INSTITUTE *for* HEALTHCARE INFORMATION TECHNOLOGY

INDUSTRY REPORT:

The State of Cybersecurity Among Georgia Hospitals

Sponsored by IHIT

TABLE OF CONTENTS

THE CYBERSECURITY CHALLENGE IN HEALTHCARE: A GROWING THREAT TO GEORGIA COMMUNITIES

What is Cybersecurity?

Cybersecurity or information technology security are the techniques of protecting computers, networks, programs and data from unauthorized access.

Southern Crescent Hospital. Calhoun Memorial Hospital. Stewart-Webster Hospital. And the list goes on. These are the names of some of Georgia's hospitals that have had to close their doors in the past several years.

366,000 full-time jobs in Georgia. That's the number of citizens who rely on Georgia's hospitals and medical professionals for their livelihood, according to the estimates provided by the Georgia Hospital Association.

Georgia health systems and the jobs they support are at risk when our hospitals are under attack, particularly cyber attacks.

Many people are aware of the legislative and regulatory pressures hospitals are under these days, but a more serious threat looms in the background — the threat of a cybersecurity attack that can expose our citizens' private health information and contribute to hospital closures, which can have a devasting impact on local economies.

These threats are growing, and the risk to Georgia communities is growing every day.

Let the Battle Begin

Cybersecurity attacks in healthcare are on the rise — around the country and here in Georgia. In fact, the Department of Health and Human Resources recently announced two significant initiatives designed to prevent, prepare for and respond to cybersecurity attacks in healthcare:

- The Department of Health and Human Services opened the Health Sector Cybersecurity Coordination Center (HC3) in Washington to strengthen coordination and information sharing within the industry and provide timely and actionable information to healthcare organizations as well as develop strategic partnerships. (October 30, 2018)
- The Food and Drug Administration and HHS announced an agreement to implement a new framework for greater coordination between the two agencies for addressing cybersecurity in medical devices. (October 16, 2018)

Now is the time for Georgia state legislators, community leaders and CIOs to take new measures to help protect our hospitals and our citizens from the severe threats these cyber attacks pose.

This paper captures the collaborative work done by 18 Georgia hospital CIOs who have come together on multiple occasions over the past 12 months to identify and document the significant challenges they face when it comes to battling these cybersecurity threats.

It is this group's expectation that once state legislators and community leaders truly understand the unique cybersecurity challenges our healthcare systems face, they will be compelled to support this group's request for state resources to help Georgia healthcare providers protect our citizens' medical information and jobs.

The Journey to In-Security

Unlike other industries, hospitals and healthcare providers are particularly vulnerable to cybersecurity attacks that can have devasting effects on both their patients' privacy and their reputation in the communities they serve. A component of the Affordable Care Act of 2010 incented thousands of healthcare providers to adopt electronic health record (EHR) systems as the Center of Medicare and Medicaid Services (CMS) sought to gain greater visibility into the rising healthcare costs and inconsistent reimbursement rates.

As healthcare providers raced to meet CMS's deadlines for federal funding incentives, CIOs were forced to make complex technology and infrastructure decisions within very short timeframes and with little insight into what this new digital world would look like down the road. Virtually all hospital financial and technical resources were prioritized for the new EHR systems, and cybersecurity initiatives took a back seat.

Healthcare Industry Public Security Breaches Reported in Georgia

YEAR	BREACHES MADE PUBLIC	MEDICAL RECORDS EXPOSED
2018	4	446,566
2017	14	381,136
2016	9	783,646
2015	8	924,953
2014	18	51,210

Source: Department of Health and Human Services, Office of Civil Rights, Breach Portal

While the physical and network security measures were well understood and could be easily enforced by a finite group of people in the hospital (IT, security and compliance resources), cybersecurity measures and strategies were relatively new at that time. The realization that every employee was now a real threat to their ability to protect the terabytes of personal health information (PHI) their organizations now possess was (and still is) overwhelming for many CIOs.

> "Cybersecurity is everyone's responsibility."
>
> — Stanton Gatewood, CISO, Georgia Technology Authority

And as the demand for greater access to this data across the fragmented user community among different care settings grew, securing the data became even more challenging.

The combination of this rapid transformation to the digital world where every device and every staff member is connected plus the necessity of maintaining older, legacy systems created an environment that was ripe for cyber criminals to prey on healthcare providers. The implications have played out in the news with hundreds of stories of hospital records being held ransom, patients' PHI being stolen, and hospitals paying millions of dollars in fines that ultimately lead to facility closures.

Why is Healthcare so Different?

While some industries, such as financial services and retail, are further along their digital transformation journeys, healthcare providers are still relatively early in the game and are competing against highly experienced, highly trained attackers.

The perfect storm formed over the past few years as massive regulatory requirements and payment reform forced healthcare providers into timeframes and investments that their razor-thin margins could not support. Hospitals and physician groups are now scrambling to catch up with their attackers and minimize the damage these breaches can have on their patients and their reputations. Below are the top reasons why healthcare is so different from other industries.

1. **The electronic healthcare record is worth more than any other data on the black market.**
   It is the most comprehensive record about the identity of a person that exists today. Victims of financial theft, such as stolen credit cards and bank account numbers, can change the data that represents their financial footprint. Victims of health record identity theft are at risk for the rest of their lives.

   Because of the permanent nature of these records that include demographic information, historical information about where you live, where you worked, names and ages of relatives, and every doctor visit and diagnosis you've ever received, the electronic health record is the most sought-after data by hackers. In fact, Forbes recently published an article, stating that each medical record could be worth $1,000 while social security numbers are 10 cents and credit card numbers are worth 25 cents.

2. **Hospitals typically operate on razor-thin margins.**
   For many hospitals, the investment needed in technology and human resources to properly secure their sprawling environments is cost-prohibitive. They are often forced to choose between providing clinical services or acquiring life-saving devices or implementing new security solutions on their servers or hiring more security resources. And for many rural hospitals who are already struggling to keep their doors open, cybersecurity initiatives get pushed to the back of the line, often until it is too late.

3. **The health system foundation is complex and constantly shifting.**
   As massive payment reform sweeps through and disrupts virtually every healthcare provider in America, organizations are turning to mergers and acquisitions at record-breaking speeds in attempt to consolidate and gain financial strength through numbers.

   For the CIO, this results in a highly fragmented and distorted IT infrastructure that must be secured while it continues to grow. The complexities of these environments continue to increase, making securing sensitive data increasingly difficult.

> "The healthcare field has the highest cost per breached record of any industry."
>
> — Ponemon Institute Study, 2018

4. **Sharing and collaboration is often prohibited.** Fearing the public outcry and reputational damage that comes with a security breach, many hospital CIOs and board members are bound to secrecy when it comes to these issues. Afterall, who can blame them given the piercing headlines and local TV news stories that are sure to follow a public breach? The hypersensitive nature of healthcare prevents CIOs from sharing insights with each other, which in turn aids their attackers.

Georgia Hospitals That Have Closed Their Doors Since 2005

- Southern Crescent
- Calhoun Memorial Hospital (Arlington)
- Charlton Memorial Hospital (Folkston)
- Hart County Hospital (Hartwell)
- Lower Oconee Community Hospital (Glenwood)
- North Georgia Medical Center (Ellijay)
- Stewart-Webster Hospital (Richland)

> "By supporting the hospital's ability to protect its citizens' health information and its data security infrastructure, state and community leaders are protecting the economic health of the entire community."
>
> — Pat Williams, President of the Institute of Healthcare Information Technology, Georgia

5. **The implications to the community are far-reaching.** The implications of a cybersecurity event in a hospital can be devastating to the hospital, its patients and the community it serves. That's because hospitals are typically one of the largest employers of the rural communities. If a ransomware attack occurs, the hospital is often unable to bear the extra costs associated with remediation activities, federal fines and in some cases, paying the ransomware fines demanded by attackers.

   If the hospital has to close its doors, the entire community suffers. And hospitals are closing at an alarming rate, to the tune of 10 percent of community hospitals since 2005. And that number increased sharply over the past eight years, with 70% of the closures taking place between January 2010 and January 2018. With more than 366,000 full-time working Georgia citizens depending on healthcare providers for their full-time jobs, the threat of cybersecurity breaches goes way beyond exposing PHI all the way to destroying rural communities.

Examples of Cybersecurity Breaches

Often, missteps in security protocols caused by lack of adequate resources are at the center of some of the biggest cybersecurity incidents worldwide.

In May 2017, several UK hospitals were still running Microsoft Windows XP machines (as many still do) and other legacy systems that were vulnerable to the ransomware WannaCry. After missing the implementation of a patch, the virus is believed to have entered via a phishing campaign, and once it gained a foothold, it spread to all other vulnerable machines on the network, encrypting them as it went.

As a result, nearly 33% of hospitals and 8% of general physician practices in the UK found their IT systems unusable. Nearly 18 months after the incident, the National Health Service put a price tag of $92M euros ($105M) and reported 19,000 cancelled appointments.

> "We know that the majority of the cybersecurity attacks that occurred over the past year could have been prevented with quality and timely information — and a heightened importance of sharing information cannot be stressed enough."
>
> — Jeanette Manfra, Assistant Secretary for Cybersecurity & Communications, Department of Homeland Security

Closer to home, Georgia-based Emory Healthcare experienced one of the largest security breaches in 2017, revealing that patient records of its Orthopedics & Spine Center and Brain Health Center had been breached, exposing names, birth dates, contact information, internal medical records and appointment information of 80,000 patients. Hackers broke in and removed the six-hospital system's appointments database and demanded a ransom to restore the site.

> In the U.S., 8,891 breaches representing 11,239,084,942 medical records have been made public since 2005.

In November, 2018, *Healthcare Informatics* publication reported a case where two regional hospitals in Ohio and West Virginia became unable to accept patients from emergency service transports following a ransomware attack on the hospitals' computer systems.

These days, it's rare to open a healthcare industry publication without reading about the latest hospital cyberattack. The number of hospitals and patients being impacted by cybersecurity attacks are staggering.

> "Short of loss of utility, cybersecurity threats represent one of the greatest impacts to the healthcare industry."
>
> — Geoff Brown, VP & CIO, Piedmont Healthcare

Now is the Time to Take Action

To better prevent and prepare for the sophistication and volume of cybersecurity attacks, hospitals are coming together.

In October 2017, CIOs from around the state gathered at the Augusta University-Medical College of Georgia to explore the issue and determine ways they could work together to make a difference. In June 2018, the group met at the Georgia State Capitol; and then in the months of August and September, the CIOs held regional working group sessions where hospital leaders gathered in small group sessions to discuss their specific challenges and exchange ideas on how to solve them.

Each of the eight working groups reported back to the collective group in a CIO Cybersecurity Fall Roundtable session that took place in October 2018 in Macon at Mercer University.

In the Cybersecurity Roundtable opening remarks, Dr. Jean Sumner B.S.N, M.S.N, M.D., Dean of Mercer University's School of Medicine, commented, "We are proud to host this group of dedicated CIOs who have shown enormous initiative to find new ways to help prevent, prepare for and respond to the very real threat cybersecurity attacks present to Georgia hospitals, particularly those serving the 1.8M Georgia citizens living in rural areas. We are living in an unprecedented time that requires state legislators, community leaders and hospital technologists to come together to form a protective barrier around our healthcare community in Georgia."

Roundtable Findings: Top Cybersecurity Issues and Concerns Among Georgia Hospital CIOs

- Preventing phishing attacks. Phish · ing / ' fiSHiNG / (noun) A social engineering technique by which an attacker tricks an employee, usually by impersonating another person in an email, and convinces the employee to give sensitive information, such as login credentials.

  With thousands of employees accessing email from all different devices, it just takes one uninformed employee to click on a malicious link to take down an entire health system. Hackers use these emails to not only access data, but also steal employee credentials that allow them to log into the systems and perform malicious activities, like generating prescriptions and directing reimbursements, under stolen credentials.

  Hospital IT leaders are challenged to educate every single employee on the rapidly evolving tricks of the trade that attackers use to compel the employee to click on the seemingly innocent link. Not only is it time-consuming and difficult to prepare and maintain the training materials, but also to ensure employees comprehend the risks and do their part to help protect the enterprise.

- Maintaining legacy technology that was not built to withstand the sophistication and volume of cybersecurity attacks. Many hospitals still depend on older systems to maintain their medical records and run their operations. Some of these systems have been around for 30 or 40 years. The complexities of these

environments, along with the shortage of technical resources who know these legacy coding languages and mainframe systems, creates a real threat for many CIOs.

- Management oversight of third-party systems that require access to PHI in order to support the patient's care journey across different settings is often like herding cats. These highly connected and highly portable biomedical devices introduce new threats that make it easy for data to walk out the door unnoticed.

  As thousands of new applications and hundreds of digital health startup technology companies flood the market each year, physicians are pressuring their IT leaders to enable them to adopt these new solutions; but IT leaders are forced to balance the need for innovation with the risks of security threats. In addition, the older devices in place are governed by the FDA, not by the IT staff or modern policy, which introduce new risks when added to the modern network without proper vetting.

  According to Patty Lavely, CIO of Gwinnett Medical Center, "Over the years, biomedical device security has been hindered by FDA regulation. As a medium-sized health system in Georgia, we have approximately 1,500 biomedical devices on our network. These devices have the potential to positively impact patient care, but they are vulnerable to a cyberattack. The number of devices hospitals have on their network continues to increase as we mature our electronic health records and improve interoperability within our health system."

  According to Geoff Brown, VP and CIO of Piedmont Healthcare, "There continues to be a shortage of coordinated resources systematically, and as an industry, we collectively appear to be losing the battle in our rural and urban healthcare organizations."

- Time and human resource constraints prevent hospital leaders from preparing for and preventing cybersecurity attacks. Recruiting and retaining IT security talent ranks as one of the highest challenges for Georgia hospital CIOs. One-person IT shops are very common, with one person being responsible for everything from provisioning a new employee to making sure the computers are working.

  Dedicating time to proactively preventing (and even preparing for) an attack is simply not an option. And if they are fortunate to hire a good IT person, they typically get courted by one of the larger hospitals with promises of more career opportunities and better compensation. In fact, one CIO shared specific details about their IT resource process, "In our rural community, it takes us about six months to find a qualified individual, two months to get them onboarded and educated about our environment, and then they get recruited to move to a larger market — and the cycle repeats."

- Cybersecurity insurance policies are not fully vetted or understood by many hospital leaders, leaving IT leaders scrambling to help the business understand the true risks that remain. Many members of the Roundtable reported not having even seen their hospital's policy, as it was reviewed and agreed upon by the legal and compliance teams without any input from IT. If the IT and business leaders do not truly understand their risks, the necessary funding and policy enforcement process typically break down.

  According to Michelle Madison, partner at Morris, Manning & Martin LLP's Healthcare Practice, "Common across all different shapes and sizes of hospitals is a gap in understanding of what hospitals think is covered and what is actually covered when it comes to their cybersecurity insurance policies. The intricacies of these policies must be intimately understood by board members, business leaders and the technologists working together to protect these organizations."

A Coordinated Effort. A Call to Action.

While Georgia hospital CIOs and IT leaders are working hard every day to protect the valuable electronic health records of our 10.55 million citizens (U.S. Census Bureau), the Cybersecurity Roundtable participants identified several opportunities where state resources could be applied help hospitals better prevent, prepare for and respond to cybersecurity attacks.

- Establish a healthcare-specific cybersecurity resource center that offers Georgia hospitals and healthcare providers access to the most current cybersecurity tools and information. Whether virtual or physical, and/or as an extension of the Georgia Cyber Center, the healthcare center would make available resources such as:

    - An electronic alert system of ongoing threats submitted that can make other hospitals aware of what is happening and potentially prevent the attack from spreading or being duplicated.

    - Incident response kits, including pre-built scenarios, incident response drills, and response/recovery collaboration protocols to guide hospitals through preparedness drills to ensure the most thorough response plans are in place.

    - Online learning center that contains HIPAA and security to assist hospitals in raising awareness and education of employees.

    - A statewide security operations center that could serve all hospitals by providing security functions such as threat intelligence, monitoring, and incident response (similar to the Multi-State Information Sharing and Analysis Center). Financially vulnerable healthcare providers could apply for grants to enable access to these tools and services.

- Establish regional online networks of IT Safe Zones where providers can confidentially share threat — and incident — response insights. Being able to access information from others about how they responded to incidents, the lessons they learned and the suggestions they have would be invaluable.

> "We must enable collaboration to improve the cybersecurity posture of all Georgia hospitals. The absense of a coordinated approach provides an advantage to threat actors."
>
> — Chris Beasley, CIO Houston Healthcare

The Time is Now

During his opening remarks at the CIO Cybersecurity Roundtable, Senator Bruce Thompson said it best: "Every single community, every single family, and every single one of us is either currently or will be impacted by a cybersecurity attack. Even though our state is ahead of others in some ways with our Augusta Cybersecurity Center, we have a whole network of fragile, rural hospitals that our constituents depend on for their health, jobs and community services. Our hospitals should be safe zones for people, but instead, they are under attack, and we need to provide resources to help them. We need all hands-on deck."

The time to act is now, for hospital CIOs, state legislators, community leaders and law enforcement resources to come together and offer our healthcare providers the assistance they need to prevent, prepare for and respond to cybersecurity attacks.

It is the hope of these 18 hospital CIOs and business leaders who have participated in these collaborative exercises that state legislators and community leaders will use the information in this paper to take action on the requests noted above and help Georgia hospitals better prevent, prepare for and respond to cybersecurity attacks and protect Georgia citizens.

CONTRIBUTORS TO REPORT

Omer Awan
Senior VP & CIO, Navicent Health

Chris Beasley
CIO, Houston Healthcare

Geoffrey Brown
VP & CIO, Piedmont Healthcare

Jeff Buda
VP & CIO, Floyd Medical Center

Jesse Diaz
VP & CIO, Phoebe Putney Health System

Shirley Gabriel
VP & CIO, University Health Care System

Gary Gower
CIO, Appling Healthcare System

Patty Lavely
Senior VP & CIO, Gwinnett Health System

Michele Madison
Morris, Manning & Martin LLP

Steven McWilliams
VP & CIO, Georgia Hospital Association

Chris Paravate
CIO, Northeast Georgia Health System

Milo Varnadoe
CIO, Warm Springs Medical Center

B. Alan Whitehouse
CIO, Wellstar West Georgia Medical Center

Patricia Williams
Institute for Healthcare IT

Ross Youngdale
Technical Director and HIPAA Security Officer, Phoebe Putney Health System

CONTACT INFORMATION

Institute for Healthcare IT

instituteforhealthcareit.org