On June 2, the Health Care Industry Cybersecurity Task Force, established by Congress, issued a draft of its *Report on Improving Cybersecurity in the Health Care Industry*, an analysis of how to strengthen patient safety and data security in an increasingly interconnected world.¹ For industry outsiders, the contents of the report (which summarizes the state of cybersecurity to be in “critical condition”) are likely to result in shock and a sense of urgency for improving cybersecurity in this critical sector. For those within the industry, the report offers a preview of potential future government regulatory action and areas that should receive additional focus.

As part of the Cybersecurity Act of 2015 (Act), Congress created this task force “to address the challenges the health care industry faces when securing and protecting itself against cybersecurity incidents.” Under the Act, the secretary of the federal Department of Health and Human Services, in consultation with the director of the National Institute of Standards and Technology (NIST) and the secretary of the Department of Homeland Security, convened a diverse group of industry representatives to discuss these issues and develop recommendations. Their subsequent work has brought to light a number of critical areas for the health care industry to address.

The release of this report could not have been timelier, coming shortly after the debilitating worldwide “WannaCry” ransomware attack that, among other disruptions worldwide, forced hospitals in England to cancel surgeries and prevented them from performing even simple X-rays in emergencies. It highlights a number of critical issues that require the health care industry’s attention. In the report, the task force reveals six imperatives along with several recommendations and action items (these are summarized in an appendix at the end of this flash report).

Our Point of View

The recommendations detailed in the task force’s report bring to the forefront several issues facing the health care industry. One of the most notable themes in the report, for example, emphasizes the growing risk to patient safety in today’s environment. That’s a departure from the traditional industry focus on privacy and data protection and suggests that there’s a gap in the cybersecurity regulatory regime that needs to be addressed quickly.

The imperatives detailed in the report will affect health care providers and medical device manufacturers alike. These organizations should not wait for the government to initiate solutions. Instead, health care providers and medical device makers should proactively increase their own efforts to bolster cybersecurity. Why? First, many of the imperatives will require funding, a slow and dodgy process during any session of Congress, let alone one marked by the partisanship currently reigning in Washington. Second, retailers and other sectors have illustrated that private industry can find solutions to security problems on their own and thus avoid potentially overreaching or misaligned legislation.

Insights for Health Care Provider Leaders

Given the report contents, we recommend that health care provider leadership consider the following actions related to key themes in the report:

- **Theme in report: Existing efforts not enough and patient safety is at risk.**
  **Action: Expand cybersecurity efforts and include patient safety.**
  The task force has created a clear sense of urgency and laid out the case that existing cybersecurity efforts within the industry have not resulted in the desired end state. Health care provider leaders should use the report release as a reflection point to review their existing investments in cybersecurity, assess the results and determine whether additional improvement is needed. In addition, health care provider leaders should note the emphasis in the report on patient safety and ensure their cybersecurity program has fully addressed risks that could result in patient safety issues, not just a data breach.

- **Theme in report: Legacy devices are a significant problem.**
  **Action: Create a concrete plan for legacy devices.**
  The task force, in particular, notes the dangers of insecure legacy operating systems
that are still running many medical devices and electronic health record (EHR) applications. Additional governmental and regulatory scrutiny can be expected related to this issue, and health care provider leaders should formulate a plan to phase out or update legacy medical devices, ideally over the next five years, and implement compensating controls such as network segmentation, enhanced monitoring and application whitelisting in the next 12 months to help address the near-term risk.

We do not believe a “cash-for-clunkers” program, as suggested in the report, will materialize before the risk of legacy devices needs to be addressed, but we do believe that manufacturers will provide discounts and easier paths to replacing legacy devices as a result of the report. Health care leaders should be cautious, however, that the new devices do not suffer from the same issues as the legacy devices (e.g., they should ensure that expectations are aligned on longevity of device usage and support of security patches).

- **Theme in report: Lack of standard cybersecurity practices in industry.**
  
  **Action: Start formally aligning to a cybersecurity framework.**
  
  The report also recommends that HHS spearhead a consensus-driven initiative to develop a health care-specific cybersecurity framework built on the minimum standard of security provided by the NIST Cybersecurity Framework and the HIPAA Security Rule. We advise health care provider leaders to begin now to think about how they would align their controls to the NIST CSF standard.

  We expect that any developed framework will build on the NIST CSF with additional controls, rather than significantly alter it, and it pays to start alignment planning now as it takes time to remediate gaps in controls. For a framework that assists with both HIPAA and NIST CSF compliance, organizations should strongly consider HITRUST CSF. The Q3 2017 update to HITRUST CSF (version 9) is planned to include support for NIST CSF certification, and HITRUST will likely also provide a mapping to any future framework developed as a result of the task force report.
Insights for Medical Device Manufacturer Leaders

Medical device manufacturer leaders should also carefully review the report and consider the following Protiviti-recommended actions:

- **Theme in report: Lack of cybersecurity focus and SDLC gaps.**
  *Action: Expand cybersecurity efforts, focus on SDLC.*
  The report contains many recommendations focused on manufacturers, highlighting the gaps that exist in device-level security. Medical device manufacturer leaders should use the report as an opportunity to reflect on whether their medical device security program is adequate, given the increased attention on this area and the risks highlighted in the report. In particular, manufacturer leaders should dramatically enhance security throughout the software development lifecycle and be able to demonstrate clear security inclusion from new product model requirements through to eventual product model retirement.

- **Theme in report: Legacy systems are a hot-button issue.**
  *Action: Increase activities for reducing numbers of in-use legacy devices.*
  The report emphasizes the need to address legacy medical devices in multiple instances, with over 33 mentions of legacy devices within the report. To avoid potential patient safety impacts of compromised legacy devices (among other negative impacts such as bad publicity and increased legislation), it is important for manufacturers to further demonstrate a commitment to working with providers to reduce the number of legacy devices in use through customer education and incentives (e.g., free or low-cost upgrades to Windows 7 for device-supporting workstations running Windows XP, rather than having to buy entirely new solutions). We do not believe that medical device manufacturers should wait for or depend on a “cash-for-clunkers” program before creatively investigating all options, as the risks are likely to be further realized before such programs become available.

- **Theme in report: Minimum cybersecurity standards for medical devices.**
  *Action: Work with industry peers to develop a standard.*
  The task force also stresses the need for a minimum cybersecurity standard for medical devices, and we anticipate that future FDA approvals will be contingent on meeting it. Given that the device development process is typically five to seven years, we suggest that manufacturers collectively begin to collaborate on a set of minimum requirements to get ahead of regulation and avoid business disruption. Such collaboration could occur within the framework of an industry group such as AAMI.
but should include representatives from all stakeholder groups (e.g., health care providers, the FDA). The payment card brands adopted such a strategy with respect to credit card security and successfully improved security practices while avoiding additional government regulation.

**Closing Thoughts**

The Health Care Industry Cybersecurity Task Force took a year to complete its report, and the result is a very thorough look at the challenges facing health care security today. We believe this report will be recognized as a key step in encouraging more urgent action to address risks to patient safety and will serve as the basis for additional government guidance and oversight in health care cybersecurity for years to come. Health care provider and medical device manufacturer leaders alike would be well served through careful review of the report and determining how their individual cybersecurity plans will be impacted.
Appendix – Six Imperatives and Related Action Items

The task force provided six imperatives and several action items for each. These are:

1. Define and streamline leadership, governance and expectations for health care industry cybersecurity. (Page 22)
   - Create a cybersecurity leader role within HHS to align industry-facing efforts for health care cybersecurity.
   - Establish a consistent, consensus-based health care-specific Cybersecurity Framework.
   - Require federal regulatory agencies to harmonize existing and future laws and regulations that affect health care industry cybersecurity.
   - Identify scalable best practices for governance of cybersecurity across the health care industry.
   - Explore potential impacts to the Physician Self-Referral Law, the Anti-Kickback Statute, and other fraud and abuse laws to allow large health care organizations to share cybersecurity resources and information with their partners.

2. Increase the security and resilience of medical devices and health IT. (Page 28)
   - Secure legacy systems.
   - Improve manufacturing and development transparency among developers and users.
   - Increase adoption and rigor of the secure development lifecycle (SDL) in the development of medical devices and electronic health records (EHRs).
   - Require strong authentication to improve identity and access management for health care workers, patients and medical devices/EHRs.
   - Employ strategic and architectural approaches to reduce the attack surface for medical devices, EHRs and the interfaces between them.
   - Establish a Medical Computer Emergency Readiness Team (MedCERT) to coordinate medical device-specific responses to cybersecurity incidents and vulnerability disclosures.
3. Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities. (Page 35)

- Every organization must identify the cybersecurity leadership role for driving more robust cybersecurity policies, processes and functions with clear engagement from executives.
- Establish a model for adequately resourcing the cybersecurity workforce with qualified individuals.
- Create MSSP models to support small and medium-sized health care providers.
- Small and medium-sized health care providers should evaluate options to migrate patient records and legacy systems to secure environments (e.g., hosted, cloud, shared computer environments).

4. Increase health care industry readiness through improved cybersecurity awareness and education. (Page 40)

- Develop executive education programs targeting executives and boards of directors about the importance of cybersecurity education.
- Establish a cybersecurity hygiene posture within the health care industry to ensure that existing and new products/systems risks are managed in a secure and sustainable fashion.
- Establish a conformity assessment model for evaluating cybersecurity hygiene that regulatory agencies and industry could rely on instead of a diversity of auditors.
- The NIST Baldrige Cybersecurity Excellence Builder should be further developed 1) specific to health care, and 2) specific to the types of health care operations that are widely deployed across the industry and that have limited access to cybersecurity resources (small hospitals or practices, rural locations, etc.).
- Increase outreach and engagement for cybersecurity across federal, state, local, tribal, territorial and private-sector partners through an education campaign that includes meetings, conferences, workshops and tabletop exercises across regions and industry.
- Provide patients with information on how to manage their health care data, including a cybersecurity and privacy grading system for consumers to make educated
decisions when selecting services or products around non-regulated health care services or products.

5. Identify mechanisms to protect R&D efforts and intellectual property from attacks or exposure. (Page 47)
   - Develop guidance for industry and academia on creating economic impact analysis and loss for cybersecurity risk for health care research and development.
   - Pursue research into protecting health care big data sets.

6. Improve information sharing of industry threats, risks and mitigations. (Page 50)
   - Tailor information sharing for easier consumption by small and medium-sized organizations that rely on limited or part-time security staff.
   - Broaden the scope and depth of information sharing across the health care industry and create more effective mechanisms for disseminating and utilizing data.
   - Encourage annual readiness exercises by the health care industry.
   - Provide security clearances for members of the health care community.

*Future Considerations:* Five points, including developing a plan to implement the recommendations, conducting a risk analysis and establishing an ongoing public-private forum similar to the task force. (Page 54)
About Protiviti

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of Fortune 1000® and 35 percent of Fortune Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Contacts

Jeff Sanchez  
Managing Director  
Leader, Data Security and Privacy Management  
+1.213.327.1433  
jeffrey.sanchez@protiviti.com

Richard Williams  
Managing Director  
Leader, Healthcare Industry Practice  
+1.469.374.2469  
richard.williams@protiviti.com

Matthew Jackson  
Managing Director, Healthcare IT Solutions Lead  
+1.469.374.2479  
matthew.jackson@protiviti.com