February 2024

Hobby Exercise 2023 After Action Report

TLP:WHITE This report may be shared without restriction. For Health-ISAC members —be sure to download the full version of the report from the Health-ISAC Threat Intelligence Portal (HTIP). Contact Membership Services for assistance.

Health-ISAC™
Collaborating for Resilience in Healthcare
SHARING SINCE 2010

health-isac.org

Abstract

Constantly evolving threats and risks within the healthcare and public health (HPH) sector require coordinated and effective preparedness, response, and recovery actions within and between the United States government (USG) and private sector entities. In recognition of the value achieved through focused discussion between healthcare sector organizations and government agencies, Health Information Sharing & Analysis Center (Health-ISAC) created the Hobby Exercise Series for the United States and Europe. The Hobby Exercises are intended to be held regularly to keep sector entities and their government partners engaged and informed on cybersecurity challenges and the best ways to respond to widely impactful incidents. This document summarizes the discussion and findings from the 2023 Hobby U.S. Exercise. Organizations can use this document to educate themselves on the challenges faced during large-scale cybersecurity incidents and to identify areas for improvement.

Contents

Introduction and Summary

In October 2023, Health-ISAC facilitated an all-day workshop and tabletop exercise with Health-ISAC members and United States Government (USG) agencies in Washington, DC. This fourth iteration of the United States (U.S.) Hobby Exercise was in keeping with prior editions in driving focused discussion among participants to:

1. Highlight and evaluate whole of sector security and resilience challenges impacting the healthcare and public health (HPH) sector including cybersecurity preparedness and resiliency, clinical, patient, regulatory and device manufacturer perspectives with agreement for action to address issues associated with a potential significant cyber incident.

2. Identify strengths and areas for improvement in timely and actionable event and incident coordination among public and private sector stakeholders during response to a significant cyber incident to include trigger levels for coordination.

3. Inform stakeholder capabilities of the HPH sector public and private sector partnerships and examine challenges faced, before, during, and after a significant cyber incident.

4. Inform development for the Healthcare sectors approach to receive, review, and report on lessons learned with associated actionable & timely recommendations for continuous improvement.

The 2023 U.S. Hobby Exercise included participants from Health-ISAC, healthcare delivery organizations (HDOs), medical device manufacturers (MDMs), pharmaceutical organizations, and federal government agencies including the Department of Health and Human Services (HHS), Food & Drug Administration (FDA), Federal Bureau of Investigation (FBI), and Department of Homeland Security (DHS). Over the course of several hours, the participants were provided with fictional situation reports that escalated across multiple phases. During each phase, questions were posed that prompted discussion regarding how the varied participants would respond, what response actions would be taken, what information they would be seeking both within their organization and from external partners, and what they would expect government agencies and other members of the sector to be doing. These conversations were held in both a large group setting and in smaller breakout groups to facilitate more in-depth discussion between participants with similar roles and responsibilities.

The daylong discussion concluded with valuable insights and practical steps organizations can build into their plans, procedures, and operations to prepare for a multifaceted incident. Open conversations, held under TLP:AMBER and Chatham House Rules, resulted in several key findings and recommendations[1] regarding sector challenges and engagement with government partners.

By the end of the exercise, the following top-level conclusions were reached:

- To varying degrees, HPH organizations share many of the same challenges to ensuring safe and secure patient care and uninterrupted business activities.
- More education and clarity is needed around what level of information sharing is appropriate and what information sharing mechanisms are safe and trustworthy between industry members and government partners.
- HPH organizations are wary of supply chain threats and vulnerabilities which are increasingly sophisticated and are not easily monitored or addressed.
- HPH organizations may not be spending enough time to think through the long tail of post cybersecurity incident effects and obligations that could have significant legal and regulatory ramifications.
- Government partners should continue to ramp up efforts to build trusted relationships and regularly update and clarify guidance as to their authorities and capabilities for both a legal and non-legal audience.

This report represents a snapshot of thoughts and ideas from a limited number of healthcare cybersecurity experts among Health-ISAC's membership across the HPH sector, and as such, should not be considered as comprehensive regarding the many challenges the sector faces. Every attempt has been made to capture the discussion faithfully and highlight the emerging recommendations to help raise awareness and inform action.

Key recommendations, grouped by major stakeholder, are:

Health-ISAC

The themes present in Health-ISAC's recommendations mirror prior exercises and represent recurring issues for continuous improvement that underscores Health-ISAC's role in the HPH sector.

- Health-ISAC can do more to educate Health-ISAC organizations and others about the resources they have access to, such as working groups, member-only communication channels, and exercises like the Hobby series.
- Health-ISAC should ensure members know they can submit incident information securely and anonymously to Health-ISAC. Ensure they understand that the information would not only be shared with other members, but that it also can be shared with external partners of their choosing, including other ISACs, government partners (United States, UK, Australia, and more), etc.
- Health-ISAC can facilitate connections to appropriate government / law enforcement entities if needed.
- Health-ISAC should provide more education and guidance on the legal and regulatory frameworks relevant to information sharing.

[1] Findings and recommendations do not represent official views or decisions of the participating organizations.

Government Agencies

- Government partners can do more to educate the private sector on their role in incident response, their relationship to other government entities during an incident or in relation to information sharing, and what the private sector should expect from them in terms of incident communications.
- Government partners should continue outreach initiatives to build trust with the private sector and minimize fears that engagement may increase the potential for legal or regulatory punishment.
- Government partners should consider more guidance on how the private sector should interpret rules and regulations, including writing for audiences like legal and the C-suite.
- Government entities may wish to consider creating or clarifying guidance for emergency or abnormal conditions. Help the private sector understand where there could be legal and regulatory flexibility in service to protecting patients and national interests.

Private Sector

- HPH sector entities should ensure they have devoted resources to identifying and mitigating supply chain risks, and to responding to potential supply chain incidents. This includes prioritizing partners, vendors, and critical services.
- HPH sector entities should encourage their Security/IT leaders to build and maintain relationships with their internal legal, compliance, and/or regulatory teams to foster greater understanding of the intersection of legal and cyber risk management and to facilitate quicker and more expansive incident response communications.
- HPH sector entities should advocate for more expansive and faster information sharing during an incident by working with senior leadership and their legal department to better identify the limitations imposed by state and federal laws and regulations.
- HPH sector entities should ensure they have considered what they may have to contend with post-incident, and how the “long-tail” of effects may result in a considerable resource burden even after containment and the resumption of full operations.
- HPH sector entities should ensure that cyber incident response plans address extended outages and regional impacts.

Tabletop Exercises

Throughout the entire exercise, the value of conducting tabletop exercises came up repeatedly. Given the context, this is unsurprising, but the questions posed by many participants and the exchange of lessons learned and ideas was particularly notable.

For many organizations, conducting tabletop exercises with the cybersecurity and technology teams is fairly commonplace and has been for many years. In recent years, this has extended up the leadership chain to include the most senior executives and boards of directors. Two main reasons were cited for this:

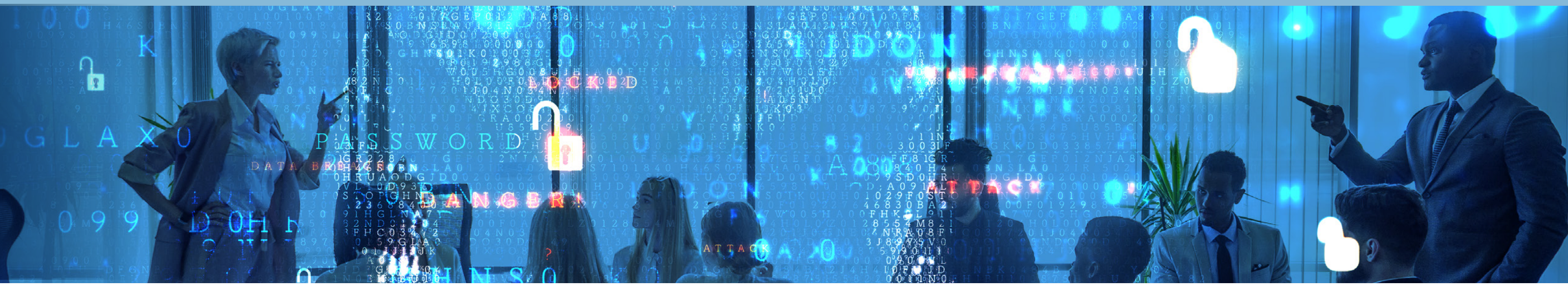
- As cybersecurity incidents have increased in frequency and severity, there is increased interest across the organization to learn more about the impacts of an attack and how to respond, how to resource cybersecurity appropriately, and understand roles and responsibilities before, during, and after an attack.
- Legal and regulatory obligations are increasingly citing senior leadership as having direct accountability for the cybersecurity of the organization, putting pressure on those leaders to be educated and ready to respond.

In both cases, well-crafted and inclusive tabletop exercises have repeatedly demonstrated their efficacy in achieving these goals. Some participants noted that they are now combining both technical and leadership tabletops in ways that further strengthen coordination and improve response actions.

The types of tabletops and approaches are varied, and impacted by the size and type of the organization. Larger organizations may find that they need to conduct multiple tabletops over time to address more focused areas. For example, a pharmaceutical company may want to practice responding to an enterprise ransomware attack in one session, but focus on a cyber-attack against a manufacturing facility in a different session.

All participants agreed that there is no “right” way in terms of content, but there were some thoughts about approach that were generally agreed to:

- Tabletops should be held in person to the extent possible. While this may not always mirror real-life circumstances in a crisis, practicing in person generally allows for high-bandwidth discussions and a more effective learning environment for most people.
- Consider bringing in outside expertise to help facilitate your tabletops. This could be through a cybersecurity services firm, outside counsel, or your insurance carrier. This does not have to be for every exercise, but getting outside perspective on a periodic basis can help to avoid blindspots or reinforcing less effective processes and procedures.
- Be sure to keep in mind special circumstances of remote offices.
- Conduct exercises at least annually, or more often as needed.
- Consider involving external partners including outside counsel, forensic investigators, key partners such as cloud services, and any organization which you might rely on during or after a cyberattack



Sector Challenges

Internal Friction: Security/IT, Legal, and Information Sharing

A significant topic of conversation during this year's exercise was the internal friction that can occur between an organization's Security/IT team and their legal counsel, especially in the early stages of an incident. In particular, participants questioned if information sharing was being unnecessarily curtailed, what legal concerns prompted this limitation, and how the issue could be overcome.

Information Sharing/Blocking

A view shared by many of the participating organizations was the expectation that information sharing in the wake of a cybersecurity incident would become severely limited as soon as their legal team became involved. Some participants cited concerns that valuable threat intelligence, indicators of compromise, and vulnerability information would not be disseminated even if it could help the broader ecosystem prepare defenses or respond and recover effectively.

Participants noted that, in general, legal and regulatory concerns were expected to lead to information sharing restrictions that minimize external communication until an incident is firmly understood in scope and impact, remediation efforts are underway, and legal obligations have been assessed and addressed. Many participants felt that this approach may be overly conservative and narrowly focused on minimizing the legal and regulatory liability of excessive information sharing at the expense of aiding the broader HPH ecosystem to understand and prepare.

While legal and compliance representation was limited at the exercise, two factors were identified that are believed to exacerbate this issue.

First, it was widely acknowledged that cybersecurity incidents typically involve legal and regulatory considerations ranging from contractual agreements with vendors and clients to concerns of litigation and class action lawsuits, to state and federal laws and regulations on privacy and cybersecurity. This complex landscape is made worse by a general lack of harmonization with regards to timelines, terminology & definitions, and reporting triggers & standards. Assessing all of these factors in real-time during an evolving incident understandably incentivizes caution.

Secondly, it was posited by participants that legal teams, especially in-house counsel, rarely have sufficient cybersecurity expertise. Without this background and a basic technical understanding of the kinds of information and data that Security/IT teams would like to share, legal teams are likely to be hesitant to allow that information to leave an organization.

Criticality of Information Sharing

The Hobby Exercise's focus on information sharing is driven by a proven understanding that it can make a world of difference to the security of individual HPH organizations and the sector as a whole. The value of information sharing might best be conceptualized as the idea that every individual Health-ISAC member organization can act as an intelligence node to every other member. Each member being capable of quickly and efficiently informing all others of threats and vulnerabilities as they arise, often shared in a HPH specific context.

The information disseminated can help organizations respond to threats before being targeted, mitigate vulnerabilities more effectively, and recover from incidents quicker. All of those outcomes have the effect of minimizing business, legal, and operational risks.

For example, beginning in 2012 and lasting for several months, dozens of US banks were targeted with sophisticated denial-of-service attacks by a group with ties to the Iranian government. Banks shared intelligence about the attacks, including warnings of pending attacks, plus remediation advice. The Financial Services-ISAC (FS-ISAC) provided a trusted platform for members to confidentially and anonymously share meaningful threat and incident information. The banks were able to use that information to successfully defend their sites from subsequent DDoS attacks.

Potential Solutions: HPH Sector

In addition to highlighting information sharing concerns, participants discussed various ways in which internal friction inhibiting information sharing could be improved. While there is a limit to what HPH sector organizations can do about the complexity of the legal and regulatory landscape beyond advocating for harmonization and standardization, several participants outlined an approach more likely to be attainable to all.

A few participants from the Security/IT side of organizations acknowledged they had found success proactively engaging with their legal team to build trusted relationships and to mutually educate each other on the nuances of, and specific concerns related to, information sharing. After all, ultimately both Security/IT and legal are risk managers for an organization and each should ideally complement the other.

Those on the Security/IT side also noted they had found success building relationships through routine meetings and inclusion in tabletop exercises and workshops. The trust that was built and the expertise that was shared has allowed several members to work towards systematizing otherwise ad-hoc cybersecurity incident response interactions to smooth internal friction and allow greater flexibility. One participant even noted that they were working towards creating a legal pre-approved form for incident information sharing that should help avoid an information blackout. Refer to Health-ISAC's Information Sharing Best Practices White Paper for tips like this and others to address these typical barriers to information sharing.[2]

Potential Solutions: Government

Participants also identified an important role for government partners in addressing the complexity and educational aspects of the information sharing issue.

Among the challenges referenced above is the notion that legal and compliance professionals at HPH entities do not often have sufficient expertise in understanding the nuances of cybersecurity laws and regulations. It was proposed that one possible solution could be the expansion of resources written for a legal audience in mind, "by lawyers, for lawyers."

[2] Health-ISAC Information Sharing Best Practices: https://h-isac.org/h-isac-information-sharing-best-practices/

Some examples of this already exist, with perhaps the most prominent one being the Cybersecurity and Infrastructure Security Agency's (CISA) *Resources for Lawyers webpage and their Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015.*[3] [4] Guidance like this, if backed and written authoritatively by government entities, could help facilitate conversations between Security/IT and legal at HPH sector organizations, ease legal and regulatory concerns, and incentivize more information sharing.

Potential Solutions: Health-ISAC

Finally, Health-ISAC also has a role to play. During the exercise, Health-ISAC representatives reiterated their ability to anonymize and share sensitive information with Health-ISAC members, other ISACs, and with government partners. Acting as a trusted hub and facilitator of information exchange is a central role of ISACs, and it is one that should help minimize the kinds of legal and regulatory risk that several participants cited as barriers to greater information sharing. Health-ISAC should continue to raise awareness of these capabilities while also building out relationships and engagement with legal and compliance elements to further explore these issues from their perspective.

This is undoubtedly a topic that would benefit from further exploration with additional legal and compliance personnel.

Supply Chain Threats and Vulnerabilities

This year's exercise scenario was intentionally designed to facilitate conversation around the increasing risks associated with supply chain threats and vulnerabilities. While this specific issue is not unique to the HPH sector, there is a heightened importance in critical infrastructure sectors and there does not appear to be any easy answers.

In particular, participants noted the following aspects as adding complexity to adequately mitigating supply chain risks:

- The difficulty of assessing third-party cybersecurity maturity and a general lack of visibility into third-party products and services
- The business and operational repercussions of cutting off third-party partners who enable critical connected services
- Limited expertise and leverage in contract/procurement negotiations
- Limited resources for supply chain security

Supply Chain Visibility

Numerous participants highlighted the difficulty in understanding the full scale of their supply chain risk due to a lack of visibility. For example, one participant outlined how their organization may have hundreds of third-party connections through various hardware and software products and services, while another participant referenced the difficulty in attaining and maintaining an accurate inventory of all their connections.

[3] Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015. www.cisa.gov/sites/default/files/publications/Non-Federal%252520Entity%252520Sharing%252520Guidance%252520under%252520the%252520Cybersecurity%252520Information%252520Sharing%252520Act%252520of%2525202015.pdf&sa=D&source=docs&ust=1701811308561846&usg=AOvVaw3SW3zYAB06g69J4BDQfMDP

[4] www.cisa.gov/about/resources-lawyers&sa=D&source=docs&ust=1701811326078909&usg=AOvVaw1l7LfIEbq9Ow3zFIZAuZED

Beyond issues of scale, participants noted a general inability to adequately gain visibility into the cybersecurity maturity of third-party partners themselves. Participants noted that while some larger healthcare entities may have the leverage to request certain cybersecurity disclosures or demand certain protections be included in contractual requirements, many small and medium sized businesses lacked that leverage or expertise.

Furthermore, participants cited the potential unwillingness among third-parties to disclose details of their cybersecurity maturity. It was the belief of some participants that many third-party partners were simply too organizationally immature to be able to understand their own cyber risk and know when their products were susceptible to currently exploited vulnerabilities.

Severing Network Connections

The supply chain discussion also ventured into the issue of cutting off access to and from third-party partners suspected of being compromised. Central to this conversation was how organizations should make the determination to sever connections, especially if the third-party in question enables critical services or business operations. Participants cited the need to assess what kind of communication they were receiving from the third-party in question, what the business impact might be, how operational capacity would be affected, and how long it would likely take to restart operations if severed.

Potential Solutions: HPH Sector

While there was no clear consensus on how individual organizations should determine that a third-party partner should be cut off, participants did appear to identify several recommendations:

- Organizations should identify the criteria and impacts, including who has the responsibility and authority to make the decision to cut off a third-party. This information needs to be documented kept in a written playbook
- Organizations should consider creating a playbook for its third-party partners outlining how the organization plans to act and what they can expect from the organization during a cyber incident
- Security/IT should work with senior leadership and other stakeholders to understand the full potential business and operational impact of cutting off a third-party partner
- Consider the offline capabilities of new products and services as a part of procurement, assessing the ability of those products and services to work “offline”

Each organization’s unique situation will likely lead to variations in approach, but questions like these were identified as a good starting point for discussion.

Potential Solutions: Government

Improving supply chain security is not just a private sector issue. The U.S. Government (USG) is in the midst of addressing supply chain issues itself with the recent push for secure software development attestations and Software Bills of Materials (SBOMs)[5]. While the government’s direct influence is limited to entities that engage with the USG, the foundations they are creating in terms of standardized frameworks, formats, and tools are useful steppingstones for the HPH sector.

[5] https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf

Potential Solutions: Health-ISAC

A successful effort that contributes to supply chain security has been the development of the tools like the Health Sector Coordinating Council's (HSCC) development of *Model Contract-language for Medtech Cybersecurity*.[6] This reference resource helps to create a uniform set of expectations and clarifies responsibilities around medical devices, including addressing cybersecurity. While this specific resource is tied primarily to HDOs and MDMs, the Health-ISAC would be well placed to explore other areas and interactions where similar model language could provide useful guidance and negotiating starting points that mitigate supply chain risk.

For example, it may be worthwhile to assess the potential of model contract language between HPH sector entities and managed services providers (MSPs). The substantial uses of MSPs, especially among less well resourced organizations, may lend itself to a sector-driven effort led by Health-ISAC to find baseline requirements, settle terminology, and highlight specific issues that HPH sector entities should seek to address with prospective MSP partners.

Conclusion

Health-ISAC would like to thank all the participants, the planning committee, our government partners, and the many others who contributed to the success of the Hobby U.S. 2023 exercise.

We demonstrated again how collaboration and cooperation ensure that our collective response to crises is both essential and possible.

We learned that there remain many opportunities for government and industry to communicate more effectively, and proactively, about their needs and capabilities.

We heard that more can and should be done to reach organizations in the healthcare sector that struggle to obtain the knowledge and resources to defend themselves as effectively as possible.

Finally, we know that there is a need and desire for more Hobby Exercises in 2024 and beyond, and we all look forward to making that happen.

Feedback and suggestions on this document are encouraged and welcome. And if you are interested in learning more about the Hobby Exercise, please email **contact@h-isac.org**

[6] https://healthsectorcouncil.org/wp-content/uploads/2022/03/HSCC-Model-Contract-language-for-Medtech-Cybersecurity-2022.pdf