SQUIRE PATTON BOGGS

HHS Task Force Identifies Critical Cybersecurity Recommendations

The recent WannaCry ransomware attack and the bevy of breaches over the past few years demonstrate that cyber risks in the healthcare arena are substantial and widespread. The Department of Health and Human Services (HHS) Health Care Industry Cybersecurity (HCIC) Task Force Report (HCIC Report), required under the federal Cybersecurity Information Sharing Act of 2015, details many risks and recommended improvements across the healthcare sector. Released on June 2, 2017, after taking into account input from a diverse group of healthcare stakeholders, including organizations, industry experts and the government, the HCIC Report identifies six "imperatives" to improve healthcare cybersecurity:

1. **Cyber Governance**: Define and streamline leadership, governance and expectations for healthcare industry cybersecurity.
2. **Increase Health IT Security**: Increase the security and resilience of medical devices and health IT.
3. **Education**: Develop the healthcare workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities.
4. **Increase Preparedness**: Increase healthcare industry readiness through improved cybersecurity awareness and education.
5. **Protect IP and R&D**: Identify mechanisms to protect research and development efforts and intellectual property from attacks or exposure.
6. **Improve Information Sharing**: Improve information sharing of industry threats, weaknesses and mitigations.

Although some of the details recommended to achieve these imperatives may be considered controversial, the HCIC Report identifies some of the most critical risks and provides examples of measures every company can take today to mitigate cyber risk.

Unique Challenges for the Healthcare Industry

The Task Force findings are largely premised on the unique challenges that the healthcare sector faces due to its sheer size, diversity and interconnected nature, including:

- **Technology Evolution**: The healthcare industry has migrated to digital records and adopted new technologies more recently and rapidly than in other sectors, in large part due to government involvement (such as the push to adopt Electronic Health Records and facilitate interoperability through patient portals). In many cases, these advances have outpaced the implementation of appropriate cybersecurity controls – leaving healthcare entities in a precarious position. The adoption of countless new electronic systems and technologies increases the attack surface – places where attackers can wreak havoc or steal data – and many healthcare organizations lack the expertise and resources to secure these new technologies properly on an expanding attack surface. The HCIC Report also acknowledges the fact that health systems maintain a complex set of legacy systems, and that these legacy systems become increasingly difficult to secure and update over time.
- **Regulatory Patchwork**: A complex patchwork of federal and state laws regulates various parts of the healthcare industry. These laws, enforced by multiple regulators, impose overlapping and inconsistent requirements that can impose significant legal and technical burdens on healthcare organizations, not to mention time spent attempting to understand and harmonize them all.
- **Unique Data**: Health-related personal information is different and more valuable than other categories of personal information, such as payment card numbers that are more easily changed. Medical data about an individual tends to be permanent (e.g., an individual's genome or mental health diagnosis) and can be used for reputational harm or a wide range of financial gain over time.
- **Competing Priorities**: Healthcare entities face particular resource constraints and often (understandably) devote those limited resources to patient care over cybersecurity, or focus on achieving "compliance" with the patchwork of regulations instead of addressing the most significant security risks. Given the immediate focus on patient health and often very minimal profit margins, security professionals within the healthcare ecosystem – as with some other industries – report difficulty demonstrating the importance of implementing cyber protections and proactive measures to address cybersecurity risk within their organizations (despite the fact that it could ultimately save the business money and reduce the likelihood of reputational damage) unless there is an attack or breach.
- **Skilled Professionals**: The Task Force argues that even if substantial funds were available to be used to secure the digital resources in the healthcare industry, there are too few people with the combined expertise in both healthcare technology and cybersecurity to meet the current demand. This particular theme runs throughout the HCIC Report.

Recommendations

The HCIC Report breaks down the six "imperatives" into more granular recommendations and tasks, including:

1. **Cyber Governance**: The report recommends harmonizing cybersecurity laws and regulations, as well as creating a healthcare-specific Cybersecurity Framework modeled on the NIST Cybersecurity Framework to create a centralized standard and consistent security language. It also recommends appointing a single cyber lead within HHS. To help smaller organizations, the report suggests exploring exceptions to the Stark and Anti-Kickback laws that would permit large organizations to share cyber resources with smaller ones.

   Although the HCIC Report correctly recommends a more "risk-based" approach, the term, which has become increasingly common in organizational vernacular, is often misunderstood. A "risk-based" approach involves identifying the worst threats an organization faces (e.g., theft of its most sensitive data by an insider) and focusing cyber defense mechanisms on mitigating those risks. This approach does not involve planning defensive measures for every theoretical cyber attack on an organization (at least not initially) but prioritizing efforts after first understanding and identifying the biggest risks it faces.

2. **Increase Health IT Security**: The report recommends improving health IT cybersecurity (such as EHRs and medical devices) through efforts to secure legacy systems by improving transparency about risks between manufacturers and users. The report advocates applying risk management throughout the technological life-cycle of each medical device or IT network and improving authentication practices, including eliminating the use of passwords as the sole method of securing accounts and mandating two-factor authentication).

3. **Education**: The report emphasizes the need for organizations to develop additional expertise to ensure cybersecurity awareness and technical capabilities, including appointing a cybersecurity leader with Board-level engagement. The Task Force also recommends funding and encouraging low-cost managed security service providers (MSSP) for small and medium enterprises.

4. **Increase Preparedness**: The report encourages increased readiness through improved cybersecurity awareness and education for the healthcare industry as a whole. This could include, for example, an educational campaign to improve "cyber-literacy" for Executives and Boards of Directors.

5. **Protect IP and R&D**: Identify mechanisms to better protect research and development efforts and intellectual property from cyber attacks. The healthcare industry, the largest investor in R&D in the US, could increase the value of intellectual property by better protecting its IP and R&D, as the current IP value is arguably undermined through constant cybersecurity attacks.

6. **Improve Information Sharing**: The report recommends broadening the scope of Information Sharing and Analysis Organizations (ISAOs) to streamline and coordinate information sharing threats, working closely with the Department for Homeland Security's National Cybersecurity and Communications Integration Center.

Action Items

In the HCIC Report, the Task Force rightfully notes that cybersecurity risk management is an ongoing process that involves a complex, interconnected set of networks, systems and devices. Organizations must navigate this challenging environment to identify risks, control for the risks and take steps to monitor and improve the effectiveness of those controls on an ongoing basis. The group, therefore, calls on industry and the government alike to take a more proactive, risk-based approach and invest appropriately into managing cybersecurity.

The HCIC Report identifies recommendations that may not apply to every organization, but key steps that every healthcare organization can take right away to better manage cyber risk include:

- Evaluate and strengthen governance over cybersecurity. Appoint an individual who has the ability and authority (e.g., independence, budget and personnel resources) to make cybersecurity a priority.
- Train the workforce and executives about good "cyber hygiene." Then retrain.
- Prepare for an incident in advance with a tailored incident response plan. Practice incident response activities with tabletop exercises at varying levels within the organization.
- Take extra steps to secure connected devices that are used in healthcare or that store patient information.

Contacts

Elliot Golding
Partner, Washington DC
T +1 202 457 6407
E elliot.golding@squirepb.com

Tara Swaminatha
Partner, Washington DC
T +1 202 457 6031
E tara.swaminatha@squirepb.com