healthcare informatics presents...

Before It's Too Late

A Compendium on Healthcare Cybersecurity

As the healthcare industry continues its push forward for more accessible data, greater interoperability, and an increased lean on mobile devices, one of the biggest questions that need to be answered is, Can patient care organizations across the U.S. properly secure the influx of data both within and outside of their walls?

Indeed, data security is as hot an issue in healthcare as it ever has been.

As such, ***Healthcare Informatics*** has created a compendium of recent articles on cybersecurity as CIOs, CISOs, and other experts across the spectrum are increasingly looking to get their organizations out in front before it's too late.

CONTENTS

Shedding Some Light on the Problem of Medical Data Loss

A Verizon Enterprise Solutions study finds that 90 percent of all industries have experienced a PHI-related data breach and almost half of PHI data breaches involved lost or stolen devices.

While the healthcare industry has the most data breaches involving protected health information (PHI), 90 percent of all industries have experienced a PHI-related data breach in the past 10 years, according to a Verizon Enterprise Solutions study report.

Also among the *study* findings, unencrypted lost and stolen devices, such as laptops, are a big problem in the healthcare industry, as 45 percent of PHI-related data breaches were related to lost or stolen assets. And, detecting a data breach continues to be a problem for organizations that handle PHI as the study found that 31 percent of incidences in 2014 took months for information security teams to detect. And, 18 percent of incidences took years to be detected. The study authors found that the incidents that took years to discover were over three times more likely to be caused by an insider abusing their LAN access privileges, and twice as likely to be targeting a server (particularly a database).

In its Verizon Protected Health Information Data Breach Report, Verizon Enterprise Solutions analyzed 1,900 data breaches and 392 million records in order to take an in-depth look how PHI breaches happen, how long it takes to discover a breach, how PHI breaches affect the doctor-patient relationship, and how to mitigate the risks. While the oldest record in the study is from 1994, most of the data security incidents in the study occurred between 2004 and 2014.

When breaking down PHI-related data breaches by industry, the healthcare industry, unsurprisingly, had the largest number of incidences at 1,403; however, one surprising detail out of the study was that all but two of the top-level industries also had PHI-related data breaches as well. For instance, finance had 113 breaches that included PHI, educational had 51 incidences, retail had 43, professional had 35 and administrative had

21 incidences. Even manufacturing had 10 incidences and trade had 10 incidences where PHI was lost.

"That's one of the more interesting points that comes out of this report, which is that PHI not just a healthcare industry problem, and, conversely, this report also shows that payment card industry (PCI) information is not just a retail problem," Marc Spitler, senior analyst at Verizon Enterprise Solutions and co-author of the Verizon Protected Health Information Data Breach Report, says.

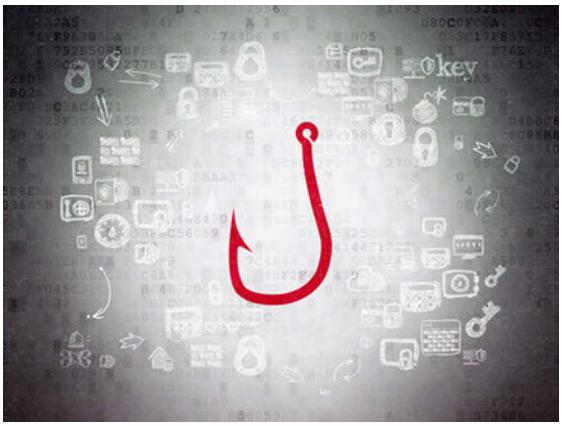
The study authors attribute the loss of PHI data in other industries to factors such as worker's compensation claims, companies collecting health or medical information for wellness programs and collecting PHI as part of managing employee health insurance programs.

For the purposes of the study, the study authors defined PHI as personally identifiable health information collected from an individual, and covered under one of the state, federal or international data breach disclosure laws. PHI may be collected or created by a healthcare provider, health plan, employer, healthcare clearinghouse or other entity.

"The main criteria is whether there is a reasonable basis to believe the information could be used to identify an individual. In the U.S., the disclosure of this type of information would trigger a duty to report the breach under the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH) and one or more of the state laws," the study authors wrote.

Also, because the purpose of the study was to focus on the most common ways PHI is disclosed, the study included records that were not only within the healthcare industry, but also records in which the data type lost was classified as "medical records" and the data subject/victim relationship was identified as "patient."

According to the study, external "actors" were behind a large number of PHI breaches (903), yet internal "actors" were responsible for 791 incidences, followed by partners with 122 incidences.



The study also indicated that the top three Actions related to PHI incidents were Physical, which is primarily theft of devices that contain PHI or tampering with devices, Error, which includes lost devices that contain PHI or mis-delivery of medical information, such as an email containing PHI sent to the wrong person, and Misuse, which entails an internal actor misusing their access to PHI in a malicious or inappropriate way.

With regard to external threats and theft, Spitler says it's important to be aware of the motives behind these PHI-related data breaches, which is typically to get to the personal information that's often included in medical records, such as names and social security numbers. Even when medical records are taken with malicious intent, it is frequently the associated personally identifiable information (PII) that is targeted and used to commit various types of financial crime, including tax fraud and identity theft.

And, there are many paths that cyber attackers can use to get to PHI data, whether it's theft, using an insider to access the data, disabling physical controls or phishing. The challenge for healthcare organizations and other organizations that handle PHI is to tailor mitigations to make it more challenging for an attacker to compromise PHI.

"No organization is completely secure, but you want to put up as many obstacles for the attacker to overcome as you can within your existing resources. The biggest challenge is that you need to stop every way an attacker can get from that first action to their final goal," the study authors wrote. "The idea is that if you make it more difficult for the attacker to get to their ultimate goal, they'll move along to an easier target."

When analyzing incident patterns, the study also found that almost half of the PHI-related data breaches (45 percent) involved lost or stolen assets, such as laptops or devices.

"It is frustrating to see this category return year after year because it's one of the more easily solved problems," the study authors wrote.

Spitler points out that encryption, particularly on portable devices not directly used for patient care, would significantly reduce the risk of a data breach even if a device is lost or stolen.

"You can completely prevent loss or stolen assets, but what you can do is lessen the impact and encryption on mobile devices is a no-brainer as it would limit the loss of the company to the physical asset itself," Spitler says. "Full disk encryption is not really a bleeding edge technology, and it's not an overly expensive technology. There's even a lot of onboard ability on these operating systems now to provide that level of encryption."

The study authors state that even if organizations only encrypt a subset of their portable assets, it will reduce the overall risk of a breach on those assets that are not directly used for patient care

The study also found that 85 percent of the PHI-related data security incidents included in the study could be described by three incident patterns—lost and stolen assets, privilege misuse and miscellaneous errors.

With regard to privilege misuse, Spitler encourages healthcare organizations to track user access as it relates to PHI data.

"Make sure that you are able to attribute access to a particular person, so everybody should have an account that is specific to them so there is no sharing of passwords," he says. Employee security awareness programs should include sanitized results of audits that catch people abusing their access as well as educating employees that abusing their access in collusion with an external entity for financial gain could result in criminal charges.

In addition to reporting PHI data breaches to HIPAA and any potential HIPAA security violations, one consequence of data breaches is the impact on the doctor-patient relationship.

"Recent studies have found that people are withholding information—sometimes critical information—from their healthcare providers because they are concerned that there could be a confidentiality breach of their records. This is not only a potential issue for the treatment of a specific patient; there are potential public health implications. An unwillingness to fully disclose information could delay a diagnosis of a communicable disease," the study authors wrote.

According to the study authors, just by examining the U.S. Department of Health and Human Services data alone, PHI for half of the population of the United States has been impacted by breaches since 2009. At the same time, public and private healthcare providers are adopting electronic medical records (EMRs), which mean more medical information is now in electronic form. And, the FBI has issued a warning that the possibility of increased cyber intrusions in the healthcare industry is likely.

There is some good news, according to the study authors, which is that organizations with PHI are detecting incidents faster and are closing the detection deficit, or the time between when data is compromised to time when the breach is detected.

The study authors concluded that healthcare organizations need to "assess processes, procedures and technologies that affect the security of these patient records." ♦

Cloud Forward: CIOs Overcome IT Security Concerns

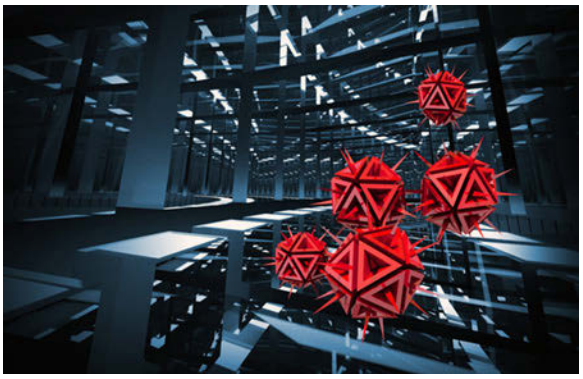
Healthcare CIOs are increasingly moving electronic patient records, including EHRs and diagnostic images, out of the internal data center and into the cloud.

The widespread adoption of health information technology by patient care organizations in the past 10 years has been transformative to the healthcare industry. In 2008, only 9 percent of hospitals in the U.S. had a basic electronic health record (EHR) systems; by 2014, that had increased eightfold with 76 percent of hospitals using a basic EHR system and 97 percent utilizing certified EHR technology, according to figures from the Office of the National Coordinator for Health Information Technology (ONC) and the American Hospital Association. With this surge in digitized patient data comes the challenge, for hospitals and health systems, to efficiently and cost effectively store and manage that data.

Healthcare CIOs are increasingly moving electronic patient records, including EHRs and diagnostic images, out of the internal data center and into the cloud. The global healthcare cloud computing market is forecasted to reach $9.48 billion by 2020, growing 20 percent from $3.73 billion this year, according to research firm MarketsandMarkets.

And, many industry experts say that the use of cloud services in healthcare is increasing steadily, despite the belief that the healthcare industry lags behind others in cloud use. In fact, results from a cloud survey by Healthcare Information and Management Systems Society (HIMSS) Analytics found that 83 percent of healthcare organizations use cloud services and only six percent of those surveyed reported having no plans to use the cloud at all.

Additionally, for the majority of respondents who organizations are using software-as-a-service (SaaS) models, the primary uses for cloud platforms are doing the following: hosting clinical applications and data, health information exchange, human resources applications and data and backup and disaster recovery. Three-quarters of respondents reported using either a private cloud or hybrid cloud services.



"Cloud, in general, is not scary anymore and most people either have their toe in the water or are fairly far into it," Greg McGovern, associate principal at the Chicago-based consulting firm The Chartis Group, says.

"Most of the healthcare organizations that we work with, when they talk about the cloud, they are generally talking about software-as-a-service," McGovern says. "The notion of infrastructure-as-a-service, or these true full-tilt cloud services, is not fully developed in the healthcare space," he adds, referencing the use in some industries of infrastructure-as-a-service players such as Amazon Web Services and Microsoft.

A 2014 Dell Global Technology Adoption Index survey found similar cloud adoption rates with 96 percent of healthcare organization respondents using or considering using the cloud, and only 3 percent having no plans to leverage cloud solutions. The Dell survey also found that the majority of healthcare providers use private or hybrid cloud solutions as well.

Many midsize and large physician groups and independent practice associations also are moving to cloud-based EHRs from vendors such as athenahealth or Practice Fusion, due to the speed of upgrades and better data recovery while avoiding costly hardware upgrades and IT personnel costs.

As previously reported in *Healthcare Informatics,* when East Georgia Healthcare Center, a federally qualified health center with nine facilities and 23 physicians, began experiencing slow computing and processing speeds due to the amount of data it was managing, the practice decided to subscribe to eClinicalWorks Grid Cloud.

"It was a smart decision for us financially and with the IT staff we have," Herb Taylor, East Georgia's IT director, says.

Taylor reports that the cloud offers better disaster recovery protection and financial security.

"You may be able to spend that $300,000 to $400,000 to get where you need to be this year, but where are you going to be in five or six years when it is time to upgrade all that hardware again? That was the big factor for

me. No matter what happens, I am paying X amount of dollars to eClinical Works. It was a no-brainer for us with 23 providers to pay the monthly fee," he says.

Investing up front in IT equipment requires capital expenditures, whereas using cloud services is an operational expense and that has been a big driver for healthcare organizations to use the cloud, McGovern says.

"The ability to pay as you go and purchase capacity as you need it and carry that as an operating expense becomes very attractive," he says.

What many healthcare leaders report about using the cloud echoes the results of the HIMSS Analytics Cloud Survey. According to the 150 healthcare IT professionals surveyed, reasons for using cloud services included lower costs than maintaining the current IT system (56 percent), faster deployment (53 percent), a lack of staff able to maintain on-premise systems (52 percent) and more robust data recovery (50 percent). Other reasons given include the need for on-demand, scalable, always on solutions (45 percent), regulatory compliance (41 percent), better information security (26 percent) and mobility of workforce (26 percent).

The need for technical resources and talent also is driving many hospitals to look at cloud applications as it can allow for better allocation of IT resources.

"If I'm a hospital deploying a Cerner solution, I might not have the technical resources that I will need to bring that up and support that environment. So it's attractive to look at a company that already has those resources and just come online with the application," McGovern says.

Speed to market can be a key benefit of the cloud as well. "If you bring something in house, it takes awhile to build up. So, if I want to bring up 500 doctors on a provider EMR, I might be looking at a six-month implementation as opposed to an 18-month or two-year implementation schedule. A lot of people are attracted to the notion that they can move in an agile fashion," McGovern says.

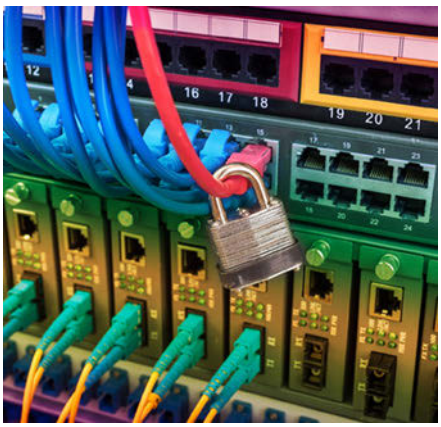
As previously reported by *HCI* Editor-In-Chief Mark Hagland, Saint Luke's Health System, a Kansas City-based integrated health system with 10

hospitals, 450 employed physicians and 2,440 affiliated physicians, shifted to a community-wide cloud-based information exchange system for diagnostic images and, and according to Deborah Gash, vice president and CIO of the Saint Luke's Health System, physicians now benefit from a streamlined process and a mobile application to pull up images on their iPads. And, the cloud-based information exchange enables better patient engagement.

"We're going to make the cloud image exchange accessible to patients," Gash says, noting that work is being done now to put a URL into the patient portal for access to studies, diagnostic images and radiology reports.

Healthcare leaders say an increased interest in the cloud also ties into the need for mobility solutions and data analytics with the shift towards population health and accountable care organizations (ACOs), and the cloud can be a critical building block for information-driven, patient-centered healthcare.

The push for data analytics requires having access to a data warehouse, and building an internal data warehouse is a huge investment, McGovern says. "So the question is, should I build my own data warehouse and bring all that information and cost into my organization, or should I start shopping around for a shared service model? Is there someone out there like a Dell that might offer that sort of analytics or data storage environment that would be most effective? I think folks are looking at cloud services not just on the applications side, but on the infrastructure side as well," he says.



Historically, there have been concerns about data security with cloud-based solutions, case in point, 61 percent of the respondents in the HIMSS Analytics survey who hadn't adopted a cloud solution cited security concerns as a reason for not doing so. But many health IT leaders say those concerns are unfounded, and many CIOs, CTOs and CISOs (chief information security officers) see the cloud as providing more security than on-site storage.

"Is security an issue? Absolutely, but no more so, and I would argue maybe even less so than with an internal data center. Security is always an issue, HIPAA is an issue, privacy and disclosure are issues whether the data is sitting in a server in your closet or sitting out somewhere on the internet. The cloud vendor, in some sense, might be able to provide better security,

as they have scale and you have a relationship with them contractually, there are business associate agreements in place. As such, the cloud vendors comply with certain standards for data security and privacy," McGovern says.

And, cloud solutions also provide CISOs and CIOs with a way to "get dollars for security" because the security is "baked into the solution from the external vendor," he adds. With many hospitals and health systems, funding for security, such as intrusion detection systems, is not a priority due to the expense, but outsourcing data storage to a cloud vendor "almost by definition gives you a certain level of security and that security will be maintained on an ongoing basis."

However, as with any outsourcing relationship, there are a number of issues that health IT leaders need to consider when using cloud solutions, and doing due diligence with regards to service level agreements and contracts is critical, McGovern says. "We've had people go into an outsource relationship for the cloud or remote-hosted services and three to five years down the road, the CFO says, 'Our costs are astronomical, why is it costing so much?' And it turns out there are all these things outside the scope of the agreement, so they might have committed to 99.9 percent uptime and then demanded more, or they have expanded and added more providers and that incremental cost was unexpected."

"It's probably going to be a 10-year marriage with that vendor, so you really need to have foresight and think about how is this going to grow and how is the world going to change and then try to build in those considerations into your contract," he says.

According to the HIMSS Analytics survey, 65 percent of healthcare organization respondents said a cloud services provider's willingness to enter a business associate agreement was an important factor when selecting a vendor.

There are also concerns around certain performance issues with cloud services, such as slow responsiveness and downtime. According to the same survey, 32 percent of respondents reported problems with slow responsiveness with cloud applications and 23 percent of respondents reported downtime and unavailability of data and applications.

"The concern around availability and uptime has been a valid concern, but internal networks go down too. The connectivity and availability of cloud services is very high and again, that gets back to the contracts and the need for good due diligence when talking to the vendor," McGovern says.

Integration services can be an issue when using cloud-based solutions as most hospitals and health systems want an integrated user experience and workflow. "The integration of the user interface and all those back-end services is a challenge, but that doesn't mean it can't be managed, it just means that it needs to be thought through so you don't end up with a bunch of siloed broken workflows," McGovern says.

Many industry experts also warn against "all-or-nothing" cloud service providers. "In this population health and ACO world, you never know who you're going to be partnering with, so locking yourself into an all-or-nothing vendor could be prohibitive," he says.

Cost savings and IT staffing challenges will likely drive continued growth of cloud solutions, and, indeed, most adopters report that they will expand their use of the cloud in the future, specifically for archived data, disaster recovery and operation apps and data, according to the HIMSS survey. ♦

McMillan at CHIME Lead Forum–Atlanta: Cybersecurity Must Move Beyond Defending the Perimeter

CISOs must act as change agents, Mac McMillan says.

Once again, prominent data security guru Mac McMillan, CEO of the Austin, Texas-based consulting firm CynergisTek, told attendees at the CHIME Lead Forum-Atlanta that healthcare organizations must do more when it comes to protecting their data.

McMillan spoke on the topic of cybersecurity on Dec. 1 to kick off the CHIME Lead Forum–Atlanta, co-sponsored by the Ann Arbor, Mich.-based College of Healthcare Information Management Executives (CHIME) and the Institute for Health Technology Transformation (iHT^2—a sister organization to *Healthcare Informatics* under the joint umbrella of the Vendome Group, LLC).

In his keynote presentation, McMillan urged attendees to make cybersecurity more of a priority in their organizations—something he has been pleading the industry to do for years. "If you don't believe that you're in a battle, you're not paying attention," he said. "People out there want to do harm. They want to steal what we have worked so hard to achieve. So we need to understand where our soft underbelly is. Why are we putting protected health information (PHI) on mobile devices and why are we not encrypting [the devices]? We leave ourselves too open [to attacks]," McMillan attested.

McMillan pointed to this year's Healthcare Information and Management Systems Society (HIMSS) Cybersecurity Survey which indicated that 87 percent of provider respondents said that information security has increased as a business priority in their organization. However, two-thirds of those surveyed said they have experienced a "significant security incident." McMillan noted that despite this, data security is still not enough of a budget priority, which "doesn't add up," considering that there has been a four-fold increase in the number of hacks this year compared with previous years. Interestingly, McMillan said that outside attackers are not going for the patient data as much as they are for the intellectual property.

McMillan told a few stories of how security in organizations simply gets glossed over. For instance, he gave an anecdote of a healthcare clearinghouse that provided billing support for about 400 hospitals on the East coast. One week, the day before all of the bills were supposed to go out to its hospital clients, the clearinghouse noticed that all of the data in its systems suddenly was encrypted. At first the organization thought it was the internal IT department that was responsible for this, but it turned out that it was indeed an outside job. What made matters worse, McMillan explained, was that the clearinghouse didn't have any of its data backed up, resulting in a huge delay to the billing cycle. What's more, not one hospital that was in partnership with the clearinghouse asked about its security protocols when signing the agreement. As such, the clearinghouse lost 40 percent of its clients after the incident, but McMillan put blame on the hospital clients as well, calling it "flat-out irresponsible of them to not ask about security."

McMillan then outlined the several challenges that chief information security officers (CISOs) are dealing with in their organizations. At the top of this list is an increased reliance on IT—more than 98 percent of all processes are now automated, more than 98 percent of all devices are networkable, and more than 95 percent of all information is digitized, McMillan noted. "Back in the day, there wasn't a concern in regards to electronic health records (EHRs), meaningful use, accountable care organizations (ACOs), and health information exchanges (HIEs)," he said. "And these are certainly good things for healthcare. They are beneficial, but with them comes added risk."

Another challenge comes in the form of insider abuse, McMillan continued, as more than half of all security incidents involve staff. "Folks still think you can do traditional audit methods as a manual process. You will fail if you do that," McMillan warned. Instead, he said, "behavior modeling, pattern analysis, and anomaly detection is what's needed. You wont catch folks based on rules and compliance. We need to do a better job of monitoring our users. The only way to catch bad actions is to monitor the behavior," he emphasized.

Further issues arise with medical devices, McMillan said, noting that Congress has recently sent HHS (Department of Health & Human Services) a letter wanting to know what the agency is doing about risk to medical

devices. "The answer is they are doing nothing at the moment," McMillan said. "There is nothing constructive being done. The OIG (Office of the Inspector General) auditing medical devices next year is not about identifying the problem, but instead about finally documenting this issue and sending it to Congress. As such, McMillan said his suspicion is that "we will see legislation with greater control over medical devices and better standards in regards to how they're developed." However, in regards to meaningful use Stage 3, McMillan said that CMS (Centers for Medicare & Medicaid Services) "moved backwards, deciding that they wanted to divorce meaningful use from compliance and from HIPAA (the Health Insurance Portability and Accountability Act). What they tried to do in Stage 3 was take all security out of it and say that it's a HIPAA issue. Meaningful use attestation used to depend on some of this [security] stuff, but now due to the Stage 3 requirements, it has less teeth," he said.

Going back to the concept of mobility and data, and the idea that medical staff are increasingly turning to their mobile devices to communicate since it's easier, faster, and more efficient, McMillan noted that the country is getting to a point where we will have 1.5 mobile devices per living person.

Right now, physicians have an average of 6.2 devices each. "This leads to confusion, and you have to wonder where data is going and whether or not it is being protected," McMillan said. To this end, he noted that theft and loss of devices are increasingly becoming bigger problems. "I always follow a simple rule: If [the device] is with me and has important information on it, it stays with me," McMillan said. "My stuff is completely encrypted, but it doesn't matter. People will lose devices and do stupid things. So let's quit putting data in places where it doesn't need to be. If I give you access, why does the data need to be stored?" McMillan asks, adding that the philosophy of having a good strong perimeter—and not worrying about what's behind that perimeter—isn't nearly good enough anymore.

Finally, McMillan mentioned that healthcare organization board involvement is part of the problem, but also part of the solution. He noted that 70 percent of board members feel they understand cyber risks, while 43 percent of CIOs/CISOs think boards are informed about threats to IT. But, board members admit their knowledge about cybersecurity is limited. As such, boards are still in the dark about security risks and incidents, and

it took the major Target, Anthem, and Community Health breaches to get their attention, McMillan said. "It's not a compliance issue, but a business issue," he said.

As such, more qualified security professionals are needed in healthcare organizations, McMillan concluded. The aforementioned HIMSS survey found that 52 percent of provider organizations had a full-time security person. Many health are systems struggling to find a qualified CISO and retain them. "The country [needs] a lot more qualified CISOs," he said. He added, "Healthcare's culture must change. We need CISOs who are not afraid to be change agents in their institutions. That's not a safe place to be, and they will have to take their lumps. But it's the only way we will make a difference." ♦

CIOs Convene: Healthcare Leaders Discuss the Biggest IT Challenges Facing Their Organizations in the Year Ahead

This past September, eight CIOs from some of the nation's leading healthcare organizations convened at the annual Scottsdale Institute Fall CIO Summit in Arizona to discuss the most important IT-related challenges their health systems are facing and the strategies to position their organizations for success over the next year.

The Summit was hosted by the Scottsdale Institute, a Minn.-based not-for-profit membership organization of health systems advanced in IT, and sponsored by Impact Advisors, a Naperville, Ill.-based provider of healthcare IT consulting services. The conversations and key findings from the Summit are outlined in the *report,* "The New World of the Health System CIO: Consumers, Consolidation and Crooks."

Following the Summit, HCI Managing Editor Rajiv Leventhal spoke with one of the CIOs who was in attendance—David Bensema, M.D., Louisville-based Baptist Health Kentucky—as well as Tonya Edwards, M.D., physician executive at Impact Advisors. In *Part 1 of that conversation,* Leventhal got a "war room" inside look at the most pressing issues CIOs are currently grappling with specifically around changing payment models and electronic health record (EHR) optimization. In Part 2, Drs. Bensema and Edwards look at more challenges that were identified at the Summit, such as healthcare mergers and acquisitions (M&A), cybersecurity best practices, and competing for patients. Below are excerpts of that discussion.

What about mergers and acquisitions are specifically so challenging for CIOs?

Bensema: I think it's about the difficulty of having the workflows for the end user appear seamless. Certainly it would be nice for our IT teams if the integration was easier and the interfacing was simpler. That's a big challenge, trying to have the end users not feel impeded by their products. That's what you hear historically, that the products get in the way. There is a need to integrate the various elements of your IT environment so the end user doesn't notice when they go from one software solution to another.

Edwards: Another big challenge is that once the decision to merge or acquire has taken place, there is a discussion about what to do about our IT systems. That decision about you will handle your IT solutions, which ones you will use, who has power to make those decisions, how you will handle using multiple systems at once, figuring out a timeframe, merging together, and consolidating—all of those things make the M&A piece very time consuming, resource-intensive, and very difficult.

Bensema: We have done two acquisitions in the last several years, and there is always a lot of talk about the governance of personnel, the nursing staff, governance of the billing department, and accounts payable, so IT becomes an afterthought. People get to love the devil they know, so even if they're on a lesser product, they're not ready to give it up. You need to have those discussions up front; you can't do it in the heat of a deal. We have had trouble with that, and it's tough to get the hospital to come over, so we have had to sustain products that we didn't want to.

We keep hearing the saying that healthcare cybersecurity will get worse before it gets better. How much of a priority is this for CIOs and what are they doing to better protect themselves?

Bensema: This was one of the more fun parts of the meeting, and it had a lot to do with Impact [Advisors] coming up with its new model for assessing maturity in the security realm. The thing is, if your board does not have this at the top of mind, if the audit committee is not already deeply involved with monitoring your security audits and passwords, if dual authentication is not implemented or even on the radar, well, those are big things that need to be done. And after you do all those things, engaging your staff to have awareness and be looking for it. I'm a physician, and I have to be aware that something could walk in at any time, so you need that situational awareness. Getting your staff to have that awareness, such as noticing that an email doesn't look normal, is key. There are clues and you need to think about that every time you open something so it becomes habit rather than time consuming even with more sophisticated phishing schemes. You can have the best firewalls and monitoring systems in the world, but they won't attack a hard firewall. They will attack a vulnerable person.

Edwards: It's the biggest fear for CIOs right now, and it's at the top of mind for everyone. Having an objective is helpful, and then it's about

having board level executive support for security work to be done and to change the culture of the workforce. There are also tactical things like working towards all healthcare data so you have a lot more control over it, and having constant education and reminders for end users.

Competing for and retaining patients was another interesting dilemma that CIOs brought up. How big of an issue is this?

Edwards: You have very different consumers in healthcare than we have had in years past. That's related to what we have seen in other industries. You look at retail or banking—they have had innovation and have been really strongly focused on convenience and user friendliness with a much more visual format. When is the last time you went inside your bank? Healthcare, conversely, has stayed pretty much the same. We are now getting innovative business plans with telehealth models and retail pharmacies, which are beginning to eat away in urgent care and primary care areas. As a family physician, to me, those areas are being eroded. Healthcare companies have tried to compete on quality, but we are missing the boat in a lot of ways. Access and availability are the differentiators, and that's what these new disruptive innovators coming from other industries are excelling at.

Bensema: That availability and convenience are such key elements for the younger patient population, the group you want in your pipeline early in this population health world so you can reduce their disease burden later. I was one of the disruptors in the Kentucky market, among the physician practices. There were eighteen retail clinics that I helped to put together across the state. The anxiety felt by the doctors, the high alert that other health systems went on when we did that, was remarkable. Telehealth is the disruption now, and doctors are struggling on if they want to participate in that. We weren't doing more than a phone call here and there with regular patients, and now systems are asking patients if they want to participate in telemedicine. A system has to compete for those lives, and if you will be doing accountable care and population health, you have to spread the risk and have a large base population by offering the elements they want so they sign up to your plan. Competition is healthy and it's heating up. From an IT standpoint, it's causing all of us to up our game, as CIOs have to be aware of that

next-level technology. Even if you're not ready to adopt it, you better be well-versed on it because someone on the board is reading something or the CEO will ask you why you're not already in this area.

What priorities will change by the time next year's CIO Summit rolls around?

Bensema: The one thing that will change, we will all be more aware on where we stand on the security maturity scales. We know what we will have to do more specifically—that's part of the evolution. You will also see a lot more care management and population health-focused software tools implemented across the system, and we will all be confused since we'll all be getting different information. The level of confusion will peak regarding population health over the next year, and then we'll start figuring our path to that. No one has the secret sauce yet.

Edwards: These same challenges that we described this year will continue to be the major ones, but they will shift in priority. You will see a lot more shift towards optimization and the preparation for population health. The interoperability piece is such a big part of being prepared for value-based care as well. ♦

Report: 2015 Was the Year of the Healthcare Security Breach

Five of the eight largest healthcare security breaches over the past five years, with almost 100 million records compromised, happened during the first six months of 2015, notes IBM Security in a report, also calling 2015 the year of the healthcare security breach.

According to data compiled by IBM X-Force Interactive Security Incidents, healthcare ranks as the leading sector for security incidents across all industries in the first 10 months of this year, with 34 percent of records compromised.

"Interestingly, healthcare has hung on to its No. 1 ranking even though the second half of 2015 has yet to see the same level of large-scale breaches affecting the healthcare industry as seen in the first half," IBM researchers wrote.

Compared to the almost 100 million records compromised in 2015, between January 2011 and December 2014, the healthcare industry accounted for only 0.63 percent of total records compromised.

"That's a significant climb," the report authors state. "The five very large security breaches mentioned earlier contributed significantly to this rise in ranking. Protected health information (PHI) data fields from those breaches included emails, social security numbers, banking and employment information and medical records."

IBM X-Force security researchers identified significant shifts in criminal behavior in recent years as the number of retail records compromised in 2015 dropped 92 percent from 2014 and that industry is experiencing a four-year low with only 5.7 million compromised records reported.

The IBM Managed Security Services Threat Research group highlighted its latest data about healthcare security breaches, and how the industry is now outpacing other sectors such as retail, in its IBM X-Force Research report. In the report, IBM states that the healthcare industry has become a

popular target due to the high resale value of protected health information, and even electronic health records (EHRs), which can contain a patient's email, social security number and banking and employment information as well as health and medical data.

"As the Ponemon Institute's 2015 Cost of Data Breach Study found, a healthcare record lost or stolen in a breach could cost the victim organization as much as $363, fully 136 percent higher than the global average cost of a data breach per lost or stolen record," the report authors state.

Also, healthcare data does not have an expiration date and the healthcare industry is still adapting to the security landscape.

In almost half of the healthcare breaches sampled, the victim organization has not to date disclosed exactly what type of attack they sustained, the report states. After that, "physical" ranks as the most prevalent attack type, followed by malware, phishing, misconfigured networks and SQL injection.

The IBM report also offered a number of recommendations for healthcare organizations to safeguard healthcare data and strengthen security, such as employing a full-time Chief Information Security Officer (CISO) to steer the organization's overall security strategy and budget.

The report also notes that the Internet of Things (IoT) can open more doors for attack and medical devices in particular can have a number of vulnerabilities. The report authors also state that it's essential to conduct security updates on devices and also recommended healthcare organizations test and evaluate devices before deploying them, restrict unauthorized access to networked devices and ensure that firewalls are up to date and perform periodic configuration reviews.

In addition, security staff should monitor network activity for unauthorized use, perform audits of the devices and perform penetration testing of medical equipment, including implantable medical devices.

The report authors also emphasize the importance of encryption, including encrypting passwords.

"Whenever possible, you should encrypt patient information, even at rest and within the EHR, segregate patient data from other data and use dif-

ferent subsets, follow the principle of least privilege allowing data access only to users who require it to do their jobs and implement devices in depth with multiple layers of security," the report authors state.

And, healthcare organizations should conduct a security framework and risk assessment and then develop an incident response plan, according to the report. ♦

Healthcare Industry Will Remain a Top Target for Data Breaches in 2016

Healthcare companies will continue to be one of the most targeted sectors by cybercriminals in 2016 due to the high value of compromised data and the ongoing digitization of medical records, according to an Experian report.

The 2016 Data Breach Industry *Forecast* by Experian Data Breach Resolution outlines five predictions for what industry leaders can expect in the coming year with regard to data breach trends and issues.

For the healthcare industry in particular, researchers predict that big healthcare hacks will make headlines, but small breaches will cause the most damage.

"While large breaches may be compromising millions of people's records in one fell swoop, smaller incidents caused by employee negligence will also continue to compromise millions of records each year. These incidents are often due to employees mishandling paper records or losing physical back-up of information," the researchers state.

Given the high value compromised data can command on the black market along with the continued digitization and sharing of medical records, researchers predict that healthcare companies will remain one of the most targeted sectors by attackers.

"In 2016, sophisticated attackers will continue to focus on insurers and large hospital networks where they have the opportunity for the largest payoff. With the move to electronic health records (EHRs) continuing to gain momentum and becoming more widely accessible through mobile applications, the attack surface continues to grow," the researchers state.

The researchers note that it's important for healthcare organizations to not only continue to invest in up-to-date security technologies, but also focus on training employees on proper data handling practices on a regular basis.

The report also highlights the rise in cybercriminals using data for corporate extortion or other scams. According to cybersecurity experts, medical records are worth up to 10 times more than credit card numbers on the black market, and this might drive hackers to look at medical records data as a mean for financial gain. According to the researchers, 38 percent of organizations report they have already been targeted by cyber-extortion.

"Moving forward, it is anticipated that businesses will begin to account for the potential of extortion in their data breach planning, including having cyber insurance policies in place that incorporate protocols for how to negotiate with cybercriminals," the researchers state.

Among the other predictions, researchers also anticipate that the EMV Chip and PIN liability shift will not stop payment breaches.

"Given the value of payments data, attackers may also look to other methods to steal this information that don't involve point of sale systems. Similar to what's happened in the European Union—where EMV has been adopted for some time—attacks may shift to focus on online transactions where cards don't need to be present," the researchers state.

And, it is anticipated that cyber conflicts between countries will leave consumers and businesses as collateral damage and that the 2016 U.S. presidential candidates and campaigns will be attractive hacking targets.

Researchers also predict a resurgence in hacktivist activities, motivated by groups looking to inflict reputational damage to a company or cause.

The report authors note that while traditional data breach threats remain, business leaders also should take note of emerging trends and update their data breach response plans accordingly.

Experian researchers also graded their 2015 data breach predictions, with mixed results, as four out of six predictions for 2015 rang true by end of this year. For 2015, researchers predicted that healthcare breaches would be a persistent and growing threat, which unfortunately has proven to be the case, and that employees would be companies' biggest breach threat, which also was accurate according to a Ponemon Institute report. That

report indicated that non-malicious employee error is the No. 1 leading cause of data security breaches.

Two other predictions that were accurate were the shifting accountability to corporate leadership following a security breach and the growing concern about the Internet of Things (IoT) as a security breach threat. ♦

Survey: Application Vulnerabilities Are Top Cybersecurity Concern for Senior Health IT Execs

The exploitation of vulnerabilities in web, mobile and cloud-based applications is the top concern of healthcare IT executives, according to a recent survey from the Chicago-based Healthcare Information and Management Systems Society (HIMSS) and Burlington, Mass.-based vendor Veracode.

The *survey* of 200 senior IT security executives in hospitals across the U.S. revealed that the potential for loss of life due to compromised networks or medical devices, brand damage due to theft of patient information, and regulatory enforcement were the top fears of respondents related to such security breaches. Indeed, a single healthcare record brings nearly 10 times the value of a stolen credit card number, combined with the competitive differentiation of intellectual property, according to the research.

In fact, the number of records stolen has grown from 2.7 million in 2012 to more than 94 million through the first half of 2015, according to the U.S. Department of Health and Human Services (HHS). As such, the rapidly expanding IT footprint, a bottoms-up technology culture where centralized security policies are difficult to enforce, and significant skills gaps around security create formidable challenges for healthcare providers to secure patient data, the survey concluded.

More specifically, liability over a breach is top of mind and providers are taking action to address their exposure. To meet liability requirements, 57 percent of survey respondents said they are increasing spending on third-party security assessments, such as code audits. Another 56 percent are inserting liability clauses into contracts with commercial software vendors to lessen the risk exposure from their software supply chain. And more than half are implementing standard frameworks such as SANS Institute Security Controls as a means to create a baseline security posture from which future improvements can be benchmarked, according to the survey.

What's more, one of the biggest challenges healthcare organizations face is addressing the fact that much of the decision-making authority is held by the doctors themselves, rather than in a centralized manner. This bottoms-up culture means that it becomes very difficult for a Chief Information Security Officer (CISO) to implement consistent security controls across departments, resulting in serious vulnerability issues for the organization.

Some healthcare organizations have already started to push to address this challenge by making cybersecurity a top institutional priority, with 65 percent reporting investment in security technologies that enable governance policy enforcement; 51 percent investing in training initiatives to educate department heads about cybersecurity; and 44 percent pushing the CEO to be an advocate for centralized IT security policy across all departments.

"There's a perfect storm brewing for 2016 in healthcare and if things continue as is, we're likely to see an increased plundering of medical records leading to increases in insurance fraud, illegally purchased medical equipment and controlled substances, or something even worse," Chris Wysopal, CTO and CISO, Veracode, said in a statement. "Remedying the problem starts with a good look at how healthcare-related software is built and making sure that security is a priority. In fact, our data from actual code-level analysis of billions of lines of code shows that 80 percent of healthcare applications contain easily avoidable cryptographic issues such as weak algorithms. Given the large amount of sensitive data collected by healthcare organizations, this is quite concerning." ♦

2016 Health IT Summits

Each year, the **Institute for Health Technology Transformation (iHT²)** hosts a series of events & programs which promote improvements in the quality, safety, and efficiency of healthcare through information and information technology. Designed to help you navigate through health IT issues, policies and strategies in an attempt to improve care, iHT² events include a variety of guest speakers and keynotes representing many diverse sectors within health care.

- **San Diego, CA — HIT Summit**
  Jan. 19–20, 2016 | Event Site
- **Miami, FL — HIT Summit**
  Feb. 2–3, 2016 | Event Site
- **San Francisco, CA — HIT Summit**
  April 5–6, 2016 | Event Site
- **Cleveland, OH — HIT Summit**
  April 19–20, 2016 | Event Site
- **Boston, MA — HIT Summit**
  June 14–15, 2016 | Event Site
- **Denver, CO — HIT Summit**
  July 12–13, 2016 | Event Site
- **Nashville, TN — HIT Summit**
  August 9–11, 2016 | Event Site
- **Seattle, WA — HIT Summit**
  Aug. 16–17, 2016 | Event Site
- **Toronto, ON, Canada — HIT Summit**
  Sept. 20–21, 2016 | Event Site
- **New York City, NY — HIT Summit**
  Sept. 27–28, 2016 | Event Site
- **Washington, DC — HIT Summit**
  Oct. 25–26, 2016 | Event Site
- **Beverly Hills, CA — HIT Summit**
  Nov. 9–10, 2016 | Event Site
- **Dallas, TX — HIT Summit**
  Dec. 7–8 2016 | Event Site
- **Atlanta, GA — HIT Summit**
  Dec. 14–15, 2016 | Event Site

www.Healthcare-Informatics.com

When you join the **Healthcare Informatics** community, you join other forward-thinking professionals involved in the planning, development, and implementation of important technological trends that will define tomorrow's healthcare. These dedicated professionals exchange a wide range of pioneering concepts as they tackle important strategic and information technology issues facing organizations such as hospitals, medical groups, and integrated health systems.

Join us as we bring together those with a shared focus on healthcare IT leadership, vision, and strategy—driving change forward by shaping innovations that point the way to the future of healthcare.

Begin My Free Digital or Print Subscription, USA

Begin My Free Digital Subscription, Canada

Begin My Free Digital Subscription, International

(Print and online format choices are available)