Threat Intelligence Report

Elevated Cybersecurity Risk Following Acquisition of Insecure Assets

Mergers and acquisitions (M&A) are complex transactions that require rigorous due diligence to ensure a comprehensive understanding of potential risks, liabilities, and conflicts. Too often, cybersecurity is overlooked as a critical component of M&A due diligence, leaving companies vulnerable to compromise. By taking a risk-based approach to cybersecurity due diligence, especially as threats evolve and the cyber ecosystem becomes more complex, organizations can accurately assess the cyber exposure and subsequent value associated with a merger or acquisition, and plan for integration in a way that minimizes cybersecurity risk.

THREAT ACTIVITY

- In February 2024, FTI Cybersecurity was engaged by an environmental services company as part of the due diligence process for a pending acquisition. The environmental services company, which was being acquired by a nuclear technologies and manufactured products provider, had suffered multiple cybersecurity incidents in the past, including a ransomware attack and a business email compromise that occurred during the acquisition process. FTI Cybersecurity conducted a comprehensive post-breach assessment to review the past incidents and confirm that there was no lingering compromise or security impact, providing the acquiring company with the confidence necessary to move forward with the acquisition.
- In February 2024, a major healthcare company was hit with a ransomware attack by the BlackCat/ALPHV group. The company had been acquired by another healthcare services company, itself a subsidiary of a major multinational health insurance and services company, two years prior. Though the parent companies' networks were unaffected by the compromise, their business operations were significantly disrupted in the aftermath of the attack. In fact, the parent firm paid out more than $3 billion to providers whose cash flows were affected by the attack on its subsidiary.
- In May and June 2023, China-based threat actors used a stolen 2016 consumer signing key to forge authentication tokens and compromise the online mailboxes of 22 organizations and over 500 individuals globally. Though the company has not been able to conclusively identify how the threat actors obtained the signing key in question, they believed the incident was linked to the 2020 acquisition of a 5G technology and advanced networking company. Prior to acquisition, an engineer at the 5G company's device was compromised by the same China-based threat actors who conducted the 2023 attack. Once the engineer was supplied with corporate credentials for the acquiring company, the threat actors were able to authenticate to the network.

THREAT ASSESSMENT

Recent threat actor activity targeting organizations involved in M&A transactions – especially those that are also highly regulated and public – highlights the cyber risks involved when due diligence is overlooked.

- **Unknown risk:** The entity being acquired may have already been compromised by threat actors who remain dormant to gain access to the acquiring company's networks and systems once the deal closes.
- **Ransomware attacks:** Threat actors can launch damaging ransomware attacks, causing financial and reputational harm to the Target or the acquiring party, as well as significantly disrupting business operations. Threat actors may specifically target organizations going through the M&A process to pressure the victim into paying a ransom in order to avoid disruptions to the deal.
- **Lateral Movement:** Threat actors may seek to compromise the network of a less-secure subsidiary, perhaps with less stringent cybersecurity protocols or fewer security resources, to ultimately gain access to the parent company's network.

RECOMMENDED ACTION

Perform pre-acquisition due diligence and remediate critical vulnerabilities: Prior to finalizing a deal, conduct a full review of the entity to be acquired, including assessing existing cybersecurity controls and interviewing relevant staff. Ahead of the close and deal announcement, ensure all high-priority issues identified during the due diligence process are remediated.

Scan the attack surface: This will help with accounting for new assets added to the ecosystem so that they can be properly managed and secured.

Build a 100 day plan: Establish a plan for the first 100 days post-acquisition to remediate remaining vulnerabilities. This should also include updating business continuity and incident response plans to account for acquired entities and subsequently inherited risks.

Establish an incident response retainer: Establish an incident response retainer with a reputable vendor to ensure rapid, dedicated, and organized investigation and remediation in the event of a cybersecurity attack.

Facilitate a table-top exercise: Conduct real-world cyber attack simulations with acquired entities to identify incident response process gaps and determine the roles of key stakeholders during a crisis.

Involve outside counsel: Establish a working relationship with cybersecurity experts who can help provide assistance before, during, and after an incident.

SOURCES

Sources include open-source information from public and private industry reporting.

- #StopRansomware: ALPHV Blackcat
- The Change Healthcare attack: Explaining how it happened
- UnitedHealth Group has paid more than $3 billion to providers following cyberattack
- Review of the Summer 2023 Microsoft Exchange Online Intrusion

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

FTI Cybersecurity Global Offices

Americas

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

EMEA

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

APAC

Brisbane
Hong Kong
Melbourne
Perth
Shanghai
Singapore
Sydney
Tokyo

CONTACT FTI CYBERSECURITY

Email: #fticybersecurity@fticonsulting.com

Phone: +1-844-CYBR-FTI (+1-844-292-7384)

FTI Consulting is an independent global business advisory firm dedicated to helping organizations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. FTI Consulting, Inc., including its subsidiaries and affiliates, is a consulting firm and is not a certified public accounting firm or a law firm. ©2024 FTI Consulting, Inc. All rights reserved.
www.fticonsulting.com