CISO GLOBAL

A **CISO GLOBAL** WHITE PAPER

MITIGATING RISK in Mergers & Acquisitions: Why **CYBERSECURITY** Due Diligence is **ESSENTIAL**

Table of Contents

For more information, please contact us
480-389-3444 or visit **www.ciso.inc**

Understanding Cybersecurity Risk

At an M&A deal's start, the acquirer should assess the target's cybersecurity profile to minimize risk exposure after closing. A recent survey[1] of IT decision makers found that only 37% strongly believed they had the skills for this specialized undertaking.

How deep should a business go with its cyber due diligence when cyber risks are often concealed and hard to detect? Are there any weaknesses that are serious enough to jeopardize the acquisition?

To **minimize** cyber risks after closing, M&A teams must incorporate **accurate cybersecurity** assessments into their **deal review**

Consider these two notable breaches:

- Marriott International — in its $13.6 billion takeover in 2016 of Starwood Hotels & Resorts Worldwide — didn't know that the acquisition's system had been compromised by a cyberattack years earlier.[2] This led to one of the biggest data breaches ever, compromised the data of 339 million guests, drew huge regulatory penalties,[3] and more.
- In 2013, malware breached the payment processing system of U.S. retailer Neiman Marcus, impacting 1.1 million customers.[4] Three months later, new investors acquired the company without detecting the breaches.

Whether to proceed, renegotiate, or terminate is a judgment call. But to minimize cyber risks after closing, M&A teams must incorporate accurate cybersecurity assessments into their deal review.

Discovering a cybersecurity issue during M&A negotiations leads to abandoned deals and renegotiated prices. When an issue is undisclosed (i.e., discovered by the acquirer during due diligence, instead of revealed by the target), 73% of those surveyed agreed it would break a deal.

Cybersecurity's Visibility Problem

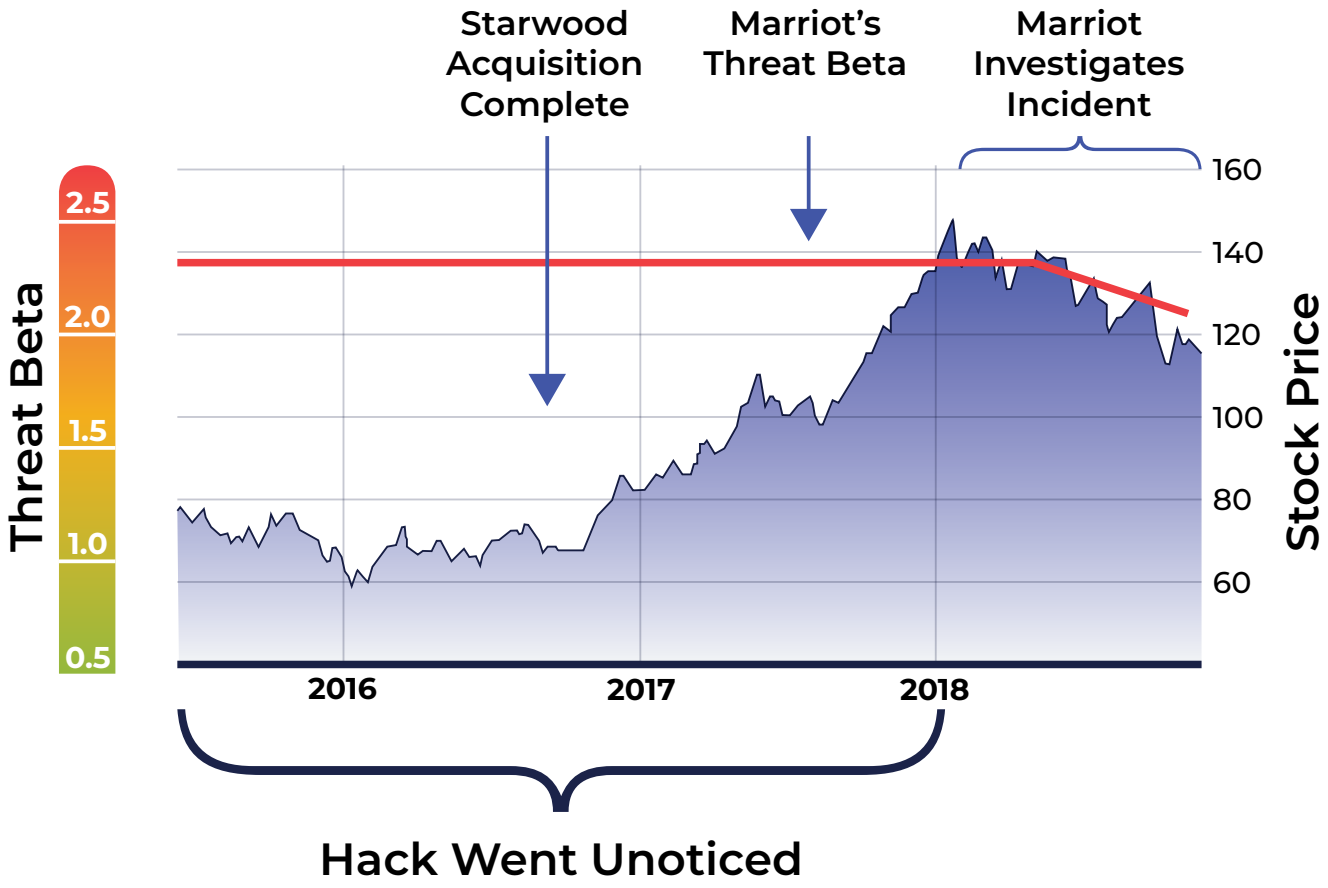
The target can't fix risks it can't see. As M&A progresses, any unforeseen incidents — including relatively minor breaches — could jeopardize the transaction.

Beyond data theft, common security failings include compromised credentials and unsecured remote access. An M&A process should align with the organizational risk profile, which is affected by a variety of factors like complexity, compliance, IP and wider digital assets, data assets, supply chains, incident history, IT and cyber integration, and human capital. Increasingly, companies looking to market themselves to buyers are conducting cyber due diligence before approaching a target.

The M&A Lifecycle

Cybersecurity equities must be considered early in the M&A lifecycle. CISO Global breaks cyber due diligence into three phases:

- Transaction readiness: The process through which the assets and liabilities of the acquired organization are analyzed for risks that might impact the acquirer's desire to purchase.
- Cyber due diligence: The stage at which an assessment seeks to uncover evidence of poor cybersecurity that might lead to a breach or additional costs for the acquirer.
- Pre-integration and divestiture: Isolating the cybersecurity-specific issues that must be remediated so the acquirer isn't exposed to additional risk during or after integration.



Transaction Readiness

Pre-due diligence checks include a transaction-readiness review of publicly available information on recent cybersecurity incidents. Other checks include background checks, dark web scans, internal incident assessments, and the results of any previous penetration tests.

Cyber Due Diligence: Identifying Cyber Risks

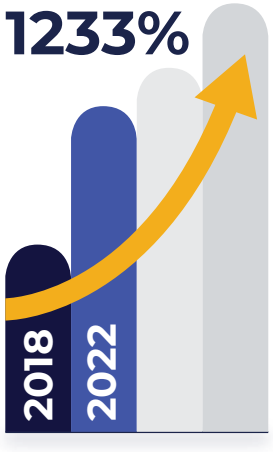
Acquirers don't have much time to gain visibility on past cybersecurity incidents and practices. Due diligence establishes an overview of the target's public cybersecurity and digital profile. When M&A reaches due diligence, the acquirer will be looking for areas of concern, including indicators of active compromise (e.g., evidence of previously undisclosed data breaches, compromised credentials, etc.), significant gaps in the target's cybersecurity program (e.g., gaps in policies and procedures that emerge when held to standards like NIST's Cybersecurity Framework [CSF]), critical public-facing vulnerabilities (e.g., public websites, servers, and internet-facing devices that have known, not-yet-patched vulnerabilities), and compliance risks.

Formal Assessments

Once the target company has been formally approached, due diligence can encompass more formal assessments, including internal incident assessment (e.g., reviewing notable cybersecurity incidents or breaches), asset tracking (e.g., reporting how the company tracks property and manages threats), gap analysis (i.e., differentiating between best practices and actual security postures), compliance (i.e., testing the compliance framework), and vulnerability reporting (i.e., enabling third parties to report vulnerabilities in public-facing systems or software).

Web-based Security Screening Scans

These scans can identify SSL certification issues, breached personal staff emails



Organizations viewing **cybersecurity** as a **critical** element of **M&A due dilligence** has risen from **one in twenty** to almost **two in three**
(Gartner, 2022)

(to determine whether employees are susceptible to spear phishing), vulnerable domains and subdomains (to prevent malicious campaigns designed to use the company's DNS to phish clients), IoT devices associated with vulnerable domains and subdomains, open and/or outdated ports, and relevant threat landscape information (to zero in on threat actors known to attack the organization's sector).

Dark Web Investigation

Dark web assessment scans, phishing-campaign investigations, and disinformation-campaign investigations allow an acquirer to find out if the target acquisition has experienced malicious data exfiltration.

Penetration Testing

A penetration test probes for weaknesses in the acquired company's systems and uncovers exploitable risks. These tests include black box (i.e., attempts to compromise a system without prior knowledge of that system), internal penetration (i.e., validating defense-in-depth by simulating the kind of compromises that frequently happens after a successful phish), web application (i.e., an evaluation of a company's public-facing web applications for vulnerabilities), and employee-readiness tests (i.e., an assessment of the behavior of employees or the physical security of a site).

Penetration-test reports can identify a wide variety of issues, including exposed services and devices, endpoint security, network design, patching, legacy systems, home working, internal controls and processes, authentication and identity weaknesses, and supply chain security.

Gap Analysis

Gap analysis is the process of identifying whether the safeguards and controls in place are sufficient to meet the standards necessary for compliance and data security best practices. Risk control evaluations include the target acquisition's risk management plan (i.e., identifying, analyzing, and addressing risks), information system activity review (i.e., preventing/addressing security violations), workforce termination procedures (i.e., removing employee access), applications and data criticality analysis (i.e., analyzing the impact of an app or data loss), testing and revision procedures (i.e., coping with contingencies), data backup plan (i.e., backing up and retrieving data), facility security plan, business associate agreements (e.g., satisfying compliance), and policies and procedures (i.e., ensuring up-to-date policies and controls).

Why Cyber **Due Diligence**?

Beyond the general requirement for risk assessment, careful cyber due diligence has important advantages.

- **Helps identify deeper cybersecurity problems at an early stage that might affect deal valuation and negotiations.**
- **It minimizes the possibility of surprises that might jeopardize a deal between public announcement and completion.**
- **It allows integration and any necessary upgrades to be planned in advance.**
- **It reduces the risk of hidden liabilities emerging in the longer term.**
- **It meets industry standards of M&A best practice.**

Pre-integration and Divestiture: Addressing Cyber Risks

Integrating the new acquisition without remediating all existing cybersecurity issues is dangerous. Important pre-integration issues include patching and vulnerability management (i.e., prioritizing gaps or inefficiencies identified in the acquisition's patching procedures), endpoint security

remediation (e.g., protecting PCs, servers, printers, IoT, etc.), cybersecurity policies and procedures (e.g., resolving any inconsistencies in firewall policies, identity and access management, and incident response and crisis management), supply chain risk assessment (i.e., looking at any systems accessed by, or data shared with, partners or third parties), and data backup and recovery assessment (i.e., assessing the acquisition's cloud-data management tools to avoid misconfiguration issues).

Assessing Startup Risk

Startup acquisitions' weaknesses may include a small or inexperienced cybersecurity team, a lack of 24/7 coverage, proprietary applications with vulnerable code, weak network design, weak compliance and gaps in policy and procedures, weak patching routines leading to exploitable vulnerabilities, weak management of third parties and the supply chain, dependence on third-party security services with weak SLA management, and a lack of response/remediation capability in the event of ransomware attacks.

How CISO Global Can Help

Using information from penetration tests and risk assessments, CISO Global provides every client with a full report that itemizes significant cybersecurity incidents, poor cybersecurity practices and/or compliance policies, suggested remediations, costs of remediations, and more.

The company's experts can coordinate patches and vulnerability management, integrate different generations of monitoring, implement training and awareness programs, provide a full cost analysis for bringing a target up to the same standard as the acquirer, and more.

The company's tools and expertise give acquirers a clear understanding of their purchase. Delivered by advisory and compliance experts, the company's reports spot issues that might affect valuation and offer ideas for mitigating problems.

With CISO Global, acquirers understand the cybersecurity risks they stand to inherit through an acquisition.

References

1. Research study: The role of cybersecurity in M&A diligence. Forescout. (2022, April 6). Retrieved February 17, 2023, from https://www.forescout.com/merger-and-acquisition-cybersecurity-report.

2. Thomson Reuters. (2019, January 4). Marriott cuts estimate on size of massive Starwood hack. Reuters. Retrieved February 17, 2023, from https://www.reuters.com/article/us-marriott-intnl-cyber-idUSKCN1OY13K.

3. BBC. (2020, October 30). Marriott Hotels fined £18.4m for data breach that hit millions. BBC News. Retrieved February 17, 2023, from https://www.bbc.com/news/technology-54748843.

4. Thomson Reuters. (2014, January 23). Neiman Marcus says about 1.1 million cards affected by breach. Reuters. Retrieved February 17, 2023, from https://www.reuters.com/article/neiman-databreach-idINL2N0KX1N220140123.

A leader in cybersecurity and compliance services, CISO Global brings together expert practitioners and thought leaders to provide tailored solutions that drive cyber resilience. The company's top-tier talent spans geographies, specialties, industries, regulatory frameworks, and focus areas and includes auditors, compliance specialists, certified forensics experts, ethical hackers, security engineers, and around-the-clock analysts.

For more information, please contact us
480-389-3444 or visit www.ciso.inc

SOC 2® Type II Audited