

EXECUTIVE PAPER · SYSTEMS RESCUE

Due Diligence Must Include the Systems

When you buy a company you buy its servers, its credentials, its old breaches and its unfinished upgrades. Boards and deal teams should make technology and cyber diligence a gate before signing and price what it finds.

AUTHOR

Chris Watkins

SERVICE

Systems Rescue

FOR

CEO, CFO, CTO, Board · 11 min read

AT A GLANCE

The problem. Acquirers inherit the target's systems on the day the deal closes, including access paths nobody has secured and intrusions nobody has found. UnitedHealth bought Change Healthcare in 2022 and lost $3.1 billion in 2024 to an attack that entered through a Change remote access portal without multifactor authentication. Marriott bought Starwood in 2016 with an attacker already inside, and was still settling with regulators in 2024.

Why it persists. Technology diligence is scheduled late, scoped narrowly and staffed thinly. Deal teams treat it as a checklist for integration planning, after price is set. In a 2025 survey, one in four CISOs said leadership pushes to close deals over thorough cyber diligence.

The recommendation. Make technology and cyber diligence a gating workstream with authority to change price, terms or timing. Test the target's access paths, identities, backups and breach history before signing. Convert each finding into a price adjustment, escrow, indemnity or closing condition, and secure the target's front door on day one.

The Decision in Front of You

Every acquisition already includes some technology review. The decision is whether that review can change the deal. In most transactions it cannot. It runs after the letter of intent, inside a data room, against documents the seller chose to share, and it reports to an integration team that inherits whatever it finds.

The stakes are set at closing. After that date the target's unpatched servers, shared administrator passwords, unsupported software and undiscovered intrusions belong to the buyer, along with the regulatory exposure attached to the data those systems hold. Remediation that could have come off the purchase price comes out of the buyer's operating budget instead.

FTI Consulting's 2026 survey of 278 senior executives at US companies with 500 or more employees found that nearly one in four had experienced a cyber incident during or shortly after a transaction [10]. Some 42% of respondents reported a significant reduction in deal value, and 20% said a deal was delayed or paused by a cyber incident [10].

What's Happening

Buyers own the target's past

Marriott announced its acquisition of Starwood in 2015 and completed it in 2016 [1]. An attacker had been inside Starwood's guest reservation system since 2014 and was not detected until September 2018 [1][2]. The breach exposed records of up to 339 million guests [3]. Marriott told the UK Information

Commissioner's Office that it had only been able to carry out limited diligence on Starwood's systems [3]. The ICO fined Marriott £18.4 million in 2020 and said that diligence is an ongoing duty, "not a time-limited or a one-off requirement" [3].

The US case closed in October 2024. The Federal Trade Commission's order covers three breaches between 2014 and 2020 affecting more than 344 million guest records, and cites failures in access controls, network segmentation, patching, logging and multifactor authentication [1]. Marriott must certify its security program to the FTC every year for 20 years and obtain independent assessments every two years [1][2]. A coalition of 50 state attorneys general obtained $52 million [2]. Their settlement also requires "improved diligence in relation to future acquisitions" [1].

Liability transfers by contract as well as by data. In May 2025 RTX, Raytheon and Nightwing Group agreed to pay $8.4 million to resolve False Claims Act allegations that Raytheon had not implemented required cybersecurity controls on a system used for 29 Defense Department contracts [9]. The alleged conduct ran from 2015 to 2021. RTX sold the business in March 2024, and it became part of Nightwing, which joined the settlement although the conduct predated its ownership [9]. The settlement involved no finding of liability [9].

Two recent cases where the gap was in the acquired company

Change Healthcare, 2024. UnitedHealth paid $13 billion for Change Healthcare in late 2022 and was modernizing much of Change's technology when the attack came [4]. On February 12, 2024, attackers used stolen credentials to log in to a Change Citrix remote access portal that did not have multifactor authentication, and deployed ransomware nine days later [5]. UnitedHealth's policy required MFA on all external-facing systems. The portal had been missed [4]. Chief executive Andrew Witty testified that some systems in Change's claims and payment business dated back 40 years, that Change's primary and backup environments were not isolated from each other, and that UnitedHealth had to rebuild the platform from scratch [4]. UnitedHealth put the 2024 cost at $3.1 billion and later estimated that about 190 million people were affected [6]. The lesson: an integration program leaves inherited access paths open until someone closes them on purpose. Less than two years after closing, one such path cost the buyer $3.1 billion.

PowerSchool, 2024. Bain Capital closed its $5.6 billion take-private of PowerSchool, the school software provider, in October 2024 [7]. Between December 10 and 28, 2024, an attacker used a single compromised credential to enter PowerSource, the company's customer support portal, and from there reached student information systems [7][8]. PowerSchool told TechCrunch that the portal did not support multifactor authentication at the time [8]. PowerSchool has not confirmed a total, though one outlet reported, citing sources, more than 62 million students and 9.5 million teachers [8]. At least 23 class actions were filed within weeks [7]. Whether the weakness could have been found before closing is not public. A support portal with direct reach into customer data and no MFA is the kind of finding a pre-signing access review exists to surface.

SIDEBAR: VERIZON AND YAHOO

The best-known price adjustment for a cyber finding predates these cases. In February 2017, after Yahoo disclosed two large breaches during its sale, Verizon was reported to be negotiating $250 million to $350 million off the purchase price [12].

Deal teams know this and still under-resource it

Executives report the problem consistently. In Forescout's 2019 survey of 2,779 IT and business decision-makers, 53% said a critical cybersecurity issue or incident had jeopardized a deal, and about 65% said their company had regretted a deal because of cybersecurity concerns [11]. The survey is now seven years old. FTI's 2026 data shows the same pattern from inside the deal team: 34% of CISOs said they are not heavily involved in transaction decisions, one in three doubt or are unsure they have authority to stop a deal over cyber risk, and only 23% of executives said they manage cyber risk proactively after closing [10].

Why the Usual Approach Fails

Technology diligence is sequenced after the price. The letter of intent fixes value and exclusivity first. By the time engineers see anything, the deal has momentum, and findings become integration tasks instead of negotiating points.

The review reads documents instead of testing systems. Data rooms hold policies, network diagrams and a questionnaire the seller completed. None of these shows whether a support portal enforces MFA or whether backups share credentials with production. Change Healthcare's own policy required MFA on external systems [4]. The written policy would have passed a document review.

Breach history is taken on trust. A target can only disclose intrusions it has detected. Starwood's attacker went unnoticed for four years [1]. A representation that the seller knows of no breach covers only the breaches it knows about.

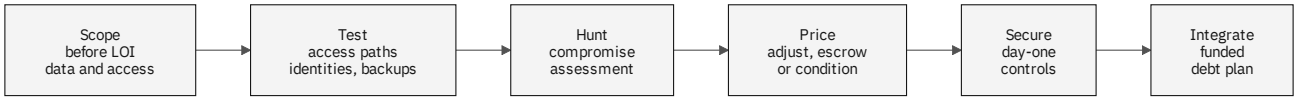
Technical debt is left out of the model. Forty-year-old claims systems and unsupported platforms carry a replacement cost the buyer will pay [4]. When that cost appears after closing it becomes a budget overrun with no counterparty.

Integration is treated as the moment to fix security. Integration takes years. Change was still being modernized more than a year after closing [4][5]. The target's weakest access path stays open until someone closes it deliberately.

The Framework: Test, Price, Secure

Treat technology and cyber diligence like financial and legal diligence: a workstream with a scope set before the letter of intent, access to systems as well as documents, and a report that goes to the investment committee before signing.

Exhibit 1. Technology diligence as a deal gate: findings reach price and terms before signing



Source: author's framework, informed by the Change Healthcare, Starwood and PowerSchool cases [1][4][7] and NIST CSF 2.0 supply chain governance [13].

Scope. Before the letter of intent, agree with the seller that technical diligence includes system access, interviews with the engineers who run production, and time for testing. Treat a refusal as uncertainty and price it.

Test. Enumerate every way into the target: VPNs, remote desktop gateways, vendor and support portals, cloud consoles, email. Check each for enforced MFA. Count privileged accounts and service credentials. Confirm that at least one backup copy is offline or immutable and isolated from production credentials, as CISA's #StopRansomware Guide recommends [14], and watch a restore.

Hunt. Commission a compromise assessment: a search of logs, endpoints and identity systems for signs of an existing intruder. This is the only diligence step that can find a Starwood before closing.

Price. Convert each finding into money or terms. Cost the remediation and the technical debt, and decide which mechanism carries it (Exhibit 2).

Secure. On the day of closing, reset privileged credentials, enforce MFA on every external path, put the target's endpoints under monitored detection and response, and connect it to your incident response process. Do this before integration starts.

Integrate. Fund the debt plan from the price adjustment, with milestones reported to the board.

Exhibit 2. Turning diligence findings into deal terms

Finding	Example	How to carry it in the deal
External access without MFA	Support portal or remote access gateway on passwords alone [5][8]	Closing condition: fixed and verified before closing
Evidence of current or past intrusion	Attacker activity found by compromise assessment [1]	Delay signing; special indemnity or escrow sized to response and notification cost; walk away if scope is unknown
Backups reachable from production	Primary and backup environments not isolated [4]	Pre-closing remediation, or price reduction equal to the rebuild cost
Unsupported or decades-old core systems	Claims platform with 40-year-old components [4]	Price adjustment for the replacement program; integration budget set from the estimate
Regulated data with weak controls	Customer or patient records under consent orders or contract terms [1][9]	Specific representations; indemnity for pre-closing conduct; regulator exposure in the model
Key systems understood by one person	No documentation, single administrator	Retention agreement and knowledge-transfer milestone before final payment

Source: author's analysis of the cited cases. Deal mechanics vary by jurisdiction and structure; confirm with counsel.

Costs, Risks, and Tradeoffs

Exhibit 3. Tradeoffs of making technology diligence a gate

Area	Cost or risk	Mitigation
Fees and time	Hands-on testing and a compromise assessment add cost and weeks to the timeline	Scope by data sensitivity and deal size; run testing in parallel with legal diligence
Seller resistance	Sellers in competitive auctions may refuse system access before signing	Make access a condition of exclusivity, or price the uncertainty explicitly
Lost deals	Findings may kill a deal the business wanted	Record the findings and reasons; review killed deals annually against what the business wanted
Confidentiality	Testing a target's systems risks disclosure of the deal	Small named team under clean-team rules; test from outside first
False comfort	A clean assessment cannot prove no intruder exists	Keep the indemnity and day-one controls regardless of findings
When this is wrong	Small tuck-in acquisitions of a team or IP with no systems or customer data carry little inherited technology risk	Run a short checklist and move the people onto your own systems at closing

Source: author's analysis.

How to Act

Exhibit 4. A one-year roadmap for the acquiring organization

Window	Actions	Owner	Milestone
First 30 days	Write a technology and cyber diligence standard: scope, required system access, compromise assessment threshold, and the findings that block signing. Give the CTO or CISO a formal sign-off in the investment committee process.	CFO with CTO and general counsel	Standard approved; CTO or CISO sign-off required for every deal above a set value
First 90 days	Apply the standard to every deal in the pipeline. Add diligence access terms to letter of intent templates. Write a day-one security checklist covering credential resets, MFA on all external paths, detection coverage and incident response handover.	Corporate development with CISO	Every active deal has a scoped technology workstream; day-one checklist tested on one recent acquisition
First 90 days	Review companies acquired in the last three years against the day-one checklist. Fix any external access without MFA.	CISO	Zero external access paths without MFA across acquired companies
First 365 days	Track findings by deal and how each was priced. Report technology debt and security remediation for acquired companies to the board quarterly. Map the program to NIST CSF 2.0 supply chain governance [13].	CFO with CTO	Every closed deal has a funded remediation plan; first annual review of diligence findings against post-close incidents

Source: author's recommendation.

Questions to Ask Your Team

1. On our last three acquisitions, when did technology diligence start relative to the letter of intent, and did any finding change the price?
2. Who on the deal team can stop or delay a signing over a technology finding?
3. Did we test the target's systems, or read documents about them?
4. How many ways in from the internet did the target have on the day we closed, and which lacked MFA?
5. Did anyone look for an intruder already inside before we signed?
6. What did we budget for the target's technical debt, and where did that number come from?
7. Which companies we acquired still run on their original remote access, identity and backup systems?
8. What do our representations and indemnities say about breaches the seller did not know about?

Closing

An acquisition transfers the target's systems to you at closing, whether or not anyone looked at them. The time to find an open portal, an intruder or a forty-year-old platform is before signing, when the finding can still lower the price or change the terms. Make technology and cyber diligence a gate with authority over the deal, test systems instead of reading about them, price what you find, and secure the target on day one.

Sources

[1] Hunton Andrews Kurth. "FTC and Coalition of State Attorneys General Announce Settlements with Marriott over Guest Data Breaches." 2024. https://www.hunton.com/privacy-and-cybersecurity-law-blog/ftc-and-coalition-of-state-attorneys-general-announce-settlements-with-marriott-over-guest-data-breaches.

[2] Insurance Journal. "Marriott Settles With States for $52M Over 2018 Data Breach at Starwood." October 10, 2024. https://www.insurancejournal.com/news/national/2024/10/10/796585.htm.

[3] Mayer Brown. "Marriott International, Inc. fined £18.4m for personal data breach by the UK ICO under the GDPR." November 16, 2020. https://www.mayerbrown.com/en/perspectives-events/publications/2020/11/marriott-international-inc-fined-18m-for-personal-data-breach-by-the-uk-ico-under-the-gdpr.

[4] Kapko, M. "UnitedHealth's Change attack: tech takeaways from CEO testimony." Cybersecurity Dive. May 6, 2024. https://www.cybersecuritydive.com/news/unitedhealth-change-attack-tech-takeaways/715200/.

[5] TechTarget. "Change Healthcare breached via Citrix portal with no MFA." 2024. https://techtarget.com/searchsecurity/news/366582824/Change-Healthcare-breached-via-Citrix-portal-with-no-MFA.

[6] Healthcare Innovation. "Change Healthcare Tallies 190 Million Data Breach Victims." January 27, 2025. https://www.hcinnovationgroup.com/cybersecurity/data-breaches/news/55263828/change-healthcare-tallies-190-million-data-breach-victims.

[7] GovInfoSecurity. "PowerSchool Faces 23 Lawsuits Over Schools' Mega Data Breach." January 20, 2025. https://www.govinfosecurity.com/powerschool-faces-23-lawsuits-over-schools-mega-data-breach-a-27331.

[8] TechCrunch. "What PowerSchool isn't saying about its massive student data breach." 2025. https://techcrunch.com/2025/02/03/what-powerschool-isnt-saying-about-its-massive-student-data-breach.

[9] U.S. Department of Justice. "Raytheon Companies and Nightwing Group to Pay $8.4M to Resolve False Claims Act Allegations Relating to Non-Compliance with Cybersecurity Requirements in Federal Contracts." May 1, 2025. https://www.justice.gov/opa/pr/raytheon-companies-and-nightwing-group-pay-84m-resolve-false-claims-act-allegations-relating.

[10] FTI Consulting. "CISO Redefined III: Navigating Cybersecurity Risks in Transactions." Press release, survey of 100 CISOs, 78 heads of M&A and 100 general counsel, August 2025. March 17, 2026. https://stocks.observer-reporter.com/observerreporter/article/gnwcq-2026-3-17-fti-consulting-study-reveals-cybersecurity-attacks-are-an-increasing-threat-to-m-and-a.

[11] National Law Review. "Cyber Diligence Study Reveals Cybersecurity Concerns Are Becoming Critical Factor in M&A." Coverage of Forescout, "The Role of Cybersecurity in M&A Diligence." 2019. https://natlawreview.com/article/cyber-diligence-study-reveals-cybersecurity-concerns-are-becoming-critical-factor-ma.

[12] Information Security Buzz. "Verizon/Yahoo acquisition price cut hardly comes as a surprise." February 20, 2017. https://informationsecuritybuzz.com/verizonyahoo-acqusition-price-cut-hardly-comes-surprise/nick-pointon/.

[13] National Institute of Standards and Technology. "The NIST Cybersecurity Framework (CSF) 2.0." NIST CSWP 29. 2024. https://doi.org/10.6028/NIST.CSWP.29.

[14] Cybersecurity and Infrastructure Security Agency, MS-ISAC, NSA and FBI. "#StopRansomware Guide." 2023. https://www.cisa.gov/stopransomware/ransomware-guide.

The views in this paper are the author's own and do not represent any employer. Scenarios are hypothetical. This paper is not legal, financial, or compliance advice.