Healthcare Industry Collaboration for better Cyber Vigilance and Resilience

**Facilitator:** Jimmy Joseph, Senior Manager, Deloitte & Touche LLP

**Panel Members:**
1. Sanjeev Sah, CISO, Texas Children’s Hospital
2. Randy Yates, CISO, Memorial Hermann Health System
3. Deepak Lakhiani, Security Architect, Hoag Memorial Hospital Presbyterian
The panel

Sanjeev Sah  
CISO, Texas Children’s Hospital

Randy Yates  
CISO, Memorial Hermann Health System

Deepak Lakhiani  
Security Architect, Hoag Memorial Hospital Presbyterian

Jimmy Joseph  
Senior Manager, Deloitte
Agenda

• Industry threat landscape
• Why collaborate?
• How collaboration can help us?
• Takeaways
Threat landscape

$575B
Annual cost to the global economy from cybercrime [1]

$221
Per capita cost of data breach is highest in US [3]

$209M
Monetary losses suffered by enterprises in 2016 Q1 due to Ransomware [2]

Industry trends....
- Extended enterprise
- Ransomware
- Acquisitions & growth
- Sophisticated intrusion techniques
- Biomed devices & IoT
- Identity theft

63%
Increase in the number of major attacks on health care organizations in 2016 [4]

4000+
Per day Ransomware attacks in the first quarter of 2016 – 300% increase from per day no. over 2015 [2]

Forrester “Understand the Business Impact and Cost of a Breach” 12 January, 2015
Trend Labs, The Reign of Ransomware, 2016
Ponemon 2016 Cost of Data Breach Study: Global Analysis

© 2017 HITRUST Alliance.
Why collaborate as an industry?

Leading by example - The Financial Services Industry

- Collaboration for tighter controls and better enforcement
- Partnerships amongst organizations for information sharing, close tracking and working with government to stay ahead of the game
- Reduced siloed attacks and better overall protection
- Intelligence gathered through communities (e.g., Financial Services Information Sharing and Analysis Center (FSISAC)) to help identify adversaries and communicate industry risk posture

What is needed - health care industry collaboration

Better risk management through...
- Agile information security control frameworks that provide cyber security guidance
- Synchronization of a wide range of regulations and leading practices

Better vigilance through...
- Threat intelligence sharing (e.g., HITRUST Cyber Threat Exchange (CTX)) and collaboration between government and private sector
- End-to-end, cyber incident detection and response centers

Better resilience through...
- Collaboration between different health care entities in the event of a security incident
- Workshops, immersive cyber simulations (e.g., Cyber RX), tabletop exercises
# How Threat Intelligence Sharing can improve Cyber Vigilance and Resilience?

Threat Intelligence Sharing enhances the scope of information available to organizations for accurate situational awareness intelligence of the threat landscape. Collaboration can generate advanced insights to industry-specific cyber threats for clients.

<table>
<thead>
<tr>
<th>Better threat landscape analysis</th>
<th>Improvements in attack detection and response</th>
<th>Shared expectations</th>
<th>Industry specific threat alerts</th>
</tr>
</thead>
</table>
| Through effective information sharing of actionable intelligence, each sharing member can achieve a better understanding of the threat landscape. | • Ability to see attacks in context  
• Accuracy of detection and response  
• Faster detection and response | A common perspective on threats, actions, and expectations improves overall coordination and organization muscle memory | Programs can be designed to alert clients to new industry specific cyber threats that will enable companies to be protected from more and greater threats. |

Collaborative vigilance and resilience improves the cyber risk posture across organizations by counteracting the increased sophistication and coordination of cyber attacks as well as faster recovery.

© 2017 HITRUST Alliance.
Takeaways

Collaboration amplifies cyber awareness among industry participants – effectively illustrating the value of working together to address cyberattacks (e.g., cyber simulation exercises)

Public-private partnerships between the health plans and providers and industry bodies such as HITRUST and HHS are furthered, demonstrating the critical role these partnerships play in protecting the industry

As incidents within the industry unfold and increase exponentially in number, effective intelligence sharing is critical to supporting effective industry-wide information sharing

Collaboration provides greater benefit for the health care plan and provider organization community by bringing together members of business, operations, technology, security, privacy, etc., for better cyber vigilance and resilience
Visit www.HITRUSTAlliance.net for more information

To view our latest documents, visit the Content Spotlight