2024 Americas Hobby Exercise 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.

Abstract

Constantly evolving threats and risks within the health sector require coordinated and effective preparedness, response, and recovery actions within and between the government 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, to be held regularly in the United States and Europe in order 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 2024 Americas Hobby 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 June 2024, Health-ISAC facilitated an all-day workshop and tabletop exercise with Health-ISAC members and United States Government (USG) agencies in Washington, DC. This fifth iteration of the Americas Hobby Exercise was in keeping with prior versions in driving focused discussion among participants to:

1. Highlight and evaluate whole-of-sector security and resilience challenges impacting the health 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 the response to a significant cyber incident, to include trigger levels for coordination.
3. Inform stakeholder capabilities of the health sector public and private sector partnerships and examine challenges faced before, during, and after a significant cyber incident.
4. Inform development of the health sector's approach to receive, review, and report on lessons learned with associated actionable and timely recommendations for continuous improvement.

The 2024 Americas Hobby Exercise included participants from Health-ISAC, healthcare delivery organizations (HDOs), medical device manufacturers (MDMs), pharmaceutical organizations, health information exchanges (HIEs), and federal government agencies, including the Department of Health and Human Services (HHS), Food and Drug Administration (FDA), Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), 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 various 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 a large group setting.

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 regarding sector challenges and engagement with government partners.

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

- **Concentration Risk:** The health sector, and health sector organizations individually, may be exposed to variations of IT concentration risk. An over-reliance on a single vendor for a variety of mission-critical products and services can create an "eggs in one basket" risk for a health sector organization if that vendor were to suffer an issue. Additionally, the sector's resilience as a whole may be exposed to concentration risk through a lack of market providers or alternatives for critical third-party services.

- **Legal and Regulatory Incentive Structure:** Health sector organizations and government partners are concerned that the current health sector cybersecurity legal and regulatory incentive structure is misaligned and does not adequately prioritize patient care and positive patient outcomes ahead of compliance and liability avoidance. There is interest in assessing how legal and regulatory incentives could be modified to better balance these issues.

- **Data Integrity:** Health sector organizations have traditionally focused on protecting the confidentiality and ensuring the availability of mission-critical data. Health sector organizations may not be well prepared to address vulnerabilities and threats to the integrity of mission-critical data or to recover critical business operations and services if the validity of mission-critical data is in doubt.

- **Resource Disparity:** Executive and legislative leaders should consider how the wide resource disparity among health sector entities necessitates multiple or flexible policy solutions to raising healthcare sector cybersecurity and resiliency. Less well-resourced organizations are no less important to their communities, and well-intentioned policies should take care to not exacerbate their struggles.

- **Cybersecurity Incident Impacts on Healthcare Practitioners:** HDOs may not be fully aware of how impactful cybersecurity incidents can be on their healthcare practitioners. HDOs should take care to assess how well trained their practitioners are to work without expected critical digital tools for extended periods. It may be underappreciated how comfortable healthcare practitioners are with analog processes and how the stress and inefficiency of these processes over a prolonged period may increase the prevalence of burnout and negatively affect the quality of patient care.

Key Recommendations, Grouped by Major Stakeholder

Health-ISAC

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

- Health-ISAC can do more to educate members and others about the Health-ISAC resources they have access to, such as working groups, member-only communication channels, and exercises like the Hobby series.
- Health-ISAC should provide more education and guidance on the legal and regulatory frameworks relevant to information sharing.
- Health-ISAC should explore deepening information sharing and collaboration with other ISACs to build trusted relationships and broaden threat awareness.
- Health-ISAC should continue to be the primary forum to facilitate health sector engagement within itself and between the health sector and government.

Government Agencies

- 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, especially around information sharing, including developing guidance with the legal and the C-suite audience in mind.
- Government partners should consider prioritizing the types of threat actor identification, multi-seal and multi-government alerts and reports, and deterrence actions that only government agencies can perform.
- Government partners should consider ways of educating the private sector on what the various departments within their agencies do, what resources they provide, and how internal information sharing works.
- Government partners should consider reassessing their regulatory approach to ensure that a regulated entity is not more concerned with compliance and liability than with patient care.
- Government partners should consider assessing concentration risk as an underappreciated risk to the security and resiliency of the health sector and should engage with the private sector to better define it, identify it, and come up with mitigations.
- Government partners should ensure they consider the wide variety of organization types and the disparity in resources that exists within the sector when developing regulations, enforcing regulations, or providing input into the development of laws and policies.

Private Sector

- Private sector organizations should ensure that they are building and maintaining trusted relationships with key third-party partners, appropriate federal regulatory and federal law enforcement agencies, and other critical infrastructure dependencies prior to an incident.
- Private sector organizations should do more to educate themselves on the state and federal laws and regulations pertaining to information sharing to demystify the risks associated with it.
- Private sector organizations should consider what kinds of protections and verification processes they have in place to ensure the integrity of mission-critical data.
- Private sector organizations may wish to consider working with regional colleagues to understand their interdependent cyber risk as it relates to mutually used mission-critical products and services.
- Private sector organizations should ensure they include practitioners when developing and revising cyber incident response plans. They should also ensure they assess the effects of prolonged cyber incidents on their staff's ability to maintain an adequate level of patient care.

Sector Challenges

In addition to the key recommendations noted above, the following three sector challenges warranted additional summarization and may be areas ripe for follow-on exploration.

Concentration Risk

Inspired by several recent incidents, the topic of concentration risk was one area this year's exercise scenario was developed to explore.

In our context, concentration risk refers to two issues that can be described as follows:

Organizational concentration risk occurs when an entity has an over-reliance on a single IT vendor for all or many of its technology solutions (e.g., operating systems, office productivity, email, chat, conference, web browser, cloud, security, or identity capabilities). In this instance, an organization's lack of a diversified IT environment creates a risk that a flaw or compromise affecting the dominant IT provider, or one of its systems, may lead to a larger incident within the organization. A more diversified IT environment may be more difficult to maintain, but may limit the "eggs in one basket" risk.

In a similar vein, sectoral concentration risk occurs when all or many of the entities within a sector have an over-reliance on the same mission-critical systems, devices, or vendors (e.g., payment processing, medical devices, health record access and exchange). In this instance, a lack of diversity or alternatives creates risks that a single point of failure may have serious implications regionally or nationally.

Several participants acknowledged the existence of both kinds of concentration risk.

One participant noted there are pros and cons to diversifying their medical device environment. A more homogenous medical device environment — in terms of the number of vendors and types of devices — makes the implementation and servicing of those devices easier. It also can contribute to security by ensuring that the tools and processes are familiar to the individual or organization servicing them. The participant noted that servicers were more likely to accidentally misconfigure something or make a mistake if they were working with multiple tools and processes.

Another participant noted that they had seen this concern raised for operational technology (OT). They described situations in which OT device manufacturers had designed products with multi-factor authentication (MFA) built in for added security, but it was disabled by a managed service provider (MSP) to ease its workload. Should that MSP be compromised, numerous organizations downstream would be at greater risk.

The discussion also encompassed concerns related to regional resiliency. It was suggested that a form of sectoral risk might arise if health sector entities in the same region or in a concentrated vertical had technology environments and third-party connections that were very similar.

An additional aspect of the discussion was a concern around the apparent lack of marketplace options for specific health sector services, or the outright market dominance of specific providers of those services.

One member highlighted how they initially thought they addressed concentration risk by having multiple clearinghouses, but that in reality, the clearinghouses were all under the umbrella of a single entity. This was echoed by another participant who was aware of an organization that believed it had contracts with multiple providers, but was unaware that each ultimately funneled through a single provider. Another member noted that the prevalence and importance of certain cloud-based infrastructure could be a concentration risk. This called into question just how segmented and diversified the health sector as a whole might be.

Solutions and Further Study

Creating a Shared Understanding of Concentration Risk (Private sector, Health-ISAC, Government)

As illustrated above, concentration risk is still a largely undefined issue that requires investment to determine its elements, types, boundaries, methods of measurement, and terminology. Without these fundamental steps, addressing the issue in a coherent and consistent way across the health sector is unlikely. The National Institute of Standards and Technology (NIST) is probably best placed to carry out such an initiative, with the help of other government agencies and private sector partners. Health-ISAC and the private sector should encourage lawmakers and presidential administrations to pursue this course.

Addressing Concentration Risk Within Organizations (Private sector)

Acknowledging that there is a limit to what can be accomplished prior to standards, best practices, or formal guidance being established, health sector organizations should be encouraged to assess how their own operational environment may be at risk through an over-reliance on a single vendor for a variety of technology solutions. Health sector organizations should be encouraged to consider how diversification might bring a security and resiliency benefit.

Addressing Concentration Risk within the HPH Sector (Private sector, Health-ISAC, Government)

While NIST may best be able to define concentration risk in a general sense, CISA, HHS, FDA, and other relevant government partners should work with the private sector and Health-ISAC to better define it within the health sector. These and other relevant stakeholders should be encouraged to work together to build upon any foundational NIST effort to establish what level of risk and what mitigations are appropriate for the health sector.

Furthermore, whether through existing initiatives at DHS/CISA or HHS, or through a private sector-led effort through Health-ISAC or the Health Sector Coordinating Council (HSCC), it may be beneficial to know where certain chokepoints exist within the health sector and how ubiquitous certain technologies may be within specific verticals. While organizations can work to identify their own concentration risk and potentially their regional risk, a national or international assessment is lacking.

Regional Collaboration for Resiliency (Private sector, Health-ISAC)

Health sector entities in the same region or in a concentrated vertical might wish to engage with each other to determine how diversified their combined environments and dependencies are. This knowledge could be used to develop or plan effective redundancies. Health-ISAC could be a useful facilitator between entities that are unfamiliar with each other.

As an example, hospital networks in the same region might wish to diversify their medical device acquisitions so that a flaw affecting a particular medical device model would not leave that entire region without access to the capability it provides. Alternatively, those same hospital networks might engage with each other to ensure that they have different clearinghouses, payment processors, or cloud service providers.

Cyber Incident Recovery Incentives

During the discussion on the long tail of post-incident recovery, one participant expressed their belief that the current legal and business incentive structure in the United States is fundamentally misaligned. The subsequent conversation highlighted how some participants felt that the United States' current legal and regulatory approach causes health sector entities to prioritize avoiding business and legal risks ahead of getting back online and minimizing patient harm.

Some participants suggested that the technical ability to bring services back could often be achieved earlier than they were, but that the timeline for the restoration of these services was sometimes delayed to assuage legal, regulatory, and business concerns. For example, some entities may prioritize more comprehensive and lengthy recovery operations, including opting for a "best practice" or obtaining a third-party attestation, than might be necessary in a given situation.

This may be incentivized by a desire to ensure that they are protecting themselves in the event of a later regulatory investigation or litigation.

No general consensus on this issue was reached in the time remaining before the end of the exercise, but participants appeared to acknowledge that legal and regulatory liability concerns and business considerations did need to be balanced alongside patient care during a cybersecurity incident and that the current balance could likely be improved.

Solutions and Further Study

Assessing Cyber Incident Recovery Incentives (Private sector, Health-ISAC, Government)

There are fair points to be made across various perspectives on this issue and there is unlikely to be a perfect solution. However, if we accept that maximizing positive patient outcomes is the primary objective, evidence suggests that the current structure of legal, regulatory, and business incentives could be adjusted to better prioritize patient outcomes.

The health sector and its government partners would likely find value from good-faith conversations around how current legal, regulatory, and business incentives drive incident response and recovery behaviors. These conversations could deepen the understanding each has of the other and may help inform the development and enforcement of regulations that improve patient outcomes. Health-ISAC would be in an excellent position to help facilitate these conversations.

In addition, in the wake of the U.S. Supreme Court decision to end Chevron Deference, the potential for existing laws and regulations needing to be revised or replaced may offer a unique opportunity to adjust these incentives.

Data Integrity

Cybersecurity within the health sector has traditionally focused on ensuring the confidentiality and availability of sensitive and mission-critical data. Part of this year's exercise asked participants to consider how well prepared they were to prevent threats and vulnerabilities from causing a data integrity compromise, what impacts they feared may result from such a compromise, as well as how they may recover.

As might be expected from a diverse group of participants, awareness of and preparedness for data integrity incidents varied. However, in general, participants noted that the threat of a data integrity compromise was a serious concern. Few participants appeared confident that they had a firm grasp on the complexities of the topic, and fewer appeared to feel comfortable that their existing policies and controls would provide comprehensive protection for sensitive and mission-critical data.

Several participants noted that identifying that a data integrity incident had occurred would be a challenge. Within an HDO context, the first red flag might be clinicians recognizing irregular or clearly wrong patient care instructions. While some participants felt that certain processes and systems might flag these kinds of irregularities, they were uncertain and noted that it may largely depend on the manner of the data integrity incident. Other participants noted that it might take several cases of wrong diagnosis and investigations following poor patient outcomes to flag a potential issue.

On the positive side, participants were able to note multiple points at which potential harm stemming from a data integrity issue might be prevented even if the underlying cause was not immediately identified.

Regarding the ability to verify that sensitive or mission-critical data had or had not been affected, participants continued to be on shaky ground.

Some were able to suggest a few potential solutions, and the most prominent discussion revolved around modern sophisticated data logging. If correctly configured and retained for a long enough period of time, log records could potentially be used to see what data was changed, when, and by whom. Another potential solution put forward was to compare older patient reports or files for notable differences. For example, a patient whose dosage for the past several years was X and was now Y might warrant further investigation.

While these methods may be able to help verify the integrity of data in some cases, participants were quick to point out that they were far from perfect.

One participant noted that if the logging system were compromised, it could become useless. Another noted that any changes made by an authorized user account may obfuscate malicious activity. Additionally, a participant noted that if the data integrity issue happened upstream, there would be nothing for them to verify, and that they are in a position of needing to trust that the third-party data they receive is accurate.

Expanding on the issue of upstream data integrity issues, one participant noted that a form of a non-malicious data integrity issue that could occur is during the matching and merging of patient data records from various sources. In this case, similar names, birthdates, addresses, and other data fields could cause conflicting or incorrect patient data.

The most sobering take from a participant was their admission that their organization's current consensus response to a data integrity issue was that they would have to go back to revalidate everyone's data, even basic demographic data.

Finally, in response to the kind of impact a data integrity incident may have, some participants noted that the loss of confidence in the integrity of mission-critical data could be profound, even if the integrity of data was not ultimately compromised.

In general, participants did not appear confident that operational disruption would easily be minimized, that patient care could be maintained, or that the issue could quickly be rectified.

Solutions and Further Study

Data Integrity Assessment and Awareness (Private sector)

Health sector organizations should be encouraged to assess how a data integrity incident could affect them, what kinds of controls, processes, and policies could be put in place to reduce the risk of a data integrity incident, and how the organization might recover from such an incident. In addition, organizations may wish to consider integrating awareness of this type of issue into general personnel training or having specific awareness training for clinical staff who may be key in identifying a data integrity issue.

Third-Party Communication and Data Verification (Private sector, Health-ISAC)

Health sector organizations should be encouraged to engage with third-party partners that deliver mission-critical data and to which they provide mission-critical data about the methods used to ensure the integrity of that data. Health sector organizations may wish to add contractual language to third-party contracts around the controls and processes put in place to ensure the integrity of mission-critical data that is provided by that partner. Health-ISAC could be an invaluable partner in facilitating these nuanced and sensitive discussions within membership.

Data Integrity Information Sharing Facilitation (Health-ISAC)

In the event of a data integrity issue, Health-ISAC could become the trusted forum and facilitator for live information sharing regarding what to look for in logs, or what databases, records, or entities may be compromised. Health-ISAC may wish to assess what processes or specific considerations might be required to facilitate this kind of information sharing and create future internal drills or table-top exercises around this issue.

HPH Sector Data Integrity Guidance and Regulation (Private sector, Health-ISAC, Government)

Appropriate government stakeholders should consider assessing the risks of a data integrity incident and should address those risks through continually updated guidance and regulation. This guidance and regulation should seek private sector input during its development and should seek to ensure alignment with other U.S. or international guidance or regulation where possible.

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 2024 Americas Hobby Exercise. Health-ISAC also is grateful for the support from Venable LLP in the planning, execution, and follow-on reporting of the Hobby Exercise, and for hosting the event in June at its offices in Washington, DC. Finally, we also appreciate TrustWave for graciously sponsoring the event.

We look forward to future exercises.

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