GoSecure

USE CASE BROCHURE

HEALTHCARE

SURGING SECURITY THREATS AND THE IMPERATIVE NEED FOR ADVANCED DEFENSIVE STRATEGIES

IMPACT IN NUMBERS

$11 MILLION

The average healthcare data breach was nearly $11 million in early 2023 - an 8% jump from the previous year.

239%

There has been a 239% increase in the number of large breaches involving hacking over the last four years.

88 MILLION

In the U.S., 88 million people have been affected by data breaches of their personal health information, an increase of 60% in 2023 compared to 2022.

Your ally to consolidate, evolve & thrive

✉ INFO@GOSECURE.AI

🌐 www.GOSECURE.AI

SAFEGUARDING DATA, ENSURING TRUST

The healthcare sector is not immune to the challenges that threaten the integrity, confidentiality, and availability of critical medical data and services. With the increasing digitization of health records, the adoption of telemedicine, and the integration of Internet of Things (IoT) devices in patient care, the sector has become a prime target for cybercriminals.

Cyberattacks, such as ransomware, phishing, and data breaches, have grown in frequency and sophistication, putting sensitive patient information and essential healthcare operations at risk.

Moreover, healthcare organizations are under immense pressure to comply with stringent regulations like HIPAA, which mandate the protection of patient data and the implementation of robust cybersecurity measures. Failure to comply can result in irreparable damage to an organization's reputation.

In this context, implementing a strong cybersecurity plan is no longer optional but mandatory. It is essential for safeguarding patient information, ensuring uninterrupted healthcare services, and maintaining the trust and confidence of patients.

HAZARDS OF A WEAK CYBERSECURITY PLAN

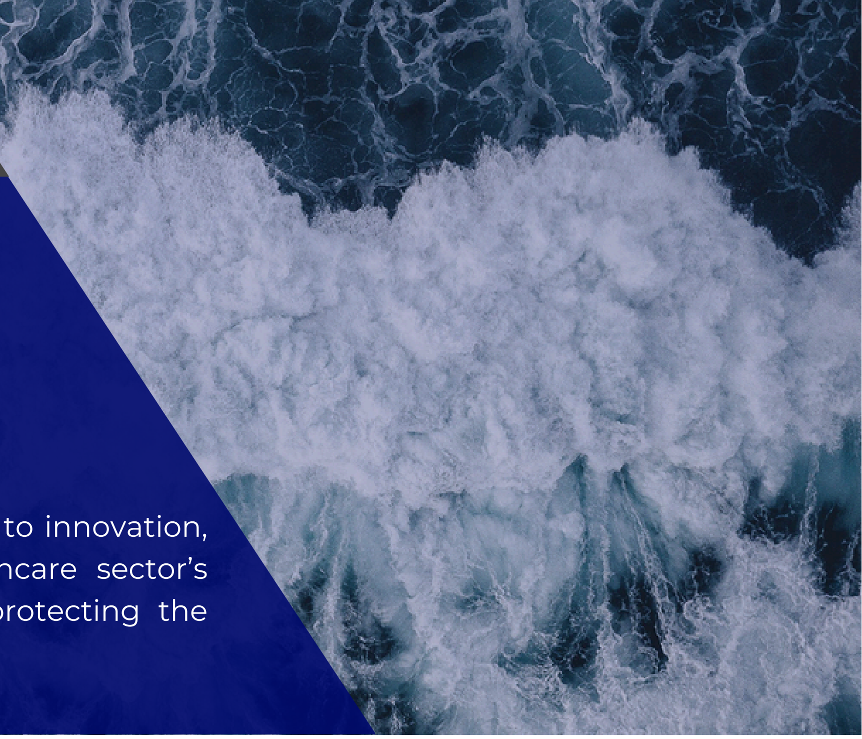
- OPERATIONAL DISRUPTION
- DATA BREACHES
- FINANCIAL LOSS
- SAFETY RISKS
- REGULATORY CONSEQUENCES
- LOSS OF PUBLIC TRUST
- IMPACT ON PATIENT SAFETY
- INTELLECTUAL PROPERTY THEFT

Worse yet, users with elevated privileges could inadvertently give attackers the "keys to the kingdom".

GOSECURE

PROTECTING PATIENTS WITH GOSECURE

Through tailored solutions, a commitment to innovation, and a deep understanding of the healthcare sector's challenges, GoSecure leads the way in protecting the industry against cyber threats.



CHALLENGES

GOSECURE'S RESPONSE

SENSITIVE DATA PROTECTION

Healthcare organizations handle vast amounts of sensitive patient data, including personal health information (PHI), which is highly valuable on the black market. Protecting this data from breaches and unauthorized access is a significant challenge.

GoSecure implements robust encryption, secure access controls, and data loss prevention (DLP) technologies to protect sensitive patient data. We ensure that PHI is stored and transmitted securely, minimizing the risk of unauthorized access.

INTEGRATION OF IOT AND MEDICAL DEVICES

The increasing use of IoT devices and connected medical equipment introduces additional vulnerabilities. These devices often lack strong security features and can be exploited by attackers to gain access to healthcare networks.

We secure IoT devices and medical equipment through network segmentation, continuous monitoring, and implementing security protocols specifically designed for IoT environments, reducing vulnerabilities in connected devices.

LEGACY SYSTEMS

Many healthcare facilities rely on outdated systems and software that may lack modern security features. These legacy systems are often more vulnerable to cyberattacks and are harder to secure.

GoSecure's solutions are designed with modern architecture compatible with legacy systems, facilitating seamless integration while bolstering security postures.

REGULATORY COMPLIANCE

The healthcare sector is subject to stringent regulations, such as HIPAA in the United States, which require robust data protection measures. Ensuring compliance with these regulations can be complex and resource-intensive.

GoSecure help healthcare organizations comply with regulations like HIPAA by conducting compliance audits, providing documentation and reporting tools, and offering guidance on best practices for regulatory adherence.

✉ INFO@GOSECURE.AI

🌐 WWW.GOSECURE.AI

Your ally to consolidate, evolve & thrive

GoSecure

Know Your Risk to Mitigate Your Risk

Counting on the confidence of premier healthcare institutions throughout North America, including key medical providers, underscores GoSecure's outstanding reputation for excellence in protecting the healthcare sector.

YOUR SAFETY IS OUR TOP PRIORITY

GoSecure stands as the premier cybersecurity ally for the healthcare sector, leveraging over two decades of expertise in safeguarding vital institutions nationwide. Trusted by industry leaders, our unrivaled experience and global footprint make us the foremost choice for cybersecurity solutions.

Drawing on our profound comprehension of the healthcare sector's challenges, our Penetration Testing Services offer comprehensive solutions tailored to healthcare providers. Our adept team conducts meticulous assessments to unearth potential vulnerabilities, preempting threats before they can jeopardize critical operations or patient data. This commitment establishes GoSecure as a trusted leader in healthcare cybersecurity.

With tailored services, an expert team, and unwavering dedication to compliance, we not only address the unique security needs of healthcare organizations but also bolster their overall cybersecurity posture.

Allying with GoSecure empowers healthcare institutions to navigate the complexities of the surging threat environment with confidence, ensuring the integrity of their operations, protecting sensitive data, and upholding trust in patient care for years to come.

CONTACT US NOW

DESIGNED TO IDENTIFY VULNERABILITIES IN YOUR ECOSYSTEM

PHISHING TESTING

- We simulate real-world phishing attacks to identify vulnerabilities in employee awareness and email security measures. Our actionable recommendations help strengthen defenses and protect sensitive patient data.

INTERNAL NETWORK

- Thorough assessments of internal networks, identifying vulnerabilities and crafting tailored solutions for optimal protection of critical infrastructure and data.

EXTERNAL NETWORK

- Identifies potential entry points, and provides ongoing monitoring and threat intelligence to enhance security and safeguard critical assets from external threats.

WEB APPLICATION TESTING

- We conduct simulated attacks on web applications to uncover vulnerabilities. Our actionable recommendations fortify defenses and safeguard sensitive data.