Table of Contents

Part I:

► What is CyberRX?
► Overview of Results
► Moving Forward Together – Summary Recommendations for Industry
► Acknowledgements and Thanks

Part II:

► Detailed Findings – Not One Size Fits All
► How it Worked
► Key Insights – Findings and Recommendations
► Moving Forward Together – Findings and Recommendations for Industry
What Is CyberRX?

► CyberRX is a series of industry-wide exercises that simulate cyber attacks on healthcare organizations; they are used to evaluate the industry’s response and threat preparedness against attacks on and attempts to disrupt U.S. healthcare industry operations.

► These exercises are conducted in partnership with HITRUST, the U.S. Department of Health and Human Services (HHS), and healthcare industry organizations.

► The exercises examined both broad and segment-specific scenarios that target information systems, medical devices, and other essential technology resources of the healthcare industry.

► CyberRx findings are analyzed and used to identify areas for improvement in the coordination of the HITRUST Cyber Threat Intelligence and Incident Coordination Center (C³); with security and incident response programs; and in information sharing between healthcare organizations, HITRUST and government agencies.

Who Participated?

► The Spring CyberRX 2014 exercise included participation by providers, health plans, prescription benefit managers, pharmacies, HITRUST C³, and HHS.
How Was CyberRX Organized?

- The Spring CyberRX 2014 exercise was held on April 1, 2014, and was a full-day of interactive simulation designed by a steering committee of industry and observed by Booz Allen Hamilton.

- The steering committee, in coordination with Booz Allen Hamilton, developed a CyberRX Exercise Playbook that outlined the rules, responsibilities, and scenarios of the exercise and organizational referee.

- Each participating organization assigned a referee who was responsible for coordinating any questions or concerns between the participating organizations.

- The referees were briefed on their roles, obligations, and responsibilities in advance of the exercise, which required that they not participate in their organization’s response.

- The referees did not receive the playbook until the day of the exercise. The Exercise Captain was Kevin Charest, Chief Information Security Officer, U.S. Department of Health and Human Services.
Overview of Results
CyberRX 2014 Objectives

Objectives for the inaugural CyberRX held April 1, 2014, included:

► Enhance awareness of cyber threats to the healthcare services industry
► Explore responses to maintain operations in the face of complex risks
► Understand systemic risk to the healthcare system and patients due to disruptions
► Promote information sharing about cyber threats and vulnerabilities among other healthcare organizations and government
As described below, participants thought the CyberRX exercise was invaluable. Participants wanted more industry- and company-specific exercises to make internal written procedures come alive, finely tune response processing, and improve the communications between internal and external industry and government stakeholders.
CyberRX 2014 – Six Key Findings and Recommendations

1. Organizations that Participate in Cyber Exercises are More Prepared for a Cyber Attack

   Regardless of the maturity and comprehensiveness of their information security program
   • Each participant identified benefits in participating in the exercise, regardless of their program’s level of maturity.

2. Organizations’ Preparedness Benefits from Improved Threat Intelligence Processing Capabilities and Increased Engagement with Stakeholders

   Organizations varied in their preparedness for processing threat intelligence or with communicating and engaging other stakeholders internally and externally.
   • This issue extends beyond IT to legal/privacy, crisis management, business/clinical operations, management and external business partners.
   • Additionally organizations vary in their appetite for and ability to process threat intelligence.
3. Industry Calls for Greater “Freedom” to Communicate and Collaborate During Cyber Crisis

Despite potential impact on legal privilege and other concerns, industry participants desired to have heightened communication and collaboration among industry participants, to corroborate/supplement intelligence, and to have a view across healthcare ecosystem, including common vendors and partners.

- Almost all of the participants desired to collaborate with other organizations and/or expressed restrictions/potential liability for doing so.
- Moreover, participants recognized that, for threat intelligence, organizations across the industry vary in their appetite for and ability to process threat intelligence.
- Accordingly, it will be important going forward to develop industry communications and responses to threats that will reflect various states of engagement.

4. HITRUST to Enhance C³ Portal, and Address Need for an Industry Cyber Threat Response Playbook

HITRUST C³ portal viewed as extremely valuable and should be enhanced to further accommodate industry-desired collaboration and cyber playbook.

- It should be noted that HITRUST and HHS have a formal relationship regarding the sharing of cyber threat information.
5. Government and HITRUST to Work on Future CyberRX Exercises and Other Means for Fostering Information Sharing

HHS and HITRUST should continue to explore developing a playbook and opportunities for industry information sharing and analysis to maintain trust in the security that is protecting sensitive health information, and support the next generation of health information technology, and patient safety.

6. A Significant Step Forward

The exercise, although limited in number of participants, was a significant step for industry in establishing an industry Cyber Exercise playbook and formal program, identifying:

• areas where industry organizations should focus;
• opportunities for greater collaboration between organizations, HITRUST and government; and
• what gaps exist where industry needs additional support to better prepare.
Moving Forward Together—Summary Recommendations for Industry
Industry and Organization Preparedness

▶ Develop Formal Cyber Response Communications Plan and Governance Charter

Formal, comprehensive, well-planned, and flexible communications strategy and governance plans must be developed prior to a crisis to ensure interactions with customers, business partners, vendors, and regulators are seamless. A formal program with defined roles and responsibilities to prevent response paralysis and to foster internal collaboration is necessary.

▶ Heighten Preparedness—Enhance Programs and Practice in Industry and Organization Internal War Games

There are significant benefits to organizations in participating in cyber exercises (and additional value when an organization can collaborate during and share lessons learned after). As a result, organizations should:

▶ Conduct healthcare, cyber war games internally, emphasizing processing of intelligence and communications internally beyond IT; and

▶ Participate in future industry exercises (like the HITRUST Summer exercise) and focus on communications with other organizations, government, and collaboration through HITRUST C³.

▶ Participate in Industry Initiatives to Develop Common and Shared Strategies

For example, there are industry and HITRUST initiatives to (i) develop tiered approach to engaging and addressing cyber risks; and (ii) develop common controls (based on HITRUST CSF) and responses that are responsive to the most common threats.
Collaboration and Enhancement of HITRUST C³ Portal

► **Continue to Use C³ as Central Repository**
Participants expressed the desire to have an organization that can enable timely, efficient, and confidential sharing of intelligence. Doing so benefits health organizations and HHS significantly, and removes barriers for sharing with negligible impact of effectiveness.

► **HITRUST C³ Portal Should Be Enhanced to Accommodate Industry-Desired Collaboration**
Incidents and related threat reports should be easily linked to be able to follow an event. Also, additional tools are needed to better facilitate collaboration amongst organizations supporting incident response, including with HHS and law enforcement.

► **Enhance Protocols Between HITRUST C³ and HHS CSIRC**
To enhance coordination and timely delivery and sharing of information between HITRUST C³ and HHS CSIRC, there needs to be better protocols to escalate incidents and issues.
HITRUST and HHS Leadership

► HITRUST and HHS Should Continue Collaboration to Advance Industry Cyber and HIT Agendas and Patient Safety.
Based on the success of the inaugural CyberRX exercise and the consensus among participants for the need for better abilities and mechanisms for industry communication and collaboration, HITRUST and HHS should continue to explore opportunities for industry information sharing and analysis to maintain trust in the security that is protecting sensitive health information, and support the next generation of health information technology and patient safety.
Actions by HITRUST

HITRUST has established a “Healthcare Industry Cybersecurity Roadmap” to outline the key items it will be implementing:

► **Linking Cyber Threat Intelligence Reports to CSF Controls**
  - By evaluating the current CSF control guidance is sufficient based on the cyber threat identified, and enable better understanding of which CSF compensating controls align with the greatest or highest volume of cyber threats. Although the CSF that already incorporates the control is the NIST cybersecurity framework, and provides healthcare-specific and prescriptive guidance, this additional information will ensure the CSF is updated more timely and guidance is aligned with cyber threats and risks. Allow it to provide even greater risk and compliance benefits.

► **Enhancing and Expanding the Collaboration and Incident Response Capabilities**
  - By improving the usability and collaboration capabilities, the C³ Portal will expedite threat awareness and response. HITRUST will consult participating organizations to ensure the specific requirements.

► **Twice a year CyberRX exercises**
  - By committing to enhance the CyberRx playbook and coordinate two exercises a year to continue to evaluate the current effectiveness of the HITRUST C³ and CSF, government collaboration and organizational preparedness with the goal of improving the industry’s cyber threat preparedness.
Acknowledgements and Thanks
HITRUST wants to personally and professionally thank Kevin Charest, DHHS, and the CyberRX Steering Committee for their participation and leadership and commitment to the industry. We also want to thank the participating organizations for their leadership and candid insights and sharing of leading practices and ideas that will help the industry:

► athenahealth
► Children’s Medical Center of Dallas
► Cooper Health
► CVS Caremark
► Express Scripts
► Health Care Services Corp
► Highmark
► Humana
► UnitedHealth Group
► U.S. Department of Health and Human Services
► WellPoint

Also, HITRUST wishes to thank Booz Allen Hamilton for providing expertise to support our first CyberRX and future exercises.
Next Steps

From the feedback provided during the exercise, HITRUST plans future CyberRX war game exercises that will be designed with heightened and enriched intelligence and more complex scenarios, including ones that foster more collaboration among participants and ones that test supply chain and vendors.

Healthcare organizations interested in participating in the Summer 2014 industry CyberRX exercise can register to receive additional information at http://hitrustalliance.net/cyberrx/

More Information

For more information about the report and insight into industry practices, please contact:

► Booz Allen Hamilton – James Koenig, Global Leader, Commercial Privacy and Health Cybersecurity and Incident Response at 610-246-4426 or koenig_james@bah.com

► HITRUST – (469) 269-1100 or info@hitrustalliance.net
Health Industry Cyber Threat Exercise, Spring 2014

Detailed Findings – Not One Size Fits All

April 21, 2014
How it Worked
How it Worked and Real-Time Information Sharing

► The CyberRX exercises are designed to affect each participant and, in some cases, require Senior Leadership involvement.

► The exercises targeted participants from HHS Central Command and Computer Security and Incident Response Center (CSIRC), health plans, hospitals, retail pharmacies, pharmacy benefit managers (PBMs), and mail order pharmacies.

► During the exercise, teams received information and interacted by conference call for real-time sharing of material with the CyberRX Exercise Captain and C³ - HITRUST’s health threat intelligence monitoring service and portal.

Facilitated Teams Assess Their Actions

► Participants played within their respective organizations with the assistance of their own referee and/or a subject matter expert provided by Booz Allen Hamilton.

► Teams were given an exercise template to capture their responses to key questions and to assess their actions during each vignette. Participant responses were used to generate the exercise insights and lessons learned.
Exercise Vignettes—Summaries

While there were seven possible vignettes designed, exercise participants faced a series of four vignettes randomly selected by the Exercise Captain:

- **Exercise One** – A major news network has just reported a posting of a large file of usernames and plain text passwords represented to be participants across the U.S. healthcare system. The report sensationally states that the file contains usernames and passwords for patients, doctors, and nurses across the industry. The conclusion of the expert is that Healthcare.gov has been compromised and offices, hospitals, and major insurance companies. These reports are widely repeated and amplified across major news networks.

- **Exercise Two** – A blogger reports customer data for three major health plan providers’ networks have been infiltrated for months and they have full access to customer data.

- **Exercise Three** – During a drug raid in California, the FBI discovers a large quantity of forged doctor prescription pads and the information gets leaked to the public.

- **Exercise Four** – Local news reports a doctor in California is being interrogated on suspicion of altering radiology readings.
Key Insights—Findings and Recommendations
Key Insights—Findings and Recommendations

► The simulation highlighted a number of insights, with participants focusing on planning and preparation, communications, and understanding the potential business impacts of a large, destructive cyber attack.

► The following insights represent a synthesis of the comments heard during the final discussion and comments entered into workbooks at the end of the simulation—these comments are not necessarily ranked by order of importance.

► Where appropriate, quotes denote actual insights pulled directly from team inputs from workbooks.
I. Industry and Organization Preparedness
Organizations Varied Widely on Level of Preparedness But All Can Benefit from Cyber Exercises

- Many organizations have many of the components of a strong program in place, yet several organizations indicated informal and/or dated procedures.

“Current staffing within operations and the current [organization] operating model does not dedicate personnel for consistent consideration of all points of entry for cyber threats. In the current state, staff is pulled away from their operational accountabilities to respond to any threat that may be identified.”

“There currently is not a clear and documented process in place at [our company] to provide guidance as to the appropriate process for handling cyber threats and/or alerts.”

“Medical device inventories exist across numerous operations and engagement is manual to determine whether devices at risk are in use. Opportunity for more systematic inventory tracking and reporting.”

“A process for identification and the addressing cyber threats and/or breaches [within organization] should be clearly documented.”

“The process to identify and react to cyber risk should be revisited consistently to ensure that the process is kept current and appropriately considers [our organization’s] exposure to cyber threats.”

“An appropriate and repeatable process should be in place to identify and respond to cyber threats that put [our organization] assets at risk.”

“[There is a need for] additional formalized procedures helping to guide individuals who may identify a cyber-threat.”
Organizations Varied in their Preparedness for Processing Threat Intelligence

Several organizations that had the program components in place were challenged to process intelligence, especially the information related to other types of organizations in the health information ecosystem (e.g., payor processing intelligence about a threat that seems to exclusively impact provider systems).

“Being able to navigate around the HITRUST C3 portal system is very helpful. Organizations do not want to learn how during a real scenario.”

“Given the uncertainty around the extent of a cyber-attack (i.e. duration, impact, downstream/upstream links), need better method to [process intelligence and] shift the entire team to monitoring versus active (i.e., suspend operations or ‘weather the storm’/stand down)”

“[Organization] IT Security Governance [should be enhanced to] recommend that Subject Matter Experts be identified such that guidance could be provided as to reasonable actions that may be taken in response to cyber threat information . . . .”
Several Organizations Were Challenged with Communicating and Engaging Other Stakeholders Internally

- Many programs that could process the intelligence and identified a potential threat struggled in communicating potential threats internally beyond IT to legal/privacy, crisis management, business/clinical operations, and management.

“Communication paths outside of InfoSec need to be mapped out in a flow-chart format to eliminate questions during the heat of an incident, or in the absence of key knowledgeable individuals.”

“In identifying cyber threats to [our organization], threats will inevitably be complex and responses may involve multiple operational areas (legal, IT Security, Privacy, etc.). Formal procedures or a RACI document should help [organization] clarify criteria that would warrant the involvement of various [internal] operational areas.”

“Communication and escalation paths need to be documented with specifics, role-to-role, for various types of scenarios.”

“Relevant information related to cyber threats should be disseminated [within our organization] timely such that action can be taken promptly and exposure risk is minimized.”

“Responsibilities of individuals that are to identify cyber risks to [organization] should be clearly stated and accountability ensured.”

“The culture within all [organization] entities should be such that the value of [organization] data and the importance of securing [organization] data is clearly understood and appropriately prioritized throughout the organization.”
II. Collaboration and Enhancement of HITRUST C³ Portal
Almost all of the organizations indicated the desire to collaborate and share information among organizations and with government to validate intelligence and enable early response.

“As information moves to and between EHR systems, the cloud, virtual environments, ACOs, HIEs, it is important to have a view of the whole health ecosystem since many of us share the same vendors and other upstream/downstream partners. This would enable us to fully understand the extent of a cyber crisis, including likely widespread impacts, and potential additional vulnerabilities.”

“It would be helpful to be able to have points of contacts at other organizations to reach out to during the early stages of a potential event to hear what they are seeing and validate what we are detecting.”

“We spend a lot of time focusing internally and concentrating on business as usual. Trying to address risk[s] like these, we would be working in vain. Exercises like this help us as an industry (even competitors), flex muscles around collaborating together.”
Participants Had Varied Opinions on How to Best to Engage Law Enforcement

- Participants indicated varied opinions as to how best to engage law enforcement and share information that could be used against an organization or break legal privilege.

“Opportunity for HITRUST C3 to facilitate a formal cross-functional discussion between named industry companies where DHHS, DHS, and other law enforcement agencies can provide insights as they develop or access to information in support of protection of our industry and our members.”

“Determine if HITRUST C3 can provide interaction with DHS and the FBI for the purpose of facilitating actionable intelligence.”

“Concerns about voiding legal privilege may impact directly contacting other organizations, but anonymous communications with HITRUST C3, HHS, and law enforcement that can be disseminated to the industry provide opportunities that should be expanded/promoted in the industry.”
HITRUST C3 Portal Viewed as Extremely Valuable, But Needs to Be Enhanced to Accommodate Industry-Desired Collaboration

- Incidents and related threat reports were not easily linked. Also, additional tools are needed to better facilitate collaboration amongst organizations supporting incident response, including with HHS.

“The structure of the portal is not conducive to collaboration. Sending in RFIs as KBAs doesn't call them out as action items, and posting the responses as KBAs doesn't explicitly link them back to the questions. Trying to follow the action on the "Intelligence Reports" tab was difficult. Using "Chatter" might have been better.... Some sort of threaded listserv would be more convenient, giving users an end-to-end view of all of the activity.”

“Having a HITRUST C3 conference call to discuss heighten risks may be a good supplement.”

“Opportunity to consider a HITRUST C3 FLASH message approach in addition to the normal threat intelligence reports. Threat intelligence provides ongoing information, but once items become an event or have the potential to impact multiple industry companies by name, a different broadcast medium would allow for differentiation and possibly automatic paging of responders.”

“Reports, news, evidence, etc., need to be centralized in a tool dedicated to this function. Email and IM chats are not appropriate, as information tends to get missed.”

“News, evidence, reports, fixes, etc., need to be maintained in a central repository, such as SharePoint. Email and IM should be discouraged for this purpose, unless it is in addition to such posting.”
III. HITRUST and HHS Leadership
Collaboration and Sharing Between HITRUST and Participating Organizations Was Viewed Positively, as well as HITRUST C³ Sharing with HHS

“There occasionally was a delay in information communication between HITRUST C3 and HHS CSIRC. Need better process to escalate incidents and issues.”

“[CyberRx was a] great way to test program and interactions with outside organizations, including HHS.”

“HIT[R]UST might facilitate the formation of an industry early responder group that could be the face of the engagement across the industry, called to convene when one or two of the executive members (in a tiered model) believe a material cyber threat impacting the industry might be suspected.”
All Organizations Found Significant Value When Asked about CyberRX Exercise

“People in organization do not understand or sensationalize security. Exercises like this raise awareness, get better at response, refine the culture, and learn from others.”

“These industry exercises are important as the impact of a widespread destructive malware attack would erode overall confidence in the entire healthcare system.”

“I appreciated the variety of scenarios, even those that didn’t apply to the organization. It was good to test the team’s ability to process [threat intelligence] information and see how/whether they could rule it out.”

“Scenarios such as this are good opportunities to develop “micro DR” plans to respond to individual threats. Such capabilities should be documented, tested, and ready to use in the event they are necessary.”

“We will continue to learn from industry best practices and input from results from this event.”
Moving Forward Together—
Findings and Recommendations for Industry
Industry and Organization Preparedness

- Develop Formal Cyber Response Communications Plan and Governance Charter.
- Heighten Preparedness—Enhance Programs and Practice in Industry and Organization Internal War Games.
- Participate in Industry Initiatives to Develop Common and Shared Strategies.

Collaboration and Enhancement of HITRUST C³ Portal

- Continue to Use C³ as Central Repository.
- HITRUST C³ Portal Should Be Enhanced to Accommodate Industry-Desired Collaboration.
- Enhance Protocols Between HITRUST C³ and HHS CSIRC.
HITRUST and HHS Leadership

- HITRUST and HHS Should Continue Collaboration to Advance Industry Cyber and HIT Agendas and Patient Safety
  Based on the success of the inaugural CyberRx exercise and the consensus among participants for the need for better abilities and mechanisms for industry communication and collaboration, HITRUST and HHS should continue to explore opportunities for industry information sharing and analysis to maintain trust in the security that is protecting sensitive health information, and support the next generation of health information technology and patient safety.

Actions by HITRUST

HITRUST has established a “Healthcare Industry Cybersecurity Roadmap” to outline the key items it will be implementing:

- Linking Cyber Threat Intelligence Reports to CSF Controls
- Enhancing and Expanding the Collaboration and Incident Response Capabilities
- Twice a year CyberRX exercises
Thank You