HITRUST Threat Catalogue Overview

Enhancing Risk Analysis and Threat Intelligence
Executive Summary

For a decade, HITRUST has worked to improve the information security posture of healthcare organizations through the creation and development of the HITRUST CSF and numerous other industry initiatives.

With escalating breaches, and an increased need for regulatory compliance, HITRUST proposes to further help healthcare organizations with the creation of an extensive threat catalogue. The catalogue will be designed to improve organizational visibility into threats posed against health information and enable organizations to prioritize their security program’s activities based on a better understanding of risk.

The HITRUST Threat Catalogue will enhance the underlying risk analyses used to develop the HITRUST CSF and help ensure the HITRUST CSF and CSF Assurance Program continue to remain current and relevant risk-based solutions.

The HITRUST Threat Catalogue will show how the HITRUST CSF addresses extant and emerging threats and ensure CSF control baselines continue to address risk commensurate with selected organizational, system and regulatory risk factors.

The alignment of threats to the HITRUST CSF will produce a combination not found in other frameworks. It simplifies the risk analysis process for healthcare organizations while reducing some of the burden, costs, and confusion experienced in attempting to achieve this level of risk management.

The threat catalogue will be developed and maintained by a new HITRUST working group, which will focus its initial efforts on 4 principle tasks:

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

Additionally, enabled by the HITRUST CTX, HITRUST will issue threat advisories based on the actual threats addressed by each control in the HITRUST CSF.

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

Enhancing Risk Analysis and Threat Intelligence

<table>
<thead>
<tr>
<th>Question</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Why do we need a threat catalogue?</td>
<td>4</td>
</tr>
<tr>
<td>What exactly is a threat catalogue?</td>
<td>11</td>
</tr>
<tr>
<td>How does it relate to the CSF and other components of the HITRUST Risk Management Framework?</td>
<td>14</td>
</tr>
<tr>
<td>What are the goals of the threat catalogue?</td>
<td>16</td>
</tr>
<tr>
<td>How will the threat catalogue evolve?</td>
<td>18</td>
</tr>
<tr>
<td>What is the role of the Working Group?</td>
<td>20</td>
</tr>
<tr>
<td>Frequently Asked Questions</td>
<td>23</td>
</tr>
</tbody>
</table>
WHY DO WE NEED A THREAT CATALOGUE?
Traditional Approach to Risk Management in Healthcare

Even in a cyber world with escalating cyber-related breaches, regulatory compliance is still one of the most significant drivers for cybersecurity and information protection in the Healthcare Sector. And amongst all the regulations applicable to the Sector, the HIPAA Security Rule is arguably the biggest driver of all. Unfortunately, “HIPAA compliance” and “HIPAA compliant” have probably been some of the most overused, yet least understood terms in healthcare. This is because the HIPAA Security Rule provides numerous standards and implementation specifications for administrative, technical and physical safeguards that, despite what the terms imply, lack the prescription necessary for actual implementation by a healthcare organization.

However, this approach was necessary as no two healthcare organizations are exactly alike, which means no single set of safeguards—embodied in a government regulation—could possibly apply across the entire industry. In other words, one size truly does not fit all.

To help ensure the implementation of a comprehensive set of ‘reasonable and appropriate’ safeguards to provide for the ‘adequate’ protection of health information by a particular covered entity or business associate, HHS requires organizations subject to the HIPAA Security Rule 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) created, received, maintained or transmitted to] … protect against any reasonably anticipated threats or hazards to the security or integrity of such information.”
Traditional Approach to Risk Management in Healthcare

Regardless of the risk management model used, risk analysis is generally the first step in the risk management process. Risk assessment (synonymous with analysis according to NIST and other government sources) is also a multi-step process, one view of which consists of seven steps.

1. Classify Information Assets
2. Inventory & Categorize Assets
3. Identify Threats
4. Assess Vulnerabilities
5. Determine Impact
6. Assess & Rank Risks
7. Develop Risk Strategies/Plan

However, many organizations fail in conducting their risk analysis for many reasons. Some of the reasons specifically related to the risk analysis model include, but are not limited to, an incomplete asset inventory, failure to categorize assets properly, limited or no understanding of asset value, a failure to enumerate/address all reasonably anticipated threats, inability to determine the likelihood of a threat occurrence or impact, control effectiveness interpreted as risk, no documentation of risk treatments (especially of risk acceptance), and the failure to address corrective actions for all risks requiring mitigation.

Of these, the threat analysis is perhaps one of the most difficult for healthcare organizations due to a lack of information and, in many cases, a lack of expertise.
Framework-based Approach to Risk Management

Generally the first step in the risk management process, the risk analysis supports the specification (selection or design) of a reasonable and appropriate set of information security controls (safeguards) that provide for the adequate protection of sensitive information (such as ePHI) from all reasonably anticipated threats. However, it is possible to specify controls without performing a traditional risk analysis. Instead, organizations can rely on a comprehensive control framework, which is already built upon a broad analysis of threats faced by similar types of organizations using similar information technologies for processing information requiring similar levels of protection.

This is the approach employed by the U.S. intelligence community, Department of Defense, and civilian agencies of the federal government with their respective information security control and risk management frameworks, which are generally based on the NIST SP 800-series publications.
Framework-based Approach to Control Selection

HITRUST takes this to the next level by integrating requirements from multiple, relevant standards and best practices to create a new minimum baseline set of controls, which are designed for healthcare organizations by healthcare organizations.

HHS risk analysis guidance can then be modified as follows:

- Conduct a complete inventory of where ePHI lives
- Perform a business impact analysis (BIA) on all systems with ePHI (criticality)
- Categorize & evaluate these systems based on sensitivity & criticality
- **Select an appropriate framework baseline set of controls**
- Further tailor the controls, if necessary, based on a targeted assessment of threats unique to the organization
- Evaluate residual risk (based on a control gap analysis and impact analysis)
- Rank risks and determine risk treatments
- Implement corrective actions and monitor the threat environment
Framework-based Approach to Control Selection

By applying a minimum baseline set of controls from such a comprehensive control framework, one can be assured the organization is providing a known, minimally acceptable level of protection for this information.
Risk Management Frameworks – Pros & Cons

It’s obvious that leveraging a control-based risk management framework such as that provided by the HITRUST CSF, which integrates multiple standards and best practice frameworks like NIST SP 800-53, obviates the need for a traditional risk analysis and greatly facilitates specification of a comprehensive and robust set of information security controls.

However, as shown on the right, controls are meant to address specific risks posed by specific threats to its information assets. And since the threat environment is known to be extremely dynamic, especially in healthcare, an organization’s controls must be continually evaluated against these changing threats to ensure its information assets remain adequately protected.

Unfortunately, control frameworks are relatively static and, in many cases, aren’t updated for years at a time. And even though the HITRUST CSF is updated no less than annually, updates are generally tied to changes in its multiple authoritative sources (such as NIST and ISO), an analysis of historical breach data and best practices. While much more responsive than other control frameworks, since updates are based on prior breaches, the HITRUST CSF controls are not as forward-looking as one might achieve by performing a risk analysis considering extant and emerging threats when updating its specified controls.
WHAT EXACTLY IS A THREAT CATALOGUE?
**Definition**

There is no generally accepted definition of the term, “threat catalogue.” In practice, a threat catalogue can be as simple as a high-level threat taxonomy or as complicated as a completely enumerated threat list with a discussion of the controls that an organization could implement to address those threats.

**Examples**

Although somewhat inconsistent if not disjointed, publicly available threat catalogues include, but are not limited to, the following:

- **National Institute of Standards & Technology (NIST) SP 800-30**: Provides approx. 100 threat events as part of its discussion of the NIST risk analysis process.

- **European Union Agency for Network and Information Security (ENISA) Threat Taxonomy**: Provides a classification of threat types and 170 threats at various levels of detail.

- **International Organization for Standardization (ISO) 27005 (available for a fee)**: Provides a list of less than 4 dozen threats.

- **Bundesamt fur Sicherheit in der Informationstechnik (BSI) IT-Grundschutz-Katalog**: Provides a comprehensive list of 370 threats along with a discussion and examples for each.

Note: none of the available threat catalogues listed currently map to ISO or NIST controls.
HITRUST Threat Catalogue

The HITRUST Threat Catalogue provides a complete list of threats, with associated metadata (e.g., threat classification / type), at a level commensurate with the HITRUST CSF controls to which they are mapped. As illustrated in the figure to the right, the catalogue will provide mappings from each enumerated threat to specific CSF control requirements, as well as reverse mappings from each CSF control requirement to the threats they address. (Illustrative example for a threat-to-control mapping is provided below.)

Threats in the catalogue will be mapped to the publicly available threat catalogues referenced in the bulleted list on the previous slide. An enumeration of common vulnerabilities may also be provided to further facilitate various types of risk analyses.

<table>
<thead>
<tr>
<th>Threat Type</th>
<th>Threat Category</th>
<th>Threat Subcategory</th>
<th>Threat</th>
<th>Ctrl No.</th>
<th>Ctrl Lvl</th>
<th>Implementation Specification (Requirements)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adversarial</td>
<td>Rootkits</td>
<td>Logfile alteration/deletion</td>
<td>Alter or delete logfiles to evade detection or forensic fingerprint detection</td>
<td>09.a</td>
<td>4</td>
<td>1. Access to system audit tools and audit trails shall be safeguarded from unauthorized access and use to prevent misuse or compromise of logs. As defined in the record retention policy or based on applicable requirements to collect and retain evidence, audit logs shall be archived.</td>
</tr>
</tbody>
</table>
3

HOW DOES IT RELATE TO THE CSF AND OTHER COMPONENTS OF THE HITRUST RMF?
How the HITRUST Threat Catalogue would support the CSF and other HITRUST Risk Management Framework components/services

Better Assurances for Internal & External Stakeholders

Better Prioritization of CAPs

“Real-Time” Changes/ Updates to Implemented Controls

Maintains Currency & Relevance of Control Framework

Better Tailoring of Control Baselines

Step 1: Identify Risks and Define Protection Requirements

Step 2: Specify Controls

Step 3: Implement and Manage Controls

Step 4: Assess and Report
WHAT ARE THE GOALS AND BENEFITS OF THE THREAT CATALOGUE?
The HITRUST Threat Catalogue adds a significant dimension to the HITRUST CSF by helping organizations understand their threats, better align threats to CSF risk factors and CSF controls, and provide greater visibility into areas with the greatest risk exposure.

- Intended to help healthcare organizations
  - Identify “all reasonably anticipated threats”
  - Conduct multiple types of risk analyses
    - General HIPAA risk analysis for initial control selection
    - Supplemental analyses for tailoring of the control baseline
    - Targeted analyses for risk acceptance, alternate control selection
  - Consume threat intelligence
    - Threat advisories tied to the controls intended to help address them
    - Allows organizations to review their readiness/preparedness as the threat environment changes
- Intended to help HITRUST
  - Maintain currency, relevance of CSF controls
  - Maintain alignment of implementation requirements with increasing levels of risk
HOW WILL IT EVOLVE?
Development Approach/Schedule

Phase 1: 1Q2017
- Develop initial threat list
- Map MyCSF requirements to threats
- Initial goal is a 60-80% solution

Phase 2: 1Q2018
- Revise threat list/mappings based on industry feedback
- Develop list of common vulnerabilities
- Develop supporting guidance on how to leverage the catalogue
  -- Supplemental risk analysis
  -- Targeted risk analysis
    --- Risk acceptance
    --- Alternate controls

Phase 3: TBD
- Identify areas of improvement / additional development
WHAT IS THE ROLE OF THE WORKING GROUP?
HITRUST Threat Catalogue Working Group Charter

Need

The HITRUST CSF is updated at least annually based on relevant, new or updated authoritative sources, such as regulations, standards and best practices, as well as due to changes in technology or root causes of data losses and breaches. Even so, the CSF may not be as responsive to a changing threat environment as one would like, as the frequency of updates to the underlying authoritative sources can range from almost a decade—as with ISO/IEC 27001—to years—as with NIST SP 800-53. So any organization relying on the next release of any control framework, not just the CSF, rather than conducting the ongoing analyses necessary to address unique, active or emergent threats, will always be reactive to some extent.

HITRUST has decided to leverage its Information Sharing and Analysis Organization (ISAO) to issue threat alerts and reports that identify the CSF controls intended to address the reported threats. When needed, the HITRUST ISAO may also provide additional guidance to healthcare organizations on verifying the effectiveness of these controls and any supplemental measures they may wish to implement.

This approach will make threat intelligence more consumable by a wider range of healthcare organizations and help ensure the industry takes a more proactive approach to addressing cyber threats than is currently possible. HITRUST will also evaluate the CSF controls related to threat intelligence issued by the HITRUST ISAO and periodically update the CSF as needed for the benefit of the healthcare industry.

An added benefit of explicitly tying CSF controls to the threats they address is that this information can help organizations demonstrate they meet HIPAA Security Rule requirements for identifying all reasonably anticipated threats as part of the requirement for risk analysis. The CSF-to-threat mappings will also facilitate the risk analyses required for risk acceptance, alternative controls, and corrective action planning.

Objective

The HITRUST Threat Catalogue Working Group's primary objective is to develop a threat catalogue that can be leveraged by HITRUST to maintain the CSF, by the ISAO for threat intelligence, and by healthcare organizations to support general risk analysis requirements.

Key Focus Areas

HITRUST expects development of the threat catalogue will require multiple iterations to ensure it can satisfy this objective. Subsequently, the working group will focus its initial efforts on four principle tasks:

- Develop a threat taxonomy for common adversarial and non-adversarial threats to ePHI,
- Enumerate all reasonably anticipated threats to ePHI for a general healthcare organization,
- Map CSF controls to the enumerated threats, and
- Identify any additional information needed to help facilitate the consumption of threat intelligence, identify necessary changes to the CSF, and support the analysis of risk for incorporation in successive iterations of the catalogue.
HITRUST Threat Catalogue Working Group Membership

Governing Chairs:
• Kevin Charest, Ph.D., DSVP and CISO, Health Care Service Corporation
• Bryan Cline, Ph.D., VP, Standards and Analytics, HITRUST
• Roy Mellinger, VP, IT Security and CISO, Anthem, Inc.
• John Riggi, Managing Director, Cybersecurity & Financial Crimes, BDO Consulting
7
FREQUENTLY ASKED QUESTIONS
Frequently Asked Questions

Q1  How do I explain the threat catalogue to my executives?
   The threat catalogue provides a comprehensive list of threats to ePHI and other types of PII and maps these threats to the HITRUST CSF control requirements intended to address them. It allows HITRUST to better align CSF requirements with emerging threats, increasing its value in risk mitigation while simplifying an organization’s selection of security controls. In addition, it provides better visibility into how organizations manage information security risk and supports better prioritization of its security-related investments, including the remediation or enhancement of existing controls as well as the implementation of new controls.

Q2  How does the threat catalogue make the HITRUST CSF better or improve its ability to help manage risk?
   By identifying and mapping threats to HITRUST CSF control requirements, HITRUST will have additional visibility into how the controls mitigate associated risk. This will help ensure the risks associated with specific threats are addressed appropriately, including any increased risk due to an organization’s specific risk factors. For example, organizations that are large, complex or aggregate large amounts of information generally present more risk, e.g., due to a larger attack surface or increased threat actor motivation, would generally require more robust controls.

Q3  Can I get involved in the working group and, if so, how?
   The Threat Catalogue is overseen by a governing board comprised of John Riggi, Managing Director, Cybersecurity & Financial Crimes, BDO Consulting; Kevin Charest, Ph.D., DSVP and CISO, HCSC; Roy Mellinger, VP, IT Security and CISO, Anthem, Inc.; and Bryan Cline, Ph.D., VP, Standards & Analytics, HITRUST; and is supported by a dedicated Working Group to continue the development and maintenance of the HITRUST Threat Catalogue. Professionals with experience in risk analysis, including threat analysis, and the implementation of control-based risk management frameworks in support of healthcare information security and privacy programs may volunteer for the Working Group by signing up at https://hitrustalliance.net/working-group-signup/. HITRUST is also establishing a process to allow individuals to contribute threat information to be considered for inclusion.
Frequently Asked Questions

Q4  When will cyber threat intelligence be linked to the threats in the catalogue?

Once the mappings between threats and CSF controls are completed, HITRUST will begin working with the HITRUST Cyber Threat Xchange (CTX)\(^1\) to relate these mappings to the more granular threats identified in HITRUST CTX threat bulletins. HITRUST anticipates this work will be complete in early Q3/2017 and be integrated into the threat bulletin process by Q4/2017.

Q5  Will all the threats to health information be listed in the catalogue?

The Working Group is focused on ensuring the threat list provided in the HITRUST Threat Catalogue’s initial release will be as comprehensive as possible. However, users of the Threat Catalogue should keep in mind that the threats are enumerated at a level consistent with the control requirements in the HITRUST CSF. Intelligence generally specifies threats at a much more granular level.

Q6  How will the threat catalogue evolve over time?

HITRUST anticipates the Threat Catalogue will be a “living document” due to the constantly changing threat environment, including planned improvements to better facilitate risk analyses and the consumption of threat intelligence. Changes will likely include modifying the threat list, enumerating common vulnerabilities, relating Indicators of Compromise (IOCs), and of course updating control requirements as they change with each CSF release.

Q7  How does the threat catalogue help me perform a risk analysis?

By understanding how HITRUST CSF controls address specific threats to ePHI, an organization can demonstrate the results of the risk analyses used by the underlying control frameworks in the HITRUST CSF, e.g., ISO 27002,\(^2\) NIST SP 800-53,\(^3\) and PCI-DSS,\(^4\) as well as other types of risk analyses. For example, it will be able to tailor\(^5\) the HITRUST CSF control baseline generated from its organizational, system and regulatory risk factors by (1) addressing any additional or unique threats or vulnerabilities it may have, which may not be addressed by a CSF control requirement in the Threat Catalogue, (2) supporting the appropriate and allowable selection of alternative or compensating controls that are not contained in the HITRUST CSF, and/or (3) the removal or relaxation of specific control requirements in its baseline to help ensure the most cost-effective, risk-based application of the HITRUST CSF to its business and clinical environment.
Frequently Asked Questions

Q8  Will the threat catalogue help me with HIPAA\textsuperscript{6} compliance?

By enumerating common threats and common vulnerabilities, an organization will have additional information in support of a risk analysis consistent with NIST\textsuperscript{7} and HHS\textsuperscript{8} recommendations, which requires an “accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of [ePHI]” (HIPAA § 164.308(a)(1)(ii)(A)) and “protect[ion] against any reasonably anticipated threats or hazards to the security or integrity of [such information]” (HIPAA § 164.306(a)(2)). Today, HITRUST does this by performing baseline assessments and leveraging assessments in underlying frameworks. The Threat Catalogue will provide an additional level of granularity.

Q9  How does threat intelligence linked to the CSF help me better protect health information?

The working group will work with the HITRUST Cyber Threat Xchange (CTX) to develop the references needed to tie granular threats identified in HITRUST CTX threat bulletins to (1) higher-level threats contained in the HITRUST Threat Catalogue and (2) related HITRUST CSF controls. This information will help organizations determine if they’ve adequately addressed extant and emerging threats by evaluating how well they’ve implemented related controls in their environment at the time they receive the threat intelligence.

Q10 How will HITRUST use threat intelligence to update the requirements in the CSF?

By understanding the control requirements in the HITRUST CSF that are intended to address specific threats identified in threat intelligence bulletins, HITRUST will be able to determine if they are adequately addressed—based on current industry accepted (aka “best”) practices. If more robust controls or enhancements are needed to adequately address the threat(s), then HITRUST would issue an Implementation Advisory to raise awareness and update the HITRUST CSF requirements in its next release.

Q11 What would prompt HITRUST to issue additional CSF implementation guidance?

A HITRUST Implementation Advisory would be issued if there is additional clarification around how HITRUST CSF requirements should be implemented to effectively address one or more threats—or as an interim measure until more stringent or enhanced control requirements can be published in the next scheduled release of the HITRUST CSF.
Frequently Asked Questions

Q12  How often will the threat catalogue be updated?

We anticipate updates to occur annually, shortly after each HITRUST CSF release, or – upon recommendation of the HITRUST CSF Threat Working Group – when significant changes in the threat environment would warrant an interim release.

[1] For more information, see https://hitrustalliance.net/cyber-threat-xchange/
[5] NIST SP 800-53 r4, Ch. 3.