HITRUST Advances Healthcare Industry Cyber Risk Management with Creation of Threat Catalogue

Threat Catalogue aligns threats to HITRUST CSF Controls to improve effectiveness of organizational risk analyses

February 1, 2017 – Frisco, TX – HITRUST announced today the creation of a Threat Catalogue to aid healthcare organizations in improving their information security posture by better aligning cyber threats with HITRUST CSF risk factors and controls, thereby providing greater visibility into areas representing the greatest risk exposure. HITRUST undertook this initiative to improve organizational visibility into threats posed against health information and to afford organizations the ability to prioritize their security program’s activities based on a greater understanding of their risks.

The HIPAA Security Rule requires organizations to “conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI).” HITRUST helped the healthcare industry address this requirement by developing a simple-to-use framework based on risk analyses performed by representative healthcare organizations and the underlying risk analyses used to produce ISO 27001 control recommendations, NIST SP 800-53 control baselines and other control-based frameworks. By integrating these analyses with relevant regulatory requirements and best practices, the HITRUST CSF provides an industry-driven standard of due care and due diligence for healthcare information that has become the most widely used in healthcare.

“HITRUST actively solicits industry input on potential changes and updates to the HITRUST CSF and, unlike other frameworks, updates the CSF no less than annually,” said Dr. Bryan Cline, vice president, standards and analytics, HITRUST and a governing chair of the Working Group. “HITRUST is now taking this level of responsiveness one step further with the new Threat Catalogue.”

The HITRUST Threat Catalogue enhances the underlying risk analyses used to develop the HITRUST CSF and helps ensure the HITRUST CSF and CSF Assurance Program continue to remain current and relevant risk-based solutions—critical elements given today’s ever-dynamic threat environment. The HITRUST Threat Catalogue affords better visibility into how the HITRUST CSF addresses extant and emerging threats and helps ensure CSF control baselines continue to address risk commensurate with selected organizational, system and regulatory risk factors.

“Most organizations do not possess the skill sets necessary to truly identify ever changing cybersecurity threats and associate these threats with the operational impact, tactical response and strategic planning required,” said Roy Mellinger, vice president IT and chief information security officer, Anthem and a governing chair of the Working Group. “The HITRUST Cyber
Threat Catalogue takes the guess work out of the process. It articulates the threats, maps these to the necessary HITRUST CSF controls, and provides organizations with a workable blueprint to define the protection mechanisms and strategies that are required.”

The explicit alignment of threats to the HITRUST CSF produces a unique combination not found in other frameworks. This combination greatly simplifies the risk analysis process for healthcare organizations while reducing some of the burden, costs, and confusion otherwise experienced when attempting to achieve this level of risk management.

In addition to the HIPAA-required risk analysis used for control selection, the Threat Catalogue can also facilitate many other types of risk analysis. Examples include the supplemental risk analyses used to tailor a control baseline to the unique needs of an individual organization or the more targeted risk analyses used to evaluate alternate or compensating controls as well as formal risk acceptance.

The HITRUST Threat Catalogue is being developed and maintained in conjunction with the formation of a new HITRUST Working Group.

“The HITRUST Threat Catalogue is a significant step forward in helping organizations better manage risk, especially cyber risk,” said John Riggi, current Head of Cybersecurity and Financial Crimes, BDO Consulting and a governing chair of the Working Group. “This is why BDO Consulting has taken an active role in its development and adoption.”

Under the guidance of the Working Group, the HITRUST Threat Catalogue will mature over time and will subsequently focus its initial efforts on four principle tasks:

1. Identify and leverage an existing threat taxonomy for common adversarial and non-adversarial threats to ePHI
2. Enumerate all reasonably anticipated threats to ePHI for a general healthcare organization
3. Map HITRUST CSF control requirements to the enumerated threats
4. Identify any additional information needed in future iterations of the HITRUST Threat Catalogue to help meet its objectives

“The proliferation of intel feeds and services, whether provided separately, or integrated into specific security tool platforms, has added to the information overload problem. What I see in the HITRUST Threat Catalogue is the linkage and practical application that will lead organizations to take tactical actions that will enhance the overall security posture in response to the current threat environment,” said Dr. Kevin Charest, divisional senior vice president and CISO, Health Care Service Corporation and a governing chair of the Working Group.

To further aid in threat management, HITRUST will issue threat advisories in the near future based on the actual threats addressed by each control in the HITRUST CSF. Enabled by the
HITRUST CTX — the healthcare industry’s leading cyber information sharing and analysis organization — healthcare organizations will receive the intelligence they need to more fully understand these threats, better prioritize its response, and ultimately improve the overall effectiveness of its operational controls.

By fully leveraging the HITRUST CSF and HITRUST Threat Catalogue, healthcare organizations will be better able to safeguard their sensitive health information and maintain the trust of their patients and members they serve.

The initial version of the HITRUST Threat Catalogue will be available in March. For more information on the HITRUST Threat Catalogue or to be notified when available please visit https://hitrustalliance.net/threat-catalogue/.

More information on the HITRUST CSF can be found at: https://hitrustalliance.net/hitrust-csf/.

About HITRUST
Founded in 2007, the HITRUST Alliance, a not for profit, 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 and managing information risk while ensuring consumer confidence in the organizations that create, store or exchange their information.

HITRUST develops, maintains and provides broad access to its common risk and compliance management and de-identification frameworks, and related assessment and assurance methodologies, as well as programs supporting cyber sharing, analysis and resilience. HITRUST also leads many efforts in advocacy, awareness and education relating to information protection.

For more information, visit www.HITRUSTalliance.net.

###

Media Contacts: Leslie Kesselring
Kesselring Communications for HITRUST leslie@kesscomm.com or pr@HITRUSTalliance.net
+1 503 358 1012