HERJAVEC GROUP

2021-2022 Healthcare Cybersecurity Report

HERJAVEC GROUP

Healthcare Cybersecurity Report

Q4 2021

Contents

Healthcare cybersecurity is a particularly complex and difficult task. With the ultimate goal of keeping patients safe while simultaneously protecting their critical and private data, it presents a challenging balancing act for cybersecurity professionals. Pile on the vast amount of IoT devices, intricate system of privileged access requirements and end users, regulatory compliance such as HIPAA, GDPR, and NIS and the unprecedented challenges of a world-wide pandemic and maintaining a strong cybersecurity posture can seem like an overwhelming and almost impossible undertaking.

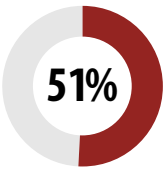
The cybersecurity paradigm shift for Healthcare

With the evolution of the cyber threat landscape, cybersecurity professionals work tirelessly to adapt and meet the challenges head on.

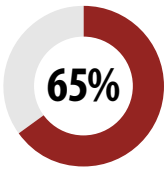
Here are the top trends for healthcare cybersecurity in 2021 and suggested guidance from Herjavec Group's cybersecurity experts.

The healthcare industry continued to be the most breached sector according to 2021 reports. The industry has seen a 51% increase in breaches and leaks since 2019. While patient privacy has always been a common concern when it comes to healthcare organization breaches, a new study has found that cyber-attacks in the industry can have devastating effects on patient safety as well. 70% of surveyed organizations reported that healthcare ransomware attacks have resulted in longer lengths of stays in hospital and delays in procedures and tests that have resulted in poor outcomes including an increase in patient mortality. 65% of respondents reported an increase in the number of patients being diverted to other facilities, and 36% reported an increase in complications from medical procedures due to ransomware attacks.

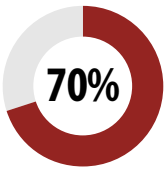
Ransomware Impacts on Patient Safety



of surveyed healthcare organizations reported an increase in breaches and leaks since 2019



reported an increase in the number of patients being diverted to other facilities



reported longer lengths of stays in hospital, delays in procedures and tests and an increase in patient mortality

Healthcare CISO's should expect:

Workflows automated to scale for security data across Healthcare locations, networks, and connected medical devices.

24/7 threat detection and security operations to meet and maintain regulatory compliance.

Constant improvement to security programming to meet industry and business demands, rather than point-in-time solutions.

Expert-level support and a vendor-agnostic, holistic approach to increase visibility and improve cybersecurity ROI.

In 2020 alone, 560 healthcare facilities in the U.S. were reported as victims of ransomware attacks in 80 different incidents.

These attacks resulted in:

- Large amounts of Protected Health Information (PHI) and other sensitive data being stolen and published
- Electronic Health Records (EHRs) being rendered temporarily inaccessible and in some cases permanently lost
- Delayed procedures, tests, and treatments

Herjavec Group predicts a continued increase in frequency and sophistication of healthcare cyber-attacks – specifically ransomware attacks – through 2022 and beyond.

Common pitfalls observed in 2021 that affect healthcare organization cybersecurity include:

- Overworked healthcare staff that are mentally and emotionally tired
- Legacy and unpatched IT systems and applications
- Understaffed IT and cybersecurity departments
- Understaffed operations
- Unsecured 3rd party partners

A recent survey found the average cost of a data breach incident was $4.24 million, the highest it has been since the creation of this study 17 years ago. **The average cost of a healthcare breach far surpassed the general average, at $9.23 million per incident** – a $2 million increase over the previous year, according to the report.

State of Ransomware Report

In 2021, ransomware attacks are not only more targeted and sophisticated but the most prolific "Double Extortion" ransomware operators have been observed holding enterprise networks hostage for sums of up to $40M USD.

Herjavec Group Threat Hunters have analyzed the most active ransomware operations in the first two fiscal quarters of 2021 and created profiles on the highest-impact ransomware families.

Learn more about the current ransomware threat landscape and the steps you can take to keep your enterprise out of the adversary's shadow.

DOWNLOAD THE REPORT

Best Practices for Healthcare Cybersecurity Teams

Visibility is Critical

With some of the most complex systems and valuable assets, securing the healthcare industry is no small feat. The best place to start is with visibility. Identifying all end users, accounts, and connected devices is key – you can't protect what you aren't aware of.

Assess Your Identity Program

A comprehensive identity program creates a strong foundation for healthcare organization cybersecurity. It allows a security team to spot truly anomalous behavior across users, devices and applications by employing robust programs in:

- Identity Governance
- Access Control (including authentication)
- Privileged Access Management.

Take a Threat-Centric Approach to Security Operations

While advancements in mobile and telehealth devices have presented exciting opportunities for reduced costs and increased healthcare quality and accessibility, it also creates a new challenge. According to the U.S. Department of Health and Human Services, the digitalization of health records, the collection, evaluation, and provisioning of patient data, and the transmission of patient data over public networks pose new privacy and security threats to patients and healthcare providers.

To address this new threat landscape, healthcare organizations should take a threat-centric approach to security and leverage services such as active threat hunting, threat modeling and added threat intelligence to enhance detection and response capabilities.

- **Threat modeling** serves as a foundation for the analysis and specification of security requirements. It identifies and prioritizes potential cybersecurity threats and vulnerabilities in systems, devices, and cybersecurity programs, providing valuable data to build informed cybersecurity strategies.

- **Active Threat Hunting** uses adversarial tactics to hunt across your endpoint tools. Human threat hunter findings support in blocking and disrupting attacks, improving detection and adding further enrichment to your threat intelligence platform.

- **Added Threat Intelligence** can combine industry leading commercial, government and open-source feeds, with outputs from your security assessments and testing engagements, to enhance security orchestration automation and response and contribute to playbook development.

> **The fundamental difference between Healthcare and other industries, is that it's not just about money. It's about lives.**
>
> **Robert Herjavec, Founder & CEO of Herjavec Group**

Focus on Cyber Resiliency

When it comes to a cyber-attack, time is of the essence. This is especially true when it comes to healthcare – it's not just the financial cost, loss of data, or even an enterprise's reputation on the line, it can come down to a person's life.

Healthcare organizations will need to make cyber resiliency a top priority to address the continued barrage of cyber-attacks we expect to see in the future. While a strong prevention strategy and program will still be essential, investing in cyber resiliency is no longer an option.

This will strengthen the organization's ability to:

- Detect anomalous and malicious activity and infections as early as possible
- Rapidly respond to breaches
- Comprehensively remediate any damage caused by an infection
- Thoroughly investigate and analyze how the threat actor was able to breach the organization's system
- Reinforce the cybersecurity posture by filling gaps and addressing vulnerabilities to ensure this type of breach doesn't happen again

Cyber resiliency tools include:

- A strong Incident Response Program including an Incident Response Preparedness Plan and Incident Response Retainer
- Integrated Managed Detection & Response
- Managed Identity & Access Management including comprehensive Privileged Access Management

Why Herjavec Group?

For over 18 years, Herjavec Group has defended global enterprises, including a diverse group of healthcare organizations, with industry-leading expertise, disciplined processes, forward-looking development, and a personalized approach to ensure mutual success. Our integrated, measurable, and threat-centric service portfolio has evolved to become the most holistic offering on the market, spanning Advisory, Professional Services, Managed Services, Identity and Access Management, Digital Forensics and Incident Response.

Leverage Herjavec Group's award-winning services offerings and roster of cybersecurity experts as an extension of your in-house team with our key differentiators:

100% CYBERSECURITY FOCUSED

We are laser-focused on security & recognized among the world's most innovative cybersecurity players.

UNBIASED, VENDOR-AGNOSTIC APPROACH

We have partnerships with best of breed providers, and are on the pulse for emerging technology trends to design & protect across any security stack.

SPEED AND AGILITY ACROSS MULTI-TECHNOLOGY, COMPLEX ENVIRONMENTS

Our cyber experts support the world's largest Healthcare and pharmaceutical environments, offering customized and flexible solutions.

COMPREHENSIVE, HOLISTIC SECURITY EXPERTISE

We offer a holistic approach to the security paradigm shift. From Advisory, Implementation, Identity, and Managed Security Services, to Digital Forensics and Incident Response Services, we strategize, deploy, respond and remediate to accelerate your cybersecurity programs.

> Once again Herjavec Group has exceeded our expectations and brought the best possible service. My phone is inundated with cybersecurity sales people selling services. From my jaded experience very, very few people deliver. Herjavec Group does.
>
> - CISO, Healthcare & HG Identity Services Customer

> When the COVID-19 Pandemic happened Herjavec Group Managed Security Services really helped us to scale and not have to send our security operations home - instead they were business as usual. Our partnership enabled my in-house team to adapt to the changing environment and allowed us to focus on monitoring and other day-to-day tasks while maintaining the security posture we had prior to the pandemic.
>
> - CISO, Healthcare Customer

MARKET LEADER IN MSS — CDM Cyber Defense Magazine Global Infosec Awards

MARKET LEADER IN IAM — CDM Cyber Defense Magazine Global Infosec Awards

SECURITY SERVICES LEADER — IDC Analyze the Future

MOST INNOVATIVE SECURITY COMPANY OF THE YEAR — CDM Cyber Defense Magazine Global Infosec Awards

5 ON THE — MSSP Alert TOP 250 MSSPs

TOP HEALTHCARE CYBERSECURITY PROVIDER — Frost & Sullivan

HERJAVEC GROUP

Robert Herjavec founded Herjavec Group in 2003 to provide cybersecurity products and services to enterprise organizations. We have been recognized as one of the world's most innovative cybersecurity operations leaders, and excel in complex, multi-technology environments. We have expertise in comprehensive security services, including Advisory Services, Technology Architecture & Implementation, Identity & Access Management, Managed Security Services, Threat Hunting & Management, Digital Forensics and Incident Response. Herjavec Group has offices and Security Operations Centers across the United States, United Kingdom, Canada and India.
For more information, visit HerjavecGroup.com or contact us at info@herjavecgroup.com.