



FOR IMMEDIATE RELEASE

HITRUST to Launch First Comprehensive Study of Targeted Cyber Threats Impacting Healthcare Industry

Lack of Empirical Data to be Addressed by Collecting and Analyzing the Methods, Magnitude and Pervasiveness of Cyber Threats

Frisco, TX – April 6, 2015 – HITRUST announced today that it is undertaking the first empirical and comprehensive study, called HITRUST Cyber Discovery, to analyze the methods, severity and pervasiveness of cyber threats targeting a variety of healthcare organizations. The study will enable a better understanding of the actual magnitude, complexity, relations of cyber-attacks, commonalities of target organizations and data, and degree of cyber threats persisting within organizations. The goal is to accurately identify attack patterns and persistence, as well as the magnitude and sophistication of specific threats across enterprises.

There are no shortage of surveys indicating that the healthcare industry is a large target of cyber attacks, with some suggesting that healthcare has led all industries with 42.5 percent of overall breaches identified in 2014, a continuation of a three-year trend¹. Unfortunately, most of this information is survey-based and lacks details necessary to better understand the scale, target, method and sophistication of the cyber threats and attacks - creating much speculation as to the extent of the impact on healthcare organizations. Cyber related breaches at Community Health Systems, Anthem and Premera Blue Cross have increased the concern and urgency.

“The level of speculation around attacks, targets and persistent threats has reached an all-time high,” said Daniel Nutkis, chief executive officer, HITRUST. “To combat this growing concern, we need more facts to better dissect threats and develop a corresponding strategy to address them. This research will provide valuable data to those charged with keeping healthcare information secure.”

The HITRUST Cyber Discovery Study will serve as an industry benchmark in the fight against cyber attacks, including data collection, analysis and reporting. Approximately 210 health plans and provider organizations will be recruited to participate in the study.

The research scope of the study will include:

- Detection of advanced persistent threat and perpetrators
- Analysis and forensics of malware and other threats
- Attacks against specific data, organizations and industry segments

Cyber attacks have the potential to impact privacy, disrupt facility operations and/or cause direct harm to patients. Healthcare organizations can create, store and exchange large amounts of patient and member data, including personal health information, personal identifiable information, financial information such as credit card numbers, enrollment forms, lab reports and clinical research. Due to the sensitivity of this information, the industry is a high value target of threat actors ranging from nation states to hactivists.

¹ Identity Theft Resource Center.



FOR IMMEDIATE RELEASE

“As an industry, we are all in the crosshairs and need vision and leadership to coordinate a unified front to defend against cyber threats,” said Raymond Biondo, divisional senior vice president, Health Care Services Corp. “This comprehensive study will give us unique insights into the actual level, targeting, degree and persistence of cyber-attacks to better focus our efforts as an industry.”

To support the collection of the highly sophisticated cyber information, HITRUST will provide participants with software, hardware and expertise to detect, analyze and monitor networks free of charge for the study’s duration, which is expected to be approximately 90 days. HITRUST has selected Trend Micro to provide the support services and tools leveraging its [Trend Micro Deep Discovery](#) technology. Trend Micro was selected based on its strength in delivering leading-edge security products and award-winning threat discovery technology, including being named a Gartner Magic Quadrant leader in endpoint protection over a 13-year span, their top rank by NSS Labs for its Deep Discovery platform, and their collaboration with Interpol and other global law enforcement agencies to combat cybercrime.

“Cyber security challenges in the healthcare industry are far broader, with more serious implications, than those faced by typical US enterprises,” said Tom Kellermann, chief cybersecurity officer, Trend Micro. “With high-value data, multiple access points and difficulties managing security updates, criminals consider healthcare an easy, and lucrative, target. We applaud HITRUST for driving this initiative, and are pleased to help identify and eradicate targeted attacks as much as possible.”

Participants will benefit from having access to highly sophisticated collection and analysis tools and resources to provide detailed information regarding cyber events and threats within their environment free of charge. In return they will be required to provide anonymized data regularly to HITRUST for analytical purposes. An initial report of findings and recommendations will be published approximately four months from the launch of the study.

There is no cost to organizations selected for participation and organizations interested in participating in the HITRUST Cyber Discovery Study can get more information or indicate interest at <https://hitrustalliance.net/cyber-discovery/> until May 10, 2015.

HITRUST Driving Healthcare Industry Towards Greater Cyber Preparedness and Response

HITRUST is recognized as the driving force enabling public-private collaboration to reduce cyber risks in the healthcare industry. The HITRUST Cyber Discovery Study is one of a number of programs that HITRUST has delivered to industry to help prepare, assess, coordinate and respond to cyber threats. Key programs include:

- CSF: A scalable, prescriptive and certifiable risk-based framework relating to information security tailored to the healthcare industry that incorporates US and International standards such as NIST and ISO, federal and state regulatory requirements, best practices and lessons learned from breach events.
- Cyber Threat XChange (CTX): Automates the process of collecting and analyzing cyber threats and distributing actionable indicators in electronically consumable format.
- CyberVision: Provides situational awareness and threat assessment capabilities by automatically notifying healthcare organizations and information security vendors of



FOR IMMEDIATE RELEASE

emerging cyber threats for which a counter measure is not available, before the exploit has been weaponized.

- Cyber Threat Briefings: Monthly cyber threat and best practice briefings, in partnership with the U.S. Department of Health and Human Services (HHS).
- CyberRX: No cost, industry-wide exercise series coordinated by HITRUST, in conjunction with HHS, to improve preparedness and response against cyber attacks.

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. Over 84 percent of hospitals and health plans, as well as many other healthcare organizations and business associates, use the CSF, making it the most widely adopted security framework in the industry. For more information, visit <http://www.HITRUSTalliance.net>.

All product and company names herein may be trademarks of their respective owners.

###

Media Contact:

Leslie Kesselring

leslie@kesscomm.com or pr@HITRUSTalliance.net

503-358-1012