Threat Intelligence Report

Cybersecurity Risks Posed by Third-Parties in the Healthcare Industry

The healthcare industry faces significant and escalating risks from third-party vendors and service providers and experiences more third-party data breaches than any other sector. Third parties often have extensive access to sensitive patient data and critical systems, making them attractive targets for cyber attacks. The industry's heavy reliance on specialized software, outsourced administrative functions, and delegated clinical tasks creates a vast attack surface, and the interconnectedness of healthcare services means that a breach in one third-party provider may have devastating downstream effects across the entire sector, potentially impacting patient care and safety.

THREAT ACTIVITY

An estimated 90% of healthcare organizations will use cloud computing by 2025, including third-party cloud-based telehealth services. The sensitive nature of patient health information makes cloud-based telehealth platforms an attractive target for threat actors. Cloud-based systems face vulnerabilities from misconfigured security settings, insecure Application Programming Interfaces (APIs), inadequate Identity and Access Management (IAM), and zero-day vulnerabilities. In February 2024, the Cybersecurity and Infrastructure Security Agency (CISA) released an advisory detailing how nation state threat actors are targeting healthcare cloud infrastructures.

The healthcare industry is heavily reliant on third-party service providers to perform functions, including claim processing and payment, electronic medical record keeping, and medical billing services. In February 2024, a major clearinghouse for insurance billing and payments in the U.S. suffered a ransomware attack that halted claims processing. This had broad impacts across the healthcare ecosystem, including delays in prescription fulfillment, insurance approvals, provider reimbursement, and patient care delivery. This attack also resulted in the exfiltration of terabytes worth of sensitive patient data.

Recent reports indicate vulnerability exploits are becoming the most common entry point in data breaches. With an average of 6.2 vulnerabilities per medical device and the growth of Internet of Medical Things (IoMT) technology, these devices are expanding the attack surface. Commonly exposed IoMT devices include picture archiving and communication systems (PACS), Digital Imaging and Communications in Medicine (DICOM) workstations, smart infusion pumps, and medication dispensing systems. Vulnerabilities facing these devices include insecure default configurations and protocols, legacy devices running on outdated software and operating systems, weak credentials, and unencrypted traffic. CISA also issued security advisories on high-severity vulnerabilities in multiple DICOM viewers, a series of remotely exploitable vulnerabilities affecting a widely used PACS, and a vulnerability in a Bluetooth-enabled device.

THREAT ASSESSMENT

FTI Cybersecurity assesses threat actors will focus their attacks in the healthcare sector on strategic third-party vendors that serve large numbers of healthcare providers, house sensitive personal health information (PHI), and operate as single points of failure for the healthcare ecosystem. This will allow threat actors to conduct high-yield, high-impact attacks without needing to target individual healthcare providers.

RECOMMENDED ACTIONS

- Implement end-to-end encryption, stringent authentication and access controls, baseline security requirements and processes, and continuous monitoring and reporting.
- Require the use of multifactor authentication for all cloud environments.
- Maintain an electronic inventory management system for all medical devices and associated software, including vendor-developed software components and operating systems.
- Conduct regular and thorough third-party vendor risk assessments, including cloud and telehealth systems, to adopt a secure software development lifecycle (SDLC) and secure supply chain processes.
- Implement a zero trust architecture by leveraging a least-privileged access strategy, applying controls around network traffic, and reevaluating legacy investments.
- Mitigate known vulnerabilities, develop a patch management plan, ensure careful coordination among providers, validate patch application, and remove any end-of-life software that cannot be patched.
- Regularly update and stress-test existing incident response, business continuity, and disaster recovery plans.
- Actively monitor systems for suspicious network activity and vulnerabilities.
- Consider complementary services or other back-ups to protect against the residual fallout of attacks against critical service providers.

SOURCES

- Healthcare Experiences More Third-Party Data Breaches Than Any Other Sector
- The Increasing Risks to Cloud Security and Telehealth in Healthcare
- Cloud Computing Adoption in Modern Healthcare
- SVR Cyber Actors Adapt Tactics for Initial Cloud Access
- APT groups increasingly attacking cloud services to gain command and control
- Change Healthcare Ransomware Attack Spotlights Single Point of Failure with Third-Party Vendor
- HIPAA Website Substitute Notice
- Reports find spikes in vulnerability exploits
- Medical Device Cybersecurity: Agencies Need to Update Agreement to Ensure Effective Coordination
- Cyber Threats to Medical Technology and Communication Technology Protocols
- CISA ICS Medical Advisories

Why FTI Cybersecurity

MULTIDISCIPLINARY EXPERTISE

Intelligence-led, expert-driven, strategic approach to cybersecurity challenges

Core team from intelligence agencies, law enforcement, prosecuting offices, and global private sector institutions

GLOBALLY POSITIONED

Ability to respond anywhere in the world

Ability to staff the largest and most complex engagements and investigations

Relationships with the top global intelligence agencies, regulatory authorities, and private agencies

INTEGRATED & COMPREHENSIVE

Comprehensive services include crisis communications, e-discovery, forensic investigations, and more

Seamless integration of FTI Consulting's expertise across service offerings

CONTACT FTI CYBERSECURITY

Email: #fticybersecurity@fticonsulting.com

FTI Cybersecurity Global Offices

AMERICAS

Atlanta
Boston
Chicago
Houston
Irvine
Los Angeles
Mexico City
Miami
New York
San Francisco
São Paulo
Seattle
Toronto
Washington, DC
Wayne

EMEA

Berlin
Brussels
Cape Town
Dubai
Dublin
Düsseldorf
Frankfurt
Johannesburg
London
Madrid
Mumbai
Munich
Paris
Zurich

APAC

Brisbane
Hong Kong
Melbourne
Perth
Shanghai
Singapore
Sydney
Tokyo