Crossing the Wall

Insights from the M&A and Activism Communications Team

FTI CONSULTING

ARTICLE

The Cyber World turns to M&A

Cybersecurity has become the predominant risk for boards and management teams to address over the past few years. Every day there is new information about evolving vulnerabilities, advancing threat actors and billions of dollars lost. As the cyber world evolves, it is increasingly clear that companies moving through a transaction could be the ideal targets. Corporate leaders need to consider why a deal can draw out bad actors, what risks this poses to the deal itself and how best to achieve success in the face of this new era of cyber threats.

Cyber Risk is Everywhere

It cannot be overstated how prevalent cyber risk has become for corporate America. A recent survey found that nearly two thirds of companies polled had been infected with ransomware in 2021.[1] It is no surprise then that more than 80% of respondents indicated that they were concerned they would be vulnerable to an attack.[2] Research shows that certain cyber attacks have risen 232% since 2019.[3]

Most media will highlight ransomware attacks, making it feel as though that is the only type of cyber risk to consider. While the vivid imagery of a company being held ransom is compelling, it is far from the only risk. Throughout the transaction lifecycle there are all sorts of ways the process can be compromised. Spear phishing, business e-mail compromise, insider threats and digital extortion are other examples of situations that are prominent in mergers & acquisitions.

[1] Culafi, Alexander. "Sophos: 66% of Organizations Hit by Ransomware in 2021." SearchSecurity. TechTarget, April 27, 2022. https://www.techtarget.com/searchsecurity/news/252516423/Sophos-66-of-organizations-hit-by-ransomware-in-2021#:~:text=In%202021%2C%2066%25%20of%20organizations,IT%20professionals%20at%20midsize%20organizations.

[2] "The State of Incident Response 2021." VMware. VMware, June 15, 2022. https://www.vmware.com/resources/security/the-state-of-incident-response-2021.html.

[3] "2022 Sonicwall Cyber Threat Report: Threat Intelligence." SonicWall, 2022. https://www.sonicwall.com/2022-cyber-threat-report/?elqCampaignId=13998&sfc=7013h000000MiQZAA0&gclid=CjwKCAiAgbiQBhAHEiwAuQ6BkmbfNdHZWbIdJBPGBn4ut4T3yR5wDxM6JrGQbSMPEUk4O5ClyAmcVxoC7MsQAvD_BwE.

The Attraction to Transactions

To understand how M&A presents a unique opportunity to cyber threat actors you must first consider the typical aim of these groups: money and information. There are compelling reasons to capture both through every phase of the transaction lifecycle.

Step one is the initiation of a transaction process. This is a highly sensitive time for any organization as it carefully considers its future. Steady maintenance of the business is paramount to preserve optionality, valuation, negotiating leverage, risk identification and much more. This is especially true for private equity firms who have often spent years reshaping a business toward achieving an exit and realizing value for investors. This vital need for stability though only heightens the attractiveness for threat actors who recognize the premium well-funded players will put on stability.

Step two is the announcement of the transaction. Thankfully, once a deal is announced the near-term tensions cited above subside a bit. However, the universe of cyber risks only expands. While a transaction process is primarily private and confidential, a deal announcement is highly public. The massive spike in media attention on announcement day is effectively hanging a sign on your business that reads "change in progress, cyber attackers welcome". Rolling forward to the close of the transaction and subsequent integration, the sign would then read "multiple systems in use, cyber attackers encouraged".

Why is Cyber a Unique Risk?

This begs the question then on why cyber is such a unique risk for dealmakers. Executing a transaction has always come with the inherent risk that one of the businesses involved goes through an unexpected crisis. These traditional types of business disruption risk create clear costs and defined operational challenges. Most of all though, these risks are rare and relatively unexpected. You certainly don't pursue a merger with the presumption one of the assets will explode.

That is where cyber is unique. Right now, it is so pervasive that companies would be well advised to presume it will be a real risk to mitigate. In fact, the FBI's Cyber Division issued a Private Industry Notification (PIN) alerting market participants that significant financial events facilitate targeting and extortion of victims.[4] That creates a series of issues for dealmakers to consider beyond the traditional cost and related business disruption of a traditional crisis matter.

When it comes to the transaction lifecycle, there are also particular risks around disclosure, loss of time and integration that these cyber events create.

How to Prepare

If dealmakers need to presume that cyber risk will occur in the transaction lifecycle, then how can you better integrate risk mitigation steps into the deal process?

First and foremost is an acknowledgement that most organizations remain poorly prepared. In fact, 56% of organizations do not have a cyber incident response plan, and only 32% think their plan is effective.[5] In short, either you, your transaction partner or both have not fully considered how to respond to a cyber event, let alone how to do so within the framework of a deal. Companies that have a cyber specific crisis communications plan tend to manage stakeholder communications more successfully. Those who have stress tested their plans or conducted tabletop exercises fare far better. Dealmakers should also consider the following when looking to mitigate cyber risk in a deal:

- **Due Diligence –** Cyber due diligence is a rapidly emerging field. It is a must have on any transaction evaluation task list. However, that work should not simply go on a shelf waiting for the integration teams down the road. This due diligence is not identifying potential risks, it is creating an understanding of presumed risks for the deal team.

- **Culture of Cybersecurity –** Unlike most crisis events, cyber is a risk that the entire deal team inherits, including advisers. Anyone made aware of the potential transaction becomes a potential vector

[4] "Private Industry Notification." Federal Bureau of Investigation – Cyber Division. November 1, 2021 https://www.ic3.gov/Media/News/2021/211101.pdf

[5] Lukehart, Ashley. "2022 Cyber Attack Statistics, Data, and Trends." Parachute. Parachute, March 25, 2022. https://parachute.cloud/2022-cyber-attack-statistics-data-and-trends/#:~:text=56%25%20of%20organizations%20do%20not,an%20effective%20data%20breach%20response.

of vulnerability. This calls for corporate leaders to instill a culture of good cyber risk hygiene at the start of the process. For example, think about the use of code names over email and text, considering where documents are stored and how documents are encrypted.

- **Leaks –** For any large transaction, speculation in the press ahead of a deal announcement is basically a fact of life. This is particularly true for auction processes of PE assets. While there are pros and cons to this sort of media coverage, dealmakers need to start accounting for cyber risk in those calculations. If a story were to run, is the company and its advisers prepared for the attention it will draw from threat actors?

- **Rapid Response Plan –** Any good transaction process will identify a rapid response plan that identifies potential leaks, activist comments, interloping bidders, etc. It is vital that these plans now incorporate potential cyber events during the transaction lifecycle. This includes a framework for how the acquirer, target and seller will communicate the attack and coordinate the response during the pendency of a deal.

The global pandemic has forced the rapid acceleration of technology adoption in every aspect of our lives. This unlocked incredible benefits, but brought with it a wave of new risks. The transaction world is no exception. It's time to

---

PAT TUCKER
Senior Managing Director
646-578-6877
pat.tucker@fticonsulting.com

MEREDITH GRIFFANTI
Senior Managing Director
571-275-1495
meredith.griffanti@fticonsulting.com

DAVID DUNN
Managing Director
267-253-0829
david.dunn@fticonsulting.com

EVAN ROBERTS
Managing Director
646-642-9277
evan.roberts@fticonsulting.com

BRIAN WALDMAN
Managing Director
914-215-4746
brian.waldman@fticonsulting.com

ORLA COX
Director
+353 1 765 0800
orla.cox@fticonsulting.com

KATE PULIO
Director
312-315-9352
kate.pulio@fticonsulting.com