate diverse perspectives, and ensure consensus. The initial findings provided a baseline for AAM participant discussion and minor refinements based on those discussions produced the final exercise findings in the AAR. The Exercise Planning Team developed two main reports, with varying levels of specificity and directed towards different audiences.

- **CS VIII Participant AAR**: Captured findings for the improvement of cybersecurity preparedness, response, and recovery. It contains an exercise overview, full findings (supported by relevant

examples/observations), lessons learned, and recommendations, as well as CS VIII Working Group Annexes. The target audience includes stakeholders, planners, and players (as applicable).

- **CS VIII Final AAR:** Highlighted productive achievements of the exercise and high-level findings. All participants vet the document prior to general release, and it does not contain the CS VIII Working Group Annexes. The Final AAR target audience is the public as the Final AAR appears on the CISA website.

Participants in each working group had the opportunity to provide insight and feedback into the overall AAR and their Working Group Annex through a controlled review process. The after-action process provided a venue to keep the momentum of a successful exercise, involving a diverse representation of the cybersecurity community, moving forward. Through this process, the Exercise Planning Team identified and socialized key findings with the trusted community. The after-action process gave the trusted exercise community an opportunity to gain a broader perspective of exercise findings and successes.

Conclusion

Over three days of live distributed exercise play, CS VIII provided stakeholders a realistic environment to stress their cyber incident response capabilities through a nation-wide, multi-sector cyberattack targeting critical infrastructure. Players examined cybersecurity plans and policies while sharing information and coordinating across the cyber response community. Public and private entities fostered relationships through exercise planning and execution which led to an improvement in their ability to share relevant and timely information. In addition, the exercise's simulated platform provided a realistic, dynamic environment to safely engage non-technical entities within participating organizations and exercise the communications aspects of their cyber incident response plans.

Building on previous CS iterations, CS VIII continued to allow for significant examination of processes and procedures throughout the cyber incident response community. The exercise enabled planners to identify strengths and weaknesses within their respective organizations while also providing the opportunity to analyze trends across the entire exercise participant set, yielding a set of findings that highlight the progress made through participating in cyber-dedicated exercises, evaluating real world events, and increasing cybersecurity preparedness activities. The findings in this report stress potential areas to improve the nation's cyber resilience and response capabilities, and CISA encourages all participating organizations to leverage these findings to improve their own preparedness posture.

ANNEX A: PARTICIPANT LIST

CISA Working Group Participants
CISA Divisions
Cybersecurity Division
Emergency Communications Division
Infrastructure Security Division
Integrated Operations Division
National Risk Management Center
Stakeholder Engagement Division
CISA Mission Enabling Offices
Office of the Chief Counsel
Office of the Chief External Affairs Officer
Office of Strategy, Policy, and Plans

Critical Infrastructure Working Group Participants[1]
Industry Entities
ABB Ltd.
Air Liquide USA LLC
Ameren
American Express*
American International Group, Inc. (AIG)
American Water
Arlington County Water Pollution Control Bureau
Axon Global
Bank of America*
Becton, Dickinson, and Company
BMO Harris Bank*
Brenntag North America, Inc.
California Water Service (Cal Water)
Celanese
Centene Corporation
Charter Communications Inc.
Checkpoint
Cisco Systems
Citibank*
The Coca-Cola Company
CommunityHealth, Inc.
Consolidated Edison, Inc.

[1] Numerous organizations, not represented here, participated in the exercise planning process but were unable to participate in the actual exercise due to operational challenges and a lack of resources.

Critical Infrastructure - Industry Entities (continued)
Dow Inc.
Eastman Chemical Company
Eli Lilly and Company
Fannie Mae*
Federal Retirement Thrift Investment Corporation (FRTIC)
Ford Motor Company
Gallade Chemical
General Motors (GM)
GrammaTech, Inc.
Hawkins, Inc.
HCA Healthcare
Hyundai USA
Ingevity
Independent Community Bankers of America (ICBA)*
Kroger
Lennox International Inc.
Lumen Technologies, Inc.
Mastercard
McKesson Corporation
Merck & Co., Inc.
Metropolitan Transportation Authority (MTA)
Morgan Stanley*
MSA Worldwide, LLC
Navistar, Inc.
Navy Federal Credit Union (NFCU)
Nuance
Organon & Co.
OU Health
PNC Bank*
San Antonio Water System
SEI Investments Company
Shell
Siemens
Stryker Corporation
The York Water Co.
Truckee Meadows Water Authority (TMWA)
University of Kansas Health System and the University of Kansas Medical Center
Upwork
Verisign
Washington Metropolitan Area Transit Authority (WMATA)

Critical Infrastructure - Industry Entities (continued)
Wells Fargo*
Zoox
**Part of the Financial Services Sector Coordinating Council (FSSCC) Monitor/Respond Group*
Coordination Bodies
American Chemistry Council (ACC)
Arizona Cyber Threat Response Alliance (ACTRA)
Automotive Information Sharing and Analysis Center (Auto-ISAC)
Communications Information Sharing and Analysis Center (Communications ISAC)
Electricity Information Sharing and Analysis Center (E-ISAC)
Financial Services Information Sharing and Analysis Center (FS-ISAC)
Health Information Sharing and Analysis Center (H-ISAC)
International Association of Certified ISAOs (IACI)
Information Technology Information Sharing and Analysis Center (IT-ISAC)
National Council of ISACs (NCI)
Oil and Natural Gas Information Sharing and Analysis Center (ONG-ISAC)
Retail and Hospitality Information Sharing and Analysis Center (RH-ISAC)
Water Information Sharing and Analysis Center (WaterISAC)
Sector Risk Management Agencies
Cybersecurity and Infrastructure Security Agency/Stakeholder Engagement Division (CISA/SED)
Environmental Protection Agency (EPA)
Department of Health and Human Services (HHS)
Department of Treasury

Federal Working Group Participants
U.S. Government Departments and Agencies
Centers for Disease Control and Prevention (CDC)
Department of Agriculture (USDA)
Department of Commerce
Department of Commerce Bureau of Industry and Security (BIS)
Department of Energy (DOE)
Department of Health and Human Services (HHS)
Department of Homeland Security Enterprise Operations Division
Department of State (DOS)
U.S. Department of Treasury
Department of Veterans Affairs (VA)
Environmental Protection Agency (EPA)
Federal Aviation Administration (FAA)
Federal Housing Finance Agency (FHFA)
General Services Administration (GSA)
National Telecommunications and Information Administration (NTIA)
Securities and Exchange Commission (SEC)

Transportation Security Administration (TSA)
**Note: Several federal departments and agencies participated in the Law Enforcement/Intelligence/Department of Defense (LE/I/DoD) Working Group and are listed in that Working Group's Participant List*

International Working Group Participants
Government Entities
Australia • Australian Cyber Security Centre (ACSC)
Canada • Canadian Centre for Cybersecurity (CCCS) • Public Safety Canada (PCS)
Finland • Transport and Communications Agency (TRAFICOM/NCSC-FI)
France • National Information Systems Security Agency (ANSSI)
Germany • Federal Office for Information Security/Computer Emergency Response Team (BSI/CERT-Bund)
Hungary • National Cyber Security Centre (NCSC-HU)
Japan • Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) • National Center of Incident Readiness and Strategy for Cybersecurity (NISC)
New Zealand • Computer Emergency Response Team (CERT-NZ)
Sweden • Civil Contingencies Agency/Department of Cybersecurity and Secure Communication (MSB/CERT-SE)
Switzerland • National Cyber Security Centre/Reporting and Analysis Centre for Information Assurance (NCSC/MELANI)
Singapore • Cyber Security Agency (CSA)
United Kingdom • National Cyber Security Centre (NCSC-UK)
United States • Cybersecurity and Infrastructure Security Agency

LE/I/DoD Working Group Participants
Government Entities
Department of Homeland Security (DHS) • U.S. Coast Guard (USCG) • Customs and Border Protection (CBP) • Immigration and Customs Enforcement (ICE)/Homeland Security Investigations (HSI) • U.S. Secret Service (USSS)
Department of Defense (DoD) • U.S. Cyber Command (USCC) • Defense Information Systems Agency (DISA) • Department of Defense Cyber Crime Center (DC3) • National Security Agency (NSA) • U.S. Northern Command
Department of Justice (DOJ) • Federal Bureau of Investigation Cyber Division (CyD) • National Cyber Investigative Joint Task Force (NCIJTF)
ODNI • Cyber Threat Intelligence Integration Center (CTIIC) • Intelligence Community Security Coordination Center (IC SCC) • National Intelligence Manager-Maritime (NIM-Maritime)
Coordinating Bodies
Cyber Response Group (CRG)
Cyber Unified Coordination Group (Cyber-UCG)

States Working Group Participants
States and Government Entities
California • California Cyber Security Integration Center (Cal-CSIC) • California Department of Rehabilitation (DOR) • California Department of Technology (CDT) • California Governor's Office of Emergency Services (Cal OES) • California Military Department (CMD)
Iowa • Iowa Attorney General • Iowa Department of Homeland Security and Emergency Management (HSEMD) • Iowa Department of Public Safety (DPS) • Iowa Department of Revenue • Iowa Department of Transportation (DOT) • Iowa National Guard • Iowa Office of the Chief Information Officer (OCIO) • Iowa Secretary of State • Worth County, Iowa

States and Government Entities (continued)
Kentucky • Commonwealth Office of Technology (COT) • Kentucky Energy and Environment Cabinet (EEC) • Kentucky Office of Homeland Security (KOHS)
Minnesota • Minnesota Department of Public Safety (DPS) • Minnesota Department of Transportation (MnDOT) • Minnesota Fusion Center • Minnesota Information Technology Services (MNIT) • Minnesota National Guard
Missouri • Kansas City Regional Fusion Center • Missouri Department of Public Safety (DPS) • Missouri Information Analysis Center (MIAC) • Missouri National Guard • Missouri Office of Administration (OA) • Missouri Office of Homeland Security • Missouri State Emergency Management Agency (SEMA) • Missouri State Highway Patrol (MSHP) • Missouri Statewide Wireless Interoperability Network (MOSWIN) • St. Louis Fusion Center • USSS St. Louis Office
Texas • Texas Department of Information Resources (DIR) • Texas Department of Public Safety (DPS) • Texas Division of Emergency Management (TDEM) • Texas Military Department (TMD) • Texas Office of the Chief Information Officer
Virginia • Virginia Commission for the Arts (VCA) • Virginia Department of Corrections (VADOC) • Virginia Department of Health (VDH) • Virginia Department of Juvenile Justice (DJJ) • Virginia Department of Veterans Services (DVS) • Virginia Information Technology Agency (VITA) • Virginia Office of the State Inspector General (OSIG) • Virginia State Police (VSP)
Coordinating Bodies
Multi-State Information Sharing and Analysis Center (MS-ISAC)