When cyber threatens M&A

Buying another company means taking on its digital operations, which can pose fresh and potentially deal-altering cybersecurity risks.

These threats can jeopardize a deal’s anticipated value unless the acquirer identifies and addresses them early in the process.

Cyberattacks on companies can do more than violate laws and regulations. A business that is being acquired or generally exploring a sale typically wants a maximum return, and the acquirer wants to make sure its target is valued appropriately and is a sustainable asset. Insufficient investment in cybersecurity and digital infections can hamper or even kill those goals by reducing the value of the target’s assets, damaging its brand and derailing its growth prospects.
Many executives say data breaches, especially public ones, can lower a deal’s valuation. That was evident in Verizon’s acquisition of Yahoo, which closed in 2017. After Yahoo’s disclosure of two massive breaches in previous years, Verizon cut its offer by $350 million, or about 7 percent of the original price. In addition, the part of Yahoo that wasn’t sold to Verizon agreed to assume 50% liability from any future lawsuits related to the data breaches.

And the goal can be more than a simple data grab. Consider a pharmaceutical company’s formula for a drug, a manufacturer’s product design or a distribution company’s transportation model. All of that is intellectual property that can be a crucial part of a deal’s value.

The risks for an acquirer in this environment are increasing. An acquisition that has existing cyber vulnerabilities can be used by threat actors to obtain access to the acquiring company as the integration progresses. The period between a deal’s announcement and closing is of particular exposure if vulnerabilities exist, given the heightened awareness and opportunity. That potential can raise anxiety among stakeholders—including investors, shareholders, customers, employees and suppliers—bringing further risk of disruption.

While cyber threats are more prevalent, it’s still rare for a breach or other issue to harm a transaction to the point that an acquirer completely walks away; delaying the transaction is a more common result. Yet delays, added costs and questions about a target’s value all have consequences for the deal process. To avoid such damage, acquirers need to understand the cyber risks of the target so they can limit surprises, model appropriately and ensure a reasonable transaction.
Knowing the cyber risks in deals

Once a transaction comes into focus and an acquirer is trying to determine the target’s real value, it needs to address two key areas: security and synergy.

**Security: History, controls and assets**
An acquirer should expect to know the details of any significant cyber events—not just breaches—and their impact on the target company. This includes incidents that may not have been shared publicly but still affected the company. What cybersecurity controls were in place at the time, and how have they changed?

How a company protects its data and intellectual property and the potential for future theft are crucial for confirming its value in an acquisition. An acquirer needs to know those controls are adequate or understand what investment will be required to improve them with the current cyber risk profile of the target.

Not all threats are external
This assessment also must consider the target’s vendors and contractors—each of which could create security gaps. An acquirer should be aware of any agreements in which third parties handle company or customer sensitive data, critical IT business processes, payments or other technology work.

And don’t forget risks around employees who may be disgruntled or worried about losing their jobs due to a transaction. More than unknown hackers or competitors, current and former employees were cited as top sources of security incidents in PwC’s latest Global State of Information Security Survey.4

Sources of security incidents

- **Current employees**: 30%
- **Former employees**: 26%
- **Unknown hackers**: 23%
- **Competitors**: 20%
- **Current third parties**: 19%

*Includes suppliers, contractors and consultants

---


---

85% of consumers

92% agree companies must be proactive about data protection.

---

won’t do business with a company if they have concerns about its security practices.
**Increased connectivity extends threats**

The critical information assets at risk of affecting deal value have expanded along with the cyber threats. Details about a company’s customers still can be valuable if stolen in bulk, while a single piece of proprietary technology, application source code, valuation models for future business development, product formulas or other intellectual property might command a high price if it’s truly unique. But businesses now face new, downstream risks, thanks to increased connectivity within companies and with customers.

For instance, today’s manufacturing supply chain is digitally interconnected – using process automation, specialty robotics, suppliers monitoring raw material levels in real time and logistics providers tracking the delivery of finished goods to customers or markets globally. This digital supply chain has incrementally increased the cyber attack surface and is only as strong as each link. These risks can even extend to specific products, with the potential for firmware to be compromised at supplier locations. As a result, the primary manufacturer in that situation needs to establish a strong third-party risk program. These risks should be considered during the deal process.

**Synergy: Compatibility and integration**

Even if an acquirer is confident that its exposure to threats is minimal, cyber issues can affect deal value in other ways. Beyond the question of weak vs. strong, cybersecurity diligence needs to determine how similar or different the target’s systems and protocols are from the acquirer.

This alignment or lack thereof can be crucial in strategic acquisitions and large deals. If cybersecurity integration activities aren’t identified and factored into the transaction on the front end, gaps between IT, cybersecurity and other business operations can slow integration and add costs, cutting into the efficiency and financial gains from the deal.

The overall deal structure has a big impact on how to plan for cybersecurity. The buyer has several operating models to consider from a deal structure perspective and could choose to continue the legacy programs at the target—for the short term or indefinitely. The buyer can also choose to integrate the companies and take the best of breed from the legacy security capabilities. Without careful and timely planning, unexpected costs could inhibit synergies and the realization of the deal’s benefits.
Taking action to limit cyber risks

While transparency is the goal, full visibility into each party’s operations is virtually impossible for companies engaged in a deal. The M&A process typically doesn’t allow much time to assess the complete state of cybersecurity at a target, and in some cases, such as an auction, access to the target can be severely limited. Absent that, there are steps an acquirer can take to reduce the potential financial costs from cyber issues.

On one recent deal, for example, target management represented that they complied with the Payment Card Industry Data Security Standard (PCI DSS) and provided supporting evidence. However, a review of the target in-store point-of-sale (POS) technology and their PCI documentation clearly showed both needed significant investment.

The POS technology was no longer supported by the vendor and couldn’t achieve compliance with the PCI DSS standard, which is required as of the first quarter of 2018. The impact of these identified issues required an additional investment of more than $2 million to upgrade the POS platform, its supporting technology and additional cybersecurity measures to maintain compliance.

Interpreting imperfect information

Cyber due diligence is similar to that for the Foreign Corrupt Practices Act and anti-bribery and anti-corruption issues. In these situations, a buyer must assess risks and vulnerabilities with imperfect information, yet it fully inherits the actions—or inactions—of the target. As a result, there could be a need for immediate remediation after the deal closes, or even between signing and closing.

In addition, because cyber events can go unnoticed for months if not years, traditional protections like representations and warranties can be ineffective. The parties in a deal may believe in good faith that all’s well, unaware that a significant threat could lie beneath the surface and may not emerge until well after closing. After TripAdvisor acquired travel site Viator in 2014, its payment card service discovered unauthorized charges on customer credit cards. Ultimately, the company learned that hackers had stolen information on 1.4 million customers.

Cyber due diligence should focus on these key areas

Security operations

Third-party risks

Cyber governance

Technology platform

Information asset value

Acquirers face four critical questions during cyber due diligence

1. Can the cybersecurity controls meet current and future needs?
2. How mature are the cybersecurity controls and countermeasures?
3. Has there been a breach, and will unknown cyber risks be introduced?
4. Is the intellectual property secure, or is it impaired?

USA Today, PayPal shelled out $238 million for company that may have had 1.6 million customers breached, Dec. 4, 2017
Payment Week, TripAdvisor’s Viator Data Breach Affects 1.4 Million Customers, Sept. 26, 2014
**Understanding cyber due diligence**

Acquirers should first take a risk-based approach to cyber due diligence in deals. As noted earlier, cyber due diligence isn’t as established nor does it analyze standardized data as other types of due diligence. Since all deals aren’t the same, they don’t require the same level of diligence.

An acquirer should have a process to evaluate the current threat landscape and identify the bad actors — external and internal — that might target the parties in the transaction. This landscape can vary by industry or region, and higher risk transactions — such as acquisitions in certain countries or in sectors that have suffered recent attacks — require greater diligence.

**Frequency brings flexibility**

The more active a business is in deals — such as serial corporate acquirers or private equity firms — the more cyber should be woven into the typical deal life cycle. Frequent acquirers should have established relationships with cybersecurity stakeholders within their firm and have a flexible cyber deals playbook to assist with cyber at each deal stage, cyber risk level and deal type. This allows those acquirers to engage cybersecurity at key points in a deal life cycle and to more effectively manage cyber risk to targets and their existing portfolio. Instead of relying solely on data provided by an M&A target, analyzing information available from outside the target is becoming increasingly valuable to understanding cyber risks.

Another outcome of managing cyber risk in deals is establishing a benchmark of cyber readiness, which can be applied to other businesses in their portfolio and used when assessing new investments. Some will conduct an annual security assessment of their portfolio companies, further preparing them for future deals.

**The need to identify and quantify**

Cyber due diligence also should reveal deal-breakers — or more likely, deal-changers — for the acquirer. Walking away altogether may be unlikely, but there may be issues that lead a buyer to reconsider the target’s value — and therefore price. An acquirer needs to be able to identify and quantify those issues and either push the target to address them before closing or renegotiate the price and possibly other terms.

The latter could be an opportunity to shift seller proceeds to remediation investment, but the acquirer needs to plan for how the issue will be addressed — and paid for — after closing and during integration. Still, the potential to shift burden to sellers may appeal to serial acquirers who are making smaller deals and are confident they can manage the risks.

Ultimately, successful cyber due diligence should yield not only a road map of critical remediation items but also the responsibility for, cost of and timeline for resolving each item.

---

**Source:** Donnelley Financial Solutions/Mergermarket survey, September 2017

---

**64%**

say cybersecurity issues are more difficult when the acquisition target is in a different country.

---

**Cybersecurity**

- **Regulated and sensitive data security controls**
- **Security and privacy controls in products and services**
- **Security controls for protection and detection**
- **Third-party security risk management**
- **Data privacy program**
- **Cybersecurity program**

To mitigate cyber risks in M&A, acquirers should assess target companies on six main areas.
Mechanisms that mitigate cyber risks

As much as they’d want full transparency, acquirers often don’t have direct access to all of the information that’s crucial for determining a target’s real value. To gain visibility into key data and other material, an acquirer and target can sign a non-disclosure agreement (NDA) and allow an independent consultant to evaluate the target and provide recommendations without sharing confidential details or proprietary information. An NDA may even be required—instead of optional—for areas such as technical testing or product code reviews.

“Clean rooms,” where independent parties can analyze key data and sensitive information, have become increasingly important for minimizing cyber risks.

Further protection for acquirers can come through transition services agreements (TSAs). TSAs are common in deals, but they only recently have started covering cybersecurity issues. Through a TSA, an acquirer and target can negotiate how the target will manage cybersecurity during the transition and the conditions under which the responsibility will shift to the acquirer. The latter can be crucial if due diligence has revealed any significant cyber issues that could decrease deal value.

Mining other intelligence

Beyond tools that are part of the deal process, companies can seek information elsewhere. Various external streams of data and information can be analyzed to produce reliable intelligence that can reveal potential risks. For instance, searching the “dark web” could unearth employee credentials and communications or product design documents that provide evidence of a breach or potential impairment of critical assets. It may also provide indicators of yet-to-be-detected breaches or attempted breaches.

Broader intelligence on cyber issues is available through information sharing and analysis centers and organizations (ISACs and ISAOs). These groups allow companies to share with each other information on digital threats and ways to combat them. ISACs originally were created in a few industries, most notably financial services and aerospace and defense. ISAOs build on the concept by spanning sectors to share expertise and experiences among broader communities of interest.

Gaining better insight into current cyber issues can help an acquirer know what to look for in assessing a target and determining its value. While interest in ISAOs has grown in sectors such as healthcare and energy, others that are highly competitive or have significant intellectual property—such as pharmaceuticals and medical devices—may be wary of substantial collaboration. That could be one reason why ISACs and ISAOs haven’t yet played a regular role in helping acquirers calculate a target’s value.
Next steps for dealmakers

For a transaction to proceed with an understanding of the cyber risks, an acquirer must incorporate cyber issues into its assessment of a deal target. With this insight, the risks and cost can be factored into the deal model, negotiation and Day One planning. This includes understanding key cyber risk indicators, including:

- The state of the target’s cybersecurity program, the compatibility and resiliency of its IT operations to cyber incidents, and which applications are vulnerable to attack—and by whom.

- The amount and nature of data and information the target is responsible for, what is most sensitive and valuable, and how it is protected.

- If and how the target complies with government regulations and global privacy requirements, and if that compliance adequately guards against industry-specific or other cyber threats.

- The costs of addressing the above concerns and the impact not only on deal negotiations and pricing but also the acquirer’s business, brand and reputation going forward.

Focusing on these areas during a deal will help minimize the chances of digital disruption that could create additional challenges—in the short or long term—and result in an acquirer regretting what once was a promising deal.

Contact us
For a deeper discussion about these issues, please contact:

Todson Page
Partner, PwC Deals
+1 408 817 1223
todson.page@pwc.com

Quentin Orr
Principal, PwC Cybersecurity and Privacy
+1 267 330 2699
Q@pwc.com

Contributors
Curt Moldenhauer, Partner, PwC Deals
John Potter, Partner, PwC Deals
Mike Cunning, Managing Director, PwC Cybersecurity and Privacy
Lorenzo Falciani, Manager, PwC Advisory Services
Jefferson George, Editor-in-Chief, PwC Deals

www.pwc.com/us/deals

© 2018 PwC. All rights reserved. PwC refers to the US member firm or one of its subsidiaries or affiliates, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. 422595-2018