Healthcare Cybersecurity Themes for 2015

...And What to do About Them

Mark Coderre, OpenSky National Practice Director – GRC & Security Services

February, 2015

Healthcare is clearly a growing cyberattack target. Like any sector, healthcare leverages technology in unique ways. OpenSky has identified five areas of risk for particular focus in healthcare. To address these risks in the industry a combination of people, information, and technology must be employed. The resilience of this sector impacts all of us and our families.

1. **Nexus of incredibly sensitive data** – Healthcare organizations steward extensive personal information including behavioral health information, clinical diagnoses, future whereabouts through appointments, employer information/badge ID, family relations, SSN, and credit card numbers. While this wealth of sensitive information is essential to provide healthcare, it also makes patients vulnerable to social spear-phishing and identity theft with potential for repeated abuse. Having this information stored as big data in data warehouses makes it easier for hackers to steal large amounts of data in a single exploit. Healthcare organizations are attractive targets because of the value, velocity and quantity of data.

What can be done? First, develop and standardize mechanisms that provide data correlation and data processing without having all the data literally in one place. There are movements in the industry around privacy algorithms, field-level encryption, and tokenization that make a record less appealing because multiple keys are needed to get the full view. Since this impacts interoperability and efficiencies across the healthcare system, the sector must agree on the architecture. While data-at-rest encryption gets lots of attention, solutions at the disk- or file-system level are designed to protect against physical threats and underlying administrator account threats. Although the data has been protected from unauthenticated users, remote attackers with credentials can still access the data. Second, we must address the various means of protecting this information in transit. The solution for this has to factor that keys can be compromised. Asymmetric key management has to be a part of your strategy. Consider *all* the places you leverage encryption in transit including your business to business transactions – there is more than your web certificates and stake. Third, we have to prevent phishing and spear-phishing. Did you know that SMTP, the underlying protocol for email, allows a user to present any email address when sending messages? It's just a data format. Protocols have been developed under a standard called DMARC that address the spoofing problem, but to be effective all organizations must adopt it.

2. **Threat motivations are unique** - We must face the stark reality that personal harm, blackmail, ideological protest, familial fraud, claims fraud, and access to drugs and equipment are all potential motivations for attacks in the healthcare industry. The industry has made efforts to address privacy concerns, but we must also focus on these other threats.

It is imperative that the sector expand its efforts as a community and share information about attempted attacks quickly. This requires industry organization, agreements, and standardized data transports and formats. To facilitate information sharing, healthcare organizations are encouraged to join the NH-ISAC. Organizations should also develop both Security Operation Centers and Threat Intelligence Specialists that work with the technology architecture function to strengthen defenses. The organization's focus should extend beyond protecting existing assets and also focus on new assets and consumer use of technology. MITRE has developed protocols to allow normative sharing of both operational and mission intelligence regarding attacks. Operational data is the means by which attacks are conducted and can be used by Threat Intelligence Specialists, in real-time, to mitigate the impact of attacks. Mission data includes information about the motives and targets. Many organizations claim to share threat intelligence, but it is critical that both operational and mission data are harvested.

Threat Intelligence Specialists can also enhance the security of the software delivery methodology by influencing threat modeling in their security procedures. The NIST Cybersecurity Framework can be a helpful primer in this area. To be effective, threat models require the development and continual monitoring of a rich set of key risk indicators across the organization. Finally, to develop an appropriate security posture, it is important to associate threats to assets, and vulnerabilities to assets, which can be managed through a Governance, Risk and Compliance strategy.

3. **Assets in healthcare are unique** – Social Access? Got it! Mobile? Got it! Cloud services? Got 'em! Add to that devices that measure your every move and administer drugs to keep you alive, and you have a significant security challenge. Healthcare organizations need to consider not just the risks of each of these components, but conduct risk assessments on their combined use. Social and mobile applications offer several assurances of on-line identity, including four that are generally accepted by NIST. Determine which level of identity assurance is appropriate for each online transaction you offer. It is a best practice that needs to be part of the application development process. Use of cloud services needs to be monitored, categorized, and governed. For example, if a file-sharing solution like Box.com is approved via Single Sign-On and encryption plug-ins, high volume data movement to and from other services can be classified as suspicious. For medical devices, the FDA and MDISS organizations are working on best practices, but agreement on who is testing, who is enforcing, and who is aggregating threat and vulnerability information is still work in progress. Finally, network segmentation can be a helpful technique to protect assets especially medical devices which have threat appeal. In the past, we have been limited to routers and firewalls which have been difficult to manage and not always effective for threat defense. Today there are many different ways to zone your

network without classic segmentation using new technologies. We've identified as many as two dozen options to consider.

4. **An identity ecosystem** – Authentication has always been the control that undermines all other controls if compromised. Many of the major breaches of 2014 exploited weak authentication controls. We must do better job of validating who is who and strongly authenticating them. In the past, strong authentication has been viewed as difficult to use and inconvenient. However, a lot has been done with technology vendors and approaches from the National Strategy for Trusted Identities in Cyberspace, Kantara and FIDO (Fast Identity Online) to make authentication better and easier. In the healthcare sector, it doesn't stop there. To provide services, the healthcare sector needs interoperability unifying health delivery organizations, insurers, labs, pharmacies, etc. A central authentication working group is required for architects to collaborate on a solution. The technology pieces are all there; the joint architecture is missing. This needs to be an industry movement.

5. **Research and Analytics** – Healthcare improvements thrive on research. Research and analytics requires de-identified big data. HIPAA rules for de-identification are not as prescriptive as PCI. Under HIPAA rules, organizations are required to strip off enough elements to de-identify records, but records need a primary field to distinguish them (call it a pseudonym). If the pseudonym is too easy to reverse engineer, then de-identified data can be re-identified. Even if the records are adequately de-identified, hackers may be motivated to reverse engineer identity given the high value of healthcare records. Research organizations don't always have strong security controls because the data is expected to be inert. If no one broke into an originating organization, which ties the pseudonym back to the real PII, the data would remain secure. This is no longer a safe assumption. When data is de-identified, it can be based on tokenization (similar to PCI approach), alternative privacy identifiers (such as those proposed by VUHID), or identity syndicate models, which are starting to evolve.

How to Ensure Security in Healthcare

Phase 1 - Establish a security baseline: Ensure compliance with HIPAA and other controls that are appropriate, such as NIST 800-53. Although compliance is required, it does not ensure security. Make compliance reporting as efficient as possible, so it is less than 10% of your overall security labor, using a solid GRC strategy and architecture. When you start to measure something, you stop doing it. Focus on your key controls, and reconsider them monthly, or at least quarterly. These controls are viewed to address 80% of threats. Regulators expect you to be focused on your risks. When you become aware of the threats to your organization, you have a better sense of which controls matter most. For vendor security assessments select one

of the common vendor frameworks gaining traction in the industry. This is a conversation that can be discussed within the NH-ISAC. Work with your software development and/or enterprise architecture organizations to secure new applications and enhancements before they are in production. If the static scan or penetration test is the first time you evaluate vulnerabilities, you are already too late.

Phase 2 – Be a security risk leader: Focus on identity ecosystems and cyber-threat analyses including integrating threat feed information with key risk indicators. Develop secure coding practices. Complete NIST Cyber Security Framework Assessments. Optimize the CISO office functions such that processes are linked and information requirements are clearly outlined. Measure your controls continually using key performance indicators, instead of annual audits. Tie your top risks together using GRC and leverage that information to drive resource utilization. Integrate your security architecture function with systems and technology architecture teams. Healthcare organizations rely substantially on technology vendors such as McKesson and Siemens, so managing enterprise risk involves understanding those risks as well. Invest in your Security Operations Center and threat intelligence functions. Be hungry for data. You can't hunt for a needle in a haystack until you know what the needle looks like.

Phase 3 – Define security for your sector: Tie threat intelligence into threat modeling for your Systems Development Lifecycle. Leverage agile development teams to conduct iterative analysis and implement security improvements in your applications. Drive a security analytics program and link analytics to your GRC (there are data relationships in both directions). Implement counter intelligence measures and undocumented, black-box controls like honeypots. Tie security architecture to the information and business architecture functions. Refer to work from The Open Group with their integration of SABSA. They tie security design right to the business analysis process.

Mark Coderre is National Director of GRC & Security Services at OpenSky Corporation
Direct: 860.833.8710
email: mcoderre@openskycorp.com

Glossary of terms

Big Data - An accumulation of data that is too large and complex for processing by traditional database management tools.

CISO - A Chief Information Security Officer (CISO) is the senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.

CMS – Centers for Medicare and Medicaid Services, an agency of the U.S. Department of Health and Human Services.

Data-at-Rest Encryption – Encryption of data that is not moving through a network. i.e. data stored on a disk, or in a database.

Data Warehouse - A repository for all the data that an enterprise's various business systems collect for analytical use.

DMARC – Domain-based Message Authentication, Reporting & Conformance, DMARC is a proposed standard that allows email senders and receivers to cooperate in sharing information about the email they send to each other. This information helps senders improve the mail authentication infrastructure so that all their mail can be authenticated. It also gives the legitimate owner of an Internet domain a way to request that illegitimate messages (spoofed spam, phishing) be put directly in the spam folder or rejected outright.

FDA – The Food and Drug Administration (FDA) is an agency within the U.S. Department of Health and Human Services. FDA is responsible for protecting the public health by assuring the safety, effectiveness, quality, and security of human and veterinary drugs, vaccines and other biological products, and medical devices. The FDA is also responsible for the safety and security of most of our nation's food supply, all cosmetics, dietary supplements and products that give off radiation.

FIDO – Fast Identity Online is an open standard for a secure and easy-to-use universal authentication interface created to address the lack of interoperability among strong authentication devices. The FIDO standard supports multifactor authentication and strong features like biometrics.

GRC - Governance, Risk Management and Compliance organization, and system(s) that ensures proper governance, risk management and compliance management of all IT systems and processes that support the business operations.

HIPAA – Health Insurance Portability and Accountability Act, a US law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers. Developed by the Department of Health and Human Services, these standards provide patients with access to their medical records and more control over how their personal health information is used and disclosed. They represent a uniform, federal floor of privacy protections for consumers across the country.

Honeypot - In computer terminology, a honeypot is a trap set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers.

Kantara Initiative - A business acceleration organization that is a global, open, and transparent community of stakeholder experts representing enterprise operators, mobile operators, service providers, eGovernment agencies, IT vendors, and consumer electronics vendors. The vision of the Kantara Initiative is to ensure secure, identity-based, online interactions while preventing misuse of personal information so that networks will become privacy protecting, and more natively trustworthy environments. The vision will be realized through adoption of relationship based digital identity solutions to support and simplify our connected lives.

Key Risk Indicators - (KRI) is a metric for measuring the likelihood that the combined probability of an event and its consequences will exceed the organization's risk appetite and have a profoundly negative impact on an organization's ability to be successful.

MDISS - Medical Device Innovation, Safety and Security Consortium is a collaborative and inclusive nonprofit professional organization committed to advancing quality health care with a focus on the safety and security of medical devices. They serve providers, payers, manufacturers, universities, government agencies, technology companies, individuals, patients, patient advocates and associations. Their mission is to protect public health and well-being by advancing computer risk management practices to ensure wide availability of innovative and safe medical devices.

MITRE - MITRE Corporation has worked closely with the U.S. Government to strengthen the nation's cyber defenses for more than four decades. MITRE works with sponsors and industry partners to adopt effective new concepts and apply solutions in awareness, resiliency, and threat-based defense. MITRE advocates a balanced security posture that combines classic cyber defense approaches with a new emphasis on leveraging cyber threat intelligence to respond and adapt quickly to a cyberattack. To accomplish this, MITRE encourages partnerships that promote sharing cyber threat information and effective tools. Their strategy thrives on a foundation of unrelenting innovation and operational experimentation.

National Strategy for Trusted Identities in Cyberspace (NSTIC, or Strategy) - a White House initiative to work collaboratively with the private sector, advocacy groups, public sector agencies, and other organizations to improve the privacy, security, and convenience of online transactions.

NH-ISAC – The National Health Information Sharing and Analysis Center is the nationally recognized ISAC for the nation's healthcare and public health critical infrastructure by the nation's health sector, US HHS, US Department of Homeland Security, NSA, FBI, and the National Council of ISACs (NCI Directorate). NH-ISAC's mission is to enable and preserve the public trust by advancing health sector cybersecurity protection and the ability to prepare for and respond to threats and vulnerabilities.

NIST - National Institute of Standards and Technology is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

NIST released the first version of the Framework for Improving Critical Infrastructure Cybersecurity on February 12, 2014. The Framework, created through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.

The Department of Homeland Security's Critical Infrastructure Cyber Community C³ Voluntary Program helps align critical infrastructure owners and operators with existing resources that will assist their efforts to adopt the Cybersecurity Framework and manage their cyber risks. Learn more about the C³ Voluntary Program by visiting the C3 Web site.

Other relevant NIST Standards are NIST 800-53 (General Controls framework), NIST 800-66 (HIPAA Security cross-reference) and NIST 800-63 (eAuthentication assurance levels).

PCI – Payment Card Industry organization that includes membership from the major credit card brands including Visa, MasterCard, American Express, Discover, and JCB. The Payment Card Industry organization published The Payment Card Industry Data Security Standard (PCI DSS), a proprietary information security standard for organizations that handle branded credit cards from the major card members? Creators? Or just brands.. Private label cards --those without a logo from a major card brand are not included in the scope of the PCI DSS.

PHI - Protected Health Information as defined under HIPAA, is any information about health status, provision of healthcare, or payment for healthcare that can be linked to a specific individual. This is interpreted rather broadly and includes any part of a patient's medical record or payment history.

Phishing - Phishing is an e-mail fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal information from recipients including authentication credentials.

PII - Personally Identifiable Information, as used in US privacy law and information security, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

SABSA – Sherwood Applied Business Security Architecture is a framework and methodology for enterprise security architecture and service management. SABSA is a model and a methodology for developing risk-driven enterprise information security architectures and for delivering security infrastructure solutions that support critical business initiatives. The primary characteristic of the SABSA model is that everything must be derived from an analysis of the business requirements for security, especially those in which security has an enabling function through which new business opportunities can be developed and exploited.

SDLC - The Systems Development Life Cycle, also referred to as the Application Development Life Cycle, is a term used in systems engineering, information systems and software engineering to describe a process for planning, creating, testing, and deploying an information system. The systems development life-cycle concept applies to a range of hardware and software configurations, as a system can be composed of hardware only, software only, or a combination of both.

Security Operation Center – a location where enterprise information systems (web sites, applications, databases, data centers and servers, networks, desktops and other endpoints) are monitored, assessed, and defended.

Single Sign-On - a property of access control of multiple related, but independent software systems. With this property a user logs in once and gains access to all systems without being prompted to log in again at each of them. This is typically accomplished using the Lightweight Directory Access Protocol (LDAP) and federation protocols.

SMTP – Simple Mail Transfer Protocol is an Internet standard for electronic mail (e-mail) transmission. First defined by RFC 821 in 1982, it was last updated in 2008 with the Extended SMTP additions by RFC 5321 - which is the protocol in widespread use today.

Spear Phishing - an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source.

Spoofing - The practice of deceiving people into believing an email or Web site originates from a source that it does not. The most common type of spoofing is email spoofing, but Web page spoofing and IP address spoofing are also common.

The Open Group - a global consortium that enables the achievement of business objectives through IT standards. With more than 450 member organizations, TOG has a diverse membership that spans all sectors of the IT community — customers, systems and solutions suppliers, tool vendors, integrators and consultants, as well as academics. TOG mission is:

- Capture, understand and address current and emerging requirements, and establish policies and share best practices
- Facilitate interoperability, develop consensus, and evolve and integrate specifications and open source technologies
- Offer a comprehensive set of services to enhance the operational efficiency of consortia
- Operate the industry's premier certification service

Threat Management - a cybersecurity management framework with the following objectives:

- Provide non-proprietary data exchange approaches (for security-related data capture and analysis)
- Characterize complex or aggregated data "patterns" in utilizing ontologies or RDF-based databases or related tools

- Provide a knowledge sharing framework for the community of defenders and security experts who analyze existing or predict future threats
- Build policies based upon Threat Activity and Threat Prediction – policies that can also be captured, manifested and distributed using Semantic technology
- Drive dynamic reconfiguration of H/W and S/W infrastructure in response to policy definition and distribution

Threat Modeling – a procedure for optimizing network security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent or mitigate the effects of threats.

VUHID - Voluntary Universal Healthcare Identification is a project with a goal to make unique healthcare identifiers available to any patient who uses the services of a regional health information organization (RHIO) or health information exchange (HIE) to:

- Enable error-free linkages of clinical information across provider sites
- Enhance patient control over the privacy their information
- Improve the quality of medical care and the efficiency of its delivery
- Reduce medical errors related to mis-identification of patients
- Decrease incidents of healthcare-related identity theft
- Help control healthcare costs as a result of these impacts

VUHID is based on two ASTM International E 31 standards (ASTM VUHID Standard E2553 & ASTM VUHID Standard E1714) to make globally-unique healthcare identifiers available to any person who wishes to have one. Global Patient Identifiers, Inc. (GPII), a non-profit organization, was formed specifically to develop and deploy the VUHID system.