HHS POINTS THE WAY FOR IMPROVED CYBERSECURITY

Last month President Trump issued an Executive Order on cybersecurity that called on all federal agencies to assess their status on information security and for the leadership to take steps required to mediate threats. Last week the Department of Health and Human Services (HHS) released its Healthcare Industry Cybersecurity Task Force report, which provides a dire picture of the vulnerable state of the country's healthcare system and embraces a progressive program long advocated in the marketplace (including at ISA) of dramatic actions required to secure it.

The report highlights that most healthcare organizations face significant resource constraints, lack intricate security infrastructures, and suffer from a skills shortage to identify, detect, and respond to potential threats.

To combat these issues, the HHS report wisely recommends several actionable items many of which follow advice long promulgated in the private sector. Three recommendations stand out.

1) Identify scalable best practices for governance of cybersecurity across the healthcare industry, and develop executive education programs targeting executives and boards of directors about the importance of cybersecurity education

Effective cybersecurity requires leadership at all levels of the organization, especially buy-in at the top levels. In the federal government, this is Secretaries and senior management. In the private sector, this is senior executives and boards of directors.

Several years ago, the private sector recognized a very similar problem with corporate boards and in 2014, ISA and the National Association of Corporate Directors (NACD) developed a Cyber-Risk Oversight Handbook and training program, which was updated in 2017. The key to this approach is to refrain from thinking of cybersecurity as a technical sense, but by embracing a full range of organizational strategic aspects.

In its 2016 Global Information Security Survey, PwC identified the Handbook and its approach as fundamentally altering the way corporate boards were understanding cybersecurity leading to, according to PwC, substantially increased budgets, better alignment between cybersecurity and organizational goals, improved cyber risk management and creating a culture of security throughout the enterprise.

HHS recommends healthcare sector governance and leadership follow the five specific core principles identified and promoted in the NACD Handbook, specifically:

- Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue
- Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances

- Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas
- Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget
- Board-management discussions about cyber risk should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach

If HHS and the health sector faithfully follow the path laid out in the NACD Handbook we can look forward to a dramatic alteration in how health care organizations understand and address the cybersecurity problem and hopefully similar positive results as we have found with corporate boards.

2) Require federal regulatory agencies to harmonize existing and future laws and regulations that affect healthcare industry cybersecurity, and establish a consistent, consensus-based healthcare-specific cybersecurity framework

The explosive growth in cyber regulations was an unintended consequence of the aggressive efforts to create cyber awareness. The "awareness" effort has succeeded so well now virtually every governmental entity has decided they need to police cybersecurity, leading to a weed-like crop of duplicative, redundant, costly, and ineffective regulations. Some ISA companies are reporting double and even triple digit increases in regulatory compliance costs without substantial improvements in security.

In fact, the increased regulation may actually be hurting the security effort as scarce cybersecurity personnel increasingly have to take time away from their security focus to address compliance regimes. .

In *The Cybersecurity Social Contract (2016)*, ISA stresses the need to not so much to de-regualte sectors like healthcare but to rationalize, harmonize, and streamline sector cybersecurity regulations.

What HHS recommends is consistent with our recommendations. HHS now advocates the healthcare sector needs to develop a single, healthcare sector-specific framework that harmonizes all privacy, security, and information risk-management requirements to eliminate opportunities for confusion and conflict. This would provide a single lexicon for the healthcare sector as well as guidance and clarity in the areas of security and cyber risk, best practices, education, and regulations.

3) Incentive the healthcare sector to implement best cybersecurity practices

Understanding the misalignment of economic incentives in the cybersecurity space and the need to rebalance the incentives has been a constant refrain for both industry and bi-partisan reports for years. ISA first called for this approach in its first Social Contract

publication in 2008, the House GOP Task Force on Cybersecurity endorsed it in 2011 and President Obama advocated for it in his Executive Order 13636 in 2013.

Yet, there has been very little work in this area and we desperately need a dynamic system that motivates continued, cost-effective security improvements through market-based incentives.

The HHS Report echoes these recommendations, calling for the federal government to evaluate incentive options, such as grant and tax incentives and good actor credits, to incentivize risk-based cybersecurity efforts within the healthcare sector.

A menu of market-based incentives has the potential to expedite adoption of safe, secure, and innovative new healthcare technologies that can improve upon the current state of security in this part of our nation's critical infrastructure.

HHS, with the release of its report, shows that government is slowly, but surely, beginning to understand the cybersecurity problem and the need to work in partnership with industry to combat it. We applaud HHS in their efforts.

Written by Larry Clinton, ISA President & CEO, and Stacey Barrack, ISA Senior Director