



CyberRX 2.0 Level I Playbook Participant and Facilitator Guide

Contents

- Background and Context. 3
 - What is CyberRX 2.0? 3
 - Why should my organization participate? 3
 - Who participates in exercises? 3
 - What are the general expectations? 3
 - What support will HITRUST provide? 5
 - Do I need an external observer? 5
 - How much will this cost? 5
- CyberRX Participation Levels. 6
- Participant Rules 8
- Scoring Construct and Rationale. 11
 - HITRUST CyberRX Level I Certificate of Completion and Scoring 11
 - What are the 10 Markers? 11
- CyberRX Playbook v2.0 13
 - Exercise 1 14
 - Exercise 2 15
 - Exercise 3 16
 - Exercise 4 17
 - Exercise 5 18
 - Exercise 6 19
 - Exercise 7 20
 - Exercise 8 21
 - Exercise 9 22
 - Exercise 10 23
 - Exercise 11 24
 - Exercise 12 25
 - Exercise 13 26
 - Exercise 14 27
- Example Scenario Run Through. 28
- Sample Issues and Questions Identified During the Exercise 30
- Appendix A – About CyberRX 32
- Appendix B – Acknowledgements. 34

Background and Context

What is CyberRX 2.0?

CyberRX is a scenario-based exercise program to assess the cyber security response preparedness of healthcare organizations. CyberRX 2.0 is the next iteration following the successful introduction of CyberRX 1.0 in 2013. The CyberRX program is overseen by a steering committee comprised of representatives from the healthcare industry, HITRUST, and Department of Health and Human Services (DHHS). See appendix A for further background and history on CyberRX.

Why should my organization participate?

CyberRX is an effort by DHHS, HITRUST, and volunteer organizations to improve cyber security maturity across the healthcare industry sector. The program was created in response to growing concerns and threats to the healthcare industry. As demonstrated from numerous organizations' responses to security breaches, how an organization responds to cyber events is equally as important as how the organization protects themselves from security risks.

Your organization should consider participating in CyberRX 2.0 to:

- i. Assess your incident response preparedness and crisis management capabilities in response to realistic and relevant cyber threats and events
- ii. Improve the maturity of your cyber security program by identifying lessons learned from the simulation exercises
- iii. Increase cyber security awareness across your organization
- iv. Engage and educate your executives on cyber security
- v. Establish/broaden partnerships and relationships across the healthcare industry to increase collaboration on cyber security challenges

Who participates in exercises?

The objective(s) of the simulation, and the selected scenario(s), will determine who from your organization should participate. The participants vary and may include your CEO, COO, CIO, CISO, Privacy, Legal, Compliance, Internal Audit, Risk, or others as appropriate.

What are the general expectations?

Preparation: An organizational coordinator is needed to plan and prepare for the exercise. It is also recommended, but not required, that participants be well versed in their own organization's cyber incident response plans and procedures. Participants should be prepared to contribute to the exercise and to maximize the learning value of each scenario.

Commitment/Duration: Depending on the participation level desired (see *Participant Rules*), each exercise will range from just a couple of hours to an entire day.

Format:

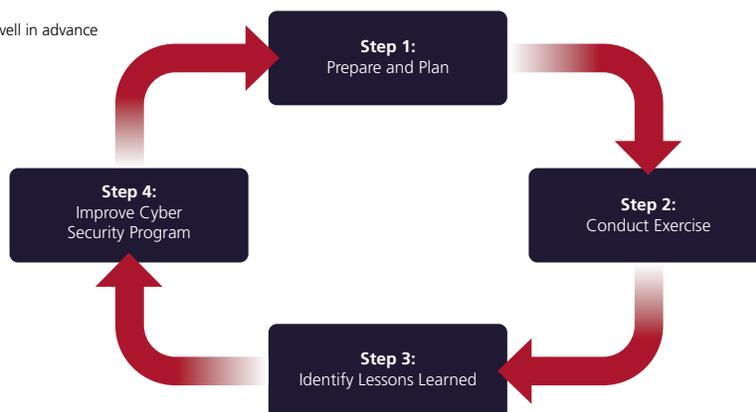
1. The facilitator will introduce the selected scenario(s) to participants along with any assumptions, artificialities, and simulations in order to ensure that the exercise is as realistic as possible.
2. The organizational representatives will discuss how to address the issue including specific immediate/near term incident response procedures, required communications (internal and external), oversight responsibilities (e.g., who will take point), additional information/resources required, legal or other compliance implications, long term planning/actions to consider and possible contingency plans.
3. As appropriate, the facilitator will provide "injection" points to keep the scenario moving forward.
4. A "hotwash" on what worked well and what were some of the lessons learned will be conducted immediately following the event.
5. An After Action Report (AAR) will be subsequently drafted and distributed to participants to formally capture the scenario lessons learned and best practices. See more specifics below:

Step 1: Prepare and Plan

- Identify goals and objectives for conducting the CyberRX exercise (e.g., use it to bring awareness to executives, assess the cyber response capabilities, and/or mature cyber security program)
- Gain organizational support and buy-in to conduct the exercise
- Identify a facilitator/observer who can be an objective party to assess if goals and objectives have been achieved
- Start planning the exercise by selecting and/or customizing select scenarios from the HITRUST CyberRX 2.0 Guide
- Identify location and medium for conducting the exercise (physical location and/or conference call)
- Schedule the exercise well in advance

Step 2: Conduct Exercise

- Selected facilitator would conduct the exercise by introducing the agreed upon scenario(s), and providing additional information at injection point, and keep the participants "on track"
- Organizational participants should be actively engaged by directing questions, identifying next steps, etc., as if the scenario is "real"
- Facilitator takes notes on strengths and challenges observed during the exercises



Step 4: Improve Cyber Security Program

- Based on lessons learned and cyber security program improvement opportunities identified, perform remediation, as applicable
- Plan for another simulation to measure progress, and for keeping the cyber security agenda on the "radar"

Step 3: Identify Lessons Learned

- The group conducts a debrief on observations and lessons learned
- Identify cyber security program improvements
- Facilitator sends a summary of the exercise conducted and lessons learned in a formal document
- If applicable, receive HITRUST Certification of Completion

What support will HITRUST provide?

HITRUST is providing this guide primarily for Level 1 participation (see *CyberRX Participation Levels*) to educate and provide materials that can be leveraged for planning and conducting the exercise. We highly recommend that your organization consider working with an external facilitator / observer who can guide the organization through the exercise as well as be an objective party. Contact any of the HITRUST CSF Assessor organizations if you or someone in your organization is interested in being an observer.

Do I need an external observer?

The HITRUST CyberRX 2.0 guide provides information that can be leveraged internally by an organization to conduct Level 1 exercise(s). If a HITRUST certificate of completion is desired and/or you would like an objective observer, your organization should leverage an external observer that is a HITRUST CSF Assessor organization.

How much will this cost?

The HITRUST guide is being provided complementary to all HITRUST members. Costs associated with any fees that may be charged by the selected observer will need to be negotiated and will vary based on the HITRUST CSF Assessor organization and participation level.

CyberRX Participation Levels

CyberRX 2.0 expands the CyberRX program into a three-tier program that supports organizations of varying cyber security sophistication levels/goals while helping evolve their cyber preparedness maturity to outpace increasingly complex cyber threats. An organization can receive a certificate of completion after each level of participation.

The three levels are as follows:

- **Level I - Local (Basic):** This level offers “table-top” simulations that can be administered by an organization to evaluate their cyber threat readiness and response that is primarily focused on internal processes.
 - **Eligibility:** Any healthcare organization and business associates can participate in Level I activities.
 - **Goals:** The Level I goal is for an organization to demonstrate, practice and improve basic cyber incident response capabilities and coordination. This level can be used as an educational awareness tool as well.
 - **Certificate of Achievement:** Organizations that successfully complete an exercise will receive a HITRUST CyberRX Level I Certificate of Completion which is a prerequisite to participate in more complex Level II/III exercises.
 - **Target Organization:** Level I is designed for healthcare organizations that are interested in increasing/maturing their cyber preparedness and are just beginning to implement a cyber-program. This level may also be used by more mature organizations who want to (1) practice on an internal, cost-effective basis or (2) use it as an opportunity to reinforce cyber awareness within their organization.
- **Level II – Regional (Mature):** Level II offers qualified participants the opportunity to exercise more sophisticated rapid detection, assessment, mitigation and response to cyber threats including coordination at the regional level. Equally important, this level expands the opportunity to enhance collaboration among participating organizations that share the same cyber security goals as well as promote partnerships that will improve the overall cyber security posture within the healthcare industry.
 - **Eligibility:** Organizations with a Level I Certificate.
 - **Goals:** The goal of the Level II exercise is to integrate healthcare organizations with mature cyber security programs into a more robust cyber incident that will challenge incident response procedures, hone their organizations skills against a realistic adversary as well as enhance industry information sharing and collaboration across the healthcare ecosystem.
 - **Certificate of Achievement:** Organizations that successfully complete an exercise will receive a HITRUST CyberRX Level II Certificate of Completion.

- **Target Organization:** This level is designed for healthcare organizations that have implemented cyber programs and safeguards. Many of these organizations will have adopted the HITRUST CSF and cyber threat monitoring capabilities in place.
- **Level III – National (Leading):** This level offers qualified participants a comprehensive simulation to evaluate internal and external cyber threat readiness, response and crisis management. It is anticipated that approximately 50 organizations will be selected in addition to the DHHS and HITRUST Cyber Threat Intelligence and Incident Coordination Center (C3) for participating in this event.
 - **Eligibility:** Any organization can participate in the Level III national CyberRX event with other industry leading organizations, HITRUST C3 and DHHS once an organization has achieved a Level II certificate from a HITRUST-sponsored regional event.
 - **Goals:** The Level III goals are for leading healthcare organization to: (a) demonstrate leading cyber prevention, response and threat intelligence practices; and (b) develop innovative information sharing models with government and across the healthcare ecosystem (c) continue to strengthen relationships and partnerships between leaders and rising healthcare organizations to fortify overall industry preparedness.
 - **Certificate of Achievement:** Organizations that successfully complete a national exercise will receive a HITRUST CyberRX Level 3 Certificate of Completion.
 - **Target Organization:** This level is designed for healthcare organizations that have very mature implementations of cyber security including cyber threat intelligence capabilities.

Participants seeking to progress to the next level of participation must obtain a certification of completion from the prior level. HITRUST will designate CyberRX observers, a list that currently includes all HITRUST CSF Assessor organizations. All organizations, directly participating or not, will also benefit from the CyberRX Exercise Playbook, a set of best practices developed in coordination with the CyberRX steering committee, HITRUST and DHHS.

Estimated Timing

We anticipate Level I exercises beginning in October 2014 with Level II starting in June 2015 and Level III is currently yet to be determined.

More information on the CyberRX program can be found at www.hitrustalliance.net/cyberx.

Participant Rules

Depending on the participation level and goals of the organization, a tabletop exercise will often be the format for conducting the exercise. Tabletop exercises can be effective when being applied in small groups of senior leaders addressing a focused issue or topic. Depending on the number of scenarios your organization decides to run, tabletop exercises can be conducted in a single day, half day or a few hours (e.g., 2-4 hrs), with the scenarios focusing on finite periods of time to address key issues (e.g., preparation phase and immediate response). Here are a few suggested guidelines:

For Participants: Participants may include representatives from Security/IT, Privacy/Legal/Compliance, business/HIMSS (and potentially others from Public Relations, Human Resources, Physical Security/Investigations and other areas, depending on your organization and scenarios selected). A facilitated group discussion allows participants to “stress test” plans or strategies to identify key issues or planning gaps.

The tabletop exercise format focuses necessary actions on specific points in time, key issues, dilemmas, or required decision points. The purpose of the format is to allow an organization to delve more deeply into and identify necessary actions, decisions, or lessons learned. This can be useful as the first stage in exploring and identifying various perspectives on new or evolving issues, or in assessing the status of current policies, governance and programs.

Things to keep in mind:

- As a participant in this exercise, participants will be asked to suspend reality and to not “fight the scenario.” There are often events in the real world that do not occur as one might expect. The intention of a tabletop exercise is not to argue about whether or not something might happen, but to explore how participants would act/respond if it did happen.
- Just as in the real world, participants may be required to make decisions with limited information. They will be required to use what information they have at hand and make the best decision they can.
- No Attribution. We recommend that discussion be on a non-attribution basis – outside of the exercise, participants are asked not to attribute any statement made or action taken during the exercise to any individual or program office/department.

For Facilitator: The facilitator's role is to outline the scenario, address questions to key participants, and identify additional issues. However, the facilitator does not provide the participants, or the organization with any "answers" to the exercise. There is often not a single right answer. It is up to the organization to determine the best approach and response for it. A facilitator can be from your organization or if a HITRUST CyberRX Level I Certificate of Completion is desired, the facilitator can be one of the HITRUST-approved CyberRX Facilitators.

Specific Facilitator expectations include:

- The role of the facilitator in a tabletop exercise is threefold: advisor, counselor, and analyst. As an advisor, the facilitator tracks the accomplishment of events related to exercise objectives, offers advice, keeps the discussion on the right track, and ensures the participant group is not wasting time on tangential issues.
- The facilitator is the only one giving full attention to the process. As a counselor, the facilitator must remember that his/her role is not about imparting information, but rather drawing out information by asking the right questions and acting as the "devil's advocate."
- As an analyst, the facilitator will interpret the rationale for the group's discussion and ultimately assess the participant's efforts based on the scoring rationale described in the next section.
- **Briefing Scenario:** The facilitator will brief the scenario content and desired exercise objectives to the participants and offer updated information based on the scenario's "playbook". Each scenario will have associated discussion questions to draw out key decisions and required actions from the participations. It is more important to understand the process and rationale leading up to "why" an action/decision was made rather than the actual decision itself. The facilitator should use these questions to drive the discussion.
- **Group Discussion:** We recommend giving the group time to adjust to the discussion in a tabletop exercise setting and then focusing the discussion on key decisions related to the agenda. However, it is important that the participants (not the facilitator) make the determinations on prioritizing decisions within the exercise.

Things to keep in mind:

- The facilitator will not PARTICIPATE in this exercise. He/she is a NEUTRAL OBSERVER, so it is important for the facilitator to remain unbiased, observe, and resist the temptation to interject his/her own solutions/opinions. When conducting the exercise, the facilitator should:
 - Remember that silence and pauses in the conversation can be a good thing as it may encourage participants to speak
 - Start the discussion with broad questions, then narrow down to the questions which need to be addressed in the move

- Insert him/herself in the discussion only to (1) clarify specific points in the scenario itself (2) ensure the team is considering all aspects of the issue and (3) keep the scenario from bogging down.
- Discourage participants from stating conclusions without providing the rationale for them
- Ask participants to explain how their response would work in the given timeline and who would be responsible for each decision or action
- The facilitator can answer basic questions from the participants, but cannot embellish his/her answer. Any interjections should be general in nature to invite deeper discussion and inquiry from the participating individuals.
- The facilitator should take notes throughout the exercise on what he/she observes, to include capturing best practices/lesson's learned. It is critical to the hotwash debrief that the facilitator records both what was done and what was not done by the participants. These observations are critical to realizing the full value of this exercise.
- The facilitator should encourage participants to have fun and keep the mood productive. We anticipate that when an organization exercises these communication links and systems we will find gaps in its processes. No one should feel poorly about the results. The goal is to improve security in this critical national asset called Healthcare.

Scoring Construct and Rationale

HITRUST CyberRX Level I Certificate of Completion and Scoring

To ensure consistency across the industry and all Level I exercises, facilitators will assess participant organizations on specific markers (“key building blocks”) to assess the strength of the organization’s cybersecurity program and efforts.

In order to earn a HITRUST CyberRX Level I Certificate of Completion and be considered eligible for the Level II exercise, participant organizations working with a HITRUST-approved facilitator must meet seven (7) of the ten (10) markers.

If your organization does not meet this requirement at the time of the war game, it can improve its program based on the war game findings and recommendations, and provide supplemental evidence of such enhancements to the facilitator to earn a certificate of completion for the organization.

What are the 10 Markers?

The following ten (10) markers are typical industry practices and are key activities, policies, or products to strengthen an organization’s cybersecurity capabilities:

Marker	Goal	Example evaluation criteria*
1. Governance/People	Is the organization able to identify and bring the right people to control/remediate the cyber incident (e.g., representatives for privacy, security, PR, legal, HR, etc.)?	<ul style="list-style-type: none"> • Were key roles and responsibilities defined and understood? • Was there communication of these responsibilities outside of the security group (or whichever group assigned the roles)?
2. Incident Response Policy and/or Guidelines	Does the organization have written processes or guidelines for incident response triage, command and control, breach response, reporting, incident notification, authorities and long term remediation/resolution?	<ul style="list-style-type: none"> • Were the processes and responsible parties for reporting and notification clear? • Was the documentation process clear? • Does the policy comply with the latest requirements under Omnibus Rule (e.g., 4-point test for non-disclosure)?
3. Internal Communications and Escalation	To ensure proper coordination and choreography, was an incident properly communicated across the entire organization, as appropriate (e.g., to Privacy/Legal/Compliance) and escalated to the business and senior management?	<ul style="list-style-type: none"> • Often communication outside of Security is delayed. Was that the case in this exercise? • Was communication protocol clearly understood among participants? • Was there a discussion of the protocols to follow, such as involving the legal team, for the purposes of maintaining legal privilege?
4. Training	To communicate expectations, does the organization have a written training plan in place for breach identification, reporting and subsequent remediation?	Does it appear the organization participants have been trained on incident response?

Marker	Goal	Example evaluation criteria*
5. Information Sharing	To help anticipate general and industry-specific threats, does the organization subscribe to and/or use threat intelligence?	Does the organization receive and leverage industry-specific threat information to better understand the risks in order to take appropriate actions (e.g., subscribe to HITRUST threat intelligence, and/or connect with peers)?
6. Vulnerability & Threat Management	<ul style="list-style-type: none"> • To minimize intrusions and incidents does the organization conduct periodic attack and penetration testing, cyber tests, intrusion detection, or other similar testing? • Does the organization have a process that requires such testing? 	<ul style="list-style-type: none"> • Did the organization refer to or leverage information from its vulnerability management processes during the war game play and response? • Does the organization have, and did the organization leverage, any advanced persistent threat (APT) scans, malware forensics, and related information for assessing and responding to the situation?
7. Asset Management and Asset/ Data Inventory	To quickly and more accurately assess whether an organization could be impacted by a threat (including where it occurred and to what extent), does the organization maintain an asset inventory of key system/repositories, including mobile devices, medical devices containing PHI along with the accountable individual(s) responsible for knowing their location?	Does the organization have and leverage an inventory repository in order to assess the risk, impact, and/or conduct further analysis during the exercise?
8. Vendor assessment	To identify potential third party risks, does the organization have an inventory of key business associates and have business associate agreements in place with them? Does the organization have a process in place for maintaining such inventory?	<ul style="list-style-type: none"> • Does the organization have a vendor assessment process included as part of its cyber programs? • Are vendors included in the organization's incident response processes? • Are vendors aware of their roles in the incident response processes? • Have your organization's business associate agreements been updated to comply with Omnibus Rule requirements for business associates?
9. Lessons Learned	To identify and prevent recurring incidents and potential vulnerabilities, does your organization maintain a log of incident/ breach resolutions and lessons learned?	Does the organization discuss and attempt to capture lessons learned from the exercise?
10. Updating plans and policies	To address and respond to changes in business operations, technology and/or new cyber threats, does your organization have a process to annually review and update its incident response and security/ cyber plans, policies, and trainings?	Did the organization discuss about updating its training or its security program to reflect lessons learned from this and/or previous incidents?

** All evaluation markers may not directly apply to a selected scenario. However, evaluation criteria may be assessed directly or indirectly depending on the selected scenario (e.g., if a scenario is about malware infection on a device, marker #7 can be assessed based on whether the asset inventory is referred to for checking potential infections on other devices during the exercise). The questions are examples, and there will be some judgment involved.*

CyberRX Playbook v2.0

Exercise Participants

The CyberRX exercises are designed to affect each participant and in some cases require senior leadership involvement. The exercises target healthcare organizations and their business partners of varying types and sizes, explicitly the following participants:

- Providers – hospitals, clinics, rehabilitation centers, long term care, nursing homes, outpatient services, surgery and urgent care centers
- Retail and mail order pharmacies
- PBMs (Pharmacy Benefit Managers)
- Health Plans
- Medical Research and clinical trial organizations
- Business associates
- General health organization

Complexity of Exercises

The CyberRX exercises are rated by complexity going from the least complex, one star (★), to most complex, three stars (★★★).

Exercise 1 ★

Your hospital utilizes an electronic health record system for managing patient care. Over the last week, a number of patients experience a severe drug reaction while admitted to the hospital. The number of instances appears to be significantly more than usual.

Status	Description
	Injection 1: Upon investigation it is determined that the patient’s electronic medical records didn’t list their drug allergies.
	Injection 2: Clinicians report also that drug allergies are missing from an EHR system and documentation demonstrates they were entered into the system 11 days ago.
	Injection 3: Upon investigation it is determined that the patient’s electronic medical records were changed, but the user ID in the change log is blank.
	Injection 4: Upon further investigation, you also find other unexplained data discrepancies within electronic medical records.
	Injection 5: HITRUST C3 publishes a report indicating a US hacker is targeting U.S. healthcare organizations with the intent to disrupt operations and erode consumer confidence by manipulating medical information.

Assumptions Made by the Organization During the Exercise

Positive Observation	Areas for Improvement

Exercise 2 ★

Your organization is notified by an external party that your organization’s network diagrams (including IP addresses, Access Control List, and firewall rules) have been posted on the public GlueBin website.

Status	Description
	Injection 1: The IP that GlueBin has recorded is that of a foreign holiday resort.
	Injection 2: Combing through the log files, you identify a webmail client connection from the same IP address. Your organization’s webmail requires a hard token to access.
	Injection 3: A senior staff member has a timeshare at this resort and frequently uses their business center. You interview him and you find out that he was at the resort at the time of the posting to GlueBin but says he did not post anything to the GlueBin website.
	Injection 4: The senior staff member tells you that he also accessed the free wireless internet provided by the resort with his work laptop.
	Injection 5: You continue to monitor the GlueBin website and see additional organizational information posted to the Gluebin website using the same IP address.
	Injection 6: You also determine that all the files posted to the GlueBin website were also in email attachments inside the senior staff member’s mailbox prior to his trip to the resort.

Assumptions Made by the Organization During the Exercise	

Positive Observation	Areas for Improvement

Exercise 3 ★

The hospital administration receives a call from Softco Software's President and is informed that computers from the hospital have been performing attacks on Softco Software's website for the last two weekends. Softco is asking for an explanation before taking action on it.

Status	Description
	Injection 1: You examine your network log and find a large amount of traffic directed towards Softco Software's website.
	Injection 2: You examine one of the internal computers identified by the network log and find an unfamiliar program running on the machine which is connected to an IP address in Canada on TPC port 6667 (IRC).
	Injection 3: You conduct a forensic exam on the machine and find out that this program was created a month prior to when a program called "super gem sorter vision quest.exe" was executed.
	Injection 4: Your examination also showed that the program was deleted but it was originally downloaded to the computer from an email attachment.
	Injection 5: You locate the email with the attachment and its subject line read "Really fun game and remember to pass it along to your friends." The email came from a .cc version of your domain that looked like your CIO's email address.

Assumptions Made by the Organization During the Exercise

Positive Observation	Areas for Improvement

Exercise 4 ★

A blood gas analyzer in your organization is indicating high sodium readings for a large number of patients. This device is isolated and not connected to a network.

Status	Description
	Injection 1: A lab technician is alerted to abnormally high sodium readings during blood gas tests and takes the device out of service.
	Injection 2: You perform troubleshooting procedures, but can find nothing to explain the erroneous readings.
	Injection 3: You also check the maintenance records and they demonstrate that the device passed initial testing when it first came in. The device also has been recently patched and its operating system and software are up to date.
	Injection 4: You call the vendor and a field technician is sent to your location and they determine that there is malware on the stand alone device. The creation and last modified date of the malware matches the same date as the last patch was installed on the blood gas analyzer.

Assumptions Made by the Organization During the Exercise

Positive Observation	Areas for Improvement

Exercise 5 ★

Your organization is using a custom Health Management and Billing software for their caregivers in the field. This software package has an internet facing webpage front end and a SQL server on the back end. Within the last two weeks all of their billing submissions to Medicare have been rejected due to missing procedure codes.

Status	Description
	Injection 1: You call the software vendor and they explain that the procedure codes are required fields and all of the procedure codes are hard coded into the webpage.
	Injection 2: You examine the SQL tables and find all the entries in the procedure code table have been deleted. You also look at the audit table and it only contains entries for the last two weeks.
	Injection 3: Upon examining the SQL server you find a large file containing the patient table stored on the root of the c: drive.
	Injection 4: You examine the web page and discover that the caregiver login name field did not perform data validation and allowed SQL statements to be sent to the SQL server.

Assumptions Made by the Organization During the Exercise

Positive Observation	Areas for Improvement

Exercise 6 ★★

Your organization is reviewing its financial records and finds \$100,000 missing from its medical equipment procurement account.

Status	Description
	Injection 1: Your audit department reviews all recent authorized orders and it confirms the missing \$100,000 as a discrepancy in the account.
	Injection 2: Your audit department contacts your organization’s bank and finds 10 payments of \$10,000 to overseas bank accounts that were unauthorized. All of these payments were made by the same procurement manager.
	Injection 3: You interview the procurement manager who claims that they never made those payments.
	Injection 4: You conduct a forensics exam of the procurement manager’s computer. During your exam, you find that the web browser on their computer was not configured to receive updates and the computer was infected with malware.
	Injection 5: You also find the malware came from a faked web site designed to look like AwesomeHealthSpace.com a popular social media site for the health care industry. In addition, you find an email with the link to the fake web site that was also located on the computer inside the procurement manager’s inbox.

Assumptions Made by the Organization During the Exercise	

Positive Observation	Areas for Improvement

Exercise 7 ★★

Your organization has outsourced its mobile application coding and hosting to a popular third-party vendor who specializes in mobile health applications. You hear on the news that there was a breach of the third-party vendor’s network (i.e., the mobile health application vendor), but the vendor has not reached out to your organization yet.

Status	Description
	Injection 1: You read a report on a security blog that your organization’s customer data has been exfiltrated for months and unknown individuals have had full access to your customer’s personal data. You contact the vendor and they assure you that their networks are secure.
	Injection 2: The third-party vendor launches an investigation. It discovers that one of their developers had implanted a backdoor in a common application code library which is used in multiple products of theirs, including the one utilized by your organization.
	Injection 3: You are contacted by the DHHS Cyber Threat Analyst Center and they inform you that they have identified the blogger as a member of a Chinese hacktivist group.
	Injection 4: Several media outlets publish the blogger’s claim.
	Injection 5: Your organization starts receiving customer complaints and so does the DHHS Office for Civil Rights (OCR) regarding the breach.

Assumptions Made by the Organization During the Exercise

Positive Observation	Areas for Improvement

Exercise 8 ★★

Your organization specializes in outpatient service and is notified that 150,000 records relating to 100,000 of its patients have been accessed by an unauthorized party through a health information exchange (HIE).

Status	Description
	Injection 1: The local media releases the news of the breach and requests comment from your organization.
	Injection 2: Your organization receives an email requesting one million dollars be transferred within eight hours to a foreign account or the perpetrator will release the information.
	Injection 3: You quickly conduct an investigation into the claim. You determine that a former foreign contractor has accessed some of the records possibly using an admin account that was shared among IT professionals supporting the HIE.
	Injection 4: You discover that the foreign contractor is no longer within the United States and is in a country without an extradition treaty.

Assumptions Made by the Organization During the Exercise

Positive Observation	Areas for Improvement

Exercise 9 ★★

Your organization is alerted that medical images of your patients are starting to show up on the 5chun discussion board.

Status	Description
	Injection 1: You are able to determine that all the records have the same physician in common.
	Injection 2: You determine that the leaked data includes 50 records from patients under the age of 18.
	Injection 3: You interview the physician and he informs you that he connects his tablet to his work PC with auto-sync enabled for viewing patient data and has synced more than 2000 records.
	Injection 4: During your interview, the physician also tells you that he cannot find his tablet, and it appears to be missing. Your asset management system shows that his tablet was encrypted with a password. You ask the physician how strong of a password he used and he tells you that he used "PASSWORD".
	Injection 5: Your network logs show that his tablet has been beaconing home and is now in a neighboring state.

Assumptions Made by the Organization During the Exercise

Positive Observation	Areas for Improvement

Exercise 10 ★★ ★

A law enforcement agency informs your organization that a copy of your EHR database has been found on a seized system.

Status	Description
	Injection 1: The seized system also contained source code for the EHR system.
	Injection 2: The application and compromised data is hosted by a cloud service provider (CSP) and does not reside inside of your network. The CSP provides Infrastructure as a Service (IaaS) hosting.
	Injection 3: The CSP claims no responsibility for breach notification or monitoring since the breach was at the application level. The CSP provides the access logs of the management console. There are unaccounted for connections from outside your network.
	Injection 4: During the forensic investigation of the CSP hosted EHR system you identify numerous failed log in attempts recorded 3 months ago to the web front end of the EHR application, and then a dramatic drop in the number of attempts. The initial forensics investigation of the machine images hosted at the CSP reveals that the CSP management console and the web front end server shared passwords.
	Injection 5: There is a direct link to link connection from your network to the CSP. Your forensics investigation reveals that there were unauthorized access attempts into your network from the CSP IaaS environment.

Assumptions Made by the Organization During the Exercise

Positive Observation	Areas for Improvement

Exercise 11 ★★

Three patients undergoing radiation therapy at your organization immediately start to show signs of symptoms of severe radiation sickness after receiving treatments from your organization. A doctor was called in to examine these patients and he determined that they all received unsafe levels of radiation during their treatment.

Status	Description
	<p>Injection 1: Your Oncology department runs a diagnostic, which does not identify any problems, but manual testing shows unsafe treatment levels. The manufacturer sends a technician who cannot find any issue with the system, but suspects sabotage and notifies the FDA. The FDA then brings in the FBI to conduct an investigation.</p>
	<p>Injection 2: Investigation by FBI highlights the fact that the console for the treatment management system which was used by the radiation therapy equipment to maintain patients' data and administer dosage was running on an operating system past its patch life cycle. Your organization had not upgraded or patched the system recently.</p>
	<p>Injection 3: The company who made the treatment management system is the only provider of patches for the system. The treatment management system also could only be run on its current operating system. The system had not been patched since it was installed.</p>
	<p>Injection 4: Your investigation reveals that the treatment management system was not listed on any security asset list and had not been scanned for vulnerabilities.</p>
	<p>Injection 5: FBI detects malware in the radiation therapy equipment. The malware had AV avoidance/ disabling features which also disabled other system safeguards leading to the over exposure. None of the equipment vendor's supplied patches would have prevented the malware from disabling the safeguards.</p>

Assumptions Made by the Organization During the Exercise

Positive Observation	Areas for Improvement

Exercise 12 ★★

A web application vulnerability/exploit has been published at DefCon for a common piece of open source software which is the base of many security tools and software applications. The software is used for input with establishing encrypted connections.

Status	Description
	Injection 1: The vulnerable open source software is integrated into the solutions provided by multiple security vendors. One of your staff, who attended DefCon, checks your systems and finds many of the webservers, VPNs, & firewalls utilize this tool.
	Injection 2: The vulnerability has been there for at least two years but has only recently been brought to public attention.
	Injection 3: Your staff recommends migrating your organizations' webservers to a competing secure fork but you are unable to secure the VPN and firewall. Both of these are dependent on the manufacturer for updates.
	Injection 4: The firewall starts detecting a high number of attacks on the VPN, trying to exploit the vulnerability.
	Injection 5: The firewall is past end of support and the manufacturer is no longer updating the OS.

Assumptions Made by the Organization During the Exercise

Positive Observation	Areas for Improvement

Exercise 13 ★★★

You receive an automated alert that a medical information database was accessed between 1:00am – 3:00am. There was no scheduled maintenance overnight.

Status	Description
	Injection 1: You find a log file indicating that the database was accessed by the default administrator account.
	Injection 2: The Database Administrator determines that the account name was "administrator" and the password "admin2014".
	Injection 3: The database contained prescription and demographic information on a large number of patients.
	Injection 4: The database also includes financial information that your organization had no authority or legitimate reason to collect. The collection of the information was contrary to your organization's privacy policies, and the public is unaware that this additional information was collected.

Assumptions Made by the Organization During the Exercise

Positive Observation	Areas for Improvement

Exercise 14 ★★ ★

A Security Information and Event Management system (SIEM) at your organization alerts on a connection and the transfer of large amounts of data to StopBox, a cloud storage hosting service. The transfer is ongoing.

Status	Description
	Injection 1: Your network administrator attempts to block StopBox, but discovers that StopBox is similar to VOIP software that has firewall avoiding technology. The StopBox traffic is encrypted and can utilize peer-to-peer communication. Your network administrator also discovered that several executives were using StopBox.
	Injection 2: You trace back the traffic and identify that a clinical intern was responsible for the data transfer. The intern was using PII data for research on their home computer. You confront the intern. She apologizes and promises to delete all the data off of StopBox. She also states that she will delete the data off her home computer once she receives it back from the NerdHerd technicians repairing it.
	Injection 3: StopBox has a restore feature for deleted files that cannot be disabled.
	Injection 4: The intern informs you that NerdHerd had to perform a full system restore due to malware they found on it.
	Injection 5: You receive word that a patient with a unique name who has a google alerts set for their name has received notifications of their PII being posted. They have reached out to your organization for clarification.

Assumptions Made by the Organization During the Exercise

Positive Observation	Areas for Improvement

Example Scenario Run Through

In this section we will run through a scenario as an example. This example is designed to foster thought and get your organization thinking about the risks, issues, and the parties involved that each unique scenario may bring to bear.

This example should not be thought of us as a prescriptive way of running the exercise. Organizations are encouraged to bring their unique skills and experience to bear to ensure the uniqueness of your organization is reflected in the exercise.

This section includes an Exercise Planning Checklist and a table of Sample Issues and Questions that may have been identified during the Sample Exercise explained below.

Sample Exercise ★ ★ ★

Monday morning your IT helpdesk receives a call from Dr. Jane and she informs them that her encrypted laptop was stolen from her home during a burglary. Your helpdesk is also informed that a USB drive was in the laptop, but she doesn't recall what is on the device. Additionally, she reveals that she had written her user name and password on a note next to the laptop.

Status	Description
	Injection 1: IT helpdesk logs a ticket for a stolen laptop in the ticketing tool and notifies the information security, compliance, and privacy offices.
	Injection 2: The privacy office contacts the police which confirm that they did receive a call from Dr. Jane reporting a burglary at her residence at 2:00am on Saturday.
	Injection 3: You perform a risk assessment which reveals that the laptop contained specific patient data such as lab testing, treatment and diagnosis data related to a new drug trial.
	Injection 4: You determine that her laptop also had social security numbers and other PII which should not have been collected on about 10,000 individuals. Dr. Jane was not authorized to have this information.

Exercise Run Through

Step	Description	Notes
Conduct the Exercise	Introductions	<ul style="list-style-type: none"> • Have participants introduce themselves and their role in the exercise
	Explanation to Participants	<ul style="list-style-type: none"> • Explain the exercise • No time pressure • No right or wrong answer • Exercise designed to stimulate discussion • Treat it as a real scenario
	Begin Exercise	<ul style="list-style-type: none"> • Facilitator introduces the scenario • Let discussions evolve naturally • Identify risks and issues, steps to be followed, etc. • Identify internal and external participants in the scenario • Use non-leading questions to stimulate conversation. For example, "what would you do this in this situation?" • Facilitator will provide injections as needed
	Document the Exercise	<ul style="list-style-type: none"> • Take notes during the discussions • Forms a basis for after exercise review • Note areas that need more research • Summarize take home points • Document issues identified
Evaluate the Exercise	After Exercise Review	<ul style="list-style-type: none"> • Give participants a 10 to 15 minute break • Review exercise objectives again • Solicit participant feedback • Document conclusions or decisions from the exercise • Document the organization's maturity level by using the 10-Markers system starting on Page 12.
Post Exercise Activities	Develop Corrective Action Plan Track Corrective Action Track Lessons Learned	<ul style="list-style-type: none"> • Track and remediate corrective actions • Document remediation and lessons learned • Save results for next CyberRX exercises

Sample Issues and Questions Identified During the Exercise

Sample Issues/Questions

1. How were the information security, compliance, and privacy offices notified? Via email, cell phone, text?
2. Do the information security, compliance, and privacy offices know what to do once they are notified?
3. Who takes the lead in your organization when an incident occurs?
4. What is the internal SLA within the organization to respond to a breach?
5. Does the organization have an incident response calling tree that is provided to the Help Desk?
6. Was the organization's Incident Response Plan put in action?
7. Did the team meet virtually or in-person?
8. How often does the team reconvene to discuss the breach?
9. Was there an asset inventory record for this laptop?
10. Was the laptop encrypted? How was this determined?
11. Was the USB encrypted? How was this determined?
12. How was the data contained on the laptop verified?
13. Can the laptop be remotely wiped?
14. Does the laptop have a LoJack type device?
15. Why did Dr. Jane take so long to notify the organization of the breach? What is the required timeframe for reporting a breach?

16. Was there a legitimate business reason for Dr. Jane to have the PHI data on her laptop?
17. When was the last time that Dr. Jane received security awareness training?
18. Is there a signed employee agreement on file for Dr. Jane where she agrees to abide by the organization's policy and procedures?
19. Does your organization have an employee sanction policy?
20. Was Dr. Jane disciplined per the employee sanction policy?
21. What was law enforcement's role in this breach?
22. What breach notifications were sent out by the organization?
23. What external organizations were notified of the breach?
24. Was internal and/or external counsel notified and involved in the breach?

Appendix A – About CyberRX

Background, Overview and Lessons Learned

Launched in January 2014, in response to growing concerns within the industry and government regarding the current state of cyber threat preparedness and response through a partnership of HITRUST and the U.S. Department of Health and Human Services (DHHS) as an industry-wide effort to conduct exercises to simulate cyber-attacks on healthcare organizations and government with the results used to evaluate the industry's response and threat preparedness against attacks and attempts to disrupt U.S. healthcare industry operations.

CyberRX includes the participation of providers, health plans, prescription benefit managers, pharmacies, medical and pharmaceutical manufacturers, and government agencies such as the DHHS. The program includes scenarios that examine both broad and segment-specific scenarios targeting information systems, medical devices and other essential technology resources of the healthcare industry.

The CyberRX program is overseen by a steering committee comprised of representatives from industry, in addition to HITRUST and DHHS. There are working groups established with industry representatives and other subject matter experts (as well as HITRUST and DHHS representation) to develop and maintain the program playbook that outlines the rules, responsibilities, and scenarios of the exercise and organizational referees.

The inaugural Spring 2014 exercise held on April 1, 2014 was a full-day interactive simulation observed by Booz Allen Hamilton. The scenarios examined both broad and segment-specific scenarios targeting information systems, medical devices and other essential technology resources of the healthcare industry. The participants were made of up leading healthcare providers, health plans, prescription benefit managers, pharmacies, HITRUST Cyber Threat Intelligence and Incident Coordination Center (C3) and DHHS. From the Spring 2014 exercise, there were several lessons learned, including:

- Allow for broad industry participation to ensure healthcare organizations of all sizes and types can effectively mitigate the risks posed by cyber threats.
- Create events and simulation scenarios of various and increasing levels of sophistication to keep pace with mounting, increasingly complex cyber threats.
- Include heightened use of HITRUST C3 cyber threat intelligence, and industry collaboration and incident response capabilities as a means to better inform and promote information sharing across the healthcare ecosystem.
- Ensure an industry framework exists that incorporates cyber threats that are comprehensive and up to date. HITRUST has committed to linking cyber threat intelligence to CSF controls and publishing monthly supplemental control guidance when compensating controls are found to be deficient, and updating the CSF controls based on this guidance.

The complete findings for the Spring 2014 exercise are available at www.hitrustalliance.net/cyberrx/.

Based on the success of the healthcare industry's first CyberRX exercise and incorporating observations and findings relating to the program, HITRUST, in coordination with DHHS, is launching CyberRX 2.0.

Following the success of the first CyberRX exercise, more than 1000 healthcare organizations of various sizes and level of cyber maturity signed-up to participate in the next exercise. As a result, the steering committee wanted to establish a CyberRX 2.0 exercise approach that supports a large percentage of the healthcare industry, allows organizations with varying levels of knowledge and resources to engage in and benefit from the program, while not burdening or minimizing the value to other participants.

In order to accommodate the larger than anticipated number of participants the program has been expanded. CyberRX 2.0 is a three-tier program that supports organizations of varying cyber sophistication levels while helping evolve their cyber preparedness maturity and keep pace with mounting, increasingly complex cyber threats to the healthcare industry.

Appendix B – Acknowledgements

Working Group Representation

Many individuals and organizations provided input into the playbook, but those Individuals responsible for directly contributing to the development of the CyberRX 2.0 Playbook were affiliated with the following organizations:

- Amazon
- Booz Allen Hamilton
- ComplySmart
- Deloitte & Touche
- HITRUST
- Medtronic
- UnitedHealth Group
- U.S. Department of Health and Human Services (Office of the Chief Information Officer)

More information on the CyberRX program can be found at www.hitrustalliance.net/cyberx.



855.HITRUST

(855.448.7878)

www.HITRUSTalliance.net