CISO Redefined Series

Navigating Cybersecurity Risks in Transactions

The Emerging Risk for Deal Makers As M&A Activity Intensifies

EXPERTS WITH IMPACT™

FTI CONSULTING

Over the past few years, cybersecurity and mergers and acquisitions (“M&A”) have been two of the most explosive growth drivers for FTI Consulting’s Strategic Communications Team. Our practitioners have deep expertise in navigating the opportunities and risks that these events present and have been involved with some of the highest profile transactions and cyber attacks in history.

It was when our teams began to find themselves working on the same projects more and more that we realized cybersecurity risk and transaction events seem to be correlated.

Transactions are hard to secure. Most people sense that time kills deals, so in the spirit of moving quickly, it’s often easy to look past the red flags of an immature security program even though those risks may lead to significant exposure down the road.

Are the speed and change that define M&A transactions causing a pattern of vulnerability that threat actors are exploiting?

Our third installment of FTI Consulting’s CISO Redefined series aims to answer that question, among others, and focuses on the nexus of cybersecurity risk and M&A activity. We approached this question by:

1. Analyzing deal activity and publicly-disclosed data breaches to see how often companies experience cyber incidents during the deal process
2. Surveying senior cyber, M&A and legal executives about their roles and perspectives regarding cybersecurity in the deal process

Our theory was that if we studied the current deal environment and overlaid our research into publicly-disclosed data breaches, we’d find a correlation between M&A activity and an increased risk for cyberattacks. And, we were right.

What’s even more interesting, though, is what our survey told us about how chief information security officers (“CISOs”), heads of M&A, and general counsels think about their partnerships and their respective roles as they pertain to cyber risk – both during the due diligence process and throughout the transaction itself.

The importance of aligning transaction processes with cyber risk mitigation efforts is clear. **Nearly half of respondents in our survey said valuation was impaired by a cybersecurity event during or just after a transaction.**

CISO Redefined III is the third study FTI Consulting has conducted regarding the role and influence of CISOs on an executive team, in the Board room and during critical decision-making moments. CISO Redefined III aims to underscore the importance of keeping cybersecurity risk top of mind during a fast-paced transaction in order to protect both reputation and valuation alike.

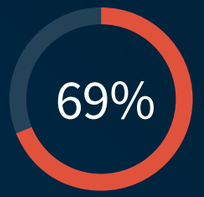
Importantly, when it comes to cybersecurity professionals and deal teams, both must do their part to help break down the barrier between moving the business forward and delivering against “security first” priorities. The two groups need to work together to change the perception that their goals are opposed to one another.

Meredith Griffanti
Global Head of Cybersecurity & Data Privacy Communications, Senior Managing Director

Pat Tucker
Americas Head of M&A and Activism Communications, Senior Managing Director

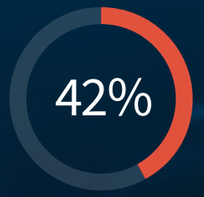
Five Key Takeaways

Negative Impact on Deal Value



More than two-thirds (69%) of those who experienced a cyber incident during or after a transaction claim it had a negative impact on the transaction in some capacity.

A majority (58%) believe the incident impaired the company's ability to reach financial targets after the transaction.



Nearly half (42%) claimed the deal value was reduced as a result of the cyber incident. Another 20% stated that the transaction was paused or delayed.

Minimized Role for CISOs in Decision Making

A plurality of CISOs do not have a seat at the table during transaction due diligence, with **one in three (33%) indicating they do not believe they have the ability to kill a transaction if the risk to the organization is too high during or after a transaction.**

Cyber Integration Post-Transaction is a Significant Challenge

Most organizations struggle to align and integrate their cybersecurity protocols and procedures post-deal, with **84% of survey respondents citing challenges in harmonizing IT systems and policies.**

Disconnect between Growth Goals & Cybersecurity Risk

Pressure to close deals quickly as cited by 41% of respondents as a factor that increases cybersecurity risk during transactions, reflecting concerns that speed can come at the expense of fully assessing cybersecurity defenses during the due diligence process, exacerbating the somewhat inherent tension between growth and risk mitigation.

Companies are Targeted and Potentially Exposed at a Critical Moment

One in four respondents (24%) admit that their organization experienced a cyber incident within 24 months after closing a transaction, revealing lasting, real-world consequences for those who do not coordinate their cybersecurity and deal teams.

From limited CISO involvement in early diligence to the operational challenges of post-close integration, these dynamics compound throughout the deal lifecycle. The result is a landscape in which deal momentum often outpaces cyber resilience, exposing organizations to preventable risk at precisely the moment they can least afford it.

Ignoring Cybersecurity Risk Impacts Value

Cybersecurity incidents can have direct and indirect financial impact on acquiring companies as they close a transaction and work to integrate the target.

Nearly 1 in 4 executives has experienced a cybersecurity incident during or shortly after a transaction (24%). Out of the deals impacted by cybersecurity incidents, 2 in 3 of these were significant events like data theft, extortion, or vendor breaches that exposed confidential information.

Perhaps the most staggering statistic gleaned from our survey was that – of the executives who experienced a cybersecurity incident during or shortly after a transaction – nearly half saw deal value reduced (42%). More than half said financial targets were impaired (58%), while 20% said their deals were either delayed or paused due to a cyber attack.

Of the executives who experienced a cybersecurity incident during or shortly after a transaction…

More Than Half Said Financial Targets Were Impaired	58%
Nearly Half Saw Deal Value Reduced	42%

1 in 4

Nearly **1 in 4 executives has experienced a cybersecurity incident** during or shortly after a transaction

2 in 3

2 in 3 of these were significant events like data theft, extortion, or vendor breaches that exposed confidential information

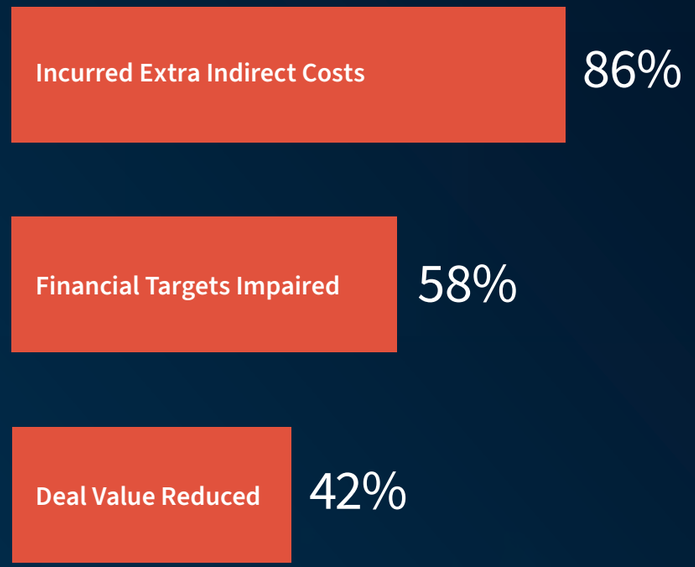
"We see this time and time again in our practice – many of our cases happen during a transaction or right after a deal closes. Sometimes it's because there was a lack of due diligence on the target and other times it's because the deal leaked and is in the headlines. Threat actors are smart; they read the news and know companies tend to be vulnerable when they're trying to close or right after when they're integrating systems – and that's when they try every trick of the trade to break in. But, the common thread is that an incident ends up costing the acquirer big time. Most often, the target and acquirer haven't even begun to think about how they'll work together to respond to a front page news cyber crisis if it occurs right after a deal closes, and that lack of coordination can have serious blowback on reputation."

Meredith Griffanti, Global Head of Cybersecurity & Data Privacy Communications, Senior Managing Director, FTI Consulting

Not only can these incidents impact the potential value of a deal – they also can slow down the integration process post-close, cause operational disruption and damage a brand's reputation or position in the market. This is why 86% of CISOs say that experiencing a cyber incident during a transaction can lead to incurring additional indirect costs – namely reputational damage (41%) and greater regulatory or investor scrutiny (32%).

Key stakeholders, and their respective needs, change during a transaction. CISOs should prioritize getting support and buy-in from the appropriate leadership teams on both sides of a transaction on a streamlined break-glass incident response plan that is specific to a cyber attack occurring during or right after a transaction. Having a plan for deal-specific considerations, like how to communicate with the buyer/target, what additional regulators need to be contacted, or how an incident might impact the work of the team overseeing integration, can help limit disruption of the deal process.

Top Consequences of Cybersecurity Incidents



"Deal teams need to account for cyber risk much the same way we think about leak risk. These unexpected disruptions can create confusion, shift value and slow negotiations. You can never eliminate the risk entirely, but the follow-on disruption from these events can be mitigated with speed and clarity of response."

Pat Tucker, Americas Head of M&A and Activism Communications, Senior Managing Director, FTI Consulting

Cybersecurity Is Seen as Important in Principle, but Is Often Sidelined in Transaction Practice

When the stakes are highest during a transaction, executives are forced to balance competing priorities while continuing to generate the momentum needed to carry the deal forward.

Good cybersecurity practices are rarely thought of as a momentum driver by non-CISOs. According to our CISO Redefined II research conducted in 2024, the vast majority of CISOs feel their role is misunderstood by company leadership, and they struggle to communicate in a non-technical way that other executives can actually understand.

Our research determined that CISOs may also feel they lack the power to act, as one in three CISOs do not believe they have the authority – or are unsure of whether they have the ability – to halt a transaction, even if they believe residual risks are too high to ignore either during or after an acquisition. This disconnect between CISOs and company leadership on risk priorities during transactions mirrors how leadership recognizes cybersecurity as important in principle but fails to ensure it is implemented in practice.

While 69% of executives recognize the importance of cybersecurity in transactions, the CISO's voice and opinions – and therefore cyber risk – are not being prioritized. Alarmingly, 67% of heads of M&A and 76% of general counsels say the CISO is very critical to a transaction, but only 34% of CISOs say they are heavily involved in contributing to decisions when executing a transaction.

"There's a clear disconnect between acknowledgment and action. Even as deal and legal teams recognize the CISO's critical role, too few CISOs are brought into the room when key transaction decisions are made. If a company truly wants to say it prioritizes cybersecurity, that commitment must hold up during M&A. Cyber due diligence needs to serve as a true stage-gate, ensuring CISOs are not only heard but empowered with the authority and insight to act decisively."

James Condon, Americas Head of Research, Corporate Positioning & Insights, Managing Director, FTI Consulting

Fast Deal Cycles Raise Risks While Collaboration Falls Short

M&A transactions often create fast-paced, high-stakes environments, in which the terms of a deal can come together quite quickly.

As part of this, the diligence process requires examining hundreds of documents, sensitive financial information and projections in a condensed timeline. While short timelines may be required in M&A, they can also result in increased security risks, according to one in three CISOs.

But that risk doesn't stop leaders from applying significant pressure on deal teams to close quickly. There can be unintended consequences from improperly balancing this tradeoff.

Given this breakdown between CISOs and senior leadership, it comes as no surprise that only 17% of CISOs said that collaboration between cybersecurity and corporate development teams increased during a transaction period. By contrast, 24% of M&A heads thought collaboration increased during this period, as did 34% of general counsels – showing a fairly notable disconnect. Ultimately, during a period when collaboration is critical, our research shows that it is in fact quite limited – respondents made clear that key functions of the business are just not working together.

1 in 3

Say **faster timelines** increase cybersecurity risks

2 in 5

Say **cyber threats increased** during the transaction period

1 in 4

Say **leaders push to close deals quickly** over conducting thorough cybersecurity due diligence

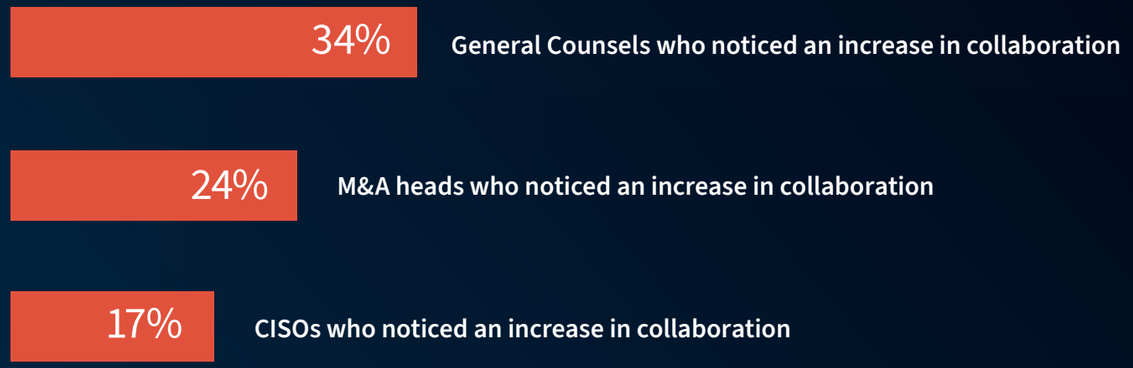
1 in 5

See **tension between executive growth goals** and cybersecurity risk tolerance

Our first edition of CISO Redefined I, reflecting results from a 2023 survey, underscores this disconnect, as we learned that 63% of CISOs believed their concerns were not aligned with senior leadership's priorities, while over half did not believe these senior leaders were completely prepared for cyber risks.

Cybersecurity leaders today face a clear challenge: they need to be viewed not as roadblocks, but as strategic partners in value creation. Earning a seat at the table requires more than technical expertise. CISOs need to show that they have business acumen and a deep understanding of other team members' perspectives and goals – and a willingness to use their cyber expertise to support those goals. The most effective cybersecurity leaders demonstrate that they can propel a deal forward by helping to protect value, defend the critical assets being acquired, and unlock efficiencies when thinking ahead to integrating systems. In doing so, they redefine the cybersecurity function – it's not a cost center; it's a core growth driver and defender.

Increase in Collaboration Between Cybersecurity and the Deal / Legal Team During Transactions



"To confront cyber risk adequately, and ensure enterprise level preparedness, CISOs need to be more than security experts. They need to be influencers, communicators, and internal deal makers. We see clear anecdotal evidence supporting the idea that CISOs who invest in these skills achieve better security outcomes."

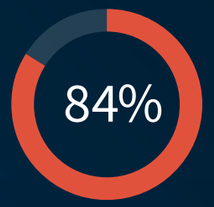
Evan Roberts, Co-Leader of Americas Cybersecurity & Data Privacy Communications, Senior Managing Director, FTI Consulting

"Investors recognize the somewhat inevitable nature of a cyber incident occurring at some point in a company's lifecycle. What they want to see, however, is that the Board is taking the appropriate proactive measures to ensure continuity and limit disruption if an incident occurs. Cybersecurity preparedness during all crucial moments, including during a transaction, has become par for the course in terms of effective Board oversight"

Garrett Muzikowski, M&A and Activism Communications, Managing Director, FTI Consulting

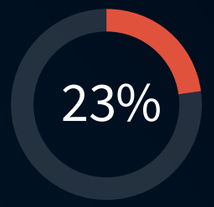
Many Organizations Are Unprepared to Manage Cyber Risk After Deals

Against a backdrop of limited collaboration among CISOs, deal teams, and general counsels, many organizations are also unprepared to manage cyber risk once a transaction closes.



84% report difficulties when aligning cybersecurity policies with another company

39% of leaders don't have an integration plan for when a transaction completes



23% of organizations are completely proactive only after a transaction has taken place

Our research shows that approximately 40% of organizations lack a defined cybersecurity or IT integration plan after a transaction closes. Moreover, 84% of executives reported challenges in aligning cybersecurity policies and IT systems following a transaction, with misaligned risk tolerance and pressure to integrate quickly rather than securely emerging as the top two obstacles.

What's particularly striking is how an organization's proactive management of cybersecurity risk diminishes as a deal progresses. During a transaction, executives are evenly split between taking a fully proactive approach (50%) and not doing so. But, once a transaction closes, that proactivity drops sharply, with only 23% of executives saying they manage cybersecurity risks proactively post-close. When combined with the already significant challenges organizations face in aligning cybersecurity policies and systems, this decline in vigilance creates a meaningful exposure point for the organization.

The challenges associated with integrating IT systems after a transaction often create a blind spot that leaves newly-combined entities exposed right when they're most vulnerable. That's because new endpoints and systems have likely just been introduced to the acquirer's network, which increases the number of ways a threat actor can gain access.

Our research boils down to the following point: post-close cyber and IT integration is poorly anticipated and managed. That is largely because success in this endeavor requires much more than simply harmonizing policies and practices. It requires securely merging two distinct technical environments and doing so in a way that doesn't expose either organization to increased risk.

Greater collaboration between cybersecurity, M&A and legal teams – both during AND after a transaction – can help to create better alignment and structure around integration plans. This will help ensure teams jointly agree on the right milestones and timelines with the right parameters in place – ultimately helping to protect value and minimize new risks.

Conclusion

Cybersecurity incidents can have a devastating impact on an organization. It's no surprise, then, that executive teams who have experienced these incidents in and around deal time note the lethal effects a cyber attack can have on financial targets and valuation.

While the risks and consequences of these incidents are well understood, and well considered in theory, during decision-making time, the voices of the executives most responsible for mitigating these risks are often sidelined. This paints a picture of risk mitigation taking a backseat to ambition and speed, putting acquiring and acquired companies on a path that takes them further away from their growth goals rather than closer to them.

By making cybersecurity and risk management a proactive and integrated part of the transaction process, companies can protect value, meet financial goals, improve the integration process, and maintain trust with key stakeholders. Security, success and growth should be intertwined – not at odds with one another.

Methodology

FTI Consulting surveyed 100 CISOs, 78 heads of M&A, and 100 general counsels across public and private organizations with at least 500 employees, representing a majority of companies with a market cap of $5 billion or more, to understand how key leaders collaborate with each other and weigh cybersecurity priorities during and after M&A deals. The survey was conducted online between August 12 – 26, 2025.

Contact Our Team for More Information:

Meredith Griffanti
Global Head of Cybersecurity & Data Privacy Communications, Senior Managing Director
meredith.griffanti@fticonsulting.com

Evan Roberts
Co-Leader of Americas Cybersecurity & Data Privacy Communications, Senior Managing Director
evan.roberts@fticonsulting.com

Jamie Singer
Co-Leader of Americas Cybersecurity & Data Privacy Communications, Senior Managing Director
jamie.singer@fticonsulting.com

Orla Cox
Cybersecurity & Data Privacy Communications, Managing Director
orla.cox@fticonsulting.com

Matt Saidel
Cybersecurity & Data Privacy Communications, Managing Director
matt.saidel@fticonsulting.com

Allison Hufnagel
Corporate Positioning & Insights, Director
allison.hufnagel@fticonsulting.com

Pat Tucker
Americas Head of M&A and Activism Communications, Senior Managing Director
pat.tucker@fticonsulting.com

Garrett Muzikowski
M&A and Activism Communications, Managing Director
garrett.muzikowski@fticonsulting.com

James Condon
Americas Head of Research, Corporate Positioning & Insights, Managing Director
james.condon@fticonsulting.com

Elizabeth Murphy
Cybersecurity & Data Privacy Communications, Director
elizabeth.murphy@fticonsulting.com

Lily Walsh
Cybersecurity & Data Privacy Communications, Senior Consultant
lily.walsh@fticonsulting.com

For more information visit our **CISO Redefined webpage**

About FTI Consulting Cybersecurity & Data Privacy Communications

Our Cybersecurity & Data Privacy Communications offering is one of the premier cybersecurity communications groups in the industry. Named the Cyber PR Firm of the Year by the Cybersecurity Excellence Awards in 2021, 2022, 2023, and 2024 and recognized by Chambers & Partners as a top global crisis communications provider, the group provides expert crisis communications counsel and support in cybersecurity preparedness and throughout the entire lifecycle of an incident, helping organizations around the world mitigate risks, improve continuity, and protect their relationships with stakeholders before, during, and after an incident. Put simply, we help our clients to communicate effectively – across any channel – to protect and enhance their interests with key stakeholders.

About FTI Consulting M&A and Activism Communications

The M&A Practice within FTI Consulting's Strategic Communications segment is consistently ranked as the top M&A communications practice globally. The team advises clients across every stage of the deal lifecycle to enhance the certainty of a successful close. From pre-announcement planning to transaction announcement and post-merger integration, the team provides an unparalleled combination of expertise in transaction communications, investor relations, public affairs, digital platforms and employee engagement. The team approaches each transaction as a multi-faceted campaign; developing and driving positive deal sentiment across stakeholder groups while minimizing regulatory risk and threat of shareholder dissent and activism.

About FTI Consulting Corporate Positioning & Insights

Our Corporate Positioning & Insights experts partner with leadership teams to design and execute multi-stakeholder communication campaigns that build, enhance or protect a company's reputation. Our approach is grounded in using data and insights to deeply understand stakeholder perceptions and needs to ensure messaging resonates and communication campaigns drive positive business outcomes.

EXPERTS WITH IMPACT™

FTI CONSULTING™

4423-0126