AHLA WEEKLY
5/18/2018

Death by a Thousand Cuts: Cybersecurity Risk in the Health Care Internet of Things

By Alaap Shah, Epstein Becker & Green PC

Risky Business: Health Care IoT

Health care continues to undergo lightning-fast transformation. Data is increasingly digital, devices are mobile, and technology is revolutionizing how care is delivered and reimbursed. Health care organizations adopt a variety of innovative technologies to improve efficiencies, quality of care, and health outcomes. As new systems are incorporated into networks and data flows are modernized, health care entities enter the brave new world of the Internet of Things (IoT).

The IoT, as applied to health care, seeks to leverage convenient, efficient, and automated devices and software applications to connect to health care information technology (IT) systems through computing networks. Health care organizations often pursue IoT efforts to find novel ways to engage patients, monitor health status, derive insights from clinical data, and advance care management and population health. Nevertheless, this rapid transformation carries risk that must be managed effectively.

Decentralization in Health Care Increases Privacy and Security Risk

By their nature, IoT architectures decentralize how and where patient data is collected, stored, and transmitted, creating significant risk to patient privacy and data security. Unlike historic technology paradigm where only a few entry points existed to a single repository of health care data, the IoT paradigm creates significantly more points of entry that can be leveraged to compromise a network and the data assets contained therein. While IoT carries enormous promise, health care organizations must responsibly carry out IoT strategies to maintain trust in the health care system as they remake how care is delivered and reimbursed. This is especially important in light of ever-increasing cybersecurity breaches impacting health care organizations and the individuals they serve.

Now that it is well recognized that the health care sector maintains valuable personal data on countless people, there is no dearth of malicious actors working to gain access to this data. To compound this problem, it is no longer just bad human actors seeking to breach the defenses of health care organizations. Strikingly, current estimates[1] indicate that about 50% of all internet traffic is *non-human* (such as bots and web crawlers), and about half of all non-human traffic is malicious in nature. In other words, at least 25% of Internet activity today is conducted by nameless, faceless programs that do not sleep or eat or otherwise interrupt their tireless pursuit to find ways to compromise systems connected to the Internet.

Unfortunately, managing security risk in health care is no longer about locking the front door or merely putting a firewall in front of your network. That paradigm no longer works. Highly distributed IT infrastructure comprised of cloud-based solutions and a cornucopia of connected devices power health care organizations. These types of highly distributed IoT infrastructures often require cooperation and coordination among multiple internal and external stakeholders. This creates

enormous risk for organizations unless appropriate risk management strategies are applied across of the entire network, including all IoT devices.

Effective Management of IoT Cybersecurity Risk

The growth in risk relative to adoption of IoT results from a number of factors. First, many IoT devices were developed with convenience and interconnectivity in mind rather than having privacy and security baked in. Second, IoT devices dramatically increase the attack surface for malicious actors to gain unauthorized access to networks, systems, and information. Third, if not properly configured, patched, and secured, IoT technologies could serve as an exploitable point of vulnerability in a network. Once compromised, IoT devices can serve as a toehold within networks to allow malicious actors to pivot into other parts of the network. Fourth, organizations are often unaware of the extent of IoT devices connected to the network such that organizations cannot effectively manage risk. Fifth, privacy and security responsibilities relative to IoT devices may be shared among organizations and their vendors without adequate clarity or communication.

Notwithstanding the cybersecurity risk posed by IoT, health care organizations can and should address such risks with robust risk management strategies. Primarily, organizations must distill baseline requirements from applicable legal and regulatory cybersecurity frameworks. This is easier said than done given the significant fragmentation of applicable standards and enforcement jurisdiction. By way of illustration, health care cybersecurity oversight mechanisms exist with numerous federal and state agencies such as:

- the U.S. Federal Trade Commission (FTC) (relating to consumer protection from unfair and deception practices);[2]
- the U.S. Department of Health and Human Services, Food and Drug Administration (FDA) (relating to medical device cybersecurity);[3]
- the U.S. Department of Health and Human Services, Office for Civil Rights (OCR) (relating to protected health information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH));[4]
- the Federal Bureau of Investigation (FBI) (relating to investigating cybercrime);[5]
- the U.S. Securities and Exchange Commission (SEC) (relating to insider trading and disclosure by publicly traded companies about cybersecurity issues);[6] and
- States' Attorneys General (relating to cybercrime, consumer protection, and enforcement under HIPAA, among others).[7]

Next, build on baseline requirements using best practices. A number of organizations issue guidance on best practices in cybersecurity such as the National Institutes of Standards and Technology (NIST),[8] the Health Information Trust (HITRUST) Alliance,[9] and the U.S. Department of Health and Human Services, Office of the National Coordinator (ONC).[10] Many of the agencies with cybersecurity-related oversight authority also issue guidance from time to time.

Finally, implement controls to manage risk related to IoT components of the IT infrastructure. These controls should evaluate IoT components throughout their lifecycle—from evaluation for adoption through sunsetting of the technology. Control strategies will vary from organization to organization but should address a combination of the following categories of activities.

1. Due diligence of IoT vendors and their products prior to acquisition and implementation;
2. Ongoing vendor management with respect to IoT technologies that are within the control of vendors or when data flows to a vendor as part of the IoT strategy;

3. Disable default accounts and reset default credentials within IoT technologies whenever possible;
4. Gain and maintain awareness of IoT technologies connected to the network through the use of network scanning software and other indexing mechanisms;
5. Develop robust policies and procedures for risk assessment, risk management, and security event response that address IoT technologies;
6. Segment out unsecure IoT technologies from core systems to reduce the size of the attack surface and minimize pivot points within the network;
7. Ensure routine anti-virus scanning and patching of IoT systems;
8. Block or otherwise limit unauthenticated IP traffic accessing and traveling IoT technologies;
9. Implement robust business continuity plans (including disaster recovery and emergency mode operations planning); and
10. Train personnel on developing and using IoT technologies with privacy and security in mind.

Practicing these principles will help health care organizations manage risk introduced by IoT technologies.

Conclusion

There is no such thing as perfect security. The threat and risk landscapes evolve continuously. Further, health care organizations continue to evolve rapidly and decentralize IT infrastructure through the adoption of IoT technologies. This climate creates the perfect conditions for significant cybersecurity risk. Nevertheless, establishing and carrying out effective risk management strategies can prevent exploitation of IoT technologies to compromise networks. As a result, effect risk management encompassing IoT architectures can reduce the likelihood and severity of data breach and the financial and reputational damage that often follows.

Alaap B. Shaw is a Member of Epstein Becker & Green PC in the Health Care and Life Sciences practice, in the firm's Washington, DC, office. His practice focuses on defense and counseling of health care entities on legal and compliance issues such as data security regulations, cybersecurity risk assessment, and fraud and abuse matters.

[1] *See* Imperva Incapsula, Bot Traffic Report (2016), *available at* https://www.incapsula.com/blog/bot-traffic-report-2016.html (last accessed Apr. 9, 2018).

[2] U.S. Fed. Trade Comm'n, Start with Security: A Guide for Business, *available at* https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business (last visited Apr. 9, 2018).

[3] U.S. Dep't of Health and Human Servs., Food and Drug Admin., Cybersecurity, *available at* https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm (last visited Apr. 9, 2018).

[4] U.S., Dep't of Health and Human Servs., Office for Civil Rights, Cyber Security Guidance Material, *available at* https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html (last visited Apr. 9, 2018).

[5] U.S. Fed. Bureau of Investigation, What We Investigate, Cyber Crime, *available at* https://www.fbi.gov/investigate/cyber (last visited Apr. 9, 2018).

[6] U.S. Securities and Exchange Commission, Cybersecurity, the SEC and You, *available at* https://www.sec.gov/spotlight/cybersecurity (last visited Apr. 9, 2018).

[7] *See e.g.* CA, Office of the Attorney General, California Cyber Crime Center, *available at* https://oag.ca.gov/c4 (last visited Apr. 9, 2018).

[8] U.S. Nat'l Inst. of Stds. and Tech., Cybersecurity, *available at* https://www.nist.gov/topics/cybersecurity (last visited Apr. 9, 2018).

[9] Health Information Trust Alliance, Cybersecurity Framework Overview, *available at* https://hitrustalliance.net/content/uploads/2016/01/NIST_HITRUST_Cybersecurity_Framework_Overview.pdf.

[10] U.S., Dep't of Health and Human Servs., Office of the Nat'l Coordinator for Health Info. Tech., Top 10 Tips for Cybersecurity in Health Care, *available at* https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf.