Cyber Storm 2020

After-Action Report

AUGUST 2020

Cybersecurity and Infrastructure Security Agency

TLP:WHITE

Table of Contents

Executive Summary 3
Exercise Overview....................................7
Exercise Findings 13
Exercise Design Summary 19
Conclusion....................................25
Annex A: Participant List 26

DISCLAIMER: This report is provided "as is" for informational purposes only. The Cybersecurity and Infrastructure Security Agency (CISA) does not provide any warranties of any kind regarding any information within. DHS does not endorse any commercial product or service referenced in this advisory or otherwise. This document is distributed as TLP: WHITE. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://www.us-cert.gov/tlp.

EXECUTIVE SUMMARY

Exercise Background

On August 10-14, 2020, the Cybersecurity and Infrastructure Security Agency (CISA) conducted Cyber Storm 2020 (CS 2020), the seventh 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. Cyber Storm exercises are part of CISA's ongoing efforts to assess and strengthen cyber preparedness and examine incident response processes. 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). CISA sponsors the 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.

Exercise Goal & Objectives

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

Exercise Objectives:

- Examine the implementation and effectiveness of national cybersecurity plans and policies;
- Strengthen and enhance information sharing and coordination mechanisms used across the cyber ecosystem during a cyber incident;
- Reinforce public and private partnerships and improve their ability to share relevant and timely information;
- Exercise communication aspects of cyber incident response to refine and mature communications strategies.

Key Achievements

CS 2020 built upon preceding iterations to provide a venue for learning and advancement. Through the exercise planning and execution process, CS 2020:

- Exercised federal, state, private sector, and international response to a significant cyber incident targeting underlying core services of the Internet, including the Domain Name System (DNS), Certificate Authorities (CA), and the Border Gateway Protocol (BGP).

- Provided an opportunity to examine internal organizational procedures, identify improvements, and consider how they inform sector, national, and international response. Organizations also gained an opportunity to identify improvements to distributed communication and coordination processes – increasingly in place due to pandemic restrictions.
- Expanded the CS participant set to include new stakeholders across the Federal Government, state governments, and private sector, including significant participation across the Financial Services Sector.
- Supported classified planning and execution efforts in tandem with the classified exercise ICE STORM 2020, facilitating interaction at an unclassified level between the intelligence community and stakeholders impacted by simulated cyber incidents.
- Examined the process necessary to convene a Cyber Unified Coordination Group (UCG).
- Enabled federal interagency discussion of relevant policy issues during a meeting of the Cyber Response Group (CRG).
- Identified opportunities to improve the flow of information between private sector and governmental organizations in order to ensure situational awareness.
- Tested the capacity of participating state and local governments to respond to cyber incidents and coordinate via the Multi-State Information Sharing and Analysis Center (MS-ISAC).
- Planned for and exercised incident response across components of the following critical infrastructure sectors: Chemical, Commercial Facilities, Communications, Critical Manufacturing, Energy, Financial Services, Healthcare and Public Health, Information Technology (IT), and Transportation Systems.
- Examined processes for incident response coordination and shared situational awareness among partners of the International Watch and Warning Network (IWWN).

Scenario & Adversary

CS 2020’s core scenario focused on three back-bone services of the Internet – DNS, CA, and BGP. These services are critical to Internet architecture, allowing users to access web pages and ensuring that only the correct users are permitted access. In spite of their importance, motivated adversaries have found many ways to cause disruption – or even eavesdrop through a man-in-the-middle (MITM) attack on network-routed traffic.

The exercise ground truth assumed that two nation state-level adversaries would work with affiliates to share tools that leveraged vulnerabilities of DNS, CA, and BGP to attack targets. Criminal “Hacktivist,” “Script Kiddie,” and “UnderNet” collectives would then use these tools to launch attacks on government and private sector organizations across the United States and abroad with the intent of compromising the confidentiality, integrity, and availability of their systems and data. Using ransomware, co-opted data would allow adversaries to ransom information, “name and shame” on the Internet, or simply debilitate an organization’s operative capacity for ideological reasons. Organizations participating in CS 2020 selected from eight Scenario Vignettes, each examining a different course of intrusion and impact, to structure their own individualized scenarios. Organizations customized the chosen vignette(s) to suit their environments and address targeted vulnerabilities; then these scenarios were tied together through dynamic exercise play between organizations.

Given the foundational importance and vulnerability of the targeted services, there was no perfect solution to the attacks, leaving the overall resolution of the scenario open-ended. However, there were mitigation strategies that organizations could use to protect themselves and harden their posture. With effective threat intelligence and information sharing, security analysts could identify initial issues, allowing organizations to begin the analysis and discovery process to locate malicious certificates and ransomware code within the boundaries of their networks, begin remediation, and harden their networks against further attacks.

Key Findings

Finding 1: CS 2020 raised awareness of long-standing and ongoing vulnerabilities in the core infrastructure of the Internet

CS 2020 raised awareness of long-standing and ongoing vulnerabilities in the core infrastructure of the Internet—specifically DNS, CA, and BGP. The spectrum of simulated attacks included data breaches, traffic interception, website impersonation, augmented phishing campaigns, and significant malware and ransomware infections. This emphasized both the vulnerability of these services and their importance to network infrastructure and business operations. Furthermore, players experienced the difficulty of identifying and addressing an attack, highlighting the value of a flexible approach to incident coordination and response and the importance of collaboration with partners like third-party vendors.

Finding 2: The exercise stress-tested components of the NCIRP and provided opportunities to practice and refine supporting activities

The exercise stress-tested components of the NCIRP and provided opportunities to practice and refine supporting activities such as incident scoring and escalation to and engagement of coordination groups. Players identified potential improvements to incident scoring across multiple sectors, refined tactical coordination processes, and identified opportunities to share outputs and information with stakeholders.

Finding 3: In increasingly distributed working environments, some organizations found distributed response could delay coordination and extend response timelines

Public and private sector organizations as well as international partners have moved toward increasingly distributed working environments – a process accelerated by the COVID-19 pandemic. Exercise play in CS 2020 afforded organizations the opportunity to apply their pre-COVID processes in a distributed environment. Some organizations found that a distributed response created new or unexpected challenges, while others did not. For those organizations that did experience challenges, distributed response could delay or limit coordination and communication efforts, challenge the ability to create shared awareness, or extend typical response timelines.

Finding 4: Broad information sharing is critical to recognizing a coordinated campaign and CISA has an opportunity to play a proactive facilitating role

The ability to recognize that multiple incidents are part of a coordinated campaign relies on active and broad information sharing. Information sharing takes place between federal cyber centers, relevant Sector-Specific Agencies (SSA), national computer emergency response teams, Information Sharing and Analysis Centers/ Organizations (ISACs/ISAOs), law enforcement, and sector peers. During a cyber incident, private and public sector organizations rely on CISA not only to lead asset response, but to facilitate information sharing to help identify and communicate risk and share mitigation recommendations. Because of this responsibility, CISA has an opportunity to play a proactive role, requesting information, facilitating information sharing, and advising on incident response, and should consider making additional resources available to facilitate this. However, CISA's ability to be proactive and connect issues depends on active reporting and information sharing by partner organizations.

Finding 5: Successful incident response requires planned, whole-of-organization coordination

Play emphasized that successful response to cyber incidents requires more than technical response expertise. These incidents have sprawling impacts to organizations' operations, brand reputation, customer and business relationships, and bottom line. Cyberattacks that impact essential business services or have public exposure require a whole-of-organization response that should be planned for in advance.

Conclusion

Over three days of live distributed exercise play, CS 2020 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.

However, the measure of a successful exercise is not only the validation it achieves, but the areas of improvement identified to strengthen the processes and policies in place. CS 2020 planning and execution allowed individual organizations to capture internal lessons learned and identify new findings to facilitate situational awareness and coordination across the incident response community. CS 2020's findings serve to enable the development of critical processes and procedures to improve the Nation's cyber resilience and response capabilities.

EXERCISE OVERVIEW

After-Action Report Purpose

The Cyber Storm 2020 (CS 2020) 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 CISA and stakeholder improvement activities.

Introduction

On August 10-14, 2020, CISA conducted CS 2020, the seventh 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. Cyber Storm exercises are part of CISA's ongoing efforts to assess and strengthen cyber preparedness and examine incident response processes. 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). CISA sponsors the 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.

CISA intended to conduct CS 2020 in early May 2020, in conjunction with the Federal Emergency Management Agency (FEMA) National Level Exercise 2020 (NLE 2020) and ICE STORM 2020, a classified companion exercise. Due to operational and planning concerns related to the COVID-19 pandemic, FEMA cancelled NLE 2020 execution events and CISA rescheduled CS 2020 for August 2020. CISA successfully executed CS 2020 from its exercise control (ExCon) cell, limited due to the COVID-19 restrictions, with a distributed planner and player set across the globe. On August 10, exercise participants conducted communications checks and final preparations. Live exercise play spanned from 0900 EDT on August 11 to 1700 EDT on August 13. On August 14, planners, players, and stakeholders participated in an Exercise Hotwash.

As an operations-based functional exercise, CS 2020 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 Goal & Objectives

Goal: **Strengthen cybersecurity preparedness and response capabilities by exercising policies, processes, and procedures for identifying and responding to a multi-sector cyberattack targeting critical infrastructure.**

Exercise Objectives:

- Examine the implementation and effectiveness of national cybersecurity plans and policies;
- Strengthen and enhance information sharing and coordination mechanisms used across the cyber ecosystem during a cyber incident;
- Reinforce public and private partnerships and improve their ability to share relevant and timely information;
- Exercise communication aspects of cyber incident response to refine and mature communications strategies.

Exercise Participation

Figure 1: CS 2020 Participating Sectors

CS 2020 had diverse participation across the public and private sector. CS 2020 exercise execution included more than two thousand globally distributed players and observers representing approximately 210 organizations – partner organizations across federal and state, local, tribal, and territorial (SLTT) governments; the International Watch & Warning Network (IWWN); and critical infrastructure sectors. Within these communities, CS 2020 players ranged from operational shop floor and front-line customer care staff, to security and technical responders, incident response teams, legal and public affairs specialists, and senior leaders.

For exercise planning and coordination, the stakeholder set consisted of seven communities: Federal, States, International, Law Enforcement/Intelligence/Department of Defense, and Critical Infrastructure, grouped into three communities for planning purposes. These communities were led by an Exercise Planning Team member who ensured coordination and collaboration within the exercise community throughout the planning process.

More than 30 federal departments and agencies participated in the exercise, including organizations responsible for threat response, asset response, intelligence support, private sector coordination, and public services. Some agencies participated directly in scenario impacts, while others performed their roles as SSAs, coordinating with their sector constituencies.

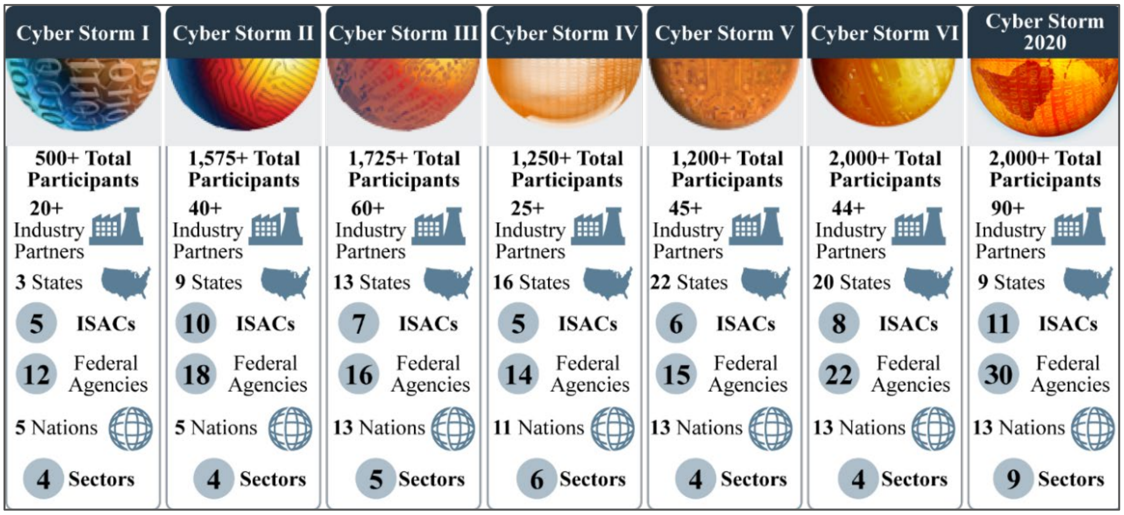
The Federal Government was joined by nine participating states, comprising SLTT administrative, public-service, and law enforcement agencies. Arizona, Iowa, Kansas, Missouri, and Utah participated as playing organizations, while Delaware, Florida, Indiana, and New Hampshire participated in a Monitor/Respond role.

More than 90 private sector partners participated in the exercise, representing nine CI sectors, divided into three CI communities for planning purposes.

The Critical Infrastructure I (CI I) Community comprised the Financial Services Sector and had robust participation in the planning and execution of CS 2020. Sixty-five financial institutions and sector-related organizations participated fully as players in the exercise or supported the exercise in a Monitor/Respond capacity. The Critical Infrastructure II (CI II) Community consisted of 22 organizations representing Healthcare and Public Health, Information Technology (IT), and Critical Manufacturing Sectors. The Critical Infrastructure III (CI III) Community comprised 20 different organizations from the public and private sectors within the Transportation Systems Sector, the Financial Services Sector, and Commercial Facilities (Retail Subsector).

Twelve partner nations from the IWWN joined the United States in exercising their information sharing and incident response coordination, all but three of which participated as full player organizations during exercise execution. Australia, Canada, France, Germany, Japan, New Zealand, Singapore, Sweden, and Switzerland played in the exercise as full participants. Hungary, the Netherlands, and the United Kingdom participated in a Monitor/Respond capacity and provided daily reports of their exercise observations and feedback.

The CS exercise series has always emphasized the importance of intra-governmental and cross-sector coordination; however, CS 2020 represented a significant expansion of private sector engagement. The COVID-19 pandemic created operational and planning complications for some, impacting levels of participation and active play. Despite this challenge, participation remained high. Figure 2 shows CS participation over the series history.



Cyber Storm I	Cyber Storm II	Cyber Storm III	Cyber Storm IV	Cyber Storm V	Cyber Storm VI	Cyber Storm 2020
500+ Total Participants	1,575+ Total Participants	1,725+ Total Participants	1,250+ Total Participants	1,200+ Total Participants	2,000+ Total Participants	2,000+ Total Participants
20+ Industry Partners	40+ Industry Partners	60+ Industry Partners	25+ Industry Partners	45+ Industry Partners	44+ Industry Partners	90+ Industry Partners
3 States	9 States	13 States	16 States	22 States	20 States	9 States
5 ISACs	10 ISACs	7 ISACs	5 ISACs	6 ISACs	8 ISACs	11 ISACs
12 Federal Agencies	18 Federal Agencies	16 Federal Agencies	14 Federal Agencies	15 Federal Agencies	22 Federal Agencies	30 Federal Agencies
5 Nations	5 Nations	13 Nations	11 Nations	13 Nations	13 Nations	13 Nations
4 Sectors	4 Sectors	5 Sectors	6 Sectors	4 Sectors	4 Sectors	9 Sectors

Figure 2: Growth in Participation Since the First CS

Key Achievements

CS 2020 built upon preceding iterations to provide a venue for learning and advancement. Through the exercise planning and execution process, CS 2020:

- Exercised federal, state, private sector, and international response to a significant cyber incident targeting underlying core services of the Internet, including the DNS, CA, and BGP.
- Provided an opportunity to examine internal organizational procedures, identify improvements, and consider how they inform sector and national-level response. Organizations also gained an opportunity to test and identify improvements to distributed communication and coordination processes – increasingly in place due to pandemic restrictions and policies.
- Expanded the CS participant set to include new stakeholders across the Federal Government, state governments, and private sector, including significant participation across the Financial Services Sector.
- Supported classified planning and execution efforts in tandem with the classified exercise ICE STORM 2020, facilitating interaction at an unclassified level between the intelligence community and stakeholders impacted by simulated cyber incidents.
- Examined the process necessary to convene a Cyber UCG.
- Enabled federal interagency discussion of relevant policy issues during a meeting of the CRG.
- Identified opportunities to improve the flow of information between private sector and governmental organizations in order to assure situational awareness.
- Tested the capacity of participating state and local governments to respond to cyber incidents and coordinate via the Multi-State Information Sharing and Analysis Center (MS-ISAC).
- Planned for and exercised incident response across components of the following CI sectors: Chemical, Commercial Facilities, Communications, Critical Manufacturing, Energy, Financial Services, Healthcare and Public Health, IT, and Transportation Systems.
- Examined processes for incident response coordination and shared situational awareness among partners of the International Watch and Warning Network (IWWN).

Scenario & Adversaries

CS 2020's core scenario focused on three back-bone services of the Internet – DNS, CA, and BGP. These services are critical to Internet architecture, allowing users to access web pages and ensuring that only the correct users are permitted access. Despite their importance, motivated adversaries have found many ways to cause disruption – or even eavesdrop through a MITM attack – on network-routed traffic.

The exercise ground truth assumed that two overseas nation state-level adversaries would work with affiliates to share tools that leveraged vulnerabilities of DNS, CA, and BGP to attack targets. Criminal "Hacktivist," "Script Kiddie," and "UnderNet" collectives would then use these tools to launch attacks on government and private sector organizations across the United States and abroad with the intent of compromising the confidentiality, integrity, and availability of systems and data. Using ransomware, co-opted data would allow adversaries to ransom information, "name and shame" on the Internet, or simply debilitate an organization's operative capacity for ideological reasons.

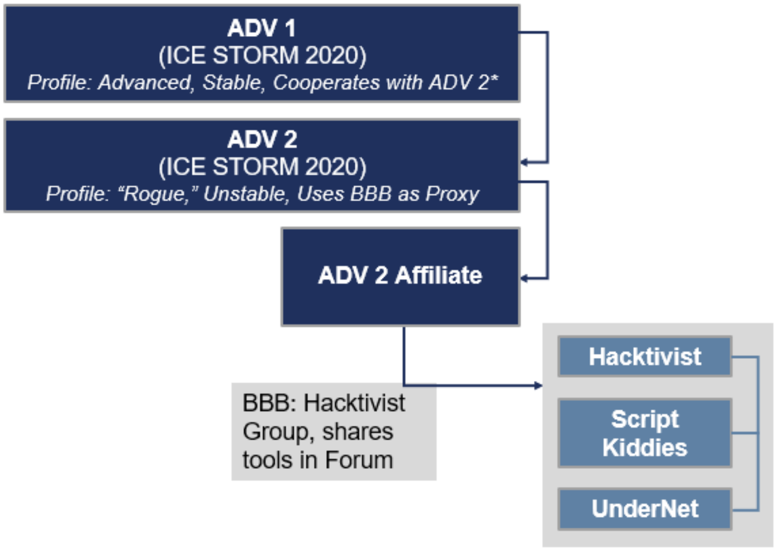

ADV 1
(ICE STORM 2020)
Profile: Advanced, Stable, Cooperates with ADV 2*
ADV 2
(ICE STORM 2020)
Profile: "Rogue," Unstable, Uses BBB as Proxy
ADV 2 Affiliate
BBB: Hacktivist Group, shares tools in Forum
Hacktivist
Script Kiddies
UnderNet

Figure 3: CS 2020 Adversary Construct

Organizations participating in CS 2020 selected from eight Scenario Vignettes, each examining a different course of intrusion and impact, to structure their own individualized scenarios. Organizations customized the chosen vignette(s) to suit their environments and address targeted vulnerabilities; then these scenarios were tied together through dynamic exercise play between organizations. Within participating organizations, response required collaboration across multiple functional teams within organizations as they connected initial indicators to a cyber source; considered and developed response strategies; and communicated with customers, stakeholders, and the public. Across participating organizations, players shared information with government and law enforcement; coordinated across industries, states, and countries; engaged with vendors; and used information provided in alerts and updates to inform response strategies.

Vignette #	Overview of Scenario Vignette
Vignette 1	An adversary sets up a "decoy" code repository site where company programmers download specialized code snippets which are "time-bombed."
Vignette 2	An organization is the victim of a massive phishing campaign. Embedded in the phishing email is a bogus certificate that automatically downloads upon clicking the link. The adversary is then able to conduct a MITM attack, data breach, or ransomware attack.

Vignette #	Overview of Scenario Vignette
Vignette 3	An adversary redirects traffic from a legitimate site to a malicious site that resembles the legitimate site. Users first navigate to the fraudulent site and are asked for their credentials. After users input their credentials, they are forwarded to the legitimate site with their applied credentials. During the process, the adversary captures the credentials in a log file to create/modify transactions, and/or change password/security questions.
Vignette 4	An adversary redirects traffic from a legitimate site to a nonexistent page (e.g., 404 error) or a fraudulent page (e.g., site with a hacktivist message). This vector can be used to create a Denial of Service.
Vignette 5	An adversary leverages weakness in the DNS protocol, either internally to their organization (insider threat) or externally, to redirect or block traffic transiting. As a result, the third-party provider's services are no longer available.
Vignette 6	A company's traffic is routed through an adversary country via BGP hijacking. All border gateway routes are altered through this country causing traffic to transit non-standard routes. Potential impacts include change in cost per packet, Denial of Service, MITM, and performance issues. This attack can also be incorporated with certificate authority abuse, so traffic can be read while being hijacked.
Vignette 7	An adversary exploited a critical vulnerability on the organization's external facing web application. The attacker leverages the exploit to dump contents of the database containing Personally Identifiable Information (PII). The sensitive information is then posted on the dark web.
Vignette 8	A supply chain compromise introduced misconfigured certificates in the chain of trust. The pre-loaded compromised certificates allow the malware installation because they "trust" the update. Leveraging this access, the adversary conducts a MITM attack or Denial of Service attack.

Given the foundational importance and vulnerability of the targeted services, there was no perfect solution to the attacks, leaving the overall resolution of the scenario open-ended. However, there were mitigation strategies that organizations could use to protect themselves and harden their posture. With effective threat intelligence and information sharing, security analysts could identify initial issues, allowing organizations to begin the investigation and discovery process to locate malicious certificates and ransomware code within the boundaries of their networks, begin remediation, and harden their networks against further attacks.

EXERCISE FINDINGS

CS 2020 functions as operational training and allows for examination and stress-testing of policies, procedures, and incident response protocols – but its greatest value lies in identifying gaps and areas of improvement to facilitate close, effective coordination across the incident response community. The Exercise Planning Team analyzed participant surveys, collected stakeholder lessons learned, and reviewed observations recorded during CS 2020 execution to incorporate experiences and feedback from across the Federal, States, Critical Infrastructure, Law Enforcement/Intelligence/Department of Defense, and International communities. The following section contains five high-level exercise findings impacting the cybersecurity community, supported by observations drawn from exercise play and identifying recommendations to improve the coordinated cyber incident response process.

Finding 1: CS 2020 raised awareness of long-standing and ongoing vulnerabilities in the core infrastructure of the Internet

CS 2020 raised awareness of long-standing and ongoing vulnerabilities in the core infrastructure of the Internet—specifically DNS, CA, and BGP. The spectrum of simulated attacks included data breaches, traffic interception, website impersonation, augmented phishing campaigns, and significant malware and ransomware infections. This drove home both the vulnerability of these services and their importance to network infrastructure and business operations. Furthermore, players experienced the difficulty of identifying and addressing an attack, highlighting the value of a flexible approach to incident coordination and response and the importance of collaboration with partners like third-party vendors.

Observations

1.1 Each organization participating in CS 2020 confronted cyber incident impacts unique to their network, structure, and line of business. The diverse array of impacts organizations experienced highlights the wide-ranging threats which the inherent vulnerabilities that these core Internet services pose. In a simplified model, DNS allows a user to find a specific Internet Protocol (IP) address – a website or server. BGP allows users to reach that IP address by selecting the chain of autonomous systems to reach the relevant IP address. CA allows users to access that IP address by establishing a trust relationship between the two parties. In the CS 2020 scenario, many attacks began with a phishing campaign, and once the adversary gained access, they were able to harvest credentials, exfiltrate data, and identify further targets. The DNS attack leveraged CA credentials gained during a phishing attack to compromise the regional DNS record for a software development hub. Time-bombed code activated at the start of the exercise, allowed the adversary to gain control over internal applications, install ransomware, and harvest user credentials.

1.2 As attackers expanded their foothold across organizations, repercussions moved beyond individual organization networks, either compromising the availability of externally-facing services or systems (e.g., cloud services), or using highjacked accounts to target partners or customers. For example, phishing emails posing as trusted vendors allowed the adversary to spread malware or compromise further organizations. Exercise play demonstrated that organizations are increasingly linked and that successful incident response is dependent on interoperability and cooperation between third-party vendors and clients.

1.3 A variety of dynamic reports, new information, and requests required responders to identify core issues and filter out the scenario "noise." Participants responded to multiple attack vectors and faced uncertainty as they attempted to understand attack origins, potential impacts/spread, the vulnerability exploited, and how to contain and fix it. They disconnected specific applications or shut down department networks as necessary to isolate malware. With the malware isolated and impacts limited, organizations moved forward with resolution and recovery.

1.4 Simulated attacks highlighted the importance of two-factor authentication (2FA). 2FA allows systems to verify network access, while also supporting incident response by leaving verifiable digital fingerprints related to DNS record changes.

1.5 Many participants observed they could benefit from new or improved cyber incident playbooks to specifically handle incidents caused by increasingly pervasive threats like ransomware.

Stakeholder-Derived Recommendations:

- **Organizations should continue to develop a cyber incident response playbook to address both core and application-specific vulnerabilities.**
- **Organizations should continue to exercise their cyber incident response capabilities and processes against a variety of scenarios, broadening their ability to handle evolving threat vectors and trends in the cyber landscape.**

Finding 2: The exercise stress-tested components of the NCIRP and provided opportunities to practice and refine supporting activities

The exercise stress-tested components of the NCIRP and provided opportunities to practice and refine supporting activities such as incident scoring and escalation to and engagement of coordination groups. Players identified potential improvements to incident scoring across multiple sectors, refined tactical coordination processes, and identified opportunities to share outputs and information with stakeholders.

Observations

2.1 The CS 2020 scenario simulated a coordinated cyberattack against federal, state, private sector, and international partners. However, since the campaign included many seemingly disparate incidents across hundreds of organizations, it required external information sharing to identify the coordinated intent. Each stage of incident response – identifying an incident, reporting, analyzing, and considering remediation options – takes time. As players began to connect the pieces and identify the campaign, CISA considered options for stakeholder engagement and recommended coordination through the UCG as laid out in the NCIRP. Players convened an initial Cyber UCG Seniors meeting and identified additional partners for inclusion in the Cyber UCG. Due to exercise timelines, outreach and follow-on meetings were not conducted.

2.2 Players used the incident severity schema contained in the NCIRP and the CISA National Cyber Incident Scoring System (accessible on CISA's website) to assess and communicate incident impacts. Players observed that impacts across multiple sectors and the potential risk environment likely warranted higher aggregate severity levels than the individual incident scores. This demonstrated the importance of consistent scoring across organizations and sectors and highlighted the importance of situational awareness, fluid information sharing, and cross-sector awareness to correctly assess severity and drive commensurate response efforts against a coordinated adversary campaign.

Stakeholder-Derived Recommendations:

- **Stakeholders should strengthen their familiarity with NCIRP processes and the CISA National Cyber Incident Scoring System in order to deepen their understanding of coordinated incident response.**

Finding 3: In increasingly distributed working environments, some organizations found distributed response could delay coordination and extend response timelines

Public and private sector organizations alike have moved toward increasingly distributed working environments – a process accelerated by the COVID-19 pandemic. Exercise play in CS 2020 afforded organizations the opportunity to apply their pre-COVID processes in a distributed environment. Some organizations found that a distributed response created new or unexpected challenges, while others did not. For those organizations that did experience challenges, distributed response could delay or limit coordination and communication efforts, challenge the ability to create shared awareness, or extend typical response timelines.

Observations

3.1 Organizations largely found that they have successfully adapted to the teleworking environment, however during the exercise some found the distributed environment brought to light unforeseen or unexpected challenges. Many players identified issues around internal communication and decision-making, as in-person meetings or "war rooms" could not be stood up. Information that may have been more easily attainable in an in-person environment, took more time to gather. Several organizations identified a lack of process related to the physical constraints of hardware response, including retrieving and re-imaging compromised computers.

3.2 In contrast, organizations that pre-adapted response to a distributed environment had clear lines of communication, methods to achieve that communication, and encountered fewer of these issues. In addition, organizations that have an established global business with multiple affiliates working together for incident response already in a distributed manner found communications to be consistent with pre-COVID conditions.

Stakeholder-Derived Recommendations:

- **Organizations should ensure their incident response plans consider both the communicative and physical challenges of the distributed professional environment to ensure that business continuity and essential services are maintained in the event of a cyberattack.**

Finding 4: Broad information sharing is critical to recognizing a coordinated campaign and CISA has an opportunity to play a proactive facilitating role

The ability to recognize that multiple incidents are part of a coordinated campaign relies on active and broad information sharing. Information sharing takes place between federal cyber centers, relevant SSAs, Information Sharing and Analysis Centers/Organizations (ISACs/ISAOs), law enforcement, and sector peers. During a cyber incident, private and public sector organizations rely on CISA not only to lead asset response, but to facilitate information sharing to help identify and communicate risk and share mitigation recommendations. Because of this responsibility, CISA has an opportunity to play a proactive role, requesting information, facilitating information sharing, and advising on incident response, and should consider making additional resources available to facilitate this. However, CISA's ability to be proactive and connect issues depends on active reporting and information sharing by partner organizations.

Observations

4.1 While many of CISA's responsibilities relate to interaction with specific affected organizations, as laid out in NCIRP, CISA has a broader opportunity to identify additional at-risk entities, disseminate new information, and facilitate information sharing and operational coordination. As live exercise play occurred over three days, a much shorter time frame than a real-world incident response effort, asset and threat responders focused on information gathering and began initial stages of information sharing. To address CS 2020's stated goal to strengthen and enhance information sharing and coordination mechanisms across the cyber ecosystem during a cyber incident, it could benefit CISA to examine processes and resources for regular stakeholder engagement and outbriefs. This could provide a great understanding of the threat and potential incident impacts, leading organizations to take preventative measures.

4.2 ISACs/ISAOs use their sector-wide awareness to foster information sharing, coordinate incident reporting and response, and in some cases, set threat levels for their sectors. During the exercise, some organizations bypassed their ISACs or did not make use of their ISAC media coordination teams to proactively communicate while maintaining unity of message. During the exercise, sectors with standing information sharing channels and strong relationships to sector organizations like ISACs/ISAOs coordinated their response more quickly and effectively.

4.3 In addition to sector coordination, cross-sector awareness helps organizations identify threats, prepare for attacks, and develop solutions. While cross-sector awareness is routinely provided by the National Council of ISACs (NCI), organizations could benefit from cross-sector awareness provided earlier and with a low barrier to access. CISA intended to hold a stakeholder call, but was unable to due to exercise and real world constraints. Nevertheless, players confirmed interest in and noted the importance of CISA holding stakeholder engagement calls with private sector partners to provide insight into cross-sector impact, government and sector coordination efforts, and the latest situational awareness. These stakeholder engagement calls would also create a venue for dialogue on recommended actions, mitigations, or remediation options.

4.4 Given the number of government agencies, coordinating bodies, and industry organizations involved in the information sharing and incident response processes, some federal and private sector exercise players identified a need for clarity regarding incident coordination pathways. For some players this lack of clarity during play resulted in delays in communication and response coordination. In addition, law enforcement entities such as the FBI (lead agency for threat response), rely on timely information sharing from private sector partners, as it is pertinent for investigative response and for seeking attribution.

4.5 Several industry participants struggled to share information as they managed incidents under privilege and worked through approvals on-the-fly. This especially impacted cross-sector coordination. Some organizations worked through required approvals in pre-incident planning, including the type of information or data that could be shared, who it can be shared with, and the approvals required.

Stakeholder-Derived Recommendations:

- **CISA should examine processes and resources for regular stakeholder engagement activities and outbriefs during and after incidents using lessons learned to help shape future response efforts.**
- **Stakeholders should develop or revisit playbooks to ensure clear lines of information sharing, analysis, and response are identified among coordinating government and sector partners, particularly CISA and the FBI.**
- **CISA should leverage collaboration with cross-sector information sharing organizations to facilitate broadly accessible, uncleared incident reporting and analysis in order to foster broader cross-sector awareness.**

Finding 5: Successful incident response requires planned, whole-of-organization coordination

Play emphasized that successful response to cyber incidents requires more than technical response expertise. These incidents have sprawling impacts to organizations' operations, brand reputation, customer and business relationships, and bottom line. Cyberattacks that impact essential business services or have public exposure require a whole-of-organization response that should be planned for in advance.

Observations

5.1 Organizations that engaged public affairs, legal, and leadership teams in proactive cyber incident planning and quickly integrated them in the initial phases of simulated response could more quickly and effectively leverage their resources, perspectives, and capabilities. Organizations who stood up response teams on-the-fly and/or did not have pre-approvals or starter messaging discovered there was a lag in time to engage externally and risked information gaps or displeased stakeholders or customers.

5.2 Organizations who appointed incident managers to coordinate response gathered information and made decisions more quickly. Incident managers are able to both lead the technical operations and function as points of contact (POC) for other areas of the business.

5.3 Players observed that communications teams that proactively engaged with media and the public can be more effective in gaining public confidence in response. Public affairs playbooks, templates, and proactive engagement with incident response managers are all useful tools which allow an organization to stay ahead of the message in an incident.

Stakeholder-Derived Recommendations:

- **Organizations should ensure there is clear unity of command when responding to an incident, and the incident commander has a defined role and responsibilities.**
- **Organizations should ensure they have a mechanism to engage key business and functional expertise in cyber incident response and practice. This includes public affairs, legal, and leadership teams and their resources.**
- **Organizations should ensure public affairs teams have pre-approved messaging and action plans preparing them to address the public impacts of a cyber incident.**
- **CISA's Office of the Chief External Affairs Officer should consider offering a briefing on the role of public communications in a crisis prior to the exercise. This would help prepare participants to engage with communications teams appropriately.**
- **To drive maximum internal coordination and gain optimal benefit from the exercise, organizations should seek to engage leadership and lines of business early, in order to gain buy-in and ensure awareness of exercise commitments with the understanding that real world events may impact participation.**

EXERCISE DESIGN SUMMARY

Exercise Planning Construct

CS 2020 required extensive coordination and stakeholder engagement throughout the exercise lifecycle. Originally scoped for 18 months, planning changes due to the COVID-19 pandemic led to a three-month postponement of the exercise. The Exercise Planning Team divided the exercise timeline into five phases to support the planning, conduct, and evaluation of the CS 2020 exercise. Within each phase, a series of events, milestones, and general planning goals moved the planning process forward. The planning process included five planning meetings, each with specific objectives that built on the progress of the last event. Throughout the process, planners engaged in cross-community interaction, public–private collaboration, and information sharing to increase awareness and achieve goals for each phase.

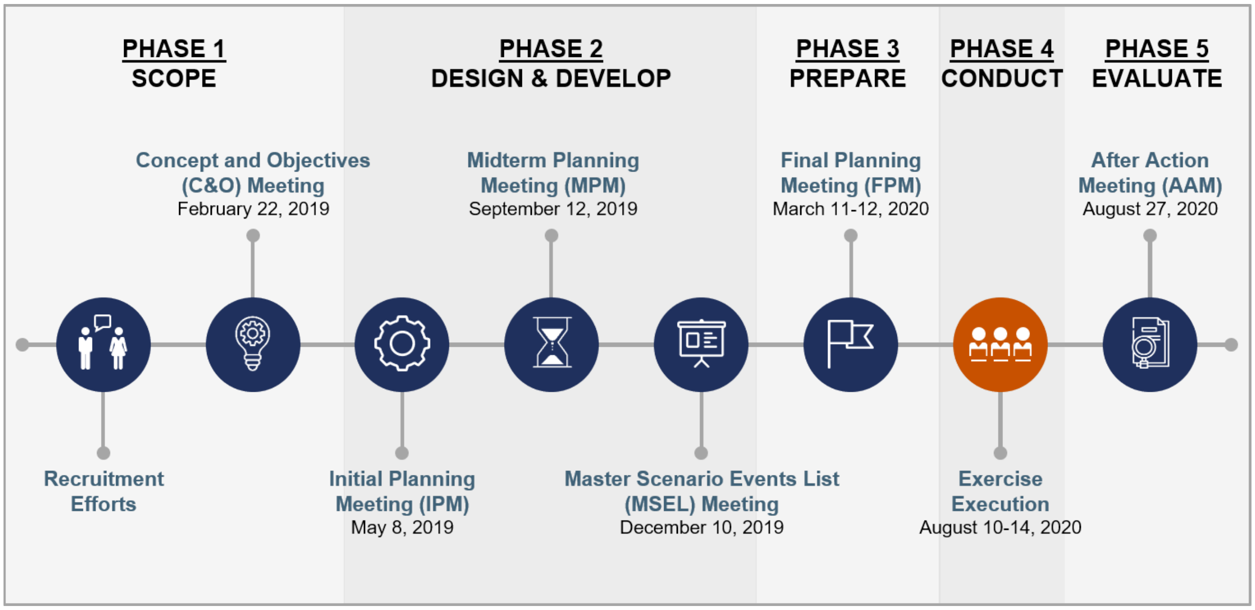


Figure 4: CS 2020 Exercise Timeline

This section describes each phase's development milestones through a comprehensive overview and explanation of the significance of each meeting and its impact in the overall exercise lifecycle.

The Exercise Planning Team leveraged the exercise execution findings and AARs from CS I-VI to maintain and implement what worked well and make improvements for CS 2020.

Scope Phase

In the initial stages of this phase, the Exercise Planning Team collaborated with CISA stakeholders on the proposed exercise concept, to include identifying the scope, goal and objectives, timeline, and potential sectors. Efforts focused on establishing the conceptual framework to set the stage for initial discussions with potential stakeholders.

February 22, 2019: Concept and Objectives Meeting

Overview

On February 22, 2019, CISA hosted the Concept and Objectives (C&O) Meeting to discuss the proposed CS 2020 scope and solicit input. At the meeting, approximately 60 stakeholders and participants discussed the goal and objectives, planning and execution timeline, recruitment targets, scenario options, and exercise structure and design principles. In addition, planners discussed alignment to FEMA's NLE 2020. CS 2020 would be one of several component exercises, including ICE STORM 2020. As originally scoped, NLE 2020 was slated to take place as a series of modules occurring from February through May 2020.

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 2020 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 on boarded, the Exercise Planning Team assigned participants to a more manageable and focused CS Community, each with a dedicated Exercise Planning Team Lead. The CS Communities created forums to discuss common issues and identify scenario impacts that would challenge their players. The CS 2020 Communities included Federal, States, International, Law Enforcement/Intelligence/Department of Defense, and three critical infrastructure sector communities: CI I (Financial Services, Communications, and Energy), CI II (Chemical, which dropped out during the planning phase due to COVID-19 impacts; Critical Manufacturing; Healthcare and Public Health; and IT), and CI III (Commercial Facilities [Retail] and Transportation [Automotive and Mass Transit]).

Design & 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 Community calls, received virtual training on CS 2020, and led all organization-specific aspects of exercise planning.

May 8, 2019: Initial Planning Meeting

Overview

CISA hosted the Initial Planning Meeting (IPM) on May 8, 2019, for nearly 130 stakeholders. The full-day meeting consisted of a series of plenary and breakout sessions designed to provide information on exercise construct and solicit input on design specifics. 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 Communities used breakout sessions to scope the participant set, plans and policies, potential attack vectors, and scenario boundaries.

Outcomes

Following the IPM, CS 2020 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 Community also stood up immediately following the IPM. CS Communities held monthly teleconferences throughout the planning process to provide updates and advance community and scenario development. In many cases, CS Community Leads also held one-on-one calls with organizations to conduct more focused working sessions on each organization’s exercise play.

September 12, 2019: Midterm Planning Meeting

Overview

On September 12, 2019, CISA hosted the Midterm Planning Meeting (MPM). Approximately 160 stakeholders attended the full-day meeting. MPM sessions provided information on planning progress and milestones, described the core scenario baseline, initiated community scenario planning, and solicited input on exercise design specifics, including NLE 2020 components. The core scenario baseline would become the unifying backstory of the local impacts on each CS Community. 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 2020 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 Community 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 Community 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 community and be further refined into the observable injects presented to players during the exercise.

December 10, 2019: Master Scenario Events List Meeting

Overview

CISA hosted the Master Scenario Events List (MSEL) Meeting on December 10, 2019. At the meeting, the Exercise Planning Team led approximately 160 attendees through a full-day of both plenary discussions and CS Community-focused breakout sessions. The plenary discussions covered exercise structure, scenario development, timing, and inject development. The community-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-community exercise play. Additional MSEL Meeting briefings provided planners with information on adversary connections, exercise resources and evaluation, public affairs guidance on CS 2020 external messaging, and the VIP Program.

Outcomes

Building on the MSEL Meeting, CS Communities 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 ExCon. CS Community 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

March 11-12, 2020: Final Planning Meeting

Overview

CISA hosted the FPM, the fifth and final major planning meeting, on March 11-12, 2020, for approximately 210 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 communities. 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 Community Leads. Communities 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 Community Leads coordinated working sessions with members of the Scenario Team and organizational planners to make edits to exercise injects. However, soon after the FPM conduct, exercise planning for some organizations stopped as priorities shifted to COVID-19 response efforts. During this time, several exercises aligned to NLE 2020 cancelled and on March 19, 2020, FEMA NLE 2020 cancelled the remainder of NLE activities. During this time, CISA postponed CS 2020's execution to determine the best and safest course of action for the exercise. The planning process resumed with two virtual re-engagement sessions, held on June 25 and June 29, 2020. Both meetings covered the same content and focused on the changes to final planning, training, and exercise conduct based on the new environment. During the meetings, the Exercise Planning Team provided planners guidance on the way forward, adjustments to exercise conduct, and fielded questions. After the meetings, the Exercise Planning Team worked with planners to re-engage in the planning process and make edits to and ultimately finalize exercise injects. The Exercise Planning Team supported exercise preparation by providing information on the virtual ExCon cell that would be stood up in lieu of the traditional ExCon. In addition, the Exercise Planning Team assisted with artifact development and contingency inject review, identifying white cell support roles, and finalizing the Player Directory. The Exercise Planning Team also provided eight virtual "Planner Training" sessions and 14 sessions of virtual "Player Training." Planner sessions provided guidelines for observing exercise play (as most planners were also functioning in the role of Controller/Evaluator due to the circumstances) and described roles and responsibilities before, during, and after CS 2020. 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

Overview

CS 2020 executed on August 10 to 14, 2020, with thousands of participants, representing entities from the public and private sectors within the United States, as well as internationally. Due to the rescheduling of the exercise and safety concerns, the CS 2020 ExCon host facility changed from the United States Secret Service Headquarters in Washington, DC, to the Booz Allen Hamilton Headquarters in McLean, Virginia. In addition, the CS 2020 VIP Program was cancelled. Due to safety restrictions, in-person ExCon participation was limited to approximately 10 individuals. The remainder of the exercise support staff participated from their current work locations, coordinating with ExCon resources such as Community Leads, Adversary Team, and Simulation Support virtually. ExCon functions included exercise management; flow control; inject review, development, and release; and simulation support. Exercise planners helped to manage play at their own organizations through interaction with the Exercise Planning Team and other planners.

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 0900 EDT on Tuesday, August 11, until 1700 EDT on Thursday, August 13. During this time, ExCon distributed more than 800 pre-scripted injects via email and phone calls. Players received additional ad hoc injects based on player response and exercise play. The Exercise Website allowed registered users to access exercise documentation, the 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 “ExCon and Planner Teleconferences” to summarize scenario play, preview upcoming activity, discuss initial observations, and answer questions. On Friday, August 14, 2020, the Exercise Planning Team, planners, and exercise stakeholders conducted a virtual 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 Survey.

Evaluate Phase

The Exercise Planning Team implemented various mechanisms to capture player action, observations, and evaluation input. During CS 2020, planners managed scenario progress monitored player interaction, and communicated any issues to their Community 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 an “Evaluation Guide,” available on the Exercise Website, to guide internal tracking and evaluation efforts. After live exercise play concluded, CISA encouraged all participants to complete and submit an After-Action Survey. There was a player-specific After-Action Survey, distributed as a “pop-up” on the exercise website and a planner-specific After-Action Survey with tailored questions. The After-Action Surveys captured feedback on key takeaways, external interaction, the effectiveness of exercise alerts, and strengths and areas for improvement from exercise play. The surveys also captured input on the CS 2020 planning and execution process.

CISA hosted an After-Action Meeting (AAM) to discuss and vet potential findings and to solicit feedback from the participant community.

August 27, 2020: After-Action Meeting

Overview

On August 27, 2020, CISA hosted an AAM for all exercise participants via WebEx. During the meeting, attendees reviewed the initial findings identified in the CS 2020 Quick Look Report and provided input on high-level findings and recommendations for improvement. Participants agreed upon the high-level findings and identified supporting observations. Participants also discussed options to address the findings. 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 this AAR.

The Exercise Planning Team developed two main reports, with varying levels of specificity and directed towards different audiences.

- **Community AAR Annex:** Captured findings for the improvement of cybersecurity preparedness, response, and recovery. It contains an exercise overview; exercise findings, supported by examples/observations; and CS Community and supplementary annexes. The Community AAR target audience are stakeholders, planners, and players (as applicable).
- **Final AAR:** Highlighted productive achievements of the exercise and high-level findings. Full participants vet the document prior to general release, and it does not contain CS Community and supplementary Annexes. The Final AAR target audience is the public as the Final AAR appears on the CISA website.

Participants in each community had the opportunity to provide insight and feedback into the overall AAR and their Community 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 2020 provided stakeholders 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.

However, the measure of a successful exercise is not only the validation it achieves, but the areas of improvement identified to strengthen the processes and policies in place. CS 2020 planning and execution allowed individual organizations to capture internal lessons learned and identify new findings to facilitate situational awareness and coordinate across the incident response community. CS 2020's findings serve to enable the development of critical processes and procedures to improve the Nation's cyber resilience and response capabilities.

ANNEX A: PARTICIPANT LIST

**Indicates an organization that was unable to participate in Cyber Storm 2020 (CS 2020) execution due to planning constraints (e.g., exercise execution date changes, resource limitations).*

Critical Infrastructure I Community Organizations
Industry Entities
ACNB
AIG
Alliance Bernstein
American Express
Bank of America
Bank of Tampa
Barclays
BGC Partners
C&N Bank
Capital One
Catalyst Corporate Credit Union
Charles Schwab
Citi
Citizens Bank
CME Group
Cowen
Daiwa Capital Markets
DTCC
Edward Jones
Fannie Mae
Fiserv
Freddie Mac
Fulton Financial
Goldman Sachs
Jeffries
JPMC
Legg Mason
Mastercard
Morgan Stanley

Critical Infrastructure I Community Organizations
Industry Entities (continued)
MUFG
Navy Federal Credit Union
NFA Futures
Northern Trust
Oppenheimer
PNC
Raymond James
SEI Investments
State Farm
Sterling National Bank
Synchrony
TD Ameritrade
TIAA
The Clearing House
USAA
U.S. Bank
Wells Fargo
Government Entities
Board of Governors of the Federal Reserve System
Commodity Futures Trading Commission (CFTC)
Conference of State Bank Supervisors
Department of the Treasury
Federal Deposit Insurance Corporation (FDIC)
Federal Housing Finance Agency (FHFA)
Federal Reserve Bank of Chicago
National Association of State Credit Union Supervisors (NASCUS)
National Credit Union Administration (NCUA)
Office of the Comptroller of the Currency
Securities and Exchange Commission (SEC)
Coordination Bodies
American Bankers Association (ABA)
Credit Union National Association (CUNA)
Financial Services Information Sharing and Analysis Center (FS-ISAC)

Critical Infrastructure I Community Organizations
Coordination Bodies (continued)
Financial Systemic Analysis and Resilience Center (FSARC)
Financial Sector Services Coordinating Council (FSSCC)
Independent Community Bankers of America (ICBA)
Securities Industry and Financial Markets Association (SIFMA)

Critical Infrastructure II Community Organizations
Industry Entities
AppGate Federal Group
Becton Dickinson
Cleveland Clinic
CrowdStrike
Eli Lilly
Ford Motor Company
GrammaTech
HCA Healthcare
Jigsaw Security
Lennox
McAfee
Merck
MSA Safety
Nuance
Sanofi
Shell
Siemens
Government Entities
New Jersey Cybersecurity and Communications Integration Cell (NJCCIC)
Coordination Bodies
Health Information Sharing and Analysis Center (Health-ISAC)
International Association of Certified ISAOs (IACI)
Information Technology-Information Sharing and Analysis Center (IT-ISAC)

Critical Infrastructure III Community Organizations
Industry Entities
American Express Global Business Travel
American Honda Motor Co.*
Ford Motor Company
Gap, Inc.
General Motors
General Motors Financial
Hyundai America Technical Center, Inc.
Navistar, Inc.
Panasonic Automotive Systems Company of America
Ralph Lauren
Subaru of America, Inc.
Toyota Motor North America
Urban Outfitters, Anthropologie Group, & Free People (URBN)
Government Entities
Department of Transportation (DOT) • Federal Aviation Administration (FAA)* • National Highway Traffic Safety Administration (NHTSA) • Volpe Center
Coordination Bodies
Automotive Information Sharing and Analysis Center (Auto ISAC)
National Retail Federation (NRF)
Retail and Hospitality Information Sharing and Analysis Center (RH-ISAC)

Federal Organizations
Government Entities
Department of Agriculture (USDA)
Department of Commerce (DOC)
Department of Energy (DOE)
Department of Health and Human Services (HHS)
Department of Homeland Security (DHS) • Customs and Border Protection (CBP) • Cybersecurity and Infrastructure Security Agency (CISA) • Federal Emergency Management Agency (FEMA) ○ Region I ○ Region IX

Federal Organizations

Government Entities (continued)

DHS (continued)

- Transportation Security Administration (TSA)

Department of Veteran Affairs (VA)

Executive Office of the President/National Security Council (EOP/NSC)

Federal Communications Commission (FCC)

United States Postal Service (USPS)

Coordination Bodies

Cyber Response Group (CRG)

Cyber Unified Coordination Group (UCG)

International Organizations

Government Entities

Australia

- Australian Cyber Security Centre (ACSC)

Canada

- Public Safety Canada (PSC)
- Canadian Centre for Cyber Security (CCCS)

France

- National Information Systems Security Agency/Cyber Crisis Management Unit (ANSSI)

Germany

- Federal Office for Information Security (BSI)/Computer Emergency Response Team (CERT-Bund)

Hungary

- Special Service for National Security/National Cyber Security Center (CERT-Hungary)

Japan

- Computer Emergency Response Team (JPCERT/CC)
- National Center of Incident Readiness and Strategy for Cybersecurity (NISC)

Netherlands

- National Cyber Security Centre (BD/NCSC/OP)

New Zealand

- Computer Emergency Response Team (CERT-NZ)

Singapore

- Cyber Security Agency (CSA)

Sweden

- Civil Contingencies Agency/Department of Cybersecurity and Secure Communication/Strategy and Coordination Section (MSB/CERT-SE)

Switzerland

- Reporting and Analysis Centre for Information Assurance (MELANI)

International Organizations

Government Entities (continued)

United Kingdom

- National Cyber Security Centre (NCSC)
- National Crime Agency (NCA)

Law Enforcement/Intelligence/Department of Defense Organizations

Government Entities

Department of Defense (DoD)

- DoD Cyber Crime Center (DC3)
- United States Northern Command (USNORTHCOM)
- United States Cyber Command (USCYBERCOM)

Department of Justice (DOJ)

- Federal Bureau of Investigation (FBI)
  - National Cyber Investigative Joint Task Force (NCIJTF)/Cyber Division

National Security Agency (NSA)

Office of the Director of National Intelligence (ODNI)

- Cyber Threat Intelligence Integration Center (CTIIC)
- Intelligence Community Security Coordination Center (IC SCC)

State Organizations

Government Entities

Arizona

- Arizona Board of Fingerprinting
- Arizona Board of Osteopathic Examiners
- Arizona Board of Psychologist Examiners
- Arizona Board of Respiratory Care Exam
- Arizona Department of Administration
- Arizona Department of Economic Security
- Arizona Department of Education
- Arizona Department of Gaming
- Arizona Department of Homeland Security
- Arizona Department of Transportation
- Arizona Department of Health
- Arizona Department of Revenue
- Arizona Department of Transportation
- Arizona Lottery
- City of Phoenix
- Scottsdale Police Department

Delaware

Florida

State Organizations
Government Entities (continued)
Indiana
Iowa - Iowa Department of Public Safety - Iowa Office of the Chief Information Officer - Iowa Secretary of State Office - Cherokee County Iowa - Jasper County Iowa - Louisa County Iowa - Sioux County Iowa - Story County Iowa
Kansas - Kansas Bureau of Investigation - Kansas Department for Children and Families - Kansas Department of Administration - Kansas Department of Agriculture - Kansas Department of Commerce - Kansas Department of Emergency Management - Kansas Department of Revenue - Kansas Information Security Office - Kansas Information Technology Services Division
Missouri - Missouri Department of Corrections - Missouri Information Technology Services Division
New Hampshire
Utah
Coordination Bodies
Multi-State Information Sharing and Analysis Center (MS-ISAC)