Information Security Challenges in Healthcare—Dialing In on Mobile Devices

It now seems more distant, but in 2007 and 2008 our world changed with the advent of the iPhone and Android respectively. Preceding those innovations, we had RIM's Blackberry®. The Blackberry® turned out to be the most secure (but eventually cumbersome) PDA—with its vertically integrated applications platform and dedicated network. As mobile devices proliferated so did the networks supporting them and the applications that could be used with them, exponentially increasing the vulnerability of our data and the attack surfaces used to exploit protectable and private information.

Mobile devices are now ubiquitous business and productivity computers continuously connected to the internet on the closest available network; repeatedly downloading and uploading a mixture of personal and corporate information. Compared to laptops, mobile devices carry some characteristics that heighten the risk of compromise. Without user intervention, they connect to networks that match the characteristics of previously known networks, which means that if someone can impersonate a known network, the device will connect to it.

Regrettably, users may not detect a well-masked malicious application that surreptitiously exfiltrates data or bogus Wi-Fi networks that impersonate legitimate networks but actually intercept or even change intended mobile device communications. Even genuine applications, operating systems and networks have weaknesses open to attack. Technology and human behavior have radically altered the landscape of data protection. The abundance of productivity and other applications for mobile devices, and our insatiable desire for easier, faster solutions that require no mental effort only exacerbate the problem.

The technological evolution of healthcare record management, remote medical services, health services and pharmaceutical products, and government and third-party payor data use and management create acute care problems for healthcare-related institutions. The prognosis seems to vacillate. In the end, the most common responses to all threats remain: human vigilance, encryption, robust authentication and password protocols, threat detection processes, and well-developed incident response plans.

So why are these information security problems so resilient and resistant to treatment in healthcare? Virtually all healthcare companies have secure document delivery tools, and train their employees on how to use them. Surveys reveal that well over eighty percent of healthcare employees understand how to use tools and understand institutional security rules, but many admit they do not use them due to convenience or necessity. A majority of healthcare workers acknowledge, when it comes to transferring healthcare data, documents, or information, they do whatever is easiest, including email. A disturbing 87 percent of healthcare workers admit to using non-secure email to send sensitive information, including PHI, according to survey data provided to *HealthITSecurity.com* by Kickstand Communications, which conducted the survey for secure file sharing services firm Biscom. Healthcare workers are 36 percent more likely to share regulated data such as patient information and credit card information via non-secure methods such as email than those working in financial services.

These trends are borne out by **Verizon's Protected Health Information Data Breach Report (2018)**, which suggests a higher incidence of serious security incidents and actual breaches than other industries experience. Healthcare saw a 47 percent jump in cyberattacks in the first quarter of 2018 compared with the fourth quarter of 2018, according to McAfee Labs. Healthcare was the most targeted sector in terms of the number of breaches in the 2017-2018 period, followed by the public sector and education.

On August 2, 2018 the FBI released a "public service announcement" regarding the deployment of Internet of Things (IOT) devices in the healthcare arena and the increased cybercrime directed to them. (**www.fbi.gov**).

There are many potential explanations for vulnerability in healthcare. One is the fact that healthcare is a target rich environment, and attacks such as ransomware are efficient, low risk crimes. HIPAA Security Rule and Omnibus Rule reporting requirements reveal events that might never surface in other fields. Another is time pressure and even medical necessity. Another is the proliferation of mobile workstations and mobile devices using a mixture of applications that are continuously reaching for updates and passing credentials to servers and services.

Often, system planners, to meet the demands of their constituents, favor speed over security, making the device data streams a rich source of data to intercept or manipulate. The risk of a user installing a mobile application or a profile that has nefarious purposes is high. The application source is a concern (the largest sources for malicious applications are application stores outside Apple and Google Play) as well as unpatched vulnerabilities in the device OS and/or applications. Not only should applications be kept updated, but good sources also have to be used to ensure that genuine updates are applied. In addition, mobile devices need to be physically protected—just having the device may be enough to expose it to infiltration.

As a large percentage of security incidents and breaches are the work of insiders, they may cause direct exfiltration of data, possibly bypassing data loss prevention (DLP) systems, and violation of administrative controls (restrictions on user behavior). Phishing and ransomware attacks by outsiders normally result from fooling users to install malicious profiles, malware or repackaged apps that then can be used to transmit or relay data.

Phishing has become the preferred method for hackers to get access to healthcare organizations to steal valuable medical data and/or deploy ransomware. The **2018 Verizon Data Breach Investigations Report** found that phishing and financial pretexting — obtaining financial information under false pretenses — represented 93 percent of all breaches investigated by Verizon, with email being the main entry point (96%). Often phishing is the way attackers deploy ransomware, which has devastated the healthcare industry over the last couple of years. DBIR found that ransomware accounts for 85 percent of the malware in healthcare.

Cyber criminals are increasingly targeting victims through a text message scam called "smishing" that can infect smartphones and let thieves steal personal and business information. That means social security numbers, addresses, and credit card information can all be vulnerable through a simple, unassuming text message you receive. It may also provide entry into work networks including credentials or facilitate future spearphishing attacks by investigating communication patterns. Hackers usually send the smishing messages with a link or phone number. If the user calls or clicks, the hacker will be able to harvest more data.

Much has been written on HIPAA compliance challenges associated with text messaging in healthcare contexts. Ordinary text messages are not private or inaccessible. A virtual cottage industry has emerged to offer HIPAA compliant text messaging platforms or protocols. Text messaging has eliminated pagers and improved critical flow of immediately needed information for treatment. Any adoption of this modality must be focused on the clinical setting and necessity for use. Further, healthcare organizations must incorporate the same types of protections that should be in place for email: network and in transit encryption, multi-factor authentication, limited access to a secure messaging account, remote device kill switch software, prevention of copying or forwarding PHI, removal of PHI from notification screens, segregation of personal messages, detailed and complete archiving of messages, and aggressive lock-out procedures for failed log in attempts.

Healthcare entities may defend against these risks on mobile devices with good password practices, and on-device encryption if enabled by the user. Another protection—biometric authentication--is taking hold, but is only as effective as the security of any accompanying back up password or PIN, which can be broken. All of these protections may still depend on the user's management of device settings and access through successful attack on the network the user accesses. Also, many institutions are opting for the virtual app/environment. This approach, particularly in the form of a Virtual Desktop Interface (VDI), has been successfully used in bring your own device (BYOD) or remote office computing environments. It can work with mobile devices and enhance authentication.

So two aspirin and call me in the morning is not viable. Minimally, to take advantage of evolving mobile communication tools and processes, healthcare entities should:

- Plan proactively to build security into implementation of new technologies;
- Test all new connected medical or mobile devices;
- Careful legal review of all third-party contracts and Business Associate Agreements when integrity of PHI or entry to network portals is at risk;
- Train, train, train employees on cyber hygiene and HIPAA and other federal and state law requirements;
- Develop a comprehensive incident response plan with specific workbooks for anticipated threats, identification and coordination of internal and external resources, and table-top practice exercises;

- Implement robust:
    - Encryption
    - Password and multi-factor authentication
    - Procedures to patch and apply all updates
    - Processes to change all default user names and passwords or device settings
    - Firewalls configured to block traffic from unauthorized IP addresses
    - Server and data segregation
    - Frequent systems/data back up
- Mark incoming emails with a simple warning to heighten sensitivity: CAUTION: External E-Mail