Deloitte.

LIFE SCIENCES & HEALTH CARE INDUSTRY
FEBRUARY 2023

Not if, but when
Navigating ransomware attacks in the health care sector

Contents

The global health care industry has seen a dramatic increase in ransomware attacks in recent years.

In 2022, healthcare facilities in the United States experienced an average of 1,410 cyber attacks per week—an 86% increase compared to 2021.[1] In Canada, meanwhile, half of the country's ransomware victims were businesses in critical sectors like health care.[2] Similarly, cyberattacks on European hospitals and health care networks rose by 47%[3] in 2020.

A key driver of this increase is the economy of cybercrime. It is a lucrative business, generating more than $1.5 trillion in revenue each year.

This leads to an incredible profit considering the approximate average cost of access to a potential target is only somewhere between $400 and $0.0004.[4]

Nearly half of ransomware attacks also result in a data breach,[5] making the following two incentives cybercriminals' top choices: personal data sales, which net approximately $160 billion per year, and ransoms from ransomware, which bring in about $1 billion annually.[6]

These are two areas where the health care industry is particularly vulnerable—hospital and health care networks.

They are chock full of valuable data, it ranges from patients' sensitive personal identifiable information (PII), prescription information, and health insurance information to internal employee records, financial records, and intellectual property — much of this data has a long shelf life, making it easy to sell and leverage for additional crimes like identity theft, extortion, or fraud.

To complicate matters, the recent global pandemic introduced new attack opportunities for cybercriminals. The industry's swift pivot to a virtual environment has exposed critical deficiencies in cybersecurity controls, especially for valuable information that remains housed on complex IT environments usually consisting of outdated and customized systems and platforms not built for this level of connectedness. Add understaffed security teams and slim cyber budgets, and it becomes clear why the health care sector is now on the cybercriminals' radars.

Unfortunately, this means a breach is almost inevitable. Fortunately, though, there are things you can do to make your organization a less appealing target and contain the damage when an attack occurs. The key is to meet today's sophisticated cyber threat actors with an effective cyber defense and the ability to confidently recover from an attack.

In this article, we explore ways to do this so organizations can keep pace in the rapidly evolving cybersecurity landscape.

Develop a defense strategy

Most organizations recognize that cyber adversaries are not individual hackers anymore but highly organized cyber gangs, state-sponsored actors, and sophisticated crime rings.

Although their attacks can take various forms and come from various places, their primary goal is typically the same: to cause as much damage to the target as possible so that the compromised organizations will pay their ransom.

With money and resources behind them, these groups achieve this goal in multiple ways. One of the typical attack patterns for the health care industry is using insiders to access the organizational networks from within—recruiting internal employees or contractors and rewarding them for acting as inside agents on their behalf. Others might breach organizational systems through third-party attacks specifically aiming at basic web applications.[7]

No matter how the cybercriminals enter a health care organization's system, in 93% of cases,[8] once the perimeter is breached, further access to local network resources becomes usually much easier.

From there, they can shut down critical systems, block access to critical information and data, or even hack connected potentially lifesaving or life sustaining medical devices—and demand a ransom to unlock them.

Beyond breaching data privacy, these attacks can have other devastating consequences—leading to potential longer hospital stays, delays in procedures and tests, and even patient mortality.[9]

To deter these perimeter breaches, health care organizations should aim to enhance their cyber defense to make it more painful and costly for threat actors to attack. Ideally, this will involve focusing on five key areas: deterring perimeter breaches (see page 04).

Deterring perimeter breaches

Boost user awareness
Users are commonly an organization’s first line of defense. Through targeted cyber training and awareness, and continuous user group performance monitoring, you can make it substantially more difficult for hackers to penetrate your perimeter.

Reduce the technical attack surface
Hackers prefer to hit organizations where they’re most vulnerable. This makes it crucial to reduce your attack surface through active vulnerability management, patching and hardening of systems, and end-user security (e.g., browser isolation).

Improve the detection rate
Because the cyber landscape is constantly evolving, you need to constantly monitor your environment so you can detect unusual behavior or signs of attacks— such as suspicious file activities on storage devices.

Limit lateral movement
If a hacker does access your systems, you want to prevent any potential compromise from spreading. By employing Zero Trust principles, like identity and privileged access management, and network segmentation, you can limit attackers’ ability to laterally move within the network.

Isolate and contain
The faster you can isolate affected systems, the quicker you can contain any associated damage. One way to facilitate this is by proactively building compartmentalization features into infrastructure design.

> “To deter perimeter breaches, health care organizations should aim to enhance their cyber defense to make it more painful and costly for threat actors to attack.”

Be resilient and sustain critical operations

While a strong defense strategy is a key element of cybersecurity, your organization's ability to respond to a breach is equally important.

Short reaction times and the ability to start immediately responding to a ransomware attack significantly improve the organizational resilience, reduce the risk of being blackmailed, and might, in extreme cases, even save lives.

This means developing response and recovery capabilities and preparing your response teams to already know what to do before a breach occurs.

Developing response and recovery capabilities

Get your organization ready and aligned
For your organization to run like a well-oiled machine in the event of a breach, it is helpful to set up cross-functional crisis and response teams ahead of time—and practice facilitating an enterprise-wide recovery through drills, exercises, stress-testing, and post-mortems of previous incidents.

Plan the recovery
Technical and non-technical plans and playbooks allow your organization to move through each stage of recovery and determine which operations should be prioritized according to business criticality.

Having an end-to-end understanding of the entire value chain is indispensable when determining recovery priorities and sequences.

Have recovery tools ready
Before you can rebuild a compromised infrastructure, the right tools and materials must be in place. This may include immutable copies of data, isolated recovery environments, and recovery orchestration and automation—all of which can significantly speed up recovery.

Manage burst capacity
To effectively respond to an ongoing attack, you need the ability to allocate resources where they are scarce and guide those that are excessive.

This includes all types of resources, from physical resources to third party provisions.

Communicate effectively
During a breach, your organization needs clear communication channels and processes—and the ability to remain transparent throughout the entire response and continuously remind people to remain calm and in control. A strong communication plan, addressing both internal and external communication needs, can help coordinate the recovery in a composed and focused way.

This is particularly important for health care organizations— you may need to communicate with patients and authorities given the sensitive nature and volume of the data breached.

Recover with confidence

As the cyber threat landscape continues to evolve, health care organizations must adapt in stride.

This means moving beyond detecting cyberattacks and protecting critical assets to honing the resilience to recover in the event of a breach.

In some cases, this may involve repairing damaged systems and data assets. In others, it may mean putting plans into place to maintain operations in the event of prolonged outages.

Either way, it requires health care organizations to lay a foundation that will safeguard their patients by keeping critical systems up and running.

This task only gets harder as the threat landscape shifts. This makes advanced preparation even more imperative.

By identifying your mission-critical services, understanding the interplay between your various systems, engaging in ongoing training, and continually refining your recovery maturity, you can go a long way towards thwarting attacks increasingly aimed your way.

Connect with us

Endnotes

[1] *https://www.securitymagazine.com/articles/98810-global-cyberattacks-increased-38-in-2022*

[2] *https://globalnews.ca/news/8427930/canadian-health-energy-sectors-increasingly-targeted-by-ransomware-attacks/*

[3] *https://www.balcanicaucaso.org/eng/Areas/Europe/Cyber-attacks-are-growing-in-the-European-Union-21652*

[4] *https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf*

[5] *https://www.kroll.com/en/insights/publications/cyber/ransomware-attack-constitute-data-breach*

[6] *https://www.techrepublic.com/article/cybercriminals-raking-in-1-5-trillion-every-year/*

[7] *https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf*

[8] *https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=70ea31106b61*

[9] *https://www.ibm.com/thought-leadership/institute-business-value/report/medical-device-security*

Kishwar Chishty
Partner – Global LSHC Industry Cyber
Leader – Deloitte Switzerland
Life Sciences Risk Advisory

kchishty@deloitte.ch

Florian Widmer
Partner – Deloitte Switzerland
Cyber and Strategic Risk

fwwidmer@deloitte.ch

John Lu
Principal – Deloitte & Touche LLP
Cyber and Strategic Risk

jolu@deloitte.com

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the "Deloitte organization") serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 330,000 people make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.