white paper

CYBER-SECURITY IN HEALTHCARE

Understanding the New World Threats

written by

John Gomez, Sensato CEO

Colin Konschak, Divurgent CEO & Managing Partner

DIVURGENT

Redefining Consulting. Transforming Healthcare.

[sensato]

Data Breach at Anthem May Forecast a Trend

The New York Times

Experts warn 2015 could be 'Year of the Healthcare Hack'

REUTERS

Exclusive: FBI warns healthcare sector vulnerable to cyber attacks

REUTERS

Patients Put at Risk By Computer Viruses

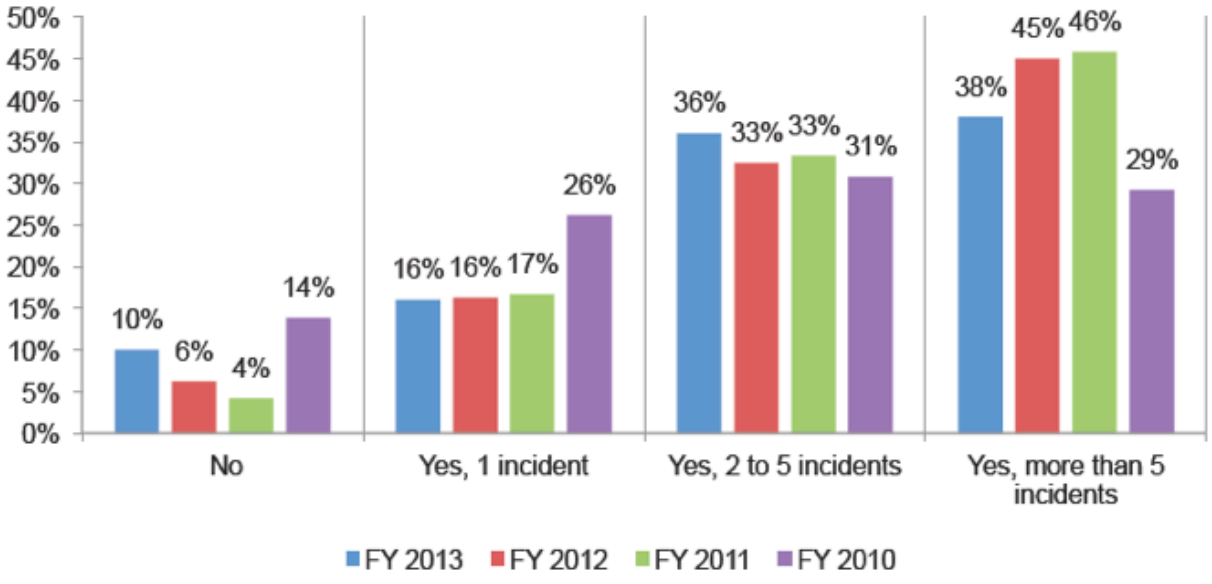
THE WALL STREET JOURNAL.

Introduction

The February 2015 cyber-attack on Anthem, in which cyber-terrorists accessed 80 million member and employee records, exposed the vulnerability of the US healthcare system in a way no other attack—whether retail or health care—has. Unlike the Target and Sony breaches the year before, incidents like the Anthem breach threatens not just the privacy and security of millions of patients, but their safety and even their lives.

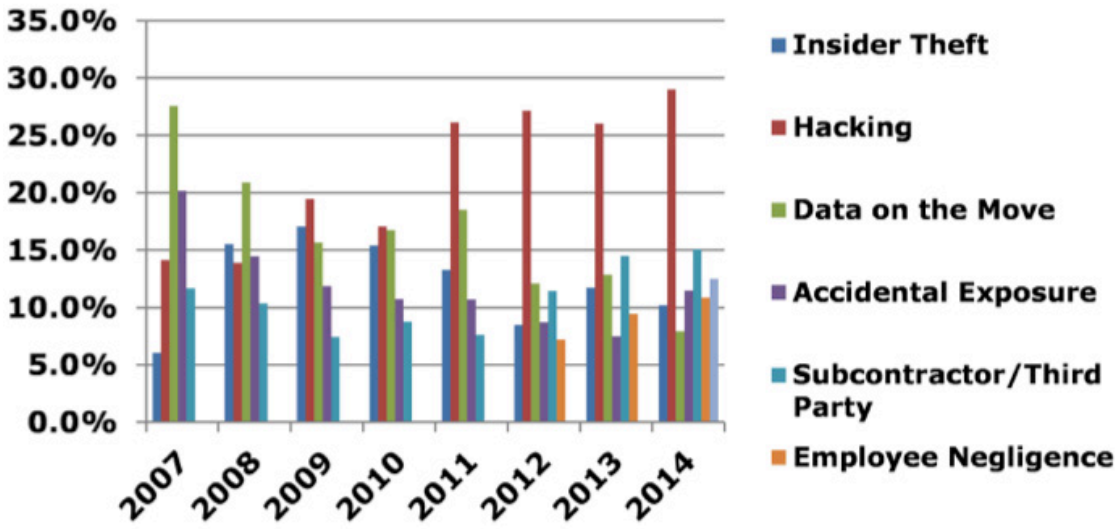
Between 2013 and 2014, healthcare companies saw a 72 percent increase in cyber-attacks, with IDC Health Insights estimating that half of all healthcare organizations experienced one to five cyber-attacks in 2014, a third of which succeeded (Figure 1).[1,2] Figure 2 depicts the most predominant types and causes of security breaches. Overall, the healthcare industry accounted for 26.4 percent of all breaches in 2014.[3] That figure, of course, pales in comparison to the Anthem breach.

Figure 1. Number of Cyber-attacks in Healthcare Organizations: 2010-2013



Source: Fourth Annual Benchmark Study on Patient Privacy & Data Security. Ponemon Institute. March 2014

Figure 2. Causes/Type of Cyber-security Breach



Source: The Year of the Data Breach -- a Recap of 2014 and Review of 10 Years of Breaches. Identity Theft Resource Center. January 19, 2015. http://www.idtheftcenter.org/Press-Releases/2014breachstatistics.html

No healthcare organization, no matter how small, is immune to cyber-threats. In fact, the threat of attack is so great that in 2014 the FBI warned healthcare providers that their cyber-security systems were not robust enough to resist hacker threats.[4] In early 2015, the Health Information Trust Alliance (HITRUST) found after a three-month analysis, today's approach to cyber-security is predominantly reactive and, for the vast majority of organizations, inefficient, and labor-intensive.[5]

There are numerous causes of data breaches, such as employees using their own devices or vendors and subcontractors that have yet to comply with the Health Insurance Portability and Accountability Act (HIPAA) Final Rule, and even the Affordable Care Act (ACA). Furthermore, regulations such as the HIPAA Final Rule and ACA brought a plethora of insecure websites, databases, and health information exchanges into the mix.[6]

Since 2011, however, hacking has become the most common cause of breaches, far surpassing accidental exposure, employee negligence, and insider theft.[3]

What most healthcare executives do not understand is that even the word "hacking," and the connotation of a 20-something computer whiz playing around, is no longer relevant. Today, the word that should be used is "attacking." Rather than nerdy techies, these attackers are highly professional, highly skilled operators. They are part of sophisticated networks, even city-states, not only bent on demonstrating that they can get into a system, but also on destroying an organization from the inside out – and reaping millions in revenue as a result. They are, in effect, the *Special Ops* of the hacking world.

The attackers fall into three realms: cyber-terrorists, who are motivated by ideology and a desire to bring attention to and win their cause; cyber-criminals, who are motivated by financial gain; and cyber-spies, who are sponsored by a nation-state and operate similarly to an intelligence agency, but are independent. Cyber-spies are believed to be behind the Sony and Anthem attacks, while cyber-criminals are believed to be behind the Target attack.

The economic impact of cyber-attacks is tremendous. The Ponemon Institute estimates they cost a healthcare system $5.6 billion a year to respond to the breach, provide defense, pay damages, and defend claims. On average, healthcare entities face a cost of about $2 million over a two-year period, the Ponemon Institute notes, while each stolen or copied record costs approximately $201.6,7 Thus, Anthem is facing a bill of at least $16 billion.

Although Anthem, like most large healthcare entities, likely has cyber-security insurance, policies generally top out at $300 million.[8] Plus, insurers will not pay the full amount if it turns out the company was negligible in any way. That may be the case with Anthem, given news reports that the stolen data was unencrypted.[9]

Infrastructure of Health Information Technology Creates Greater Vulnerability

The healthcare system is far more vulnerable to attacks than other industries, in part because of the way its information technology (IT) systems evolved over time. Most grew by being piecemealed together with software and hardware purchased from different vendors and jury-rigged to work together.

As a result, today's healthcare organizations have hundreds of systems, many running antiquated applications on legacy hardware. The level of complexity is to an extent that no one person within the organization has a holistic understanding of how the system operates.

> *"We assumed in the early days that each manufacturer was responsible for the security of their applications and they were," said Senior Vice President and Chief Information Officer Bert Reese, of Virginia-based Sentara Healthcare. "But as we started to integrate the applications, our customers did not want multiple sign-on codes, so we lashed the systems together and gave them single codes."*

The average hospital has thousands of devices and machines with computer chips, ranging from wireless blood pressure cuffs that transmit data into the electronic health record (EHR), to CT scanners, MRI machines, and even surgical robots. Anything with a computer chip offers attackers an entry point – even if the device is not connected to the Internet.

For example, an attacker could pose as a patient, employee, or supplier to gain access to a healthcare system's infrastructure. Once inside the physical walls of the organization, it really does not matter if the computing device is connected because the attacker can connect to or access the device.

A 2014 study from the SANS Institute found the devices most likely to be attacked include call contact software, digital video systems, firewalls and routers, radiology imaging software, and video conferencing systems.[10]

Then there are more mundane systems such as closed circuit television, webcams, remote door controls, and patient access systems, most of which fall under the purview of security rather than IT. Just imagine attackers installing malware on all security cameras, then watching as someone punches in an access code for your most secure areas.

The reality is that the "attack surface" for healthcare organizations is much wider and more complex than in any other industry.

It was the growth of the EHR that became health care's superstorm Sandy.

> *"For a long time, our security was paper records," said Reese. "If they fell off a truck that was a breach. Now we have a treasure trove of data and information in a target-rich environment for all types of hacking."*

Today, attackers could infiltrate the EHR and delete important patient data, such as information about a penicillin allergy or diabetes. If anything happens to the patient as a result, the hospital or physician is responsible.

The Uncommon Common

Although discussions around healthcare cyber-security tend to center on patient records, that is not what should be keeping CIOs and others in the C-suite up at night. Instead, they should be worrying just as much, if not more, about the security of their financial records, online education programs, staff scheduling databases, and, most importantly, the thousands of devices throughout their facility that are so critical to providing medical care. The C-suite should be worrying about the uncommon common.

Mining the Cloud

The mass movement to storing data in the cloud only increases a healthcare system's vulnerability. In 2014, 40 percent of healthcare organizations used the cloud, up from 32 percent in 2013.[11] By 2020, that number is expected to rise to 80 percent.[2] Despite these increases, nearly all IT administrators view the cloud as a serious threat, with just a third in one survey confident their information was secure.[11]

The problem is that most companies share servers with other companies, which may have different levels of security. If one is breached, it is likely that all will be breached. While large retail organizations like Wal-Mart have gone to dedicated servers, the price is typically too prohibitive for most healthcare entities.

If you are a fan of the Showtime drama Homeland, you probably recall the episode in which terrorists kill the vice president by hacking into his pacemaker. This scenario is far from fiction. In 2013, renowned hacker and security researcher, Barnaby Jack, discovered that pacemakers could be remotely disabled. Unfortunately, he died just days before he was to demonstrate this ability at a security conference. That same year, Vice President Dick Cheney revealed that five years earlier his cardiologist deliberately deactivated the wireless capability of his pacemaker because of concerns it could be used to harm Cheney.[12]

Pacemakers are hardly the only devices at risk. In 2011, security researcher Jerome Radcliffe hacked into his own insulin pump and blood glucose monitor to demonstrate how easy it would be to compromise their function and harm someone with diabetes.[13,14]

A 2013 Wall Street Journal investigation found that malware had infected at least 327 devices at Veterans Administration hospitals, including x-ray machines and equipment in a catheterization lab, which forced the lab to temporarily close.[15] What is most disturbing about the Wall Street Journal's investigation was that some IT executives contacted said, "they weren't aware that such problems were possible."[15] Indeed, a 2012 survey of 80 healthcare entities found that barely a third included IT security and/or data protection activities for US Food and Drug Administration (FDA)-approved medical devices.[16]

That year, FDA warned device makers that their equipment could be infected with malware and viruses that put patients at risk. However, even the agency does not know the extent of the problem because it does not require healthcare providers or device makers to report adverse events related to malware infections.[17]

More recently, the National Cyberspace Center of Excellence (NCCoE) released a paper warning about the security risk that an infusion pump, ubiquitous throughout hospitals, presents. One major issue researchers found was that many pumps have hard-coded usernames and passwords that are not changed when employees leave the hospital. [18]

Part of the problem with devices is that most were approved without appropriate safeguards; updating them now, manufacturers argue, would require additional FDA approvals (even though the agency has said that devices do not need to be recertified). The reality is that it would be costly and time consuming to retool and retest legacy devices.[18]

The Threat from Third-Party Vendors

The weakest link in any organization's cyber defenses is its supply chain, everything from the outsourced dietary and housekeeping departments to the copier repair person. Their systems interact with yours, true, but they also interface with other customers' IT – providing another portal for attackers.

Healthcare organizations know this. Just a third participating in a 2014 survey were confident that their business associates were meeting the requirements of the HIPAA Final Rule, and would be able to detect, assess, and notify their organization in the event of a data breach.[6]

Another entry point into large healthcare systems is through physician offices, which typically have relatively unsophisticated systems with minimal security that are connected to hospitals and other large medical facilities. As physicians increasingly provide access to patients through online portals, their vulnerability increases. Thus, the idea of going after small physician practice and then launching an attack into a hospital is very real.

New Rules for Medical Device Security Do Not Go Far Enough

In October 2014, the FDA released its final rule on cyber-security management for medical devices. However, the rule applies only to premarket submissions, not to devices already in use. It is also couched in language that recommends rather than requires, with the agency advising that manufacturers develop a set of cyber-security controls to "assure medical device cyber-security and maintain medical device functionality and safety."[19]

Today's Cyber-Threats – Worse than Tom Clancy Imagined

The main take away from the Anthem attack is that sophisticated organizations, on the level of our own Department of Defense (DoD) and National Security Foundation (NSF), are behind it.

Yes, it sounds like a Tom Clancy novel, but this is not fiction. Of particular concern with the Anthem breach is the cyber-terrorist organization Deep Panda, which has strong ties to China and verified attacks with sophisticated intelligence-gathering objectives. Even more frightening is that Deep Panda has a five-year strategic attack plan focused on healthcare targets.

Deep Panda and groups like it are highly skilled and polished with very mature tactics, techniques, and practices. They are also very patient, willing to sit for months or longer once they have access to a system. Indeed, Anthem reported that its attackers may have had access to its system as early as 2004.[20] These disparate groups also work together, sharing information and codes.

Many also offer Espionage-as-a-Service (EaaS). This means they infiltrate an organization's networks and wait until a customer requests something from that company. Then the EaaS vendor prepares a statement of work, signs a contract with the customer, and attacks a system from within. They are purely profit driven, with no concerns about ideology or religion.

Cyber-terrorists typically strike a company more than once. For instance, it appears that Anthem may have been the victim of parallel attacks – initial phishing assaults focused on employees, which enabled the hackers to deposit malware into corporate email accounts; followed by attacks via Domain Name System (DNS) to deploy the malware and create a central command center within the network. This malware enabled the attackers to monitor network traffic, take over webcams, and capture confidential data.

Cyber-terrorists and cyber-criminals operate on the Dark Web, the part of the Internet that is not indexed by mainstream search engines, but requires special software to access. It is an entire ecosystem focused solely on doing harm.

Current Efforts Are Not Enough

It is nearly incomprehensible how unprepared healthcare entities are for cyber-attacks given the magnitude of the threat.

In one survey of executives in 600 large companies, 13 percent of whom worked in the healthcare sector, just 48 percent said their firms had invested in technologies to detect and respond to such attacks, while just a third said they had security incident and event management technologies. Additionally, just a fifth said their organizations continually monitored their systems, while 44 percent said they never monitored their systems or did not know if their systems were monitored.[11]

A three-month investigation from HITRUST of the challenges the healthcare industry faces in managing cyber risk found that nearly all organizations acknowledged minimal understanding of the impact of cyber-threats on their current cyber-security products and the unique applications, systems, and devices they protect.[5]

Part of the problem is denial. As one CIO said during a roundtable discussion on the topic with a security firm: "The reason no one bought your service was that, frankly, if we found out about security holes, then we would have to fix them. It is easier to react after the fact than to convince everyone we need to do something before it happens. Not to mention that we have a ton of other stuff going on and this just adds to an already overworked and under resourced group within most hospitals."

"Good enough" is not good enough. Even if Anthem had encrypted its records, it would not have mattered because the attackers entered the system as high-level administrators who would have had access anyway. Hiding a service set identification (SSID), which most healthcare organizations do, is not enough either. The reality is that hackers can find a hidden SSID or wireless access point within minutes, then launch a "man in the middle (MIM)" attack.

An MIM attack is when someone hijacks a system, getting between the end user and the computing resource desired and funneling all data to their own network rather than your network.

That is not to say that organizations should not be taking basic steps like blocking anonymous email accounts, websites, and IT addresses – steps too many fail to implement.

Organizations need to adopt a good offense, not just react to threats. This requires a comprehensive risk management assessment that starts with the belief that significant security is possible, focusing attention on the most critical areas of information, and locking down those areas.

Although it is nearly impossible to achieve 100 percent security (even the CIA, NSA, and DoD are only at about 90 to 95 percent), hospitals should aim for at least 80 percent. Yes, it is expensive, but people's lives are at stake.

Need for C-Suite Involvement

A year ago, CEOs would never lose their jobs over a security breach. Then came Sony, Target, and, quite probably, Anthem. Now, a CEO can miss his or her quarterly numbers a few times and keep their jobs; allow a major security breach on their watch, and they not only lose their job, but their careers.

"The C-suites are not prepared to handle the onset of questions and levels of interest from their boards," said Sentara's Reese. "The reality is that the C-suite may not entirely know what it's doing." Indeed, a 2014 Ponemon survey found that just a third of the nearly 600 companies polled said their board of directors, chairman, and CEO were involved in plans to deal with a data breach.[11]

In addition, a survey of 203 C-level executives by ThreatTrack Security found that nearly three-fourths did not even believe that the CIO should be part of the leadership team. While 55 percent of respondents said the CIO should assume responsibility for data breaches, just 46 percent said they should be responsible for cyber-security purchasing decisions.[21]

So any cost/value analysis of tightening security must incorporate the cost and value to the reputation and professional life of those in the C-suite.

Culture Is Key

Technology did not detect the Anthem breach – an IT employee did. The employee was logged onto the system and noticed someone else using the account. If not for one person doing his job, the attack could have gone undetected for months, even years. To that point, a 2012 Ponemon survey of 80 healthcare entities found that employees discovered about half the breaches; the other half came from an audit or assessment.22

Of course, it works the other way too, with many breaches made possible by human error, such as falling for a phishing scheme. That is why healthcare companies cite employee negligence as their greatest security risk.6

Thus, superior cyber-security requires a culture of security with intensive, personalized, ongoing training to ensure that all employees – from housekeeping to the C-suite—understand their role in preventing a breach. Employees should also know that they may be sued for malfeasance if they contribute – even inadvertently – to a security breach.

However, barely half of large organizations have training and awareness programs for employees with access to sensitive or confidential personal information.[11]

> *"The art of security is seven parts technical, and three parts cultural." --- Bert Reese, Senior Vice President & Chief Information Officer, Sentara Healthcare*

Are You Next?

If you cannot answer the following questions with a strong "**yes**," then you may not be prepared for the current and coming cyber-security threats.

1. Do you know if you are already compromised? A 2014 survey of nearly 600 companies in 2014 found that nearly a fifth did not even know if their company had a data breach.[11]
2. Is your supply chain strong? If you are not establishing a level of security with your partners, then you have a big hole in your security.
3. Do your board and C-suite understand the threats and risks to your institution from cyber-attacks?
4. Do you have a response plan to an attack? A 2014 survey of nearly 600 organizations found that while 73 percent had data breach response plans and teams, few felt their companies were "effective" or "very effective" in developing such plans.[11]
5. Do you regularly test and update your response plan? When asked, in one survey, about how often healthcare organizations updated/reviewed their data breach response plans, only 3 percent reviewed plans each quarter, 14 percent reviewed plans once each year, and a shocking 37 percent had not reviewed or updated data breach response plans since they were first put in place.[11]
6. Do you use more than one organization to assess and test your security? Using the same vendor over and over, leads to a kind of IT Stockholm syndrome, in which the vendor begins to think like the company.
7. Do your IT and Security Departments work together? Security is no longer monitoring cameras and infrastructure; it is working with IT to ensure those tools are not compromised and that there is a cohesive and holistic strategy around security – whether physical or cyber.
8. Is your workforce adequately educated about cyber-security threats and their role in minimizing them? The real question is "Would you invite Deep Panda to attack your system?" If not, then the headlines in the media will not be about your organization's loss of data; but about the loss of patient lives.

References

1. Russ N. Secure Healthcare in the Age of Targeted Attacks. Symantec Corporation. 2014.
2. Insights IH. IDC Reveals Health Insights Predictions for 2015. November 20, 2014.
3. The Year of the Data Breach -- a Recap of 2014 and Rerview of 10 Years of Breaches. Identity Theft Resource Center. January 19, 2015. http://www.idtheftcenter.org/Data-Breaches/the-year-of-the-data-breach-recap-2014-and-ten-years-of-data.html.
4. Finkle J. Exclusive: FBI Warns Healthcare Sector Vulnerable to Cyber Attacks. Reuters. April 23, 2015. http://www.reuters.com/article/2014/04/23/us-cybersecurity-healthcare-fbi-exclusiv-idUKBREA3M1Q920140423.
5. HITRUST. Healthcare Organizations Lack Tools for Cyber Situational Awareness and Threat Assessment March 4, 2015.
6. Ponemon Institute. Fourth Annual Benchmark Study on Patient Privacy & Data Security. March 2014.
7. Ponemon Institute. 2014 Cost of Data Breach Study: United States. May 2014.
8. Rubenfire A. Anthem Hack Will Shake up Market for Cyber Risk Insurance. Modern Healthcare. February 5, 2015.
9. Yadron D, Beck M. Health Insurer Anthem Didn't Encrypt Data in Theft. The Wall Street Journal. February 5, 2015.
10. Filkins B. Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon. SANS. 2014.
11. Ponemon Institute. Is Your Company Ready for a Big Data Breach? The Second Annual Study on Data Breach Preparedness. September 2014.
12. Peterson A. Yes, terrorists could have hacked Dick Cheney's heart. Washington Post. October 21, 2013.
13. Deloitte. Medical Device Hacking: An Ominous Threat. Deloitte Insights. 2013.
14. Insulin Pumps Vulnerable to Hacking. Associated Press. August 4, 2011.
15. Weaver C. Patients Put at Risk by Computer Viruses. The Wall Street Journal. June 13, 2013.
16. Ponemon Institute. Third Annual Benchmark Study on Patient Privacy & Data Security. March 2013.
17. Fu K, Blum J. Controlling for Cybersecurity Risks of Medical Device Software. Communications of the ACM. 2013;58(10):21-23.
18. O'Brien G, Khanna G. National Cybersecurity Center of Excellence. December 18, 2014.
19. Food and Drug Administration. Content of Premarket Submissions for Management of Cybersecurity in Medical DevicesOctober 2, 2014.
20. Terhune C. Anthem says hackers had access to customer data back to 2004. Los Angeles Times. February 12, 2015.
21. ThreatTrack Security. No Respect: Chief Information Security Offices Misunderstood and Underappreciated by Their C-Level Peers. 2014.
22. Ponemon Institute. Third Annual Survey on Medical Identity Theft. June 2012.

About the Authors

John Gomez is the CEO of Sensato, a cyber-security & privacy firm exclusively focused on healthcare. Previously, John was the CTO/co-President of Allscripts, a leading provider of healthcare information solutions. During his time with Allscripts, John helped lead Eclipsys as CTO and also oversaw their Business Development and International Business Unit, which was responsible for operations in AsiaPac, the Middle East and South Pacific. John was also the CTO of WebMD and worked at Microsoft in various capacities, including the development of their Advanced Technology Centers as well as the design/development of several key product offerings. John was also part of the team that built the first on-line bank during his time at HR Block's Advanced Engineering Group. Prior to his work in high-technology, John worked as Director of Financial Systems for American Re-Insurance in Princeton, NJ. During his career John has worked with small startups to multi-national, billion dollar public companies overseeing teams of 2,000 plus team members. He is often called on to lecture on product design, leadership and operational excellence and future trends across industries.

Colin Konschak is the Managing Partner and CEO of Divurgent. He is an accomplished executive with more than 20 years of experience and a record of achievement in quality service delivery and project management for healthcare operations, P&L management, strategic planning, and alliance management. He currently leads Cyber-security and Privacy initiatives for Divurgent. Colin is a registered pharmacist, possesses an MBA in health services administration, is board certified in healthcare management from the American College of Healthcare Executives (ACHE), and is a Six Sigma black belt. Colin is a fellow in both the Healthcare Information Management System's Society (HIMSS) and ACHE.

COMPANY OVERVIEW

Divurgent and Sensato Partnership brings an in-depth understanding of the complexities, technologies, and, most importantly, security-related vulnerabilities and challenges facing today's health IT organizations and leaders. This unique partnership provides healthcare organizations a means to lower risks, decrease vulnerabilities, and evolve their understanding of cyber-security.

Sensato is a boutique technology firm that specializes in simplifying cyber-security and privacy for healthcare. Sensato was founded in 2013 by John Gomez and provides a variety of consulting and software solutions to the healthcare industry. Further details about Sensato can be obtained by e-mailing info@sensato.co or visiting www.sensato.co

Divurgent is not the typical healthcare consulting firm. As a nationally recognized company, we are committed to healthcare evolution and the strategies and processes that make it possible. We help our clients evolve in payment and delivery reform, as well as patient engagement, providing higher quality of care, lower cost of care, and healthier communities.

Focused on the business of hospitals, health systems and affiliated providers, Divurgent believes successful outcomes are derived from powerful partnerships. Recognizing the unique culture that every organization offers, we leverage the depth of our experienced consulting team to create customized solutions that best meet our client's goals. Utilizing best practices and methodologies, we help improve our client's operational effectiveness, financial performance, and quality of patient care. For more information about Divurgent, visit us at www.divurgent.com

REDEFINING CONSULTING. TRANSFORMING HEALTHCARE.

Divurgent is committed to healthcare evolution and the strategies and processes that make it possible. We help our clients evolve in payment and delivery reform, as well as patient engagement, providing higher quality of care, lower cost of care, and healthier communities.

JOIN THE DISCUSSION. CONNECT!

DIVURGENT
Redefining Consulting. Transforming Healthcare.

[sensato]

HIMSS North America PLATINUM Corporate Member

CHIME College of Healthcare Information Management Executives

MODERN HEALTHCARE BEST PLACES TO WORK

www.divurgent.com | 757.213.6875 | info@divurgent.com