Testimony of Daniel Nutkis
CEO of HITRUST Alliance
Before the Homeland Security Committee,
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
Hearing entitled: “The Role of Cyber Insurance in Risk Management”
March 22, 2016

Prepared for Submission

Chairman Ratcliffe, Ranking Member Richmond, and distinguished Members of the Subcommittee, I am pleased to appear today to discuss the role of cyber insurance in risk management, and initiatives underway by HITRUST and the healthcare industry to ensure its role is enhanced. I am Daniel Nutkis, CEO and founder of the Health Information Trust Alliance, or HITRUST. I founded HITRUST in 2007, after recognizing the need to formally and collaboratively address information privacy and security for healthcare stakeholders representing all segments of the industry, including insurers, providers, pharmacies, PBMs and manufacturers. HITRUST endeavored—and continues to endeavor—to elevate the level of information protection in the healthcare industry, ensuring greater collaboration between industry and government, and raising the competency level of information security professionals.

In my testimony today, I would like to highlight how HITRUST helps elevate the industry’s cyber awareness, improve cyber preparedness and strengthen the risk management posture of the healthcare industry. In particular, I want to point out how cyber insurance is integral to this process.

There should be no question as to the significance that managing cyber risk and an organization’s ability to respond efficiently and effectively to cybersecurity incidents plays in cyber resilience. To aid industry in cyber risk management, threat preparedness, and response, HITRUST has implemented numerous programs in coordination with industry stakeholders as part of its overall risk management framework (RMF).

The HITRUST RMF provides a risk-based control framework, specifically the HITRUST CSF, which is a scalable, prescriptive, and certifiable risk-based information privacy and security control framework. It provides an integrated, harmonized set of requirements tailored specifically for healthcare.

Healthcare organizations are subject to multiple regulations, standards, and other policy requirements, and commonly accepted best practice standards, including implementing the NIST Cybersecurity Framework. However, these “authoritative sources” often overlap in the depth and breadth of their requirements, which, when integrated and harmonized, can often be mutually reinforcing when intelligently applied in the intended environment.

To ensure the HITRUST CSF remains relevant, it is reviewed and updated at least annually. The review not only takes into account changes in underlying regulations and standards, but it also considers best practices and lessons learned from security incidents, incident response exercises, and industry post data breach experiences.

This level of comprehensiveness, relevance, and applicability is why over 80 percent of hospitals and health plans, as well as many other healthcare organizations and business associates, have adopted the HITRUST CSF, making it the most widely adopted privacy and security framework in healthcare.

Also distinctive to the HITRUST RMF, the HITRUST CSF Assurance Program delivers a comprehensive, consistent, and simplified compliance assessment and reporting program for regulatory requirements, such as HIPAA, HITECH, and other federal and state requirements, and the sharing of assurances between and amongst covered entities and business associates. Specifically designed for the unique regulatory and business needs of the healthcare industry, the HITRUST CSF Assurance Program provides healthcare organizations and their business associates with a common approach to manage privacy and security assessments that enables efficiencies and contains costs associated with multiple and varied information protection requirements. The CSF Assurance Program incorporates specific guidelines to allow a broad array of leading industry professional services firms to perform services, while allowing HITRUST to oversee quality assurance processes to ensure assessments are rigorous, consistent, and repeatable.

An additional benefit of using the HITRUST RMF is that it supports assessment and reporting for multiple and varied purposes,[1] such as the evaluation of AICPA's Trust Services Principles and Criteria and SSAE-16 SOC 2 reporting "scorecards" against regulatory requirements and best practice frameworks, such as HIPAA, the NIST Cybersecurity Framework, and State-based covered entity privacy and security certifications like the SECURETexas program.[2]

Just last month, HITRUST announced the availability of a new guide to assist healthcare organizations in implementing the NIST Cybersecurity Framework. This new guide was developed in consultation with the Healthcare and Public Health (HPH) Sector Coordinating Council (SCC) and Government Coordinating Council (GCC), along with input from other sector members and the DHS Critical Infrastructure Cyber Community (C3), to help HPH Sector organizations understand and use the HITRUST RMF to implement the NIST Cybersecurity Framework in the HPH Sector and meet its objectives for critical infrastructure protection.

I would also note that the availability of the HITRUST CSF, HITRUST CSF Assurance program and this implementation guide also provides an excellent basis for the Department of Health and Human Services (HHS) to leverage "voluntary, consensus-based, and industry-led guidelines,

[1] Healthcare organizations have been saving roughly 25-30% of audit costs when leveraging a HITRUST RMF Certification and a SSAE-16 SOC2 audit. Similar underwriting and auditing savings are also envisioned as the cyber insurance industry matures.

[2] SECURETexas is the first state program of its kind in the country offering privacy and security certification for compliance with state and federal laws that govern the use of protected health information (PHI).

best practices, methodologies, procedures, and processes that serve as a resource for cost-effectively reducing cybersecurity risks for a range of healthcare organizations."

HITRUST has spearheaded initiatives in other areas of cybersecurity as well. In 2012, after identifying the need for coordination among stakeholders, HITRUST launched a cyber-threat intelligence sharing and analysis program to provide threat intelligence, coordinated incident response and knowledge transfer specific to cyber threats pertinent to the healthcare industry. This program facilitates the early identification of cyber-attacks and the creation of best practices specific to the healthcare environment and maintains a conduit through the Department of Homeland Security (DHS) to the broader cyber-intelligence community for analysis, support, and the exchange of threat intelligence. HITRUST was also the first to track vulnerabilities related to medical devices and electronic health record (EHR) systems, which are both emerging areas of concern.

This program became the foundation for the HITRUST Cyber Threat XChange (CTX), which significantly accelerates the detection of and response to cyber threat indicators targeted at the healthcare industry. HITRUST CTX automates the process of collecting and analyzing cyber threats and distributing actionable indicators in electronically consumable formats (e.g. STIX, TAXII and proprietary SIEM formats) that organizations of almost all sizes and cybersecurity maturity can utilize to improve their cyber defenses. HITRUST CTX acts as an advanced early warning system as cyber-attacks are perpetrated on the industry. The HITRUST CTX is now offered free of charge to the public and has gained wide acceptance within the healthcare industry. HITRUST is also a federally recognized Information Sharing and Analysis Organization (ISAO), has strong relationships with DHS and the Federal Bureau of Investigation (FBI), and considers them integral partners in better addressing the threat landscape facing healthcare today and strengthening the continuum of care.

HITRUST also developed CyberRX, now in its third year, which is a series of industry-wide exercises developed by HITRUST to simulate cyber-attacks on healthcare organizations and evaluate the industry's preparedness against attempts to disrupt U.S. healthcare industry operations. These exercises examine both broad and segment-specific scenarios targeting information systems, medical devices, and other essential technology resources of the HPH Sector.[3] CyberRX findings are analyzed and used to identify general areas of improvement for industry, HITRUST, and government and to understand specific areas of improvement needed to enhance information sharing between healthcare organizations, HITRUST, and government agencies.

I only share this information to provide context on our engagement, experience, knowledge, and commitment in supporting the healthcare industry around cyber risk management.

Now to the specifics of the topic at hand. We can all agree that managing the risks associated with cyber threats requires a comprehensive approach to risk management, including the implementation of strong security controls such as the HITRUST CSF, continuous monitoring of control effectiveness, and routine testing of cyber incident response capabilities, such as in CSF

[3] See https://www.dhs.gov/healthcare-and-public-health-sector

Assurance and CyberRX. Commonly applied “network hygiene” only covers what is referred to as “basic blocking and tackling.” Cyber information sharing, such as that facilitated by HITRUST CTX, is designed to help organizations go beyond basic “hygiene” by alerting organizations to potential cyber threats, however, information sharing is very much dependent on the maturity of participating organizations and their ability to consume and respond to the potential threat indicators that have been identified.

While there is not a perfect solution to cybersecurity; the best strategy is to prevent, detect, and respond before the adversary achieves their objective.

A data breach in the healthcare industry not only has financial and reputational effects on the company targeted by the threat actors, but the effects could be dramatic for members, patients, and their families due to the nature of the data disclosed. Personal health information or identities could be stolen directly from hospitals, insurance companies, pharmacies and from any business associate supporting these organizations. Beyond the privacy implications of data breach incidents, these breaches have the potential to disrupt operations of a healthcare facility or affect patient care. The various complexities, interdependencies, and unique attributes all create various risk levels that need to be considered across the continuum of care.

And HITRUST firmly believes cyber insurance and cyber insurance underwriters can play a key role in supporting an organization’s overall risk management strategy and help provide for the “adequate protection” of patient information.

Organizations have relied heavily on cyber insurance as one of the means to reduce the overall financial impact of cyber-related incidents or breaches. But after numerous cyber-related breaches affecting healthcare organizations over the past few years, it is clear that healthcare data is one of the prime targets of malicious cyber threat actors who strive to monetize the data they seize. As a result of increased targeting by threat actors and recent incidents, underwriters have determined the risks were greater than they had anticipated given the methods leveraged to evaluate risk and, subsequently, healthcare organizations’ cyber insurance premiums have increased dramatically.

In many cases, companies who underwrite cyber insurance struggle with an effective way to evaluate cyber risk and the full extent of a company’s cybersecurity controls.

Every cyber insurer customarily uses a specific application for insurance, and each application differs substantially. These tools are intended to be used to help insurers gain an understanding of key risk controls, but are not intended to be used as part of a comprehensive assessment. Additionally, many cyber insurance carriers rely on a wide array of supplemental questionnaires intended to provide them with additional insight to support coverage and pricing decisions. However, the industry lacks a consistent underwriting process, given that the questions and applications can vary significantly from one carrier to the next.

Insurance underwriters have always been investigating ways to efficiently and accurately evaluate risk and help healthcare organizations ensure health information systems and services are adequately protected from cyber risks.

Leveraging HITRUST's role in aiding industry in risk management, HITRUST approached Willis Towers Watson (Willis), a leading insurance broker, to explore ways to leverage the HITRUST RMF to allow insurers to better evaluate cyber risk and to also address three concurrent needs:

1. Ensure people, processes and technology elements completely and comprehensively address information and cybersecurity risks;
2. Identify risks from the use of information by the organization's business units; and
3. Facilitate appropriate risk treatments, including risk avoidance, transfer, mitigation, and acceptance.

HITRUST and Willis established the following approach to educate and substantiate the value of leveraging the HITRUST RMF as the basis for their cyber underwriting programs in the healthcare industry:

1. Compare the use of the HITRUST RMF, and the HITRUST CSF in particular, to current application-based risk evaluation and pricing methodology;
2. Map the HITRUST CSF to insurer applications to demonstrate how it addresses the current application process and the additional depth it provides;
3. Show how superior risk evaluation efficiency and consistency can be achieved using assessment scores and summaries without sacrificing detail;
4. Identify where the HITRUST CSF assessment scores and summaries can replace current application elements and other risk management gathering methods;
5. Use test cases to substantiate accuracy and efficiency of the HITRUST CSF as a key underwriting resource in risk evaluation that allows an underwriter to compare an application-based risk evaluation to HITRUST CSF assessment-based risk evaluation;
6. Correlate claims with HITRUST CSF scores for test cases in support of a pricing framework aligned with the scores;
7. Provide feedback to HITRUST on successful attack scenarios to bring underwriter experience and any key concerns into the HITRUST CSF development process to improve risk management; and
8. Explore a pricing framework based on HITRUST CSF certification and various levels of control maturity in the certification process.

By leveraging a standardized approach to control selection and risk assessment and reporting, underwriters and other stakeholders can obtain risk estimates that are accurate, consistent, repeatable, and evolving, that is, risk estimates that take evolving risks and threats into consideration.

The goal is to integrate risk management into the underwriting process without adding confusion or unneeded complexity. HITRUST and Willis studied the relationship between HITRUST CSF and CSF Assurance control assessment scores, risk, coverage, and premiums to provide a simple, but effective data point to complement existing underwriting models.

After many months analyzing the benefits of an underwriting program leveraging a robust risk management framework, both HITRUST and Willis saw immediate value in the approach and began educating underwriters on a cybersecurity assessment methodology that would provide the industry with consistent, repeatable, reliable, and precise estimates of cyber-related risk. The HITRUST CSF and CSF Assurance program would provide underwriters with the information they could use to better understand an organization's residual cyber risk, and apply to their underwriting process.

The benefits of the HITRUST RMF-based underwriting model for cyber insurance in the healthcare industry allows organizations to maximize the benefits of demonstrating an enhanced information security posture. Ultimately, the better controls you have in place, the less likely you are to experience a breach. If a breach does occur, the potential impact will likely be contained and mitigated. This will translate into lower premiums and broader coverage for organizations who meet certain criteria defined by the HITRUST CSF. This is in many respects analogous to a "good driver discount program".

In addition to streamlining the underwriting process by leveraging their existing risk assessment, it also encourages organizations to consider the financial implications of cyber-related risks. Specifically, analyzing the impact on premium from investments reducing their cyber risks. Which is the mindset and behavior we would like to see organizations engage.

Over the past five months, HITRUST and Willis have worked to educate cyber insurers regarding the use of the HITRUST CSF and CSF Assurance program in supporting the cyber risk underwriting process. Insurers have found the HITRUST CSF to offer many advantages over the existing approaches, including providing a comprehensive and mature controls framework, aligning strong controls with risk, and accurately and consistently measuring residual cyber risk.

Allied World was the first company to offer preferred terms and conditions based on meeting the HITRUST CSF certification standards. After review and analysis, Allied World U.S. has determined that the HITRUST CSF framework and CSF Assurance methodology, will enhance its underwriting program in terms of efficiency, consistency, and accuracy, allowing it to better align the effectiveness of an organization's security controls with cyber insurance premium levels.

The review also concluded that organizations that had obtained a HITRUST CSF Certification generally posed lower cyber-related risks than those organizations that have not. The comprehensiveness and improved risk reporting enabled by the HITRUST CSF and the CSF Assessment summary scores in place of many of the standard information security application questions create a more streamlined and consistent application process. Allied World will also provide HITRUST with loss data in order to ensure the HITRUST CSF control guidance accurately reflects the associated risks.

In addition, Willis and HITRUST are in discussions with five other cyber underwriters regarding leveraging this approach, with an expectation that two more will be participating by midyear. It is clear that this approach is a win-win for the healthcare industry, underwriters, and of course, the members and patients whose information they are responsible for safeguarding.

For healthcare organizations, it drives better behavior in the industry, supports better control selection, and helps prioritize remediation activity, which ultimately provides better protection for patients. For cyber insurance underwriters, it ensures premium costs are proportional to risk, provides more targeted coverage relevant to actual risks, and ultimately provides a more sustainable underwriting model.

As you can see, the cyber security and risk management challenges facing the healthcare industry are complex and in some cases daunting, in many cases unique to industry dynamics, and they evolve at a pace that is unrealistic to manage by regulations and strict governmental policy or high-level policy document.

HITRUST, in partnership with industry, has been constantly working to establish programs to aid industry in mitigating cyber risks and is committed to be the link between the public and private sector that will continue to provide value and strengthen our industry, our government, our economy, and our nation as a whole against the growing cyber threats we face.

HITRUST saw an opportunity to bring relevant industry stakeholders together to help healthcare organizations better manage cyber risk and help the insurance industry better align cyber insurance premiums with this risk by leveraging a formal framework, like the HITRUST RMF. Risk management methodologies help companies address applicable regulations, standards, and best practices, and healthcare and insurance industry threat data helps identify high-risk controls requiring executive attention and link incidents to controls guidance. In many ways, this breach data helps inform insurance loss experience and allows cyber underwriters to play a key role in understanding where losses are occurring.

HITRUST also believes this current cyber insurance platform could provide the risk management focus to further drive innovation and encourage healthcare organizations to invest in maturing their information protection programs. HITRUST is working with underwriters to improve actuarial data and provide better estimates of risks while using threat and incident data to improve control selection within the HITRUST RMF. While we believe we have a novel approach and are leveraging new partners to grow its acceptance, mandates have the potential to stifle the innovations taking place in the marketplace. This market-based approach will provide a better insurance product for policyholders while allowing organizations to grow and mature their information security programs.

HITRUST, through its many tools and programs, remains committed to ensure that the healthcare industry can properly address these challenges. Cyber insurance will be a key component in HITRUST's approach to cybersecurity and cyber risk management, and we are excited about pioneering this approach to strengthen risk management.

Thank you again for the opportunity to join you today and share these insights. I look forward to your questions.