October 2019

WHITE PAPER

H-ISAC SHARES MITIGATION AND PREPAREDNESS STRATEGIES FOR HEALTHCARE BLENDED CYBER & PHYSICAL THREATS

H-ISAC™
HEALTH - ISAC

www.h-isac.org

H-ISAC SHARES MITIGATION AND PREPAREDNESS STRATEGIES FOR HEALTHCARE CYBER & PHYSICAL BLENDED THREATS

ABSTRACT

Sharable outcomes aggregated from the Health-ISAC Blended Threats exercise series provide actionable information for the H-ISAC community to discuss, exercise, prepare for, and respond to black swan events. The six workshops enabled participants to focus on enterprise risk management. Exercise discussions yielded shared success strategies, identified opportunities to enhance security postures, and addressed several challenges from the viewpoint of healthcare delivery organizations (HDOs), medical device manufacturers (MDMs) as well as healthcare information technology (IT) vendors.

This paper shares valuable ideas and considerations for the H-ISAC community to adapt and further develop to increase security and preparedness in a complex and blended threat environment.

KEY TAKEAWAYS

1

Whole-of-Organization Approach

– Cybersecurity programs should be looked at as an important component of the whole business.

2

Plan Now to Prepare for a Threat

– Browse the nine topics identified for Preparation and Practice to see where your organization is lacking and where to start planning a best response.

3

Cyber and Physical Security Connection

– The Best Practices section and the Areas for Sector Improvement sections identify processes for cyber and physical security personnel to work together, which departments should be connected and how to keep the chief levels informed during an incident.

PREPARING FOR A BLACK SWAN EVENT

INTRODUCTION

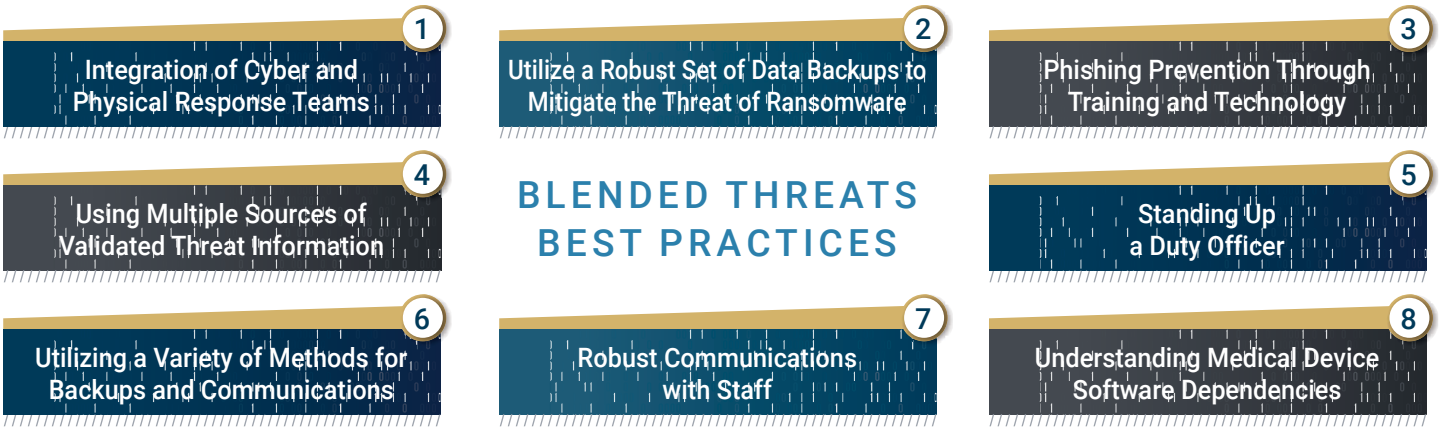
Evolving technology threats and risks are causing implications across the Healthcare and Public Health (HPH) Sector. Understanding the value of focused discussion between public and private healthcare organizations, medical device manufacturers and healthcare information technology (IT) vendors, the Health Information Sharing & Analysis Center (H-ISAC) conducted six Blended Threats Workshops across the United States. A goal of these exercises was to create consensus on approaches to building layered defenses and then sharing the outcome to bolster security for its membership community and the greater HPH Sector.

The workshop series concluded with valuable insights and practical steps organizations can build into their operations - and practice on a consistent basis - to prepare for a multi-faceted threat incident. Open conversations in response to exercise scenarios resulted in sharable best practices, areas for improvement, and challenges identified for healthcare as well as partner organizations to consider.

Workshop participants realized the value of knowing an organization's threat surface and agreed that blended threats are truly a business problem – not simply an IT problem. Blended threats can affect multiple areas of an organization's operation and require the preparation of a whole-of-organization approach, including Legal, General Counsel, CFO, Compliance Officers, Risk Officers, Biomedical Staff, and Board Members. Consensus was that blended threats should be viewed overall as a patient safety issue.

A blended threat was defined within the workshops as a natural, accidental, or purposeful physical or cyber danger that has or indicates the potential to have crossover impacts and harm life, information, operations, the environment, and/or property. All attendees agreed that to effectively prepare for and respond to a blended threat incident, cyber and physical security personnel need to operate together as one team. Eight Best Practices were identified to create the most effective response posture for mitigating a blended threat.

BEST PRACTICES FOR BLENDED THREAT MITIGATION & PREPARDNESS



1 Integration of Cyber and Physical Response Teams

Weekly meetings between physical security and cyber security teams keep all significant stakeholders in the loop during steady state operations. When emergencies occur, these weekly meetings become the foundation from which a more integrated and complex response effort can be built.

2 Utilize a Comprehensive Set of Data Backups to Mitigate the Threat of Ransomware

Many problems created by ransomware can be ignored by having a robust data backup policy. Executed properly, a detailed backup policy, including third parties, can strongly position an organization to ignore the hackers and minimize the disruption to the workday. Companies should consider adopting a routine that includes off-site (cloud) backups, a daily schedule, and redundant locations for the files. Having a robust backup system can potentially eliminate the need to even consider paying a ransom.

3 Phishing Prevention Through Training and Technology

Take advantage of commercial products, procedures, and technologies when combatting the threat of phishing. Run consistent phishing exercises and customize responses for offenders. Consider tracking simulated phishing success rates across job titles to focus education efforts on rarer, but more critical leadership clickers. A one-on-one conversation is also extremely helpful in reducing failure rates for phishing tests. To avoid security problems caused by personal email, organizations can use virtual machines (VM) for staff to connect to personal email accounts.

4

To create an accurate assessment of an organization's threat environment,

Use Multiple Sources of Validated Threat Information

A wide range of sources are available, including H-ISAC, cybersecurity vendors, private mailing lists, FBI's Internet Crime Complaint Center (IC3) InfraGard, DHS including Protective Security Advisors (PSA) Industrial Control Systems Computer Emergency Response Team (ICS-CERT), Health and Human Services (HHS), state police, and sector peers. Establish process and procedures to validate information, such as a multi-department communications committee, to review formal communications (during an incident) prior to public release.

5

Stand up a Duty Officer

Have a duty officer trained on how to address critical situations to serve as primary contact for employees to report cyber concerns. A 24/7 duty officer allows an organization to quickly respond to employee reports of suspicious or unusual cyber behavior.

6

Organizations should establish a **Variety of Methods and Backups for Communications** to re-establish communication between employees during an internet outage or other emergency that limits communications options. Multiple methods of communication help to prevent confusion during a disaster or attack. A mixture of cellular, landline, and cloud-based communications solutions, as well as pagers, walkie-talkies, and other systems can be used as backups for catastrophic communication failures. Distribute and regularly update printed data sheets with mobile phone numbers and/or contact information on a third-party chat service. Contact information for immediate superiors can be physically printed on employee identification cards. H-ISAC is currently in discussions to serve as the home for an industry-wide contact list that could provide multiple points of contact for critical sector personnel and government partners.

7

Craft a **Robust Communications Plan** and practice it ahead of time in order to make sure it meets the staff's needs when an incident occurs. This plan will establish where/how/when to send accurate and useful information and instruct staff regarding external communication during an incident.

8

Understand Medical Device Software Dependencies

Manufacturers who have catalogued the underlying software dependencies within their products can quickly determine the potential impact of any reported vulnerabilities. Organizations should be able to quickly bring all product security experts together to compare what is known against the underlying software dependencies within the inventory of products they manage and determine how much risk any incident creates for its customers. MDMs should create and maintain a record of all third-party dependencies their products utilize, such as a software bill of materials, to understand the supply chain that a product is dependent on.

AREAS OF IMPROVEMENT WITHIN THE HEALTHCARE SECTOR

Exercise participants explored multiple opportunities to further enhance security and resiliency across the healthcare community and in partnership with vital stakeholders. Areas of improvement are defined as opportunities for stakeholders to enhance their security posture. This paper focuses on 19 areas where our membership community can improve in preparedness and emergency response to blended physical and cyber threats. These areas are divided into 3 main focal points: The Whole Organization, What to Prepare and Practice, and Opportunities for Building Capabilities.

Focal Point 1: Information Security is not in the Basement – it is Everywhere

Isolation of the information security area is not in the best interest of the whole business. Proper Integration, effective communications pathways and established network authority is needed before, during and after a blended threat incident.

A Clear Communications Pathway Between MDMs' and HDOs' Information Security Teams is Needed

The security teams of MDMs and medical device owners have difficulties acquiring contact information for each other. The IT department often doesn't learn about a device until after its installation. For HDOs, the IT team is often not the owner of a device and therefore not likely to be contacted by device vendors with critical remediation information. Another approach to help avoid rogue installations and shadow IT during medical device installations would be taking greater control of the organization's network with Network Access Control (NAC) policies.

The Need to Treat Malware as a Business Problem Rather than Just an IT Problem

Treating malware attacks as a problem solely for the IT department limits the resources and flexibility of an organization's response to an event. Approaching malware attacks as a business problem brings in the executive level, where decision-making can allow for flexibility during a rapidly changing situation. Organizations can appoint an executive to prepare for and execute decisions during an incident. This executive can educate leaders on the logic behind the response effort before an incident rather than explaining these complex issues during an incident.

HEALTH SECTOR AREAS FOR IMPROVEMENT

WHOLE-OF-ORGANIZATION

- No clear communications pathway between MDMs and HDOs
- Treat malware as a business problem, not just an IT problem
- Integration between IT and Biomedical teams
- Establishing authority over the network as a security professional

Integration Between IT and Biomedical Teams

IT and biomedical teams can have overlapping responsibilities and concerns regarding medical devices. IT professionals suggested sharing personnel and jointly exercising incident response plans as useful foundations from which to build better coordination and integration between the teams.

Establishing authority over the network as a security professional

To avoid resistance during time critical periods, it would be useful for IT teams to *have written* documentation of their authorities over the network from leadership before a critical situation, especially where two departments might have overlapping authorities.

Focal Point 2: What to Prepare and Practice

Both single person security teams and global security operations centers can use these listed areas as a benchmark of where to focus on and what can be improved to best situate your organization for a blended threat. Every plan, no matter how detailed, is only as effective as it is practiced and improved upon.

HEALTH SECTOR AREAS FOR IMPROVEMENT

PREPARATION AND PRACTICE

- HDOs can function automation only for a limited time
- Building relationships before an event
- Lack of awareness of network connections and security dependencies
- Educating clinicians on device maintenance
- Coordinating and maintaining an accurate inventory of medical devices
- Schedule incident updates for executive level officers
- Bringing the Legal Department into the information sharing process
- Bringing Sales Representatives into the incident response process
- Setting Expectations with Security Vendors

HDOs Can Function Without Automation for Only a Limited Time

When critical lifelines such as electricity or communications systems are lost, HDOs might falter at sustaining operations without internet connected devices during a longer than experienced outage such as can be caused by malware or natural disaster. HDOs should analyze and exercise their emergency operations plans to determine how long that operational posture can be realistically maintained.

Building Relationships Before an Incident

To have an effective working relationship with an individual or organization during any major incident, it is best to invest in building that relationship beforehand. Prior to an incident, security personnel should meet with law enforcement, government agencies, vendors, managed security service providers (MSSP), and/or security researchers with whom an organization would need to rely. Consider applying for group membership, such as an FBI InfraGard chapter or going to networking events. Attending H-ISAC sponsored-events can help ensure the right people are in the room to discuss emergency preparedness and response, and H-ISAC can also serve as a resource to connect companies with appropriate government liaisons, such as DHS Protective Security Advisors or FBI Private Sector Coordinators.

Lack of Awareness of Network Connections and Security Dependencies

Due to Connections with clinics, vendors and other third parties, it can be difficult for HDOs to fully map and maintain awareness of their networks. During a cyber incident, this lack of awareness can slow down the organization's ability to respond to the crisis. Does your organization have a complete and regularly updated catalogue of third party connections? Are hospital network security staff familiar with the networks of their clinics and of how they connect back to the hospital?

Educating Clinicians on Device Maintenance

Clinicians can become an important part of network defense. HDOs should educate clinicians on the possibility that malfunction of a medical device could be due to malware infection and when to contact IT security. Consider training clinicians on basic cybersecurity maintenance techniques, such as applying simple patches to devices.

Creating and Maintaining an Accurate Inventory of Medical Devices

Before conducting a risk assessment of medical devices, it is important for an organization to have an accurate inventory of its devices. Having a system in place to maintain a comprehensive understanding of all medical devices on an organization's network will help multiple areas of risk management.

Scheduled Incident Updates for Executive Level Officers

Establishing an update schedule with a timeline for executive level officer updates during incidents will both inform executives and also give the incident response team a framework to reduce distractions as they do their jobs.

Bringing the Legal Department into the Information Sharing Process

Most legal experts do not fully understand the scope of the information sharing environment and the problems it tries to solve. Engaging the legal department can provide concrete benefits to the speed and flexibility with which the organizations can act and the HPH Sector can respond during widespread incidents. IT departments should consider dedicating resources to legal outreach.

Bringing Sales Representatives into the Incident Response Process

The sales representatives for MDMs are not currently well-integrated into the cyber incident response process. Involving this role in the process could allow for better information sharing and patch deployment. During an incident, there could be value in having those contacts ahead of time. When patching and remediation information becomes available, sales representatives can ensure it gets to the right department and, if questions arise, connect these departments back to the MDM's technical experts.

Setting Expectations with Security Vendors

Security vendors and clients can have a more effective relationship if they are working with the same criteria. Not all HDOs have the capabilities to process information sent by information sharing organizations, such as Indicators of Compromise (IOCs). It is best to keep up a continuous dialogue between the HDO and technical peers at the vendor. This allows the vendor to prioritize their attention and better understand the threats most concerning to the HDO.

Focal Point 3: An InfoSec Wish List for the Health Sector

There are significant opportunities for building useful guidance and capabilities to increase understanding and benefit healthcare organizations, medical device manufacturers, and security vendors.

Guidance in Preserving Medical Devices for Forensic Analysis

The healthcare community needs guidance from trusted organizations on how to best preserve medical devices during an incident for forensic analysis.

HDO Incident Response Plans do not include Medical Device-Focused Modules

Organizations should consider investing resources in developing medical device specific annexes to their established incident response procedures. This effort will require bringing together relevant stakeholders and deciding how to mitigate those risks through additional targeted policies, procedures, and guidelines.

Coordinating and Simplifying the Distribution of Remediations

Improvements can be made by simplifying the distribution of patches and other remediation methods for at-risk medical devices on an organizational and sector-wide basis. Having a centralized repository of patches available, each specific to the incident at hand, was identified as a valuable resource to help HDOs focus on fixing impacted devices. MDMs and HDOs should consider working together to create clear guidelines to ensure HDOs can respond to the ever-changing cyber threat environment and reduce the vulnerabilities in their systems in a timely manner.

Building Malware Analysis Capabilities by MDMs

During an incident, malware analysis is necessary to understand how devices are compromised and what needs to be done to secure them. Two challenges were identified: safely obtaining a copy of the malware and safely analyzing the sample, especially on the targeted medical devices.

HEALTH SECTOR AREAS FOR IMPROVEMENT

BUILDING CAPABILITIES

- Guidance in preserving medical devices for forensic analysis
- Building walware analysis capabilities by MDMs
- HDO incident response plans do not have medical device-focused modules
- Coordinating and simplifying the distribution of remediations
- A better understanding of cyber insurance
- Documenting and distributing lessons learned on a national level

Better Understanding of Cyber Insurance

Acquiring cyber insurance is still a complicated decision for most healthcare organizations and the decision should be a well-researched one. There is still a lack of standardization among offerings in the cyber insurance market for HDOs. However, participants who spoke about their experiences found value in having insurance and that the processes of acquiring insurance was a useful way to ensure that all prevention and response boxes were checked.

Documenting and Distributing Lessons Learned on a National Level

Defining and practicing the process of documenting after-action items following a significant emergency helps organizations build long term resilience into their company.

HEALTHCARE SECTOR CHALLENGES

H-ISAC Blended Threats workshop participants identified five challenges they face within the healthcare sector. Challenges are defined as inherent issues that, in today's threat environment, are unable to be truly eliminated, just mitigated.

1. Difficult to maintain security of medical devices after installation
2. Deciding whether or not to pay the ransom
3. "Drive-By" Infections
4. Understanding the cyber risk profile of small clinics when executing plans
5. Training all staff to handle media during a large event

Difficult to Maintain Security of Medical Devices after Installation

Despite many solutions offered by the market, it is still difficult to maintain the security of medical devices intended to operate for a decade or more. It is a struggle to continuously secure a legacy medical device no longer supported by the device manufacturer or dependent on software no longer supported by the software's manufacturer. The lifetime of a device is often longer than the workstation it is plugged into. Many medical devices are constantly in use, making it difficult to apply patches on an as needed basis. Properly segregating networks or negotiating continuous service contracts with vendors may help; however, no solution or approach was found that could fully eliminate the impact of this challenge.

Deciding Whether or Not to Pay the Ransom

Variables driving this decision include patient safety, the number of infected devices, the cost of the ransom, the cost of recovery, the content of the lost data, the criminal organization, the organization's legal responsibilities, and the long-term cyber threat profile of the HPH Sector. If an organization does decide to pay the ransom, threat actors often request payment in cryptocurrencies, the most popular of which is Bitcoin. Bitcoin transactions take several days and can be difficult for those unfamiliar with the process.

"Drive-By" Infections

The majority of medical devices have third-party software dependencies. If the underlying software suffers from a vulnerability, so do the medical devices on which they depend. "Drive-By" infections happen when exploits affect a medical device despite it not being the primary target. Participants noted that this reality is why discovering and understanding the vector of infection is critical to how the medical device industry will respond.

Understanding Small Clinic Cyber Risk Profiles When Executing Continuity Plans

There is no mechanism to determine which HDOs are also infected in case patients need to be transferred due to a cyber incident. During a combination cyberattack and natural disaster event, there would be limited bandwidth for the appropriate personnel to check their networks for infection, especially if patients from a larger hospital were being distributed to smaller clinics.

Training All Staff to Handle Media During a Large Event

It is a challenge to train all personnel, especially those whose job focus is not public relations, on how to handle the media during emergencies. Participants at one workshop noted employees had been targeted by reporters pretending to be the general public during their off-campus breaks. This can result in potentially concerning quotes for the public relations team to address.

CONCLUSION

The H-ISAC Blended Threats Exercise Series enabled participants across the healthcare sector to brainstorm about enterprise risk management issues for healthcare organizations. Threat scenarios showed the importance of understanding what needs to be protected in an organization, knowing what can be lived without during an extended period, defining the organization's threat surface and building in layers of defense accordingly.

Workshop discussions provided new ideas, shared successes and challenges from the viewpoint of HDOs, MDMs and vendors. Participating organizations gained an enhanced understanding of the healthcare sector security environment to share with the H-ISAC community. The workshop series results provided information for this whitepaper to share with the extended HPH sector.

H-ISAC thanks all participating organizations in the six workshops that have candidly shared their ideas and experiences for the betterment of our community's collective security and preparedness with additional thanks to the workshop hosts (Boston Scientific, Gilead Sciences, Christiana Care Health System, Philips, Johns Hopkins University Applied Physics Laboratory, and Cedars-Sinai Medical Center). H-ISAC also thanks Symantec, who generously sponsored the exercise series.

Feedback on this white paper and suggestions for future topics are encouraged and welcome. Please email us at contact@h-isac.org

www.h-isac.org