Infosys® | Knowledge Institute

BEING RESILIENT

OVERCOMING HEALTHCARE'S CYBERSECURITY CHALLENGE

Infosys®
Navigate your next

BEING RESILIENT. THAT'S LIVE ENTERPRISE.

Cyberattacks in the health and life sciences sectors have surged in the aftermath of the coronavirus pandemic and imposed lockdowns. Some leading cybercrime gangs promised to stop their attacks on health care institutions until COVID-19 is under control.[1] But many hackers are taking advantage of the crisis.

The number of attacks associated with the coronavirus have significantly increased since mid-February. From January to March 2020 there were 907,000 total COVID-19 spam messages and there was a 350% increase in phishing sites. (See Figure 1.)

Figure 1. January to March 2020 cyberthreat trends

907K total COVID-19 spam messages	**220%** increase in spam from February to March 2020
48K hits on malicious URLs	**260%** increase in malicious URLs from February to March 2020
737 detected malware related to COVID-19	**148%** increase in ransomware attacks
522K active phishing sites as of March 2020	**350%** increase in phishing sites from January to March 2020

Source: Infosys

Recently, the U.K.'s National Cyber Security Centre (NCSC) and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) warned health care organizations involved in coronavirus response. They urged organizations in these sectors to improve cybersecurity and to ask staff to change their passwords.[2]

In April 2020, criminals targeted the World Health Organization; Within one week, hackers leaked online more than 450 active email addresses and passwords that belonged to WHO employees, who worked on the coronavirus response.[4]

The health care industry has always been an attractive sector for criminals, for a number of reasons. Hospitals and clinics have low levels of automation for information support and security. Often the available equipment is heterogeneous and is based on outdated software. Additional threats are associated with digital transformation, remote data access, trust deficit, and lack of training in online risks.

Spiraling cost of health care

Health care costs in the U.S. are increasing at a faster rate than the U.S. economy is growing annually. Employers in the segment are struggling to compete in the global market as employee costs continue to escalate. The presence of many intermediaries in the Rx (drug) segment results in higher costs and inadequate clinical efficacy.

Fragmented care delivery and segregation of financing from care delivery make comprehensive reforms and efficiency improvements very difficult. Payers (public and private) are trying to shed the risk of insurance by passing it on to providers and members.

The COVID-19 pandemic is expected to have far-reaching impact on the industry. It is expected to increase the percentage of telemedicine and other pandemic management areas. The home health care market itself is expected to reach US$515.6 billion by 2027, with a CAGR of 7.9%.[5]

This creates many vulnerabilities — the biggest six of which we have described below.

Risk one: Ransomware attacks

Since 2016, there have been 172 ransomware attacks on health care organizations in the U.S. These attacks have cost the U.S. health care industry more than US$157 million.[6]

Ransomware takes control over the files in an infected system and, in turn, attackers demand large sums of money. Hackers are then able to hold the hospitals at their mercy until the leadership meets their demands. Such attacks can cripple complete operations for health care facilities and services segments. Electronic medical records and documents, interconnectedness of hospital operations, and outdated information technology equipment working via the internet increase the threat surface.

> The NetWalker Ransomware Gang is currently the biggest threat to the healthcare industry

Currently, the biggest threat to the health care industry is the NetWalker Ransomware Gang.[7] The ransomware is spreading via spam emails claiming to provide information about SARS-CoV-2 and COVID-19 cases.

Given that so much medical equipment is critical to save lives, and has to always be on, any downtime on these systems can wreak havoc and threaten lives. For this reason, ransomware is often successful in extracting money from vulnerable targets.

The University Hospital of Brno was cyberattacked in March of this year. The hospital has one of the Czech Republic's biggest COVID-19 testing labs. The incident caused severe delays in surgical procedures as the hospital was forced to cancel operations and relocate new and critical patients to other hospitals.[8] While little is understood about this attack, it is suspected to be a ransomware one.

One of the biggest attacks in the health care sector occurred in 2017 when WannaCry ransomware penetrated the U.K.'s National Health Service (NHS) hospitals. The attack caused a massive disruption by canceling 19,000 appointments. It is estimated that US$115 million has been lost as a result of the attack and one-third of NHS trusts were affected.[9]

Risk two: Telemedicine and remote connectivity

Today, hospitals and clinics operate at limited capacity due to the rapid spread of the coronavirus. They accept only patients who cannot be treated at home. Patients with mild health problems are offered an online consultation. Although telemedicine has been around for more than a decade, prior to the pandemic outbreak, patients were skeptical about virtual visits to doctors. Today, people are forced to change their habits for the sake of their own safety. Even those who were previously against online consultations now have to accept them, as there are few alternatives.

"Before the virus, video appointments made up only 1% of the 340 million or so annual visits to primary care doctors and nurses in Britain's National Health Service."[10] Now the health service in the United Kingdom has told thousands of clinics to switch to

remote consultations. What makes this change striking is that prior to the coronavirus, telemedicine companies had limited access due to regulatory restrictions and a cluttered bureaucracy. Now the main barriers to the spread of telemedicine are collapsing. The regulations are loosening across the world, including in Europe, where standards for privacy and data protection are very strict.[7]

Currently, health organizations are scaling telehealth and their operations simply because they have to. But the more information technologies a company adopts, the higher its cybersecurity risk profile becomes. This creates new ways for criminals to penetrate the company's networks. It is worth noting that when the emergency is over, this trend is likely to stay.

Risk three: Sensitive data protection (PII/PHI)

Personal health information (PHI) is worth a lot of money to attackers. On the dark web, PHI can sell for as much as US$1,000.[11] Criminals can capitalize on stolen medical records via methods of extortion, medical identity theft, or tax return fraud and the opening of new lines of credit.

In February 2020, a phishing campaign targeted employee accounts of a California health care network. It is possible that around 200,000 current and former patients were affected in this attack as their personally identifiable information (PII) might have been exposed.[12]

In January 2020, the health care records of nearly 50,000 patients may have been compromised due to the unauthorized access to two employees' email accounts of a Minnesotan hospital.[13]

A Federal Bureau of Investigation report[14] states that each electronic health record can sell for US$50 on the black market, as compared to US$1 for a stolen Social Security number or credit card number. Over the past 10 years, more and more data breaches are being reported. With the increase in digital adoption across the health care and life sciences domains, the collection and storage of patient health care records has also increased. This makes data protection challenging.

Risk four: Insider threats

Human errors and equipment misuse happen more often than hacking. The IBM Security Cost of Insider Threat report found that the top causes of insider threats are negligence (63%), credential theft (23%), and criminal insiders (14%). More than 50% of reported incidents were caused by negligent employees or contractors. The overall cost of negligence is US$11,450,000, while the cost of credential theft remediation is US$871,686.[15]

The 2019 Verizon Data Breach Investigations report[16] lists insiders as the most common threat actors in the health care industry. Insiders have security access, organizational trust, and knowledge of procedures.

Insider "actors" can come in a variety of forms. They can be employees who become victims of phishing that can compromise the network or those who lose a work device that contains confidential information. An inside threat can even simply be caused by vulnerabilities from misconfigured servers, such as in the 2019 University of Washington Medicine breach. The breach had data of 974,000 patients exposed for three weeks.[17]

Of course, insiders can also be those who intentionally give away access and sell someone's PII/PHI for profit.

In 2016, the Jackson Health System hospital in the U.S. terminated the employment of the hospital unit secretary who was suspected of stealing confidential patient information over several years. Some 24,000 patient records with Social Security numbers, names, birthdates, and home addresses were compromised.[18]

Risk five: Confidential research and development (R&D) data and formulas in the pharmaceutical industry

Research labs produce intellectual property. Health care organizations that invest in R&D can face significant money loss due to a breach. A recent study in the JAMA Network found that an average cost of bringing a new drug to market is nearly US$1 billion, while the average time for the product to reach market is nine years.[19] Stolen high-value information such as drug formulas, patents, and R&D data can bring a massive benefit to competitors. It can save the competitors the time and money that they would otherwise spend on research. This makes R&D information very valuable and profitable for both stakeholders and cybercriminals.

> In May 2020, the FBI (U.S.) and the National Cyber Security Centre (U.K.) announced that pharmaceutical and academic institutions involved in COVID-19 vaccine research were at an increased risk of cyber attacks

This threat is even more salient during the battle against COVID-19. In May 2020, the FBI,[20] which is in the U.S., and the National Cyber Security Centre,[21] which is in the U.K., both announced that cyber hackers were targeting pharmaceutical and academic institutions involved in researching vaccines for the disease.

Risk six: Health care apps and connected devices

The 2019 Verizon Mobile Security report states that 25% of health care organizations had mobile security incidents. The mobile health care app market is growing rapidly. The Google Play and Apple App stores both offer thousands of apps available for download. Some of these apps are convenient but also lack the protection of sensitive data transmission.

Fitbit, Apple Watch, and other fitness devices collect personal data that get stored in public and private clouds. The health apps collect personal data from individuals at a much greater volume. Because people place too much trust in these apps, they rarely find out which companies are collecting their data and where their data is stored. If security isn't built into the app during the software development process, cybercriminals can breach a health care organization through a mobile device. This is an issue because there is no firm governance and/or no threat protection mechanisms established. Also, medical devices are found to be five times more vulnerable to URGENT/11[22] vulnerabilities than normal devices.

> Medical devices are 5x more prone to URGET/11 vulnerabilities compared to regular devices

Secure before it is too late

To cope with the coronavirus, hospitals are undergoing an accelerated digital transformation. And digitalization inevitably brings new security challenges. Medical institutions have critical infrastructure that is vital for the public well-being. Their databases and research facilities hold high-value assets. As these assets become digital, hackers see an opportunity to profit. Unfortunately, health care companies usually operate on a very low margin. On average, only 5% of a health care IT budget is allocated to cybersecurity.[23] In most cases, companies start to think about security only when an incident has already occurred.

It is critical that people can trust health care providers with their data. To ensure this trust, organizations need to secure and protect the information that they have. To be resilient to cyberthreats, health care and life sciences businesses need to build a highly adaptive security ecosystem. To do that, they need to focus on the following recommendations.

Enforce IT hygiene

IT hygiene should be implemented and maintained across all IT and medical devices that are connected to the network. Often IT hygiene requirements can be stringent, which can impede business processes. To balance the requirements with business needs, it is important to make IT hygiene requirements flexible.

To enforce IT hygiene, businesses need to ensure security monitoring and logging along with real-time threat intelligence that provides context-specific information to security analysts.

Vulnerabilities can appear in different elements of the IT stack — in servers, the database, the network, the endpoints, etc. The technology original equipment manufacturers (OEMs), such as Microsoft, Cisco, and Oracle, release software patches that help remediate the vulnerabilities. As most breaches try to exploit known vulnerabilities, it is extremely important that businesses apply software patches to close those vulnerabilities.

Recommendation No. 1: Golden templates and hardening guidelines

Adhere to prescribed gold standards for operating systems and hardening guidelines across the organization.

Up-to-date operating system (OS) and patches. Ensure that all systems are patched with the latest security patches and create a process for security updates.

Replace outdated medical devices and implement IoT security practices for remote connected devices.

Hardening guidelines. Internet-facing and high-risk systems should be hardened as per industry best practices.

Older legacy application. Compensating controls should be implemented for systems with an outdated OS that cannot be upgraded.

Recommendation No. 2: Zero Trust model

Augment existing systems using Zero Trust principles as part of normal development cycles. Zero Trust principles can be adopted at the organization level to guide the evolution of security architecture. These principles will help to design and build strong multidimensional and comprehensive security parameters.

Network segmentation for separating mission-critical systems (such as life support systems) from other systems will help in preventing lateral spreading of malware or attacker access.

Provide only **"least privileged access"** to get the job done. This will help in reducing the threat surface.

Implement 100% **multifactor authentication** to prevent unauthorized access.

Use **secure web gateways for remote access** instead of traditional VPNs.

Expose only required applications for remote access instead of connecting remote users to corporate network.

Address new threat surface

Businesses need to build defense mechanisms based on the new threat surface, which is a result of remote working. It is also important to consider the motivations of multiple threat actors. Insiders, competitors, and nation-states are all driven by different motivations. While some criminals want to capitalize on PHI data, state-sponsored attacks can target labs to get coronavirus vaccine information.

To protect against the current threats, health care and life sciences businesses need to secure remote access controls, disable insecure services and protocols that are not needed, and enforce endpoint controls to prevent data leakage.

Recommendation No. 3: Data security focus

To provide comprehensive data protection, use the following considerations:

Automatic classification. Implement automated systems for data identification and classification, data encryption, and data masking.

Loss monitoring. Use DLP (Data Loss Prevention) systems for email, network, and endpoints for real-time loss monitoring.

Encryption. Use industry-best encryption and data-masking solutions.

Access reviews. Conduct periodic access reviews to ensure access is available for authorized users only.

Secure by design

Cybersecurity is everyone's responsibility. Each individual is a weak link that can potentially grant criminals access to the system. Doctors, nurses, hospital staff, critical care givers, and scientists at pharma companies need to be educated about existing security risks and how to handle them. The culture of security is a continuous process and has to be driven across the entire organization.

> The culture of security is a continuous process which has to be driven across the entire organization

To create this culture, organizations need to make the "secure by design" concept a bedrock for their digital transformation. They need to embed security in every aspect of all programs across their business, applications, infrastructure, cloud, and data. It is crucial to create the end-to-end visibility of security metrics, which can be leveraged to continuously enhance security.

Recommendation No. 4: Secure by design principle

Ensure cybersecurity thinking during systems development.

It is important to establish **secure coding guidelines and embrace email security and dev-sec-ops** for all development programs.

For both cloud and on-premises environments, **continuous**

compliance monitoring and management using vulnerabilities identification and real-time patching need to happen.

Reduce the threat surface proactively by evaluating devices connected to the network and applying appropriate controls.

Focus on **managing threats, vulnerabilities, risks, and incidents** rather than focusing only on regulatory compliance.

Finally, to raise awareness, use mandatory quizzes and certifications in planned **security awareness campaigns** about social engineering attacks.

Improve compliance, governance, and risk management

To have a better visibility of cyber risks, businesses need to rethink their compliance and governance processes. To improve these processes, companies need to ensure a balance between security and privacy obligations. They need to document and lay out compliance requirements to ensure compliance with various legal regulations such as HIPAA, PHI data, and GDPR. They also need to enable easy access to tools and monitoring.

Recommendation No. 5: Compliance and risk management for vendors/ partners

To secure data and protect against attacks in an interconnected evolving digital health ecosystem, an effective partner risk management program is required.

Do a **proactive partner risk evaluation** using an industry-standard security posture assessment as well as a questionnaire-based approach.

To plan for appropriate controls and levels of access, **do a risk-based partner segmentation**. Then evaluate partner access using **Zero Trust principles.**

An integrated governance and escalation framework (with clear ownership and integrated workflows) are both required for managing the partner risks. Use customized IT **systems and governance for effective third-party risk management.**

Managed detection and response

The changing threat patterns and constantly evolving technology tools and processes demand constant focus on the improvement of a company's security posture. The cybersecurity arena needs people with different sets of skills who can deal with threat-detection technologies, access management, governance risk and compliance, and much more. And almost 90% of health care IT security leaders state that they lack the skilled cybersecurity professionals needed to achieve a better security posture.[24] But there are companies that can provide the necessary support.

Recommendation No. 6: Managed detection and response

Plan for fast detection and **quick IT recovery** to improve resiliency in case of a breach.

Use **behavior-based** anomaly detection and sandboxing for those threats, which cannot be detected using signature-based systems.

Use well-defined **playbooks** for fast detection and response.

Use AI and automation for reducing false positives and proactive threat hunting.

A managed security services organization can help health care companies with a holistic data security program. Working with such a company significantly reduces costs, increases visibility, and protects an organization against breaches.

Most important — prioritize cybersecurity

Health care is the most expensive industry when it comes to the cost of a data breach. According to the 2019 Cost of a Data Breach report, the cost of a breach in the health care industry is US$6.45 million.[25] Despite this fact, health care providers spend significantly less on cybersecurity than other regulated industries spend on the initiative. But with increasing risks due to digitalization, remote work, and telemedicine, there is no more doubt about whether cybersecurity is worth the investment. Because of this, health care providers have begun to change their attitudes toward their IT budget management. From 2017 to 2021, the health care industry will spend a cumulative US$65 billion on this.[26] Today, cybersecurity needs to be the highest priority. Health care providers need to find the right program for investment — embracing one that will be aligned with their goals and strategy.

References

1. "Ransomware Gangs to Stop Attacking Health Orgs During Pandemic," Bleeping Computer, 2020
2. "Cyber Warning Issued for Key Healthcare Organizations in UK and USA," NCSC, 2020
3. "WHO Reports Fivefold Increase in Cyber Attacks, Urges Vigilance," WHO, 2020
4. "Cyber-Crime During the COVID-19 Pandemic," UNICRI, 2020
5. "Worldwide Home Healthcare Market Analysis 2020-2027 - Global Market Forecast to Reach USD 515.6 billion by 2027," Globe News Wire, 2020
6. "172 Ransomware Attacks on US Healthcare Organizations Since 2016 (Costing Over $157 Million)," Paul Bischoff, CompariTech 2020
7. "NetWalker Ransomware Gang Targeting the Healthcare Industry," HIPAA Journal, 2020
8. "Cyberattack on Czech Hospital Forces Tech Shutdown During Coronavirus Outbreak," Sophie Porter, Healthcare IT News, 2020
9. "WannaCry Cyber Attack Cost the NHS £92m as 19,000 Appointments Cancelled," Matthew Field, The Telegraph, 2018
10. "Telemedicine Arrives in the U.K.: '10 Years of Change in One Week,'" The New York Times, Benjamin Mueller, 2020
11. "Data Breach: A Summary of Healthcare Security Incidents in March 2020. Are you a victim of Medical Identity Theft?" Alina Bziga, Security Boulevard, 2020
12. "California Healthcare Data Breach Could Impact Nearly 200,000 Patients," Adam Bannister, The Daily Swig, 2020
13. "Data Breach Affects Around 50,000 Patients at Minnesota Hospital," CISOMAG, 2020
14. "(U) Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain," FBI Cyber Division, Private Industry Notification, UNCLASSIFIED, 2014
15. "The Cost of Insider Threats 2020," IBM Security, 2020
16. "DBIR Report: Healthcare," Verizon, 2019
17. "Health Data of 974,000 UW Medicine Patients Exposed for 3 Weeks," Health IT Security, Jessica Davis, 2019
18. "Media Statement – Patient Information Breach," Press Release, Jackson Health System, 2016
19. "Estimated Research and Development Investment Needed to Bring a New Medicine to Market, 2009-2018," JAMA Network, 2020
20. "China-linked hackers are targeting US coronavirus vaccine research, FBI warns," CNBC, 2020
21. "State Hackers Target UK Unis for #COVID19 Vaccine Research," Phil Muncaster, Infosecurity Magazine, 2020
22. "URGENT/11 Cybersecurity Vulnerabilities in a Widely-Used Third-Party Software Component May Introduce Risks During Use of Certain Medical Devices: FDA Safety Communication," U.S. Food & Drug, 2019
23. "Top Cyber Security Risks In Healthcare [Updated 2020]," INFOSEC, 2020
24. "87% Health Orgs Lack Security Personnel for Effective Cyber Posture," Jessica Davis, Health IT Security, 2020
25. "Cost of a Data Breach Report highlights," IBM Security, 2019
26. "15 Cybersecurity Statistics To Diagnose The Ailing Healthcare Industry," Cybercrime Magazine, 2020

Authors

Vishal Salvi

SVP and Chief Information Security Officer, Infosys
vishal.salvi@infosys.com

Venky Ananth

SVP and Head of Healthcare, Infosys
venkateshwaran_a@infosys.com

Yulia De Bari

Consultant, Infosys Knowledge Institute
yulia.debari@infosys.com

About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision making on critical business and technology issues.
To view our research, visit Infosys Knowledge Institute at infosys.com/IKI

For more information, contact askus@infosys.com

Infosys®
Navigate your next