Cybersecurity & Healthcare

How healthcare has become a top target for cybercriminals—and what you can do to prepare and protect
CONTENTS

03  Cybercrime is on the rise with healthcare as a primary target
04  The threat continues to grow
05  How and why are these breaches happening?
08  What do these attacks look like?
09  At what cost?
10  The time to act is now
12  10 steps toward protecting the healthcare environment
14  How AT&T can help you
16  Are you confident in your cybersecurity?
Cybercrime is on the rise with healthcare as a primary target

The healthcare industry is under constant attack from cybercriminals.

Almost 32 million patient records were breached in the first half of 2019. That’s significantly higher than the 13.2 million record breaches reported to the U.S. Department of Health and Human Services in the entirety of 2018.

Surprised? You shouldn’t be. Cybercriminals have discovered the value of the medical records and private data healthcare organizations hold. Personal information, social security numbers, medical history—all of these easily accessed, sold, and exploited.

Security breaches cost the industry a substantial amount of money—and they also seriously erode public trust. The industry is starting to take note and is investing more in its cybersecurity posture, but most institutions face significant constraints. Small budgets, outdated IT architecture, staff with low security awareness, and industry-specific compliance regulations all contribute to their security concerns.

It’s time for the industry as a whole to accelerate adoption of strategies, tactics and best practices—already well defined in the larger information security community—to enhance protection of patient data, endpoints, and mission-critical systems.
The threat continues to grow

The extraordinary number of breaches in 2019 is a continuation of a trend that has accelerated in the last few years. Since 2016, the industry has experienced at least one health data breach a day.

In 2018, that number reached 365, which HIPAA Journal, using data compiled by the U.S. Department of Health and Human Service’s Office for Civil Rights, says is a 2% increase from 2017.

Half way into 2019, there have been 285 disclosed breach cases involving 500 or more compromised records, according to HCI Innovation Group.

Beazley Breach Insights states that healthcare entities reported the highest number of cybersecurity incidents in 2018, almost twice the amount of financial services institutions.
How and why are these breaches happening?

The cybersecurity issue in the healthcare industry is both a technological and a cultural one. While widespread outdated systems and poor web code make the industry ripe for cyberattacks, a busy workforce that is typically uninformed about everyday threats makes it easy for attackers to get sensitive patient information. According to a report from Kapersky, nearly a third of a surveyed 1,800 healthcare employees said they had never received any cybersecurity training.

In addition to often inadequate IT budgets, which is unfortunately all too common across many industries, here are some of the top obstacles faced by healthcare organizations, according to two separate reports from Frost & Sullivan and the Healthcare Information Management Systems Society (HIMSS):

1. Healthcare is getting outbid for top cybersecurity talent
Cybersecurity salaries increased 8% in 2018, according to Frost & Sullivan’s report, the US Healthcare Cybersecurity Market, 2018-2023. Frost & Sullivan cites the Exabeam 2018 Cybersecurity Professionals Salary and Job Report as saying that only 27% of cybersecurity professionals in healthcare are satisfied with their pay. There is a resource pinch as healthcare competes with other verticals for the limited number of experts.

2. Low rate of phishing testing
“Phishing” is the attempt to obtain and exploit sensitive information such as passwords and usernames by disguising oneself as a trustworthy entity most commonly through email communication. It’s one of the most popular tactics of cybercriminals. The HIMSS 2019 Cybersecurity Survey revealed that almost 20% of healthcare organizations do not conduct phishing tests and thus do not have a system in place to protect themselves from one of the most common forms of cyberattacks.
Healthcare IT is fragmented

Frost & Sullivan says healthcare IT is fragmented with hundreds of applications and multiple electronic health records (EHRs), each with their own security layers. The need to interface with multiple access controls makes the introduction of additional security systems a daunting task for already-overextended IT personnel.

Lack of a standardized security approach and testing

A healthcare organization can approach security from multiple routes, including the HITECH guidelines for healthcare cybersecurity and the general HIPAA guidelines. The National Institute of Standards and Technology also has a cybersecurity framework that provides general guidance on implementing cybersecurity. Uncertainty about which approach to take, and the potential for incompatibility with an existing structure, makes organizations more reluctant to invest in new cybersecurity solutions, according to the Frost & Sullivan report.

Pervasiveness of legacy systems

When compared to other industries, healthcare has a higher propensity to rely on legacy operating systems, according to the HIMSS report. This older, outdated architecture can often make a cybercriminal’s job way easier. This is understandable, as medical devices and healthcare-oriented systems have a unique level of complexity that can make it difficult to change. However, as cyberthreats continue to rise, stakeholders will need a plan to modernize their industrial control systems to be able to implement best security practices.
Personal health information is **50 times** more valuable on the black market than financial information*

The biggest causes of healthcare data breaches in 2018 were**:

- Unauthorized access/disclosures: **39.18%**
- Theft: **11.50%**
- Lost PHI/ePHI: **3.56%**
- Improper disposal of PHI/ePHI: **2.47%**
- Hacking/IT. incidents: **43.29%**

---

What do these attacks look like?

Here are some of the common cyberthreats faced by healthcare organizations as defined by the Department of Health and Human Services in its *Health Industry Cybersecurity Practices* report.

**E-mail phishing**
Email phishing is an attack designed to trick employees into disclosing information by disguising oneself through email communication.

**Scenario**
An administration staff member receives an email from an entity disguised as IT staff requesting login credentials for a system update.

**Consequence**
Several patient records were accessed and compromised for identity theft.

**Possible Prevention**
Staff training on recognizing common tell-tale signs of phishing emails and best practices of interacting with suspicious communication.

**Loss and theft of equipment or data**
Unattended or misplaced mobile devices or USB drives are an easily exploitable method of obtaining sensitive records or internal network access.

**Scenario**
A busy doctor accidentally forgets his laptop in a hospital common area.

**Consequence**
A thief steals the laptop and accesses and downloads hundreds of medical records for sale on the dark web. The hospital is now operating without crucial information for several of their patients.

**Possible Prevention**
Robust encryption on sensitive data to help prevent unauthorized access. Data recovery and backup systems.

**Unauthorized access/ hacking of connected medical devices**
Many of today’s hospitals deploy a vast network of cellular and Wi-Fi-connected medical devices that, if unprotected, can be remotely accessed for malicious intent.

**Scenario**
A hacker takes over an unprotected file server that maintains function over all heart monitors in the ICU.

**Consequence**
Shut down heart monitors have put many patients at extreme risk.

**Possible Prevention**
Security practices such as patching, hardening, and threat detection services for the network and connected devices.
At what cost?

In their 2018 Cost of Data Breach Report, IBM and Ponemom Institute found that healthcare data breaches cost an organization on average $408 per compromised record.

But the financial impact may not even be the worst of it. A study by insurance giant Aetna revealed that, on average, consumers rated privacy and data security as more important aspects of healthcare than cost and getting personalized care. Further, according to Radware’s 2018 Consumer Sentiments: Personal Data and the Impact on Customer Loyalty, the clear majority (68%) of consumers said that, when a company suffers a data breach, they must be convinced that the security issue has been addressed and any damage has been rectified before continuing to do business with the brand. Even worse for the organization’s bottom line, 1 in 10 consumers will walk away entirely from the brand.

Percentage of patients that ranked the following aspects as ‘very important’:

- Privacy: 80%
- Data Security: 76%
- Cost: 73%
- Personalized Care: 71%
- Coordination among providers: 68%

$1.4M: Estimated cost of each data breach in the healthcare industry, behind only retail and high tech**

Top 5 largest data breaches in 2018***:
- LifeBridges Health: 500,000 patients
- Health Management Concepts: 502,416 members
- CNO Financial Group: 566,217 customers
- UnityPoint Health: approx. 1,400,000 patients
- AccuDoc Solutions: approx. 2,650,000 patients

[4/5 are healthcare industry specific]
The time to act is now

The cyberthreat facing healthcare organizations is extensive, and the consequences of a breach could be detrimental to not only your business, but to your patients’ wellbeing.

“Healthcare cybersecurity practices are moving in the right direction with some degree of uniformity. The findings also suggest there is room for improvement. While there is positive progress, budgets allocated to cybersecurity are still quite small. The lack of knowledgeable cybersecurity personnel also continues to hinder progress. Legacy systems, too, present a problem in need of novel solutions.”

- 2019 HIMSS Cybersecurity Survey

“Cybersecurity in healthcare is not a fix-it-and-forget-it proposition. It’s a 24/7 issue that will need to be visited regularly to provide that the defenses are as state-of-the-art as the attacks.”

- Maria Lensing, VP of Healthcare Solution at AT&T Business

“Cybercriminals are always evolving and changing their TTPs (tactics, techniques, and procedures) to avoid detection and take advantage of a bigger return on their investment, or simply take the path of least resistance. That’s why organizations need to stay on top of the threat intelligence that’s feeding their security controls, continuously updating it with new information as well as internal and external feedback. This will provide for resiliency in threat detection even as cybercriminals change their approach.”

- Jaime Blasco, Vice President and Chief Scientist AT&T Cybersecurity
While most organizations have a governance, risk, and compliance (GRC) committee in place, less than 50% of organizations have a board-level committee overseeing their cybersecurity program.

10 steps toward protecting the healthcare environment

Here we outline the steps healthcare professionals need to take as they move to bolster their cybersecurity. These are recommended course-of-actions from the AT&T Cybersecurity team specific to healthcare organizations.

1. **Conduct a holistic third-party audit.** First, understand the system you’re protecting, and expose its vulnerabilities. This requires an independently drawn picture of your security state, including devices, permissions, network architecture and security practices. This is required for HIPAA compliance.

2. **Monitor your critical assets.** As one health system CEO has put it, hospitals are basically information systems. Every intelligent device will eventually become connected, so you must be able to continuously monitor your network and cloud environments to quickly identify attacks, control data flow, and mitigate and control disruptions.

3. **Protect your endpoints.** From phones to laptops to desktops to connected medical devices, everything must be included in a defense plan.

4. **Structure and segregate your data access.** Implement robust encryption and authentication technology and protocols, and isolate medical devices, which may use outdated OS or security technology.
5. **Watch for anomalous activities.** Is a doctor—at the hospital yesterday—trying to access data from Russia today? It may not be the doctor.

6. **Analyze inbound and outbound traffic.** Data can identify and stop attacks whose fingerprints have been identified elsewhere. A global analytics model helps find threats that are directed toward, or even coming from, your hospital.

7. **Test the system regularly for vulnerabilities.** This includes mock phishing exercises, penetration testing, social engineering, vulnerability scanning, etc.

8. **Train your people.** A strong security culture starts at the top. Security awareness training must be systematic and relevant. Make it a repeating fact of work life.

9. **Know what threats exist.** While some cyber threats are ubiquitous, others specifically target healthcare organizations. Keep a vigilant watch on the global threat landscape as threats evolve and new threats emerge.

10. **Create your breach response plan.** Your network will be—or has been—breached. Actions taken after identifying the breach determine and limit the extent of the harm.
How AT&T can help you

AT&T Cybersecurity helps healthcare organizations to accelerate and simplify cyber risk and compliance management with solutions combining edge-to-edge security technologies, the deep security expertise of our SOC analysts and cybersecurity consultants, and the unrivaled visibility and threat intelligence of AT&T Alien Labs. Through this unified approach, we help healthcare organizations to achieve “security without the seams” by addressing the vulnerabilities that exist where people, processes, and technology meet.

AT&T Cybersecurity provides tailored solutions for healthcare organizations that can help them to:

- Assess their risk posture and develop strategies to improve it
- Regularly penetration test their environments and scan for vulnerabilities
- Increase security awareness of their employees and simulate phishing attacks
- Protect against DDoS attacks
- Continuously monitor and detect threats against networks and endpoints
- Respond to identified threats and security breaches in a timely, efficient manner
- Address HIPAA and other regulatory compliance requirements

Find out more about AT&T Cybersecurity
AT&T Cybersecurity sits in a unique position as a network provider:

- **274 petabytes**: amount of traffic traversing our network everyday
- **200**: countries and territories covered by the AT&T network
- **100 billion**: number of potential probes for vulnerability AT&T sees everyday
Are you confident in your cybersecurity?

Many executive leaders think they are. But, a recent cross-industry study from AT&T shows a vast disconnect between how C-level executives feel about their security and the feeling of concern their trained IT security staffs have. This disconnect often leads to many of the vulnerabilities found in the healthcare industry today.

To find out just how vulnerable your organization may be and see which questions you need to ask your IT gatekeepers for an effective self-assessment, click here.

Take our free cybersecurity assessment

© 2019 AT&T Intellectual Property. AT&T, Globe logo, and DIRECTV and registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change. | 14674-101119