CONNECTED HEALTH:

Balancing Clinical Care Goals with Security Needs

A doctor is working with a diabetic patient. The doctor recommends that the patient use a mobile app that enables him to electronically share glucose readings with clinic staff on a daily basis. As such, nurses can closely monitor the patient's progress and alert the doctor if treatment intervention is needed. Through this simple electronic communication, care improves. And, while the patient doesn't really want his glucose readings to get "hacked" and become public knowledge, the fact of the matter is that he is not really concerned about it, as he doesn't think his blood sugar readings are all that interesting or valuable to anyone.

The security risks, unfortunately, do not start and stop with the patient's glucose readings. "The real pernicious thing is that the app could be set up to transmit data directly to the hospital through some kind of HL7 (Health Level Seven) integration. And, if the patient is using the app on an unsecured network where the device has been breached in some way, then the credentials used by the app to log into the hospital system can be compromised," said Jonathan Cohen, vice president of product strategy at Synchronoss, provider of secure mobility solutions. "So, a lateral attack on the device could be used to get to the hospital's electronic medical records system and the treasure trove of information that it houses."

Indeed, once an unauthorized user gains access, plenty of harm can be done, according to Lee Kim, JD, CISSP, CIPP/US, director of privacy and security at HIMSS. "After the target is profiled by the attacker, a delivery mechanism is selected for the payload (e.g., a malicious e-mail attachment to be delivered via a phishing e-mail) and the compromise or exploit is executed (if successful). Malware is harder to detect due to advances, such as fileless malware, steganographic malware, and malware which is individually customized for the target (thus diluting the value of indicators or compromise)," she warned.

Synchronoss

Produced in partnership with

HIMSS Analytics

Therein lies the security risks associated with seemingly innocuous applications and connected devices. What's more, the fact that healthcare data, which often contains a patient's financial information in addition to personal health information, is worth more than $300 per record on the black market[1] – compared to an average of $158 per record across all other industries[2] – makes this risk one that cannot be ignored. Indeed, healthcare organizations are struggling in an environment where attacks are becoming more common and virulent. In fact, 80 percent of providers in 2016 admitted that their organization had experienced a recent "significant security incident," according to the *2016 HIMSS Cybersecurity Survey*.[3]

Balancing promise and peril

Innovative mobile technologies and valuable web-based applications such as physician and patient portals promise to help organizations improve clinical care and succeed under value-based models. The challenge boils down to simultaneously taking advantage of the multitude of connected health solutions to improve patient care while also maintaining – or even increasing – security.

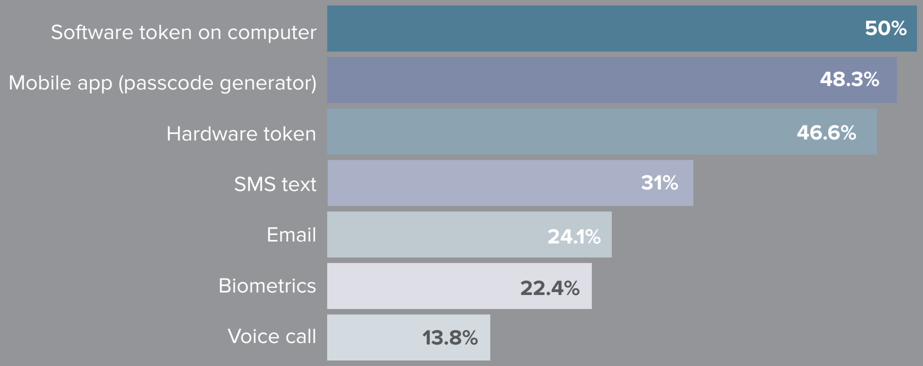
"When you open up all these avenues to information, you inherently increase the exposure you have to security issues, threats and risks. It's a double-edged sword. Healthcare organizations want to become more collaborative and provide more access points to information. When they do that, however, they greatly increase the risk not only to the confidentiality of that data but to their security position in general," said Michael Wood, product marketing manager at Synchronoss.

In fact, data security becomes exponentially more complicated as organizations add applications and access points. "Greater complexity means greater attack surface," Kim said.

One way to improve security in such an environment is to verify the identity of users – both healthcare professionals and patients – who are gaining access to the system. As such, healthcare organizations need to ensure that users are who they say they are, especially when they are accessing protected health information (PHI) and personally identifiable information (PII). Ensuring secure online access has become so important, in fact, that it is part of the federal government's Cybersecurity National Action Plan, which was issued in February of 2016. A critical component of this plan focuses on empowering Americans to better secure their online accounts by moving beyond just usernames and passwords, and adding an extra layer of security. In fact, to accomplish this goal, the National Cyber Security Alliance, together with nonprofit membership organizations and private sector companies, has launched the "Lock Down Your Login" campaign, a public-private campaign designed to enable every American to better secure their online accounts through the use of strong authentication.[4]

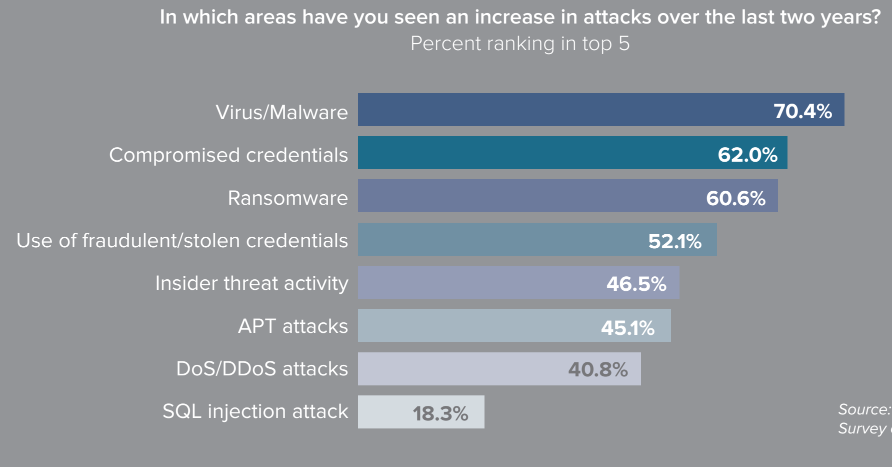
> *A lateral attack on the device could be used to get to the hospital's electronic medical records system and the treasure trove of information that it houses."*
>
> **Jonathan Cohen**
> *Vice President of*
> *Product Strategy*
> *Synchronoss*

FIGURE 1. As security mechanisms, multi-factor authentications (MFAs) ensure individuals are authenticated through more than one required validation procedure. Below are the most common methods.



Source: HIMSS Analytics/Synchronoss Survey of healthcare IT leaders, 2017

FIGURE 2. Increases in attacks most likely come from virus/malware, ransomware and compromised credentials.



Source: HIMSS Analytics/Synchronoss Survey of healthcare IT leaders, 2017

Multi-factor authentication (MFA) can potentially serve as a powerful component of such efforts. MFA is a security mechanism in which individuals are authenticated through more than one required validation procedure. A combination of validation techniques is used to verify identity and allow access (Figure 1). As such, MFA adds another layer of security on top of the commonly used username and password.

"If you have the ability to take something that you know (a username or password), and match that with something you have in your possession, (some type of device) or something you are (a biometric), then it is significantly more difficult for someone to hack into systems by simple brute force attack," Cohen said.

Taking control

The need for this heightened access control is undisputable. Consider the following: According to the 2016 Verizon Breach Report, 63 percent of confirmed data breaches involved leveraging weak, default or stolen passwords, and more than 95 percent of web-application incidents involved stolen credentials.[5] And, according to a recent research conducted by HIMSS Analytics on behalf of Synchronoss, 62 percent of the 75 C-suite, director and manager level IT professionals responding to a survey cited compromised credentials as an area where they have seen an increase in attacks over the last two years, ranking second just behind virus/malware, which was cited by 70.4 of respondents (Figure 2).

Fortunately, healthcare leaders have acknowledged the value of MFA, as 83 percent of healthcare organizations employ the security technology, according to the HIMSS Analytics/Synchronoss study (Figure 3). Nearly 9 of 10 survey respondents cited the ability to directly control security as the reason their organizations adopted MFA over other data security options (Figure 4).

The problem: Most healthcare organizations are not leveraging MFA where it counts. In fact, only 56 percent of organizations use MFA with their electronic medical records (EMRs); 52 percent with e-prescribing for controlled substances; 28 percent with patient portals; and just 25.3 percent with physician portals, according to survey results (Figure 3).

"There's no magic bullet," Cohen said. "MFA is one defense that should be included in a robust defense in depth strategy. But frequently it's one that's overlooked."

Many healthcare organizations do not fully leverage MFA because of perceived inconvenience. "Healthcare providers are under pressure to efficiently provide high quality care and see more patients to lower the cost per encounter. Even taking an important step to improve security often won't be taken if it adds obstacles to access," Cohen said.

Even if the second authentication method is not overtly time consuming, busy clinicians are apt to balk. "The last thing a clinician wants to do is fumble around for a token or enter an additional passcode to enter into a system. Even those trivial amounts or extra effort are resisted by clinical users," Cohen noted. "And so, the challenge becomes how do you cost effectively get the security of a second or multiple factors added into the authentication process without adding any additional time into the process?"

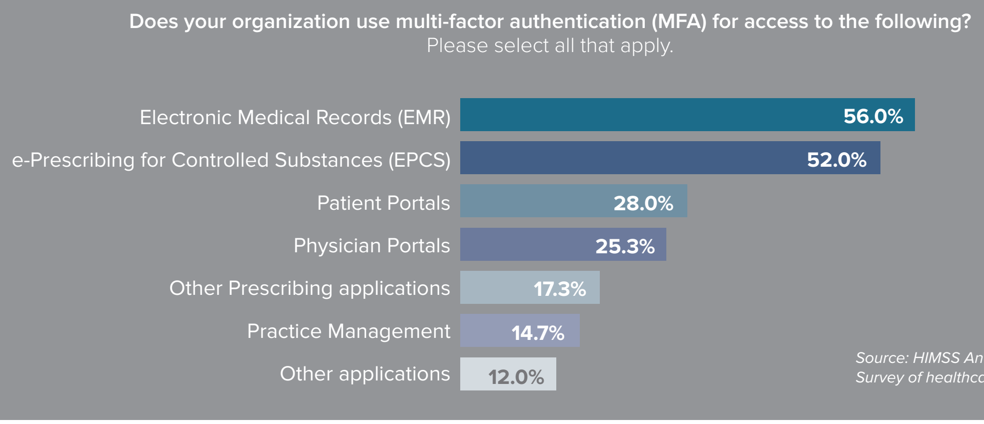
Unfortunately, many commonly used authentication methods come up short when subjected to this litmus test. Hardware tokens, which cost anywhere between $40 and $100 each, are not easy to use, because clinicians have to carry around one more thing. "Imagine, you're a physician and you are on call and you drive to the hospital at 3 a.m. only to discover that you have left the token at home," Cohen posed. "Now what do you do?"

Sending verification codes by text is another less-than-optimal authentication method. Receiving and entering the extra verification code takes time, and that disengages clinicians and patients. "Patients often have a hard enough time just using the username and password. Now, you are going to add this code that is sent to text – and that will be a challenge for many – especially patients who are elderly or not technology savvy," Cohen said.

To make MFA more usable, vendors need to provide solutions that "integrate the MFA with hardware that you buy off the shelf, so there is no additional expense. It has to be a cost-effective solution for the provider and one where users are not fighting with the technology," Kim said.

> *"MFA is one defense that should be included in a robust defense in depth strategy. But frequently it's one that's overlooked."*
>
> **Jonathan Cohen**
> *Vice President of Product Strategy*
> *Synchronoss*

FIGURE 3. 83% of respondents use MFA; EMR and EPCS access most likely to use MFA.



Source: HIMSS Analytics/Synchronoss Survey of healthcare IT leaders, 2017

For example, proximity log-in is one cost-effective authentication method that can help to remove the end-user friction without sacrificing security. With this method, solutions leverage an identity credential bound to a Bluetooth-enabled smartphone. To gain access, users simply walk up to the computer or mobile device and verify their identity through their personal smartphone. With the option of quick response (QR)-based authentication, there's no need to enter usernames and passwords. Where increased security is desired, an additional PIN or password can be incorporated to add another layer of security onto the authentication process.

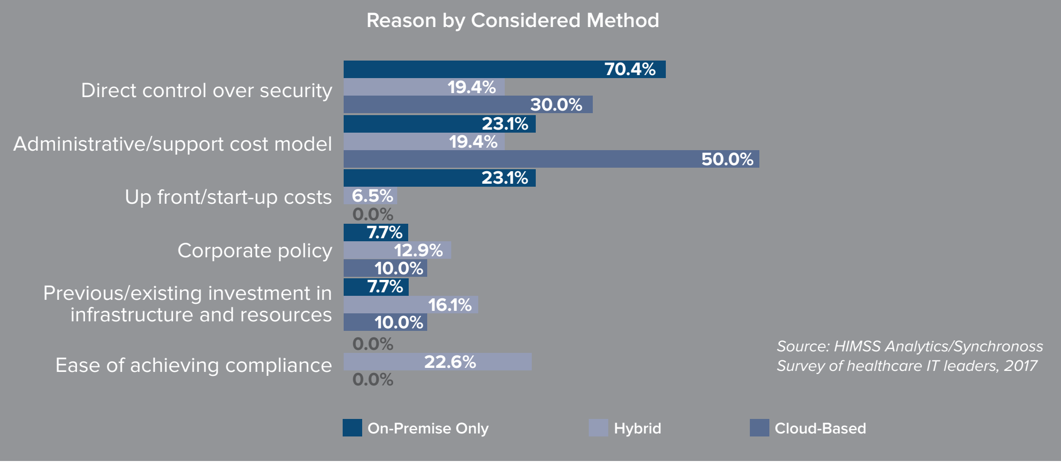
"Having a credential on their smartphone confirms that they are who thy say they are. So, there is no longer a need to enter lengthy pass codes to verify identity," Cohen said. "Users simply log in and access the application they need because their smartphone vouches for their identity. With this method, healthcare organizations remove the friction, but not give up on security."

As such, healthcare organizations can empower staff members and patients to fully leverage connected health technologies and, in the process, move toward improved clinical outcomes – without requiring cumbersome additional steps to verify identity and, perhaps more importantly, without putting PHI and PII at risk.

> *"It has to be a cost-effective solution for the provider and one where users are not fighting with the technology."*
>
> **Lee Kim, JD, CISSP, CIPP/US**
> *Director of Privacy and Security HIMSS*

FIGURE 4. Security top reason for on-premise MFA implementation considerations.

What is the main reason your organization would choose the specified method over the others?



Source: HIMSS Analytics/Synchronoss Survey of healthcare IT leaders, 2017

For more information on the HIMSS Analytics / Synchronoss survey or Synchronoss solutions, contact info@synchronoss.com

References

[1] FireEye & Synchronoss Analysis.
[2] 2016 Cost of Data Breach Study: Global Analysis. Ponemon Institute/IBM. 01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN
[3] 2016 HIMSS Cybersecurity Survey. http://www.himss.org/hitsecurity
[4] The White House. FACT SHEET: Launch of the "Lock Down Your Login" Public Awareness Campaign. whitehouse.gov/the-press-office/2016/09/28/fact-sheet-launch-lock-down-your-login-public-awareness-campaign
[5] 2016 Verizon Breach Report. verizonenterprise.com/verizon-insights-lab/dbir/2016/

Synchronoss

About Synchronoss:

Synchronoss (NASDAQ: SNCR) is an innovative software company that helps enterprises, healthcare and government agencies realize and execute their goals for mobile transformation now. Our simple, powerful and flexible solutions serve millions of mobile subscribers and a large portion of the Fortune 500 worldwide today. For more information, visit us at: http://synchronoss.com/industries/healthcare.