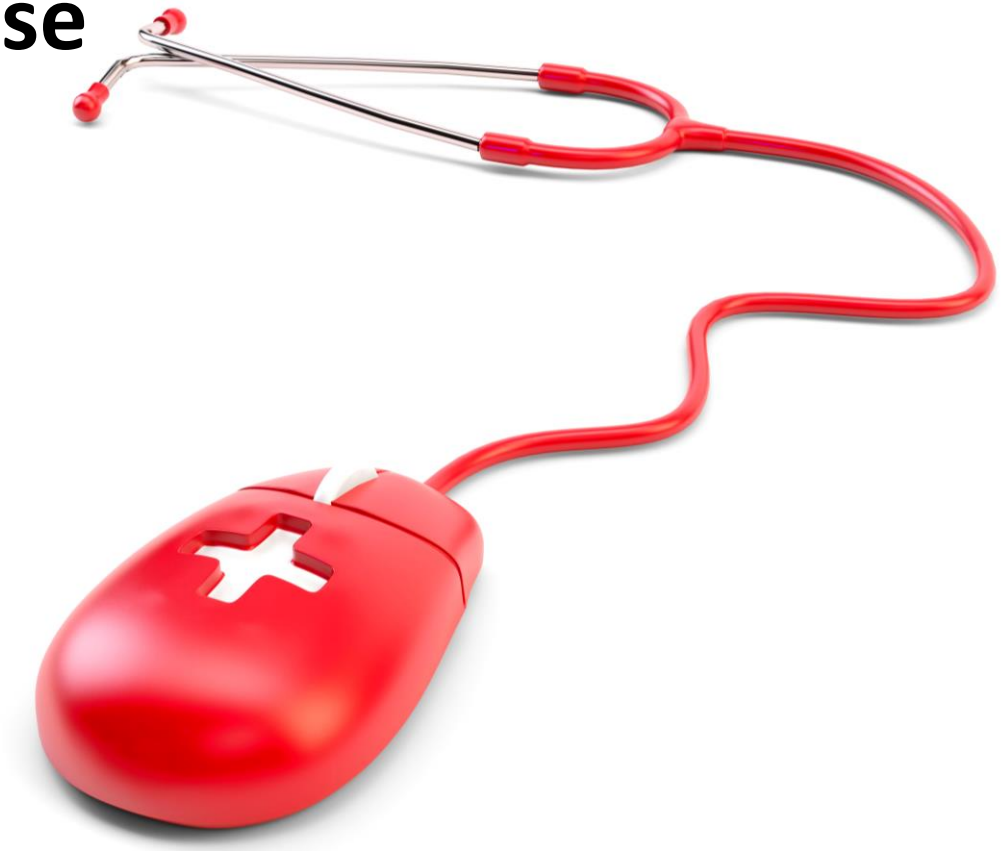
HITRUST
Health Information Trust Alliance

Deloitte.

CyberRX: Health Plans Cyber Simulation Exercise

After-Action Report



December 2015

Contents

1 Executive summary

2 Background

3 Exercise design

4 Observations

5 Recommendations

6 Key takeaways

7 Acknowledgements

8 Next steps

HITRUST Health Information Trust Alliance Deloitte.

Executive summary

CyberRX is a series of no-cost, industry-wide exercises created and coordinated by HITRUST in conjunction with the Department of Health and Human Services (HHS), with the mission to mobilize healthcare organizations and explore innovative ways of improving preparedness and response against cyberattacks intended to disrupt the nation's healthcare operations. C*yberRX: Health Plans is a cyber simulation exercise designed specifically for health plans and insurers. The exercise was facilitated and observed by Deloitte Advisory.*

Exercise overview

Objective

- To provide participants the opportunity to test their cyber incident readiness and to identify ways to enhance existing cyber incident response plans and processes

Participants

- 250 individuals from 12 health plans across 13 US states

Delivery structure

- During a four-hour session, participants responded to systematically delivered cyber incident simulation content, discussing necessary response actions and key decisions to be made

Simulation scenario

- A threat actor compromised the systems of a fictitious health plan company, gaining access to member protected health information (PHI) and initiating fraudulent health claims on a mass scale

Participant learnings

The nature of cyber incidents

- Cyberattacks are becoming increasingly pervasive and sustained, and can quickly escalate into significant business crises.
- Open and accurate lines of communication are critical components of incident response and should consider internal parties, third parties, law enforcement and government agencies

The cyber incident lifecycle

- Cyber incidents can take months or years to recover from – recovery objectives must factor in both capabilities enhancements as well as confidence enhancements
- Incident response requires cross-functional coordination, documentation, and stakeholder communication

Planning for cyber

- It is imperative that incident response plans include specific communication and team processes
- Simple, flexible and distributed plans provide guidance to responsible parties throughout the organization
- Understand where and when outside help is needed to assist and have a way of getting these capabilities beforehand
- Regularly conducting cyber simulations will build muscle memory among cyber incident responders

HITRUST Health Information Trust Alliance Deloitte.

Background – *introduction*

In April 2015, HITRUST, Deloitte Advisory, and a planning committee initiated planning for the *CyberRX: Health Plans Cyber Simulation Exercise* with the goal of exercising the capabilities of a group of health plans to respond to a wide-scale cyberattack.

Exercise motivation

Recent events have raised awareness of the increase in cyber threats and attacks targeted at the health plan industry. Cyberattacks provide little forewarning and can occur suddenly or over a period of time. This variability requires health plans to focus on cyber incident readiness, response, and recovery.

About CyberRX

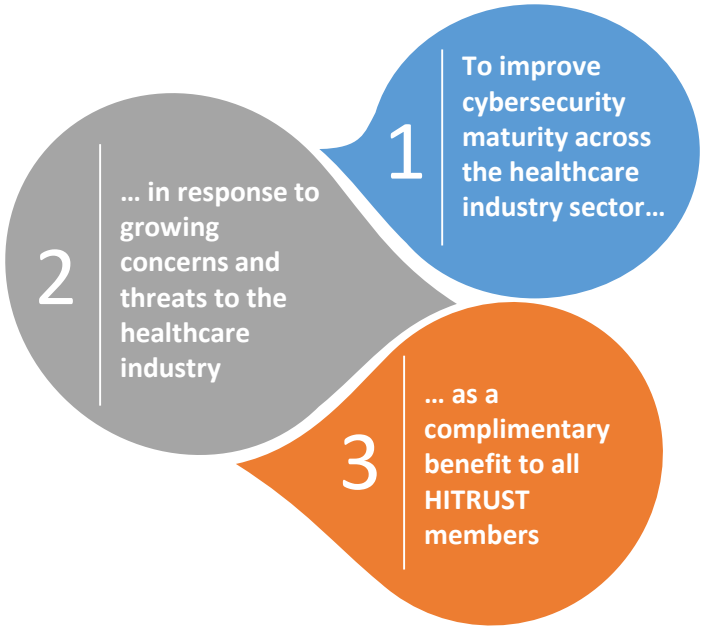
CyberRX 2.0

CyberRX 2.0 is a scenario-based exercise program to assess the cybersecurity response preparedness of healthcare organizations.

The Team

The **CyberRX** program is overseen by a steering committee comprised of representatives from the healthcare industry, **HITRUST**, and **HHS**.

Purpose of CyberRX



HITRUST Health Information Trust Alliance Deloitte.

Background – *objectives*

The *CyberRX: Health Plans Cyber Simulation Exercise* was a four-hour event designed to explore the current state of health plan industry resilience and to achieve four key objectives:

HITRUST Health Information Trust Alliance Deloitte.

Exercise design – *delivery model*

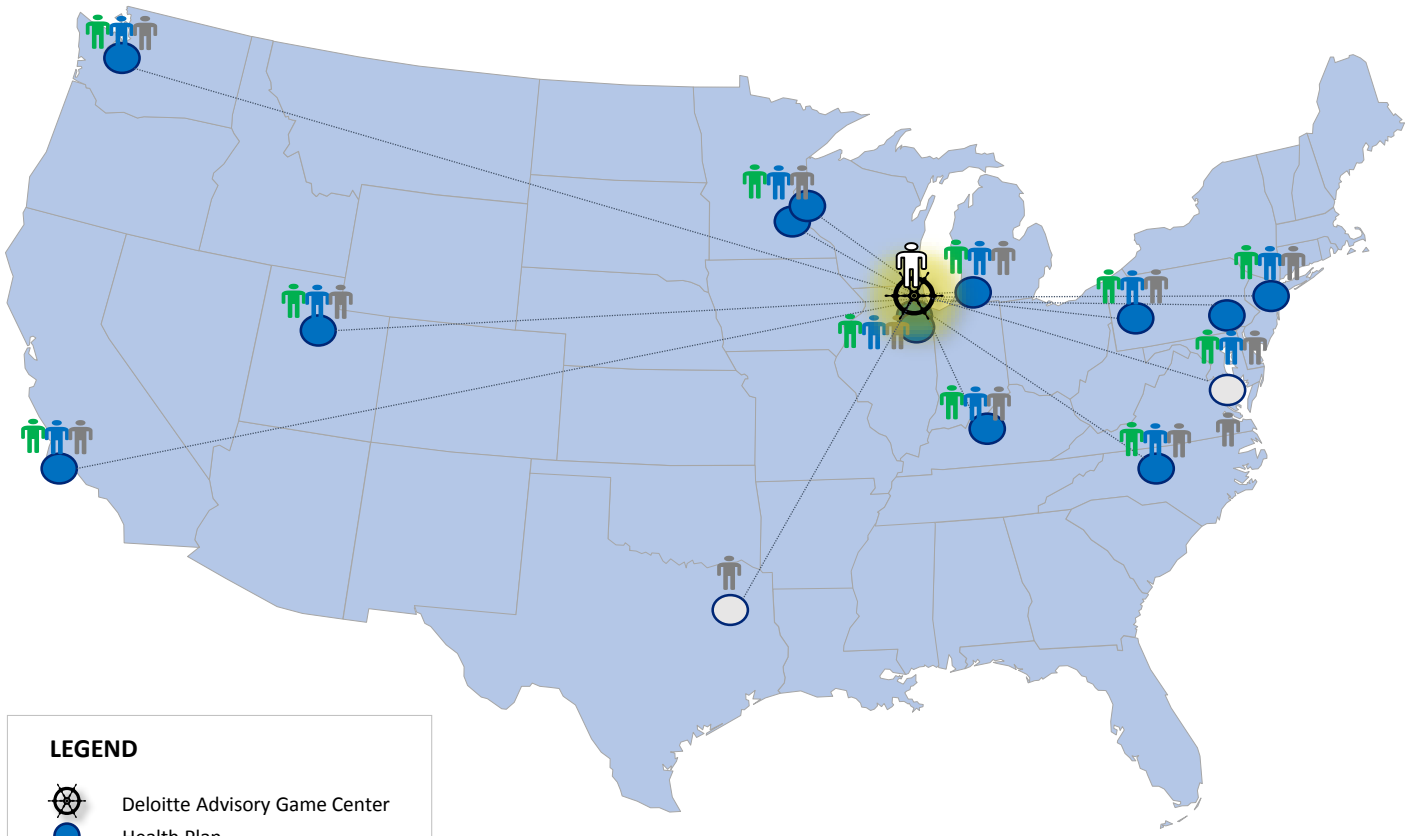
12 Health Plans • 250 Participants • 13 US States

BLUE TEAM
Wargame **players** that responded to exercise injects

WHITE TEAM
Wargame **facilitators** that managed direction, pace and content of the exercise

GREEN TEAM
Onsite **referees** that worked with the facilitators to manage the exercise

GRAY TEAM
Stakeholders that observed player decisions and actions



HITRUST Health Information Trust Alliance Deloitte.

Exercise design – *simulation scenario*

The *CyberRX: Health Plans Cyber Simulation Exercise* simulated an unauthorized access to claims processing and fraud analytics engines. In the process, the perpetrator gained access to member protected health information (PHI) and subsequently submitted fraudulent health claims.

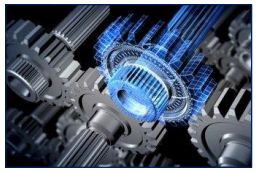
1

Following a premeditated carjacking, a laptop is stolen from an employee of a third-party vendor.

2

A cyber criminal organization gains access to patient records and the fraud analytics engine.

3



Back-end of fraud analytics engine is altered to approve targeted false claims.

4

False insurance claims are submitted and approved.

5

Claims payments sent to fictitious providers result in millions of dollars in losses.

6

Members receive record of claims indicating payment for services which were never rendered. False claims reported to call center by the members.

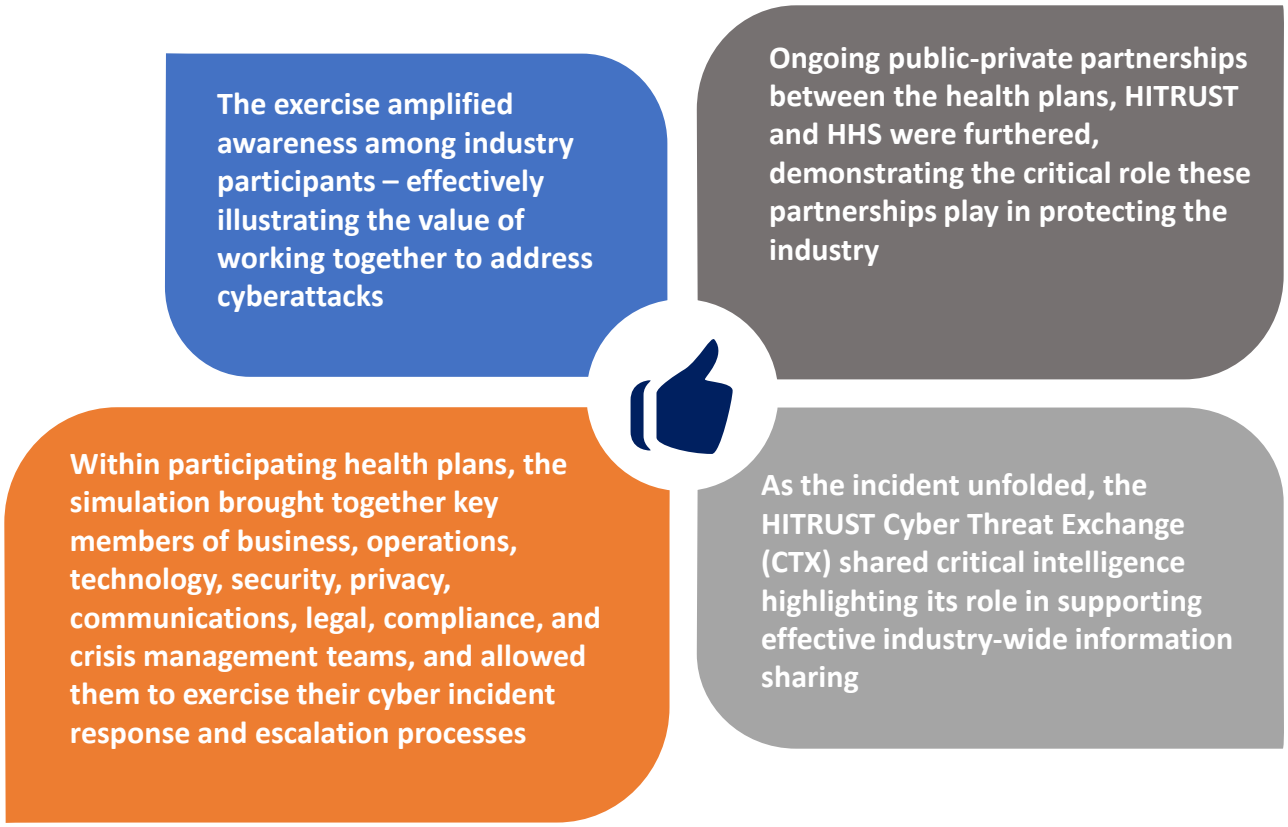
7

Fraudulent claims volume ramps up across multiple health plans as personally identifiable information (PII) and PHI files are sold on the black market.

HITRUST Health Information Trust Alliance Deloitte.

Observations – *overall successes*

The *CyberRX: Health Plans Cyber Simulation Exercise* effectively tested many of the industry-wide cyber incident response and crisis management processes and protocols that the health plan industry has worked to improve over the last several years.



Observations

	Observations	Perspectives
Third Parties 	Game injects implicated a third-party vendor and most participant health plans acted decisively in contacting the vendor and reviewing contracts. The third party was non-responsive, leading to general frustration. Interestingly, most plans did not proactively create third-party communications of their own.	Increased reliance on and integration with third parties require tight integration between third-party risk management functions and cyber incident response programs. Program reviews and joint exercises are critical components to third-party oversight efforts.
Analysis vs. Response 	Some health plans were challenged by the lack of technical detail related to the source of the incident. These organizations focused on forensic analysis over assessing business impacts and engaging key stakeholders.	During cyber incidents, the demand for information far outpaces the supply. Decisions may be required with incomplete information. Engaging a variety of perspectives improves decision-making when information is incomplete.
Command Structure 	Strong personalities tended to dominate conversations when gameplay required decisions not covered in existing command structures and plan documents. These personalities often drove decisions outside of their defined responsibilities.	During the course of an incident, natural leadership skills may emerge. Embracing initiative and driving response must be balanced against effective governance and incident command.
Cyber Insurance 	Cyber insurance claims were a frequent consideration, however a general lack of certainty about response and reporting requirements, loss quantification, and claim submission was observed.	Cyber insurance is an evolving industry with notable variances across insurers and policies. Aligning policy requirements to cyber incident response plans can allow for effective data gathering and reporting processes.
Fact or Fiction 	Several injects were designed to introduce noise into gameplay. Many participants took this content at face value and moved to react and respond. Assumptions made during gameplay were often taken as fact, leading to decisions based on conjecture.	Vetting data points, gathering different perspectives, and documenting assumptions and actions can aid in distinguishing the signal from the noise.

Observations

	Observations	Perspectives
Industry Communications 	Three organizations were simulated in the exercise injects: HITRUST; a fictitious health plan named ResponseHealth; and a shared third-party vendor. Proactive engagement from game participants to these organizations was minimal.	Despite calls for increased industry collaboration, active collaboration remains elusive. Further development of formalized engagement protocols is recommended.
Internal Communications 	Participating health plans varied significantly in communication outside of technical teams. In organizations where business engagement was limited, decisions were made based purely on technical information.	Clear, direct, frequent, and scheduled communications are critical to supporting an effective cadence and informing business, operational, and technical strategic decision-making.
Law Enforcement 	Several participating health plans engaged law enforcement early in the process when no evidence of a crime had been established. Many of these participants did not have a clear plan for how to engage and what information would be provided.	Engaging law enforcement can aid in evidence compilation and preservation, however acting too soon may lead to a loss of control over the incident investigations, response, and recovery.
Plan and Training 	All health plans had cyber incident response plans available but only two participants referenced the documents during game play.	While the pace of play did not support strict adherence to comprehensive plan documents, cyber incidents similarly escalate at a rapid pace. Quick reference guides drive information accessibility and support informed and time-sensitive decision-making during training exercises and live fire.
Regulatory Compliance 	Few participants took action to report the breach when regulatory thresholds for notification were reached.	Incident response teams should be aware of regulatory landscape in order to maintain compliance and protect the organization from litigation. Training and cyber wargames are important program compliance elements.

HITRUST Health Information Trust Alliance Deloitte.

Recommendations – *industry-wide*

The exercise identified opportunities to improve incident response and crisis management procedures by strengthening coordination among the industry participants.

Industry-wide incident command structure and processes

- Establish formal procedures that stress the integration of cyber incident response plans across industry groups, health plans, and HHS
- Elevate the role HITRUST and trusted government partners play in health plan cyber incident readiness, response, and recovery activities
- Increase awareness about government and law enforcement resources available to assist the health plan sector by designing training programs centered on appropriate engagement

Systemic risk assessment and decision processes

- Establish effective escalatory paths between business and technology leaders during cyber incident analysis and response
- Invest in capabilities to support risk analytics, information sharing, and crisis communications

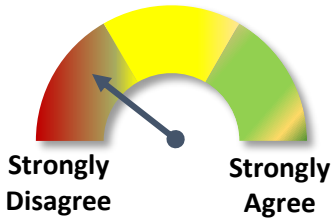
Communication and information sharing

- Enhance protocols that promote increased communication and information sharing among health plans
- Formalize public awareness and communications strategies with a view to promoting trust and confidence in the health plan industry
- Institutionalize procedures for integrating cyber insurance partners and third-party vendors in incident response plans
- Continue maturation of ongoing cyber threat distribution by increasing awareness of public-private information sharing paths and industry cooperation with law enforcement

Recommendations – *individual health plans*

Results of individual health plan surveys and compiled observer notes identified additional opportunities to improve incident response and crisis management procedures.

Was your current incident response plan adequate to protect your members and organization during this cyber incident scenario?

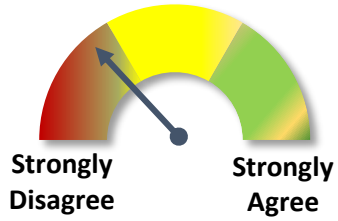


Recommendations

- Regularly exercise and update incident response plans to increase success and organizational confidence
- Incorporate lessons learned from exercises into plans and playbooks
- Train key stakeholders and resources in plan requirements to identify gaps in capabilities and increase staff and organizational cyber incident readiness

---

Do you have clear communication flows within your organization and with external parties?

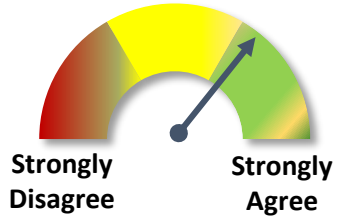


Recommendations

- Implement a communications plan covering all internal and external (including governmental) key stakeholders
- Identify appropriate spokespersons for each of the key stakeholder groups and align messaging to audience
- Assess the effectiveness of communication plans to all stakeholders through separate communications tests and within cyber wargame activities

---

Do you see a need to improve your cyber response capabilities?



Recommendations

- Align cyber incident response activities with other organizational resilience efforts including crisis management, business continuity, disaster recovery, and emergency response
- Create quick reference guides to improve rapid response capability
- Establish a Cyber Incident Response retainer to provide surge support for time-sensitive technical investigation and forensics activities

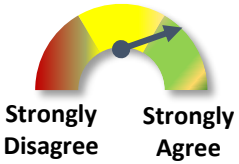
HITRUST Health Information Trust Alliance Deloitte.

Recommendations – *disparity of perception*

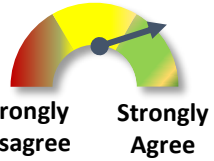
Results of individual health plan surveys and compiled observer notes identified additional opportunities to improve cyber wargaming activities.

What participants said

Do you feel your organization had clearly delineated roles and responsibilities as the simulation progressed?



Do you feel you have the individuals with the required skill set in your organization to respond to a cyber incident?



What we saw

- Observers noted that some plans struggled with roles and responsibilities outside of technical teams.
- Limited engagement of third parties including industry contacts, regulatory bodies, and law enforcement suggests a need to document points of contact and rules of engagement.
- Strong voices tended to dominate discussions, blurring the lines between roles and defined processes.

Answers to direct & attributable survey questions varied significantly from independent observations and informal commentary offered during gameplay

Recommendations

Exercises and cyber wargames should incorporate formal and informal methods for gathering honest feedback.

- Continue to use independent third-party observers to ensure that frank and independent observations and recommendations are provided.
- Use anonymous surveys and/or interviews from internal participants to provide more accurate, aggregated metrics against key performance and result indicators.
- Periodically immerse cyberattack responders in a simulated and interactive cyberattack scenario to allow organizations to honestly evaluate their cyber incident response preparedness and identify cyber incident response capability gaps.

HITRUST Health Information Trust Alliance Deloitte.

Key takeaways – *confidence vs. capabilities*

At the most strategic level, recovering from a cyber incident involves an important balance between recovering or enhancing capabilities and restoring confidence among a broad spectrum of stakeholders.

Capabilities Considerations

- **Business and operational** capabilities are disrupted when cyberattacks disable technology solutions
- **Information technology** capabilities inform decision-making and support critical business processes
- **Cyber risk** capabilities secure the environment, provide better visibility into ongoing threats, and reduce the impact of future attacks

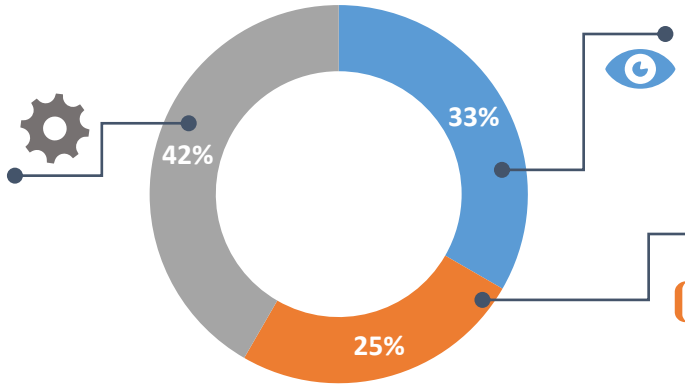
Confidence Considerations

- **Customers and members** are immediately concerned with direct personal impacts
- **Employees** can be overwhelmed by negative publicity and increased chaos
- **Business partners** are concerned with the threat of cross-contamination and long-term integrity
- **Regulators** monitor consumer protection, existential threats, and broad industry impacts

Results

At the conclusion of the exercise participants were asked to prioritize long-term recovery efforts by selecting from a range of strategic initiatives. Each option presented focused either on recovering capabilities or rebuilding stakeholder confidence.

5 of the 12 plans focused on rebuilding **capabilities**. Confidence restoration is critical to minimizing brand and reputational impacts.



4 plans prioritized **confidence** initiatives. Capability enhancements are necessary to sustain confidence gains.

3 plans **balanced** the restoration of capabilities and confidence.

HITRUST Health Information Trust Alliance Deloitte.

Acknowledgements

Supporting organizations

Deloitte Advisory

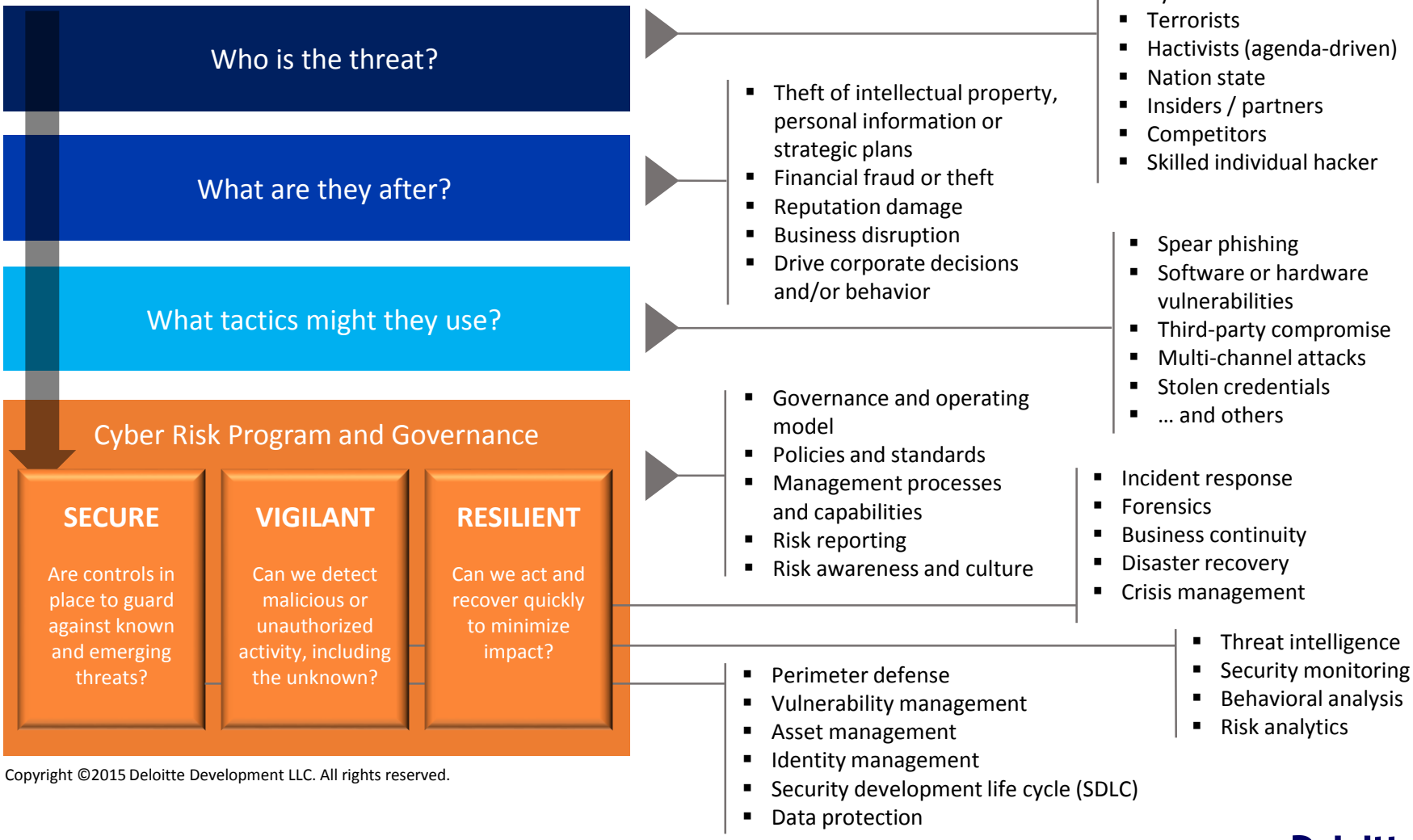
Program Committee

- Health Information Trust Alliance (HITRUST)
- US Department of Health & Human Services (HHS)
- Blue Cross Blue Shield of Michigan
- Health Care Services Corporation
- Highmark Health
- Humana
- United Health Group

HITRUST Health Information Trust Alliance Deloitte.

Establishing risk-driven incident response capabilities

Health Plan executives set risk appetite and drive focus on what matters most. It starts by understanding who might want to attack, why, and how.



Deloitte.

Next steps

- The data collected from this and other CyberRX exercises is used to define and enhance future exercises and programs
- We encourage organizations to participate in a CyberRX exercise
- For more information on the CyberRX program visit hitrustalliance.net/cyberrx/

For additional information about the *2015 CyberRX: Health Plans Cyber Simulation Exercise* or building *Secure.Vigilant.Resilient.*™ organizations, contact:

Deloitte Advisory

- **Emily Mossburg**, Principal, Cyber Risk Resilient Executive, Deloitte & Touche LLP, emossburg@deloitte.com
- **Mark Ford**, Principal, Healthcare Cyber Risk Services Executive, Deloitte & Touche LLP, mford@deloitte.com
- **John Gelinne**, Director, Cyber Wargaming, Deloitte & Touche LLP, jgelinne@deloitte.com

HITRUST

- Phone 855-HITRUST or email info@hitrustalliance.net

HITRUST Health Information Trust Alliance Deloitte.

Appendix

HITRUST
Health Information Trust Alliance

About HITRUST

Founded in 2007, the Health Information Trust Alliance (HITRUST) was born out of the belief that information protection should be a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges. HITRUST, in collaboration with public and private healthcare technology, privacy and information security leaders, has championed programs instrumental in safeguarding health information systems and exchanges while ensuring consumer confidence in their use.

HITRUST programs include the establishment of a common risk and compliance management framework (CSF); an assessment and assurance methodology; educational and career development; advocacy and awareness; and a federally recognized cyber Information Sharing and Analysis Organization (ISAO) and supporting initiatives.

www.HITRUSTalliance.net

Deloitte.