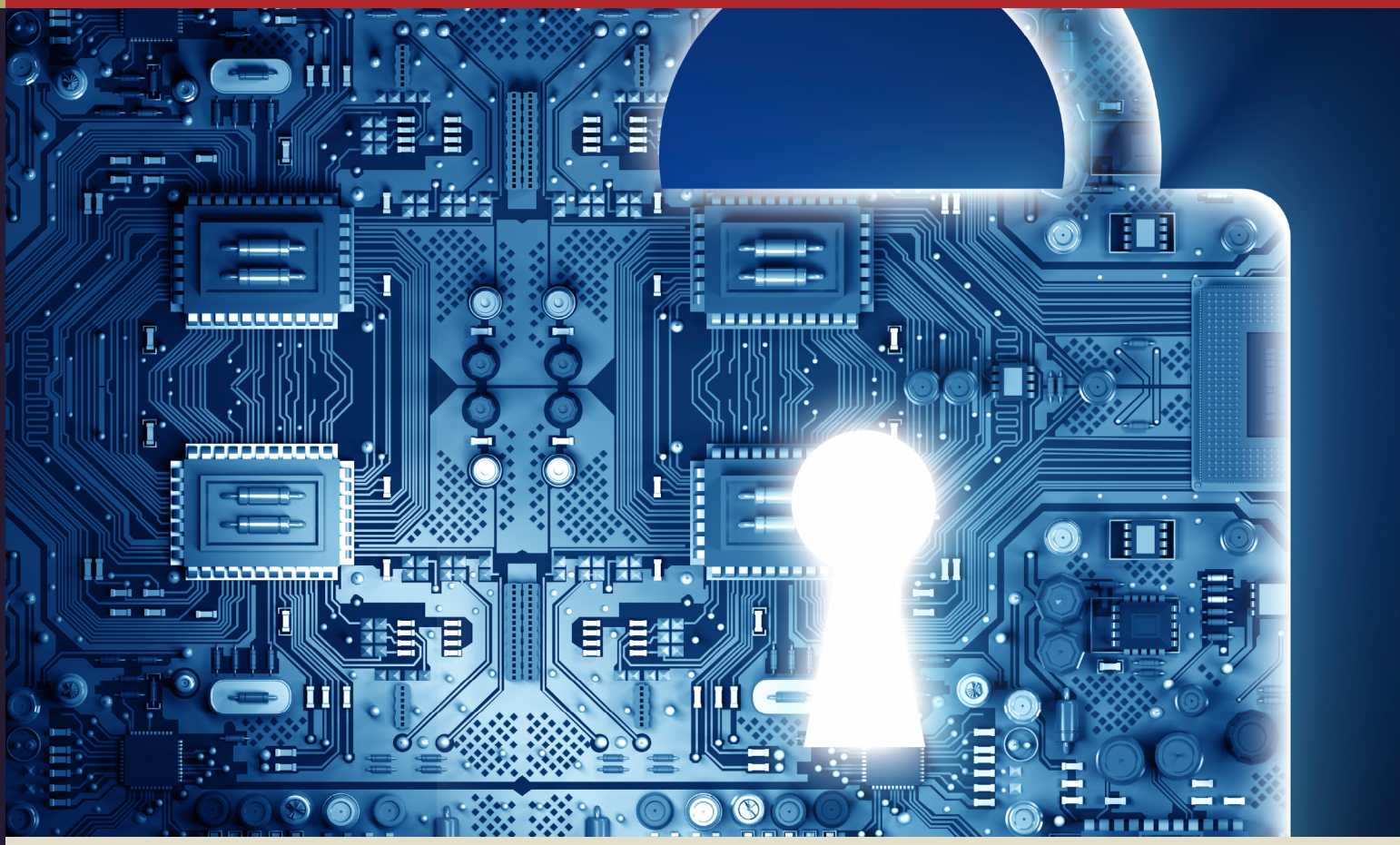
HITRUST
Health Information Trust Alliance



Healthcare's Model Approach to Critical Infrastructure Cybersecurity

How the Industry is Leading the Way with its Information Security Risk Management Framework

June 2014

Executive Summary

The United States has seen a marked increase in the use of electronic information and a resulting increase in the level of exposure to cyber attacks, which target an organization's use of cyberspace for the purpose of stealing information or disrupting, disabling, or destroying related information resources. As a result of these ever increasing cyber threats, the President directed the National Institute of Standards and Technology (NIST) to work with the private sector to develop the Framework for Critical Infrastructure Cybersecurity. The NIST Cybersecurity Framework provides an overarching incident management-based model that industries, industry sectors, or organizations can leverage to identify opportunities for improving their management of cybersecurity risk.

The Health Information Trust Alliance (HITRUST) Risk Management Framework (RMF)—consisting of the Common Security Framework (CSF), CSF Assurance Program, and supporting methods, tools and services—is a model implementation of the NIST Cybersecurity Framework. Consistent with the framework, the CSF provides a comprehensive, prescriptive, yet flexible information security control framework that leverages the risk analysis used to develop its supporting authoritative sources. The CSF Assurance Program pairs with the CSF providing the mechanism for sharing information security assurances with internal and external stakeholders in a consistent and repeatable way. In addition, the HITRUST Cyber Threat Intelligence and Incident Coordination Center (C^3) provides actionable intelligence on active and emergent cyber threats to sensitive health information and supports multi-organization collaboration on incident management and response activities.

However, despite annual updates that consider changes in best practices and vulnerabilities identified through data breach analysis, the CSF—like the authoritative sources upon which it is built—can become stale with respect to a constantly changing threat environment. In addition, organizations vary in how well they are able to consume threat intelligence in a meaningful way. In many cases, organizations struggle with assessing their cyber readiness based on standard threat intelligence reports.

HITRUST intends to address these problems by 'changing the game' with respect to how threat intelligence is used. The HITRUST C^3 will issue threat alerts and reports that indicate which CSF controls address which identified threats, provide additional guidance as needed to help organizations assess the effectiveness of these controls, and recommend supplemental controls when additional risk must be mitigated. The same information will also support HITRUST's goal to make timely, relevant updates to the CSF even though the authoritative sources integrated into the framework may not be updated for years at a time.

This approach provides significant advantages over other approaches and no other information security framework in any industry uses an approach to help organizations define and continuously maintain the controls needed to proactively manage information security risk due to active and emergent threats. By better integrating the CSF with threat intelligence, healthcare organizations can implement controls tailored to their specific risk factors and unique threats and maintain the currency and relevance of those controls in a constantly changing threat environment.

The healthcare industry as a whole has made significant progress in the last two years in maturing its cyber threat preparedness - establishing the HITRUST C^3, holding industry-wide monthly cyber threat briefings, performing industry cyber preparedness drills (CyberRX), and now updating the CSF to address cyber risks in a timely manner. There is still more to be done, but the healthcare industry is now taking the lead with its cybersecurity framework.

Contents

Executive Summary 2

Introduction 5

Cyber Threat Landscape 6

Addressing Cybersecurity 8

Key Elements of a Cybersecurity Program 9

NIST Cybersecurity Framework 9

Healthcare's Implementation of the NIST Cybersecurity Framework 11

Improving the HITRUST RMF thru Threat Intelligence 17

Final Thoughts 20

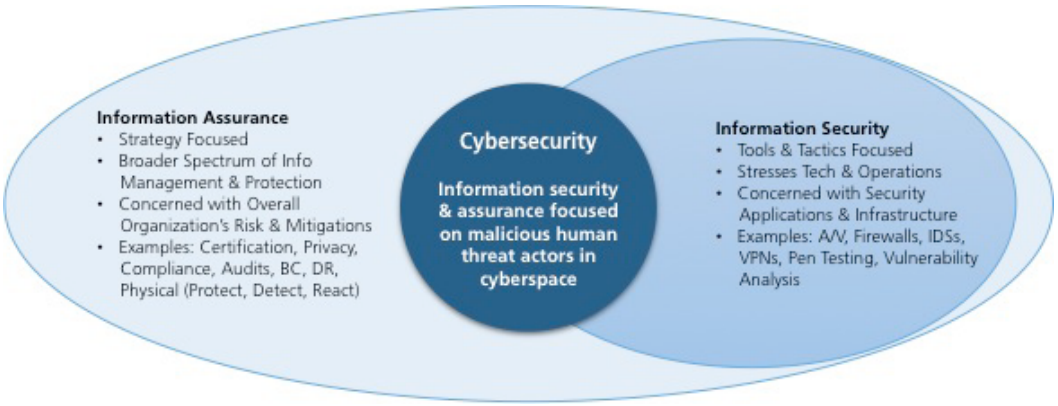
About HITRUST 21

Introduction

What exactly is cybersecurity?

According to the Committee on National Security Systems[1], cybersecurity refers to an organization's ability to protect or defend the use of cyberspace—a global domain within the information environment consisting of an interdependent network of information systems infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers—from cyber attacks. Cyber attacks are further defined as attacks, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Although the definition of cybersecurity is quite broad, cybersecurity is clearly a component of information security[2] and information assurance[3] focused on malicious threat actors in cyberspace.



The definition of cyberspace is also quite broad and necessarily includes both internal and external malicious threat actors. However, cybersecurity does not address non-malicious human threat actors, such as a well-meaning but misguided employee, or non-human events such as power outages, busted water pipes, and 'acts of God.'

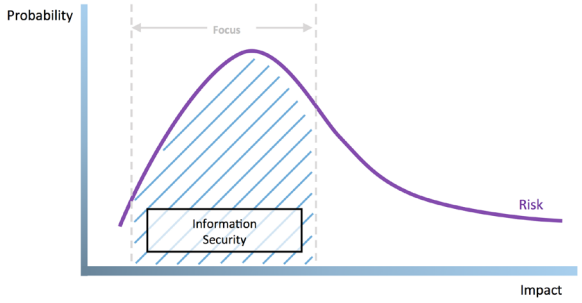
[1] *CNSSI 4009 (2010). National Information Assurance Glossary*

[2] *Information Security is defined as "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."*

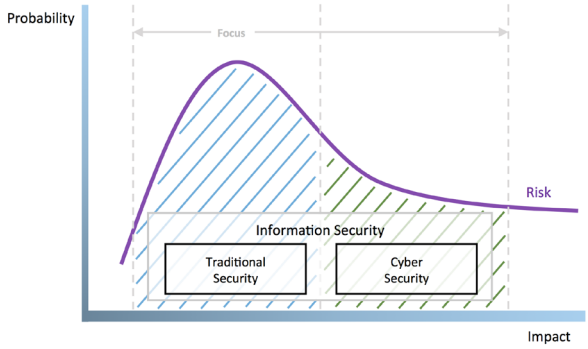
[3] *Information Assurance (IA) is defined as the "measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities."*

Cyber Threat Landscape

Now that we understand the difference between traditional information security and cybersecurity, it will be easier to convey recent changes in the threat landscape.



The figure above is intended to depict risk as a function of the probability that a threat will successfully exploit a vulnerability and the potential impact on an organization should that occur. As we move up the diagram, the probability increases and, as we move to the right, the potential impact increases. There is also a relatively long tail to the right that conveys a significant number of low probability, high impact threats. Cyber threats, that is threats posed by malicious threat actors in cyberspace, have historically fallen into this category. As a result, many organizations in the healthcare industry have been focused on more traditional information security risks, which is represented by the shaded area or "zone" under the curve. The relative size of this zone is generally determined by factors such as risk appetite, cost effectiveness, organizational culture, availability of resources and, of course, the relevant threat landscape. However, as depicted in the next figure, the threat landscape has evolved to the point that cyber-related risks that were once considered unlikely began occurring with regularity.



This trend can be attributed to:

- Higher maturity of detection and attack tools and methods (exploits)
- Increased diversity and motivation of attackers (threat actors)
- More electronic information and networked applications (vulnerabilities)

Cyber attacks targeting healthcare entities also appear to be on the rise. In fact, the percentage of data breaches (43.8%) and records breached (9.6%) in healthcare exceed those in credit, finance and banking (3.7% and 0.9%, respectively), according to an Identity Theft Resource Center (ITRC) study of 2013 breaches across all sectors[4]. According to a 2012 study by the Ponemon Institute, some 94 percent of medical institutions said they've been the victim of a cyber attack.

A subsequent 2013 SANS-Norse study[5] also provides clear evidence that many healthcare organizations fail to detect these attacks and remain compromised. The study showed that, over a period of two months, 375 healthcare organizations were identified as the source of malicious outbound traffic, with 72% of these entities being healthcare providers. Many of these organizations produced such traffic over the entire two month period, which indicates they never detected or corrected the problem.

Unfortunately, the problem just keeps getting bigger as the healthcare industry moves from paper records to electronic health record systems and entities continue to interconnect these systems through health information exchanges and other business arrangements. Thanks to incentives for adoption and penalties for non-adoption under the Medicare and Medicaid programs, the use of electronic records grew significantly over time. By 2008, still only 41.5% of office-based physicians reported using any electronic system, but that is more than double the number in 2001. According to HealthIT.gov[6], 64% of an estimated number of 4,836 hospitals received an incentive payment in 2012 for the meaningful use of an EHR. At the end of 2013, that number grew to 90%.

The industry would do well to remember why criminals used to rob banks. If you don't, it's because that was where the money was. Today, there are more lucrative ways of stealing money, not the least of which is identity theft. Once limited to the credit, banking and finance sector, the most profitable type of fraud stemming from identity theft is now Medicare fraud. According to a 2009 CBS "60 Minutes" investigation[7], Medicare fraud cost the program an estimated $60 billion dollars per year. In 2012, that number has risen to anywhere from $75B to $250B, according to the FBI[8].

[4] *http://www.idtheftcenter.org/ITRC-Surveys-Studies/2013-data-breaches.html*

[5] *http://pages.norse-corp.com/rs/norse/images/Norse-SANS-Healthcare-Cyberthreat-Report2014.pdf*

[6] *http://dashboard.healthit.gov*

[7] *http://www.cbsnews.com/news/medicare-fraud-a-60-billion-crime-23-10-2009/*

[8] *http://www.foxbusiness.com/personal-finance/2013/02/22/how-big-is-medicare-fraud/*

Yet, despite the rising risk within the healthcare industry to cyber attacks and cyber crime, healthcare organizations continue to underinvest in their security programs. Almost 60% of respondents in a November 2011 Healthcare Information and Management Systems Society (HIMSS) Security Survey[9] indicated that their IT budget dedicated to information security had increased in the past year, 53% admitted that the total allocated to information security was 3% or less of their operational budgets. According to a January 2012 survey[10] of compliance professionals by the Society of Corporate Compliance and Ethics and the Health Care Compliance Association, only 27% of the over 970 participants felt that they have enough resources for their compliance programs.

Although evidence suggests cyber-related risks are indeed on the rise, HITRUST wanted to determine if the risks are as real as the hype would indicate. Subsequently, HITRUST performed an analysis of 128 separate incidents tracked by the HITRUST Cyber Threat Intelligence and Incident Coordination Center, or C^3, in September of 2013.. From the analysis, HITRUST identified numerous incidents of PHI, financial, and other personal information in healthcare organizations being targeted and successfully accessed. And although there was no documented evidence of medical device vulnerability being successfully exploited, there is general consensus in the industry that it may only be a matter of time.

Addressing Cybersecurity

In its December 2011 report, "Critical Infrastructure Protection: Cybersecurity Guidance is Available, but More Can Be Done to Promote Its Use"[12], the GAO found similarities in cybersecurity guidance and practices across multiple sectors, even though much of this guidance is tailored to business needs or to address unique risks and operations, and recommended promoting existing guidance to assist individual entities within a sector to identify "the guidance that is most applicable and effective in improving their security posture." But even before the GAO released its report, HITRUST worked with prominent healthcare organizations to create the HITRUST. Officially launched in April of 2012, the C^3 is the single best source of intelligence on threats targeted at healthcare organizations and medical devices, providing actionable information for strategic planning and tactical preparedness, and coordinated response for both large and small organizations.

Less than a year later, President Obama issued Executive Order 13636 (EO), "Improving Critical Infrastructure[13] Cybersecurity" on February 12, 2013, which called for the development of a voluntary Cybersecurity Framework to provide a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" for the management of cybersecurity risk. As a result, HITRUST reviewed several cybersecurity-related best practice frameworks, including the SANS 20 Critical Controls for Cybersecurity[14] and, in June 2013—identified 59 CSF controls[15] determined to be most relevant to cybersecurity, which helps provide assurances as to how well one is addressing cyber-specific threats.

---

[9] *http://www.himss.org/News/NewsDetail.aspx?IemNumber=4376*

[10] *http://www.hcca-info.org/Resources/View/ArticleId/194/Stress-Compliance-and-Ethics.aspx*

[11] *http://www.gao.gov/products/GAO-12-92*

[12] *http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf*

[13] *Critical infrastructure is defined in the EO as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."*

[14] *http://www.sans.org/critical-security-controls*

[15] *http://hitrustalliance.net/content/uploads/2014/05/HITRUST-Cybersecurity-Preparedness.pdf*

After three cybersecurity framework workshops, NIST published their August 28, 2013, discussion draft of the Preliminary Cybersecurity Framework for critical infrastructure in advance of their Fourth Cybersecurity Framework workshop in September but made the draft available to the general public for review as well. NIST released a "final" public draft of the Preliminary Cybersecurity Framework in October of 2013, and the final version was released in February of 2014[16], which HITRUST formally integrated into the CSF and CSF Assurance Program in April of 2014, with version 6.1.

Key Elements of a Cybersecurity Program

There are three key elements that must be addressed to ensure an organization implements a robust and comprehensive cybersecurity program: threat modeling, threat intelligence[17] and collaboration. Threat modeling may be accomplished either through a traditional risk analysis or the selection of a control baseline from an appropriate security framework. A good framework helps an organization:

- Ensure people, process and technology elements completely and comprehensively address information and cybersecurity risks consistent with their business objectives, including legislative, regulatory and best practice requirements
- Identify risks from the use of information by the organization's business units and facilitate the avoidance, transfer, reduction or acceptance of risk
- Support policy definition, enforcement, measurement, monitoring and reporting for each component of the security program are adequately addressed

Threat intelligence is essential for an organization to understand and proactively address active and emerging cyber threats, and collaboration with other public and private sector entities allows an organization to address cyber threats more efficiently and effectively than it otherwise could.

NIST Cybersecurity Framework

The NIST Framework for Improving Critical Infrastructure Cybersecurity[18] ("Cybersecurity Framework") relies on existing standards, guidance, and best practices to achieve outcomes that can assist organizations in managing cybersecurity risk by providing a common language and mechanism to:

1. Describe their current cybersecurity posture
2. Describe their target state for cybersecurity

[16] *http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm*

[17] *Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets … used to inform decisions regarding a response to that menace or hazard. (https://www.gartner.com/doc/2487216/definition-threat-intelligence)*

[18] *http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf*

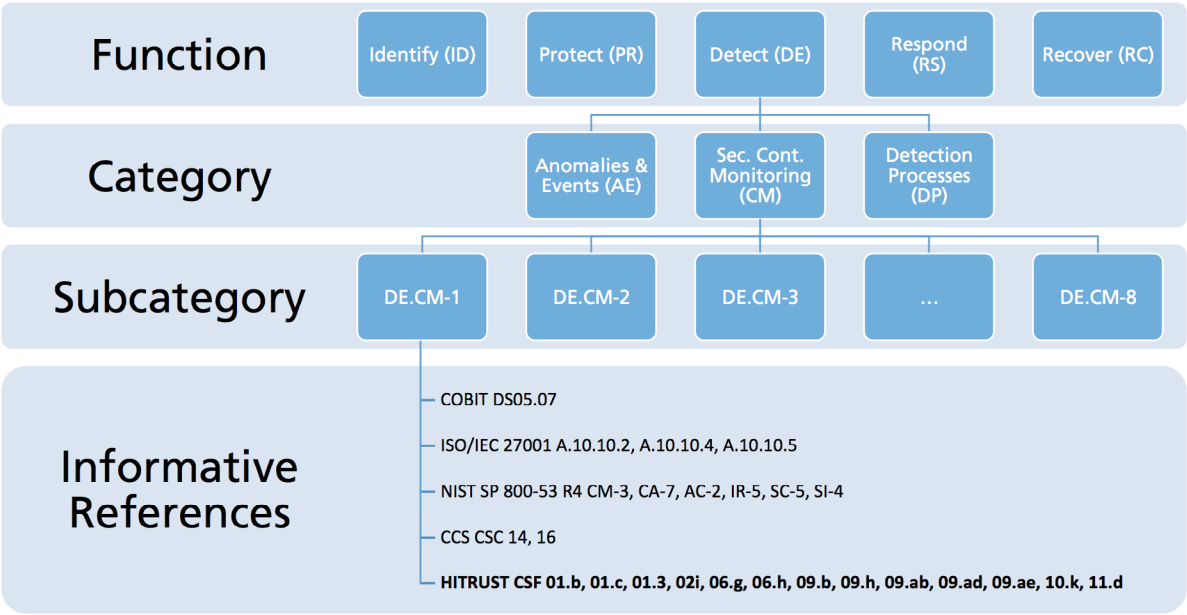
3. Identify and prioritize opportunities for improving the management of risk

4. Assess progress toward the target state

5. Foster communications among internal and external stakeholders

The Cybersecurity Framework is intended to complement rather than replace an organization's existing business or cybersecurity risk management process and cybersecurity program. Instead, organizations should use its current processes and leverage the Framework to identify opportunities to improve an organization's management of cybersecurity risk. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one. In other words, the NIST Cybersecurity Framework provides an overarching set of guidelines to critical infrastructure industries to provide a minimal level of consistency as well as depth, breadth and rigor of industry's cybersecurity programs.

Although the NIST Cybersecurity Framework leverages the NIST risk management framework (RMF) outlined in NIST's Special Publication 800-series documents, it is different in several respects. Perhaps the key difference is that the NIST Cybersecurity Framework is an overarching framework that categorizes cybersecurity requirements using what is essentially an incident management process.



Specifically an organization must:

1. Identify threats and vulnerabilities to information assets
2. Protect the assets by applying appropriate safeguards or controls
3. Detect when the controls are compromised and/or threats exploit one or more vulnerabilities associated with these assets
4. Respond to these compromises or exploits
5. Recover or restore information assets to their pre-existing, usable state

Under each of these functions are a series of categories and subcategories of protection, which are similar to the HITRUST CSF's control categories and control objectives.

Healthcare's Implementation of the NIST Cybersecurity Framework

Now let's take a look at the HITRUST RMF[19], which consists of the HITRUST CSF, the CSF Assurance Program, and—because we're focused on cybersecurity—the HITRUST C^3. The HITRUST RMF provides:

- A control framework, the CSF, that is tailored specifically for healthcare by the industry that:
  - Consists of an integrated, harmonized set of requirements as compared to individual references to controls in NIST and other frameworks
  - Is updated at least annually to keep the controls current and relevant
- A risk-based rather than compliance-based set of requirements that are tailorable to an organization's specific risk factors
- An implementation-level maturity model that supports control assessment and evaluation
- A formal validation and certification program that helps organizations provide necessary assurances to management, regulators, business partners and other stakeholders, all of which is supported by
  - A pool of vetted assessor organizations and centralized quality assurance processes to ensure consistent and repeatable assessments and analysis
  - Operational-level support for framework implementation, including specific support for cybersecurity through the HITRUST C^3

[19] *https://hitrustalliance.net/documents/csf_rmf_related/HITRUST-RMF-Whitepaper-2015.pdf*

When comparing the CSF controls most relevant to cybersecurity with the NIST subcategories, one finds they are generally consistent with one another; however, not all the Cybersecurity Framework requirements may be specifically addressed by the CSF implementation specification nor may all CSF requirements be adequately addressed by NIST. This is due primarily to the categorization of CSF controls into those considered (1) most relevant, (2) relevant, and (3) least relevant.

Critical Infrastructure Framework Subcategories that were not addressed (wholly or in part) by CSF controls determined to be most relevant to cybersecurity include ID.BE-2, Organization's Role (in the Cyber Ecosystem); PR.DS-6, Protection of Intellectual Property; and PR.IP-5: Environmental Protection of Personnel & Information Technology. One CSF control determined most relevant to cybersecurity that did not appear to fit into the NIST Cybersecurity Framework was CSF 10.b (ISO A.12.2.1), Input Data Validation. In addition, the best CSF control for the NIST requirement may not be the one deemed most relevant to cybersecurity, e.g., 06.a addresses identification of legal requirements better than 03.a.

As a result, more robust coverage of the NIST Cybersecurity Framework may be achieved by mapping in additional controls from the CSF, which makes sense given the NIST Cybersecurity Framework addresses approximately 80% of the controls in the moderate-level baseline. (HITRUST's position is that the NIST Cybersecurity Framework interprets the definition of cybersecurity rather broadly, as evidenced by its requirements around physical and environmental protection.) In the end, HITRUST completely integrated the NIST Cybersecurity Framework into the April 2014 CSF v6.1 release by updating control implementation specifications as needed.

HITRUST RMF processes and activities are also consistent with the NIST Cybersecurity Framework, as depicted in the table below.

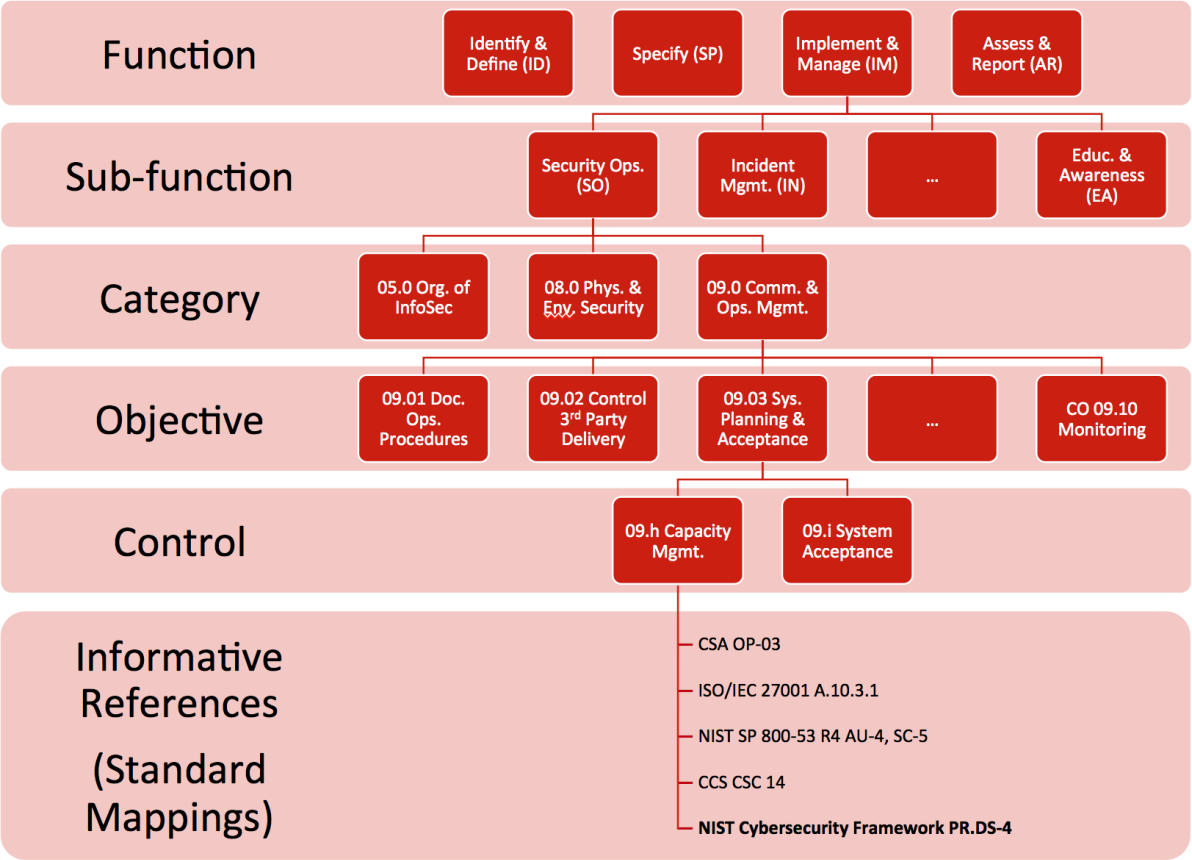
Cybersecurity Framework	HITRUST Framework
Step 1: Make Organization-wide Decisions	Adopt the HITRUST CSF
Step 2: Establish a Target Profile	Determine CSF control baseline using multiple risk-factors; identify alternate controls as needed
Step 3: Establish a Current Profile	Undergo a CSF assessment
Step 4: Compare Target and Current Profiles	Request CSF validated or certified report
Step 5: Implement Target Profile	Prioritize and implement corrective actions identified in the report

In addition, the HITRUST CSF and CSF Assurance Program fully supports a common, consistent mechanism for the communication of risk information to stakeholders (third parties) as required by the NIST Cybersecurity Framework, and continuous updating of prescriptive CSF implementation specifications provides additional information to address "gaps" in the NIST Cybersecurity Framework, also as recommended.

Both frameworks also employ a maturity model, although the HITRUST RMF model is focused at a lower level than the model proposed by the NIST Cybersecurity Framework. The following table provides rough approximations as to how an organization would likely score on a HITRUST CSF assessment for a given organizational-level tier in the NIST Cybersecurity Framework.

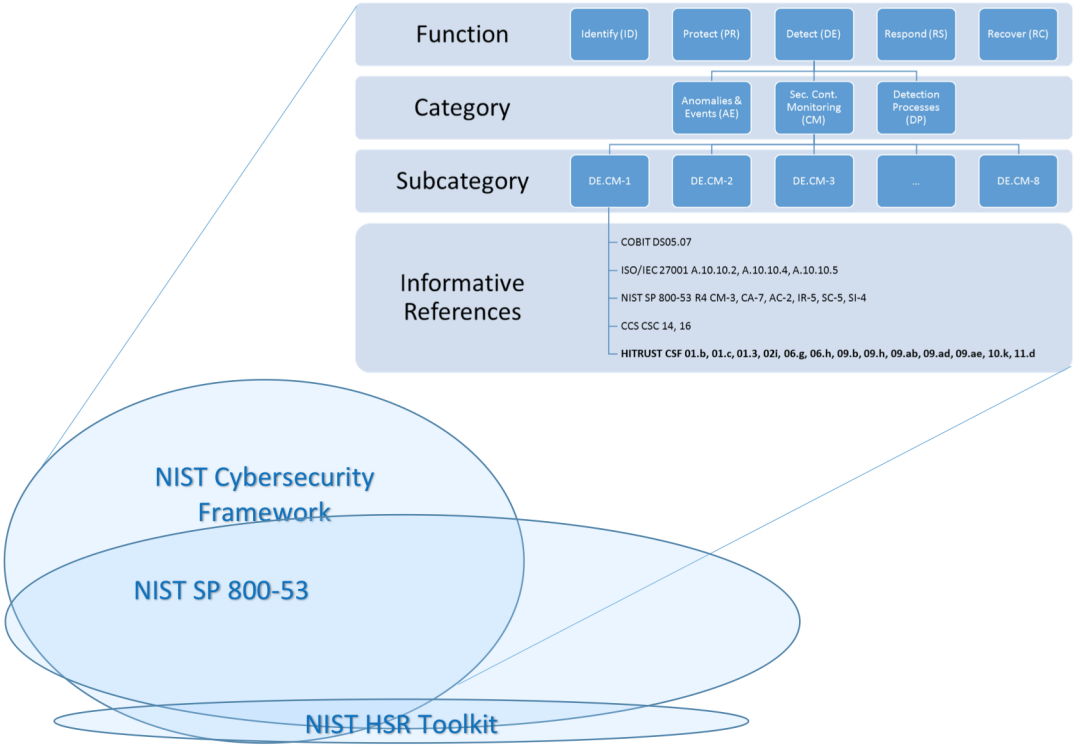
Cybersecurity Implementation Tiers	Cybersecurity Implementation Tier Description	Approximate HITRUST Maturity Levels	Approximate HITRUST Maturity Rating
Tier 0: Partial	Organization has not yet implemented a formal, threat-aware risk management process and may implement some portions of the framework on an irregular, case-by-case basis; may not have capability to share cybersecurity information internally and might not have processes in place to participate, coordinate or collaborate with other entities.	Level 1 – Partial Level 2 – Partial Level 3 – Partial Level 4 – Non-compliant Level 5 – Non-compliant	1 to 3-
Tier 1: Risk-Informed	Organization uses a formal, threat-aware risk management process to develop [target] profile [control requirements]; formal, approved processes and procedures are defined and implemented; adequate training & resources exist for cybersecurity; organization aware of role in "ecosystem" but has not formalized capabilities to interact/share info externally.	Level 1 – Partial Level 2 – Compliant Level 3 – Compliant Level 4 – Non-compliant Level 5 – Non-compliant	3- to 3+
Tier 2: Repeatable	Organization regularly updates [target] profile [control requirements] due to changing threats; risk-informed policies, processes and procedures are defined, implemented as intended, and validated; consistent methods are in place to provide updates when a risk change occurs; personnel have adequate skills & knowledge to perform tasks; organization understands dependencies/partners and can consume information from these partners.	Level 1 – Compliant Level 2 – Compliant Level 3 – Compliant Level 4 – Partial Level 5 – Partial	4- to 5-
Tier 3: Adaptive	Organization proactively updates [target] profile [control requirements] based on predictive indicators; actively adapts to changing/evolving cyber threats; risk-informed decisions are part of organizational culture; manages and actively shares information with partners to ensure accurate, current information is distributed and consumed to improve cybersecurity before an event occurs.	Level 1 – Compliant Level 2 – Compliant Level 3 – Compliant Level 4 – Compliant Level 5 – Compliant	5 to 5+

Now let's take a look at the HITRUST CSF, the CSF Assurance Program, and—because we're focused on cybersecurity—the HITRUST C³.

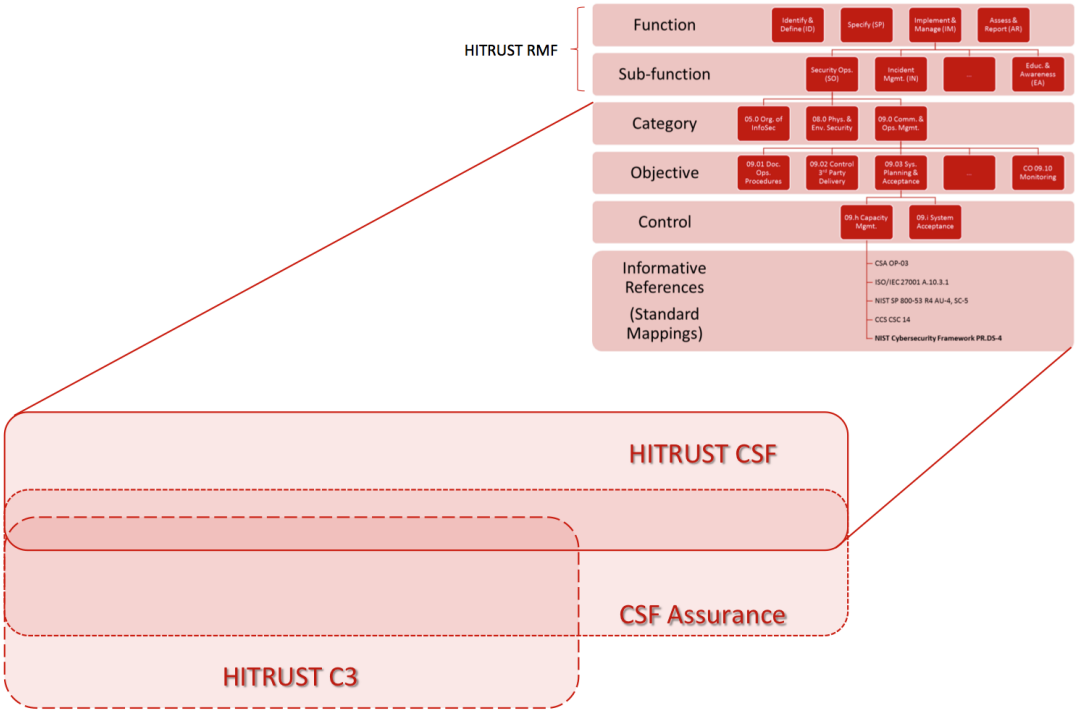


Although the HITRUST CSF is based on what NIST calls in their Preliminary Cybersecurity Framework document, a traditional cybersecurity risk management framework, ISO 27001/2, the CSF can be represented in the same manner as the NIST Cybersecurity Framework. The key difference between the two is that the functions and sub-functions are described in the HITRUST RMF, and the categories, objectives, controls and standard mappings are contained in the CSF itself. Another key difference is the CSF provides a harmonized set of detailed control specifications (requirements) specific to the healthcare industry and provides standard mappings to the underlying requirements (authoritative sources), whereas the NIST Cybersecurity Framework merely incorporates these individual, detailed requirements by reference.

As a result, one can roughly represent the relationship between the NIST Cybersecurity Framework, NIST SP 800-53, and—because we're speaking to the healthcare sector—the NIST HSR Toolkit as shown in the figure on the next page.

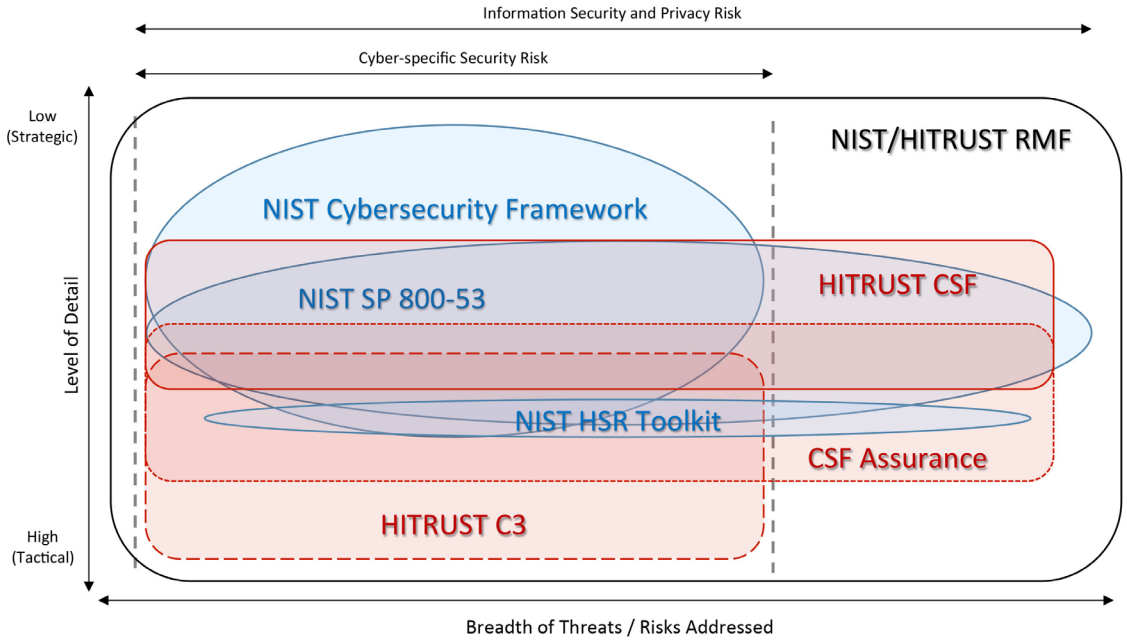


And as with the NIST Cybersecurity Framework, the CSF can be similarly represented.



Again, the HITRUST C³ capability is included as it directly supports the incident management process used by the NIST Cybersecurity Framework to categorize cybersecurity activities (controls or safeguards) according to defined functions and sub-functions. The HITRUST C³ provides industry-specific cyber intelligence and provides a mechanism for organizations to share information and collaborate on responses to specific incidents.

One can now directly compare the HITRUST RMF to the NIST Cybersecurity Framework with respect to the level of detail provided, from the tactical to the strategic, and the breadth of the threats and risks addressed.



As one can see, the NIST Cybersecurity Framework doesn't provide anything new per se. What it does provide, is exactly what was advertised—a high-level framework by which critical infrastructure industries can develop and implement industry, sector, or organizational-level risk management programs that are holistic, based upon a common set of principles, and can be communicated with stakeholders regardless of organization, sector or industry.

HITRUST provides an RMF that is consistent with the NIST Cybersecurity Framework for the healthcare industry and either meets or exceeds the requirements by addressing non-cyber threats and providing a robust assurance program as well as specific operational support to the industry through the HITRUST C³, training programs and other initiatives. In fact, the HITRUST RMF is a model implementation of the NIST Cybersecurity Framework for the healthcare sector.

Improving the HITRUST RMF thru Threat Intelligence

While the use of a standardized control baseline to manage risks makes the process of control selection easier for an organization that doesn't have the expertise or resources to perform the threat modeling necessary to develop a custom set of reasonable and appropriate controls, it is still expected to tailor these controls to any unique threats it may reasonably anticipate. Unfortunately—in many cases due to the lack of expertise cited earlier—many if not most organizations take the position that the minimum baseline set of controls is simply "good enough."

This is one of the reasons why HITRUST is actively engaged in keeping the CSF current. 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 it must in order to remain current, since the frequency of updates to the underlying authoritative sources varies, ranging from almost a decade—as with ISO/IEC 27001—to years—as with NIST.

So despite all good intentions, the framework remains relatively static with respect to the cyber threat environment. Subsequently, organizations relying on the next release of any control framework rather than conducting the analyses necessary to address unique, active or emerging threats—including the CSF—will always be reactive. HITRUST has decided to take the lead and address this problem of providing more timely updates to the CSF by leveraging the HITRUST C^3's cyber threat intelligence sharing capabilities, so that organizations leveraging the CSF can better address active and emerging threats.

The HITRUST C^3 has been providing shared threat intelligence to aid participating organizations in preparing and responding to cyber threats and events for almost two years. Now, in cooperation with the Department of Health and Human Services (HHS), the HITRUST C^3 is providing monthly cyber threat briefings and C^3 alerts to all qualified organizations. A qualified organization is any organization employing a function or activity involving the disclosure of individually identifiable health information, provided that said organization does not provide security products or services. Additionally, any federal, state, or local agency or department may qualify and participate in these shared intelligence briefings.

In addition, HITRUST and HHS held a Health Industry Cyber Threat Preparedness Summit in December 2013, to discuss numerous topics around the healthcare industry's cyber threat preparedness and coordination and response. One of the recommendations from the Summit was to evaluate the industry's preparedness and the HITRUST C^3's effectiveness through an industry-wide cyber attack and response exercise. The first CyberRX exercise held in April 2014, was predominantly comprised of Summit participating organizations, such as Children's Medical Center Dallas, CVS Caremark, Express Scripts, Health Care Service Corp, Highmark, Humana, UnitedHealth Group and WellPoint.

Besides aiding organizations in evaluating their own processes, the exercises are designed to evaluate both broad and segment-specific scenarios targeting information systems, medical devices and other essential technology resources of the healthcare industry in order to:

- Develop a better understanding of the healthcare industry's cyber threat response readiness
- Measure the effectiveness of the HITRUST C^3 in supporting the healthcare industry and opportunities for improvement
- Test the coordination with the U.S. Department of Health and Human Services relating to cyber threats and the healthcare industry response
- Document threat and attack scenarios of value for future exercises engaging additional healthcare industry organizations and in support of industry preparedness

However, not all organizations are capable of consuming and subsequently acting upon this threat intelligence in a meaningful way.

Organizational Cyber Threat Maturity

	Basic	Aspirational	Developing	Integrated
Description	Rudimentary implementation of security policies. No implementation of security procedures or technologies.	Policies establish a continuing cycle of assessing risk and implementation and use monitoring for program effectiveness. Formal, up-to-date, documented procedures are provided to implement the security controls identified by the defined policies.	IT security procedures and controls are implemented in a consistent manner everywhere that the procedure applies and are reinforced through training. Initial testing is performed to ensure controls are operating as intended.	Effective implementation of IT security controls is second nature. Policies, procedures, implementations, and tests are continually reviewed and improvements are made. A comprehensive IT security program is an integral part of the culture.
Value Add	Awareness of healthcare-specific vulnerabilities and sector-wide threats.	Prioritization of healthcare-specific vulnerabilities and sector-wide threats.	Indicators of emerging threats to healthcare sector.	Collaboration on emerging threats to healthcare sector.
Primary Benefits	Increased understanding of threats and need for security investment.	Ability to apply resources to high priority issues; efficiency gains from prioritization.	Early warning of threats to entity based on detection and analysis of threats to like entities.	Dynamic understanding of threats to healthcare industry and increased ability to analyze potential targeted threats (specific intent to harm).

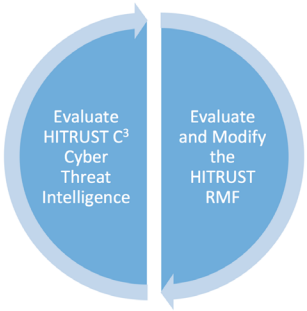
As shown in the table above, maturity can range from the very basic to a fully integrated incident management capability. In many cases, the resources and competencies are simply not available to the organization due to various organizational, fiscal or other factors. So what can HITRUST do to help facilitate the goals of the NIST Cybersecurity Framework to share threat intelligence and improve the state of cybersecurity in an industry the size of healthcare?

HITRUST recommends that healthcare organizations align themselves with a three-tiered capability model—evaluate, engage and act—based on their relative maturity or capability to consume threat intelligence: basic, aspirational, developing and integrated.

Organizational Cyber Threat Maturity	Cyber Intelligence Tier	Description of Intelligence Tier
Integrated	Act	Act upon cyber threat intelligence
Developing	Engage	Engage in cyber threat detection and analysis
Aspirational	Evaluate	Evaluate cyber threat-related controls to ensure compliance
Basic		

Organizations should move from a compliance posture of evaluating controls to acting upon threat intelligence as they mature their organization's incident management capabilities. There are greater risks with the lower approaches, although just how much may be hard to say. But those engaging in threat detection, for example, can remediate vulnerabilities more rapidly than those waiting on alerts and other threat intelligence, which must evaluate and modify their relevant controls or, if using a framework, leverage control updates when they occur.

Subsequently, HITRUST is working with members of the HITRUST C³ community to develop a common taxonomy and catalog of enumerated threats that can be used to map cyber threats against the CSF controls designed to address them. By tagging threat intelligence reports issued by the C³, organizations can evaluate related controls to determine if the threats are adequately addressed and, if not, modify them or implement new ones as needed to manage risk to an acceptable level. HITRUST will also evaluate the CSF controls related to threat intelligence issued by the C³ and periodically update the CSF as need for the benefit of the healthcare industry.



The following example from a C³ Threat Intelligence Report should help illustrate the intent of this initiative:

> *"On March 28, 2014, at 9:14 PM EDT, an unknown actor posted over 900 email addresses and associated clear-text passwords to a popular content-sharing website. Included in the post was one healthcare entity's email address and password. The data didn't appear elsewhere on the publicly-searchable Internet, suggesting that the leaked content was original and not a repost from previously stolen information. The source of the data was unknown at this time. Although the posting of this data did not appear to pose a serious threat to the healthcare organization, there was the potential for increased exposure if the employee utilized this email password on other systems, as those accounts could also be susceptible to compromise."*

More specifically, the threat this example considers is essentially the compromise of a user password resulting in possible loss of confidentiality, integrity and availability of information and information resources. There are many user authentication-related controls in the CSF, including some specific to password use that could be implemented to prevent such a breach. Such controls include CSF 01.b, User Registration; 01.d, Password Management; 01.f, Password Use; and 02.e, Information Security Awareness, Education and Training.

Some possible preventive or corrective measures an organization might consider reviewing based on this incident would be to consider the use of tokens or biometrics in addition to passwords on sensitive systems, making sure that existing password expiration and reuse requirements are satisfactorily addressed, and—since the threat intelligence didn't indicate how the password was compromised—ensuring passwords are encrypted in storage and transmission for all systems and networks in the environment. Given the possible reuse of passwords across multiple systems, an organization could also verify annual training addresses the safeguarding of passwords and password reuse as well as timely awareness messaging to the workforce on these issues.

With respect to a possible impact on CSF content, HITRUST may consider modifying language in 01.f that allows the use of a single, quality password for multiple accounts that are not synchronized or specify the need to provide additional protections for password-based systems, e.g., by implementing risk-based authentication or single sign on (SSO) for all user accounts in the organization.

Final Thoughts

There are only two viable means of selecting a comprehensive set of security controls to support a robust information security risk management program. An organization can conduct a traditional risk analysis and design a custom set of controls, or one can leverage the risk analysis used to create a control framework like ISO, NIST, or the HITRUST CSF, select an appropriate baseline, and tailor the controls to meet the unique needs of the organization. But regardless of the approach taken to determine these controls, they can become stale over time due to an ever-changing threat environment.

This is true even for organizations that design their own controls. Although these organizations may very well have the capability to periodically update their risk analysis and redesign their controls, there will always be a gap between active and emergent threats and those threats addressed by the controls in their environment. However, organizations can clearly close this gap by receiving and responding appropriately to real-time and near-real time threat intelligence.

The same benefit can be realized for organizations that do not have the capability to design their own controls or the maturity to consume standard threat intelligence by adopting and tailoring an appropriate control baseline and receiving threat intelligence that

1. Ties threats to the controls intended to address those threats
2. Provides additional guidance as needed to help ensure the effectiveness of related controls
3. Recommends supplemental controls when additional risk must be mitigated

The same threat intelligence, additional guidance, and supplemental control recommendations can also support HITRUST's goal to make timely, relevant updates to the CSF even though the authoritative sources integrated into the framework may not be updated for years at a time.

This is a real 'game changer.' No other information security framework in any industry uses this approach to help organizations define and continuously maintain the controls needed to manage information security risk in a constantly changing threat environment.

About HITRUST

HITRUST[20] was formed from an alliance of healthcare organizations to address the growing need and broad desire within the industry for a common security framework—a set of common standards and supporting methodologies—that would provide a minimum baseline set of security requirements, tailorable to a specific size and type of organization, which would improve trust as well as mitigate potential liability from breaches of sensitive information. HITRUST believes that improvements in the state of information security and privacy in the industry are critical to the broad adoption, utilization and confidence in health information systems, medical technologies and electronic exchanges of health information, which is necessary to improve the quality of patient care while lowering the cost of delivery.

HITRUST has more than 7 years' experience as the only industry-wide information protection standards body and certification authority in healthcare providing a consistent approach to certification, risk acceptance and shared trust through the HITRUST CSF, CSF Assurance Program, and supporting methodologies and tools such as the HITRUST CSF Assessment Methodology and MyCSF.

HITRUST takes great pride in helping drive the adoption and widespread confidence in sound risk management practices through the risk management framework, education, advocacy and other activities, such as our annual HITRUST conferences, the implementation of the Cyber Threat Intelligence and Incident Coordination Center (C^3), co-development of the (ISC)2 HealthCare Information Security and Privacy Practitioner (HCISPP) credential[21], and partnership with the Texas Health Services Authority[22] (THSA) on the Texas Covered Entity Privacy and Security Certification Program[23], the first state-level certification of federal and state legislative and regulatory compliance in the United States.

[20] *http://hitrustalliance.net/*

[21] *https://www.isc2.org/HCISPP/Default.aspx*

[22] *http://hietexas.org/about-thsa/overview*

[23] *http://hitrustalliance.net/texas/*

HITRUST

Health Information Trust Alliance

855.HITRUST
(855.448.7878)
www.HITRUSTalliance.net