CyberSaint SECURITY

State of Ransomware Attacks In Healthcare Report

CyberSaint Report 2022

Introduction

Malicious actors use ransomware to attack large enterprises, government organizations, and SMBs. The healthcare industry is one of the hardest-hit critical infrastructure sectors. Cybercriminals had capitalized on the sector's generally weak and dated cybersecurity stance. They ramped up the volume of attacks during the COVID-19 pandemic when healthcare systems were already crumbling under pressure and scrutiny. Phishing scams, DDoS attacks, and data breaches plague the healthcare sector. Business email scams have increased by 1,500% since 2015.

It's widely acknowledged that healthcare systems lag behind in developing mature cybersecurity programs. And while ransomware rapidly evolves and becomes increasingly complex and sophisticated - healthcare organizations are still struggling to catch up. Legislation like HIPAA and HITECH ensure patient information protection but fail to mandate critical security practices or mandate compliance.

With a shortage of healthcare workers and overwhelmed hospital systems, hackers were able to hide amongst the chaos and deploy attacks while the pandemic diverted attention away. When the pandemic first took hold in 2020, cybercriminals attempted an estimated 230.4 million ransomware attacks. Over 500 healthcare organizations experienced a ransomware event. Ransomware is the most prominent cyber risk to the industry. It can spread through networks and third-party partners and extort some of the largest organizations in the country. Each attack put lives on the line as malware paralyzed system networks, disabled emergency services, and confiscated patients' protected health information (PHI) and financial information.

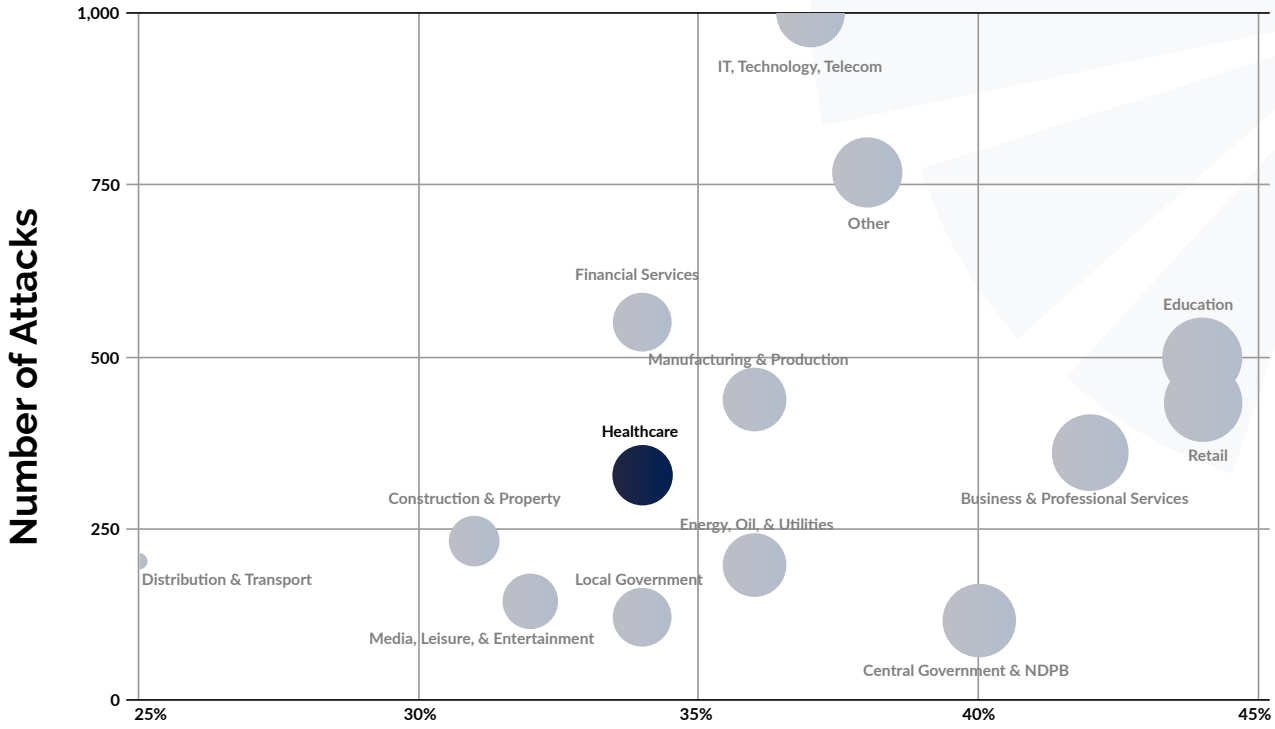
Malicious actors specifically target healthcare organizations with ransomware because of the sector's propensity to payout. Over a third of healthcare organizations reported that they were likely to pay out a ransom, even if there is no guarantee that organizations will recover the data. Unlike other infrastructure sectors, hospital systems and outpatient facilities do not have the leverage to bargain with cyber criminals or the propensity to wait for help. It is difficult for organizations to pause operations, restore their systems through a backup, and wait to resume business - patient care is their priority. In response to the onslaught of attacks, the FBI, the Cybersecurity and Infrastructure Security Agency (CISA), and the Department of Health and Human Services (DHHS) coauthored a cybersecurity ransomware advisory that provided organizations with best practices and threat information.

The healthcare sector is also highly dependent on other critical infrastructure sectors like emergency services, IT, and communications. Healthcare systems become an even larger glaring target for hackers with a highly valuable supply chain.

Ransomware Attacks in Healthcare

When Universal Health Services (UHS) experienced a ransomware attack in September 2020, operations were down for eight days. This single attack cost the company $67 million, and the patient risk grew each day that services were down. The attack forced frontline workers to run operations on pen and paper for EHR systems. Following the UHS attack, the University of Vermont (UVM) Health Network experienced a ransomware attack that rendered networks unusable for 40 days. Health facilities in Vermont and northern New York could not provide adequate care to patients or ensure that PHI was safe for over a month.

Amount of Ransomware Attacks by Industry



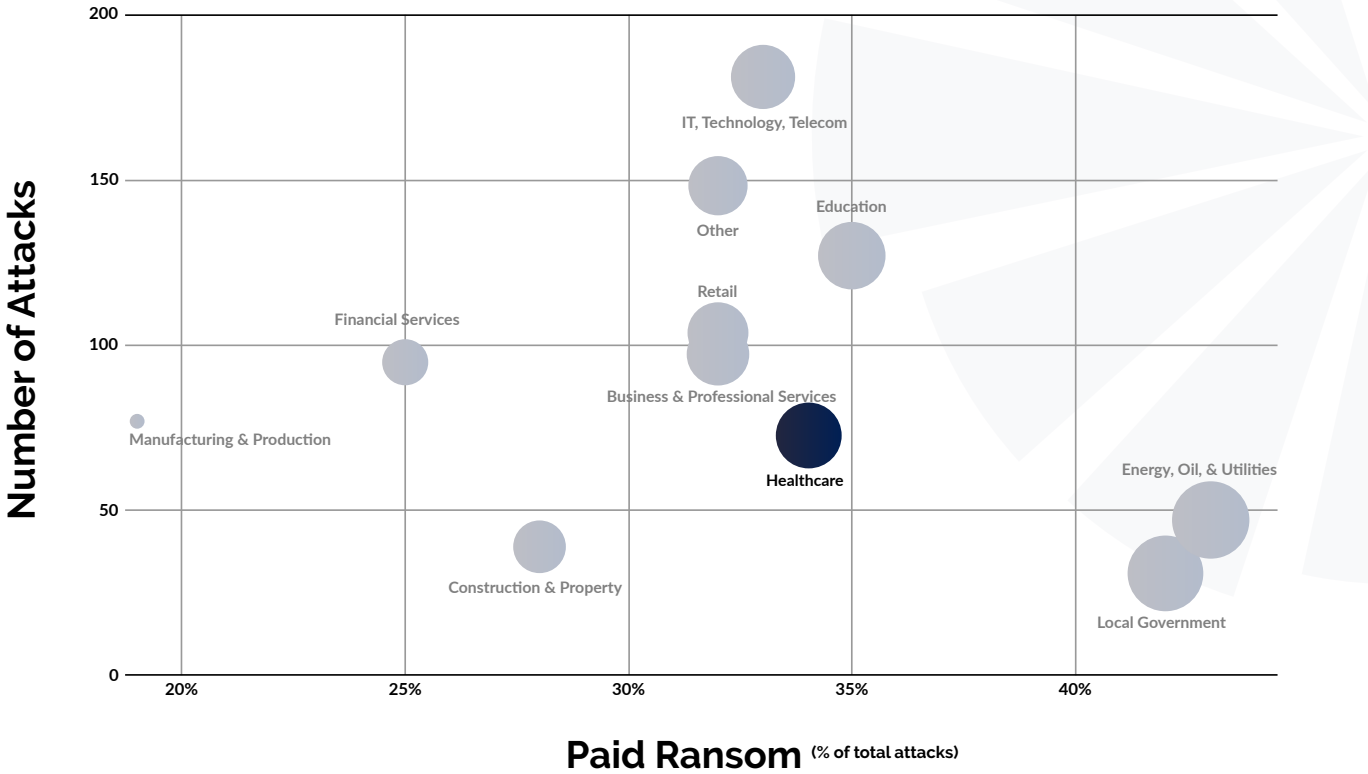
The unexpected onset of the pandemic led to last-minute remote setups for telemedicine and increased usage of medical devices.

A healthcare ransomware attack invites the risk of wiped patient history, appointment cancellations, and augmented prescriptions. The unexpected onset of the pandemic led to last-minute remote setups for telemedicine and increased usage of medical devices.

Insulin infusion pumps, smart pens, and implantable cardiac devices are potential avenues of entry that hackers can manipulate. Malicious actors need one IoT device to hack to access a healthcare network. Conversely, a compromised network puts medical devices at the disposal of hackers to increase or decrease medical dosages. The rapid pace of implementation meant that many devices and networks were not patched securely and were unguarded points of entry for cybercriminals.

New medical or IoT devices are rolled out faster than security officials can detect potential vulnerabilities. The surface area for attacks has grown alongside the growth of ransomware-as-a-service (RaaS) and malware kits. While healthcare organizations may never fully mitigate ransomware threats, many steps can be taken to improve prevention, remediation, and recovery. The first is acknowledging and accepting that cybersecurity risk is paramount to business operations, and executive leaders need to allocate resources for cybersecurity.

Propensity to Pay Ransom by Industry

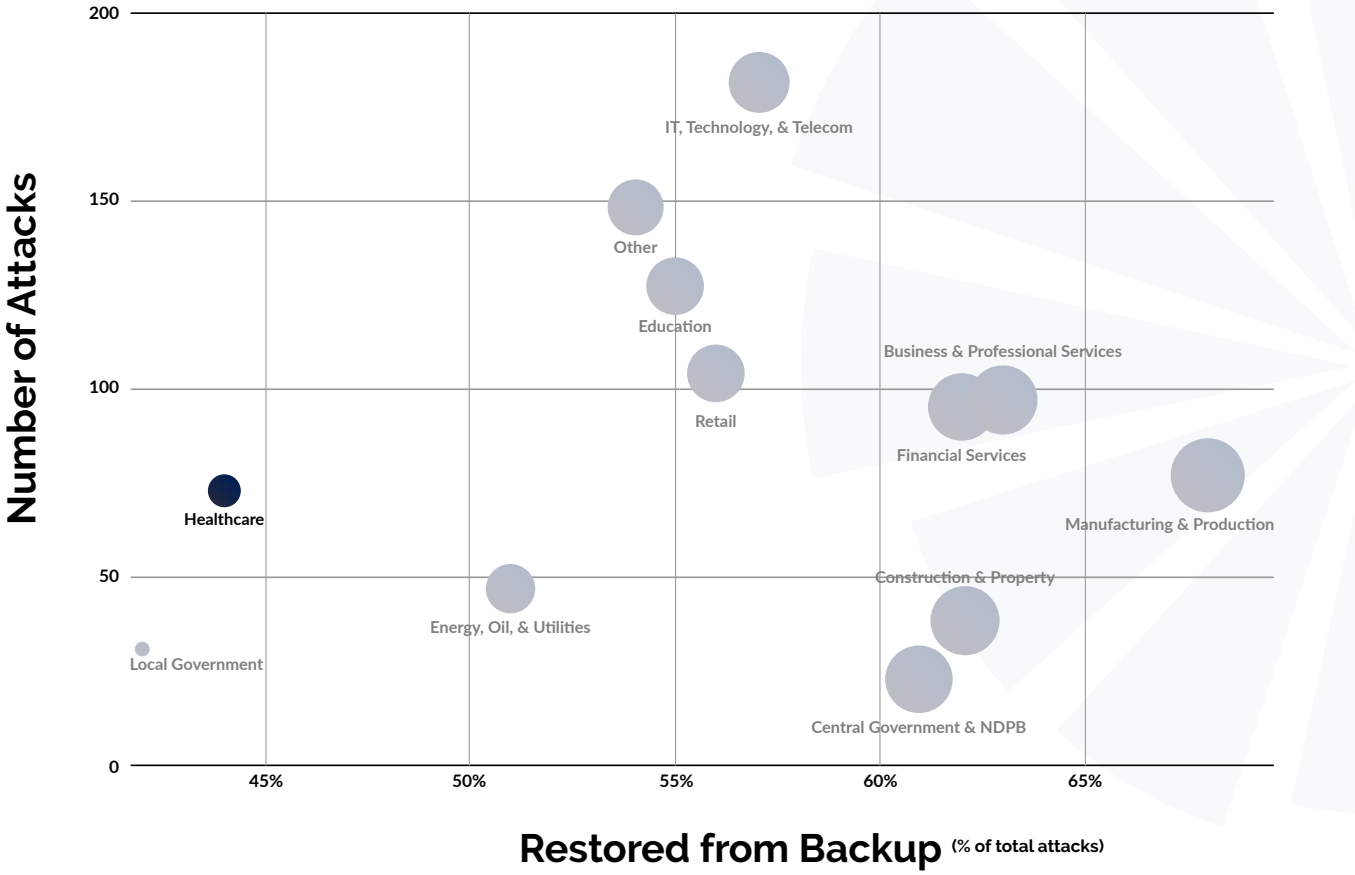


For most healthcare organizations, leaders combine cybersecurity with IT operations. A poll on IT budgets found that about a quarter of respondents stated that leaders dedicated three to six percent of their IT budget to cybersecurity. It can be challenging for CISOs to propose more allocation when budgets are already run thin, and health facilities are overwhelmed.

According to a survey conducted by the Healthcare Information and Management Systems Society (HIMSS), healthcare organizations will have to increase their cybersecurity spending by 24%. Still, only 40% of respondents said their organization would make the necessary financial investments. CISOs need to generate interest in cyber investment at the board level. Security teams need to collaborate with executive leadership and contextualize cybersecurity as a business's core functioning.

Developing dedicated resources and a team for cybersecurity in healthcare organizations is a must. Ransomware threats will continue to evolve and grow in scope, and facilities need security programs to prevent threats from growing into full-scale attacks. Along with investment and interest in cybersecurity, leaders need to establish a risk management solution that monitors security posture and complies with significant frameworks like the NIST Cybersecurity Framework (CSF) Profile for Ransomware Risk Management.

Ability to Restore Data Using Backups Following Attack



Data presented as a function of total ransomware attacks in represented industries against percentage of companies able to restore data from backup. Relative size of bubbles in charts representative of percentage of companies able to restore from backup (bigger bubble, greater ability to restore from backup).

How Can the Healthcare Industry Level Up Against Ransomware

The NIST Ransomware Profile sets the stage for advancing an organization's cybersecurity program. The framework provides comprehensive guidelines for organizations to identify critical security objectives, assets, and controls. Health systems can reduce their overall risk of ransomware events by complying with the NIST CSF Profile for Ransomware Risk Management.

By adopting this standard, healthcare systems can gauge their level of preparedness and understand gaps in their strategy. Healthcare companies do not need to worry about requirement overlap as the NIST Ransomware guidelines work in conjunction with HIPAA security requirements. The NIST Ransomware Profile builds on the five essential NIST CSF functions: identify, protect, detect, respond, and recover. The first three functions are key for prevention measures. Prevention is crucial for healthcare systems as they do not tend to wait for recovery methods once hacked. Security teams need to emphasize the importance of prevention functions.

The NIST Ransomware Profile advises that organizations establish an incident recovery plan with defined protocol and roles along with robust prevention measures. Recovery should also include regular system backups periodically tested and maintained communication with key internal and external stakeholders. The FBI maintains that healthcare organizations should not respond by paying the ransom as it incentivizes malicious actors to continue targeting healthcare systems.

Healthcare organizations need a risk management tool that can keep up with its fast-paced environment. With patients' lives on the line every time a ransomware event strikes, companies should utilize a tool that prioritizes time-saving and cost-saving measures - like CyberStrong and its newest counterpart, CyberBase. CyberSaint's AI-assisted automation gives security teams at SMBs and large enterprises real-time insights into risk monitoring and assessments. Equipped with automated and continuous monitoring, security teams can stay updated on ransomware threats, critical gaps, and control failures that security teams might have glossed over otherwise.

Health systems can reduce their overall risk of ransomware events by complying with the NIST CSF Profile for Ransomware Risk Management.

With CyberBase or CyberStrong, organizations at different scales can detect and prevent threats from developing into full-scale attacks and ensure seamless hospital operations. Healthcare facilities need a solution that will protect their critical supply chain partners in critical infrastructure sectors like the emergency services sector and chemical sector. CyberSaint's platforms can task out custom control sets to third parties and automate vendor assessment monitoring. The COVID-19 pandemic continues to strain healthcare facilities, CyberSaint's comprehensive risk management solutions can help organizations scale up against an ever-evolving threat.