M&A and Cyber–Eyes Wide Open

Asking the right questions to gain clarity around cybersecurity

Adam Golodner
Global Cybersecurity & Privacy Group Leader

Today, cyber issues are top of mind around the world. Strikingly, the United States has declared that cyber is the number one national security threat to the U.S. It is also an economic security issue. The European Union, India, China, Russia and Brazil are all in various stages of adopting new cyber laws and policies. The issue has top priority at the World Economic Forum, the Business Roundtable and the Chamber of Commerce.

Cyber is certainly about nation-state-to-nation-state intelligence activity, but it is also about the theft of intellectual property, threat to critical infrastructure, sale of consumer data, disruption of service, destruction of data or assets, loss of confidence and brand value, and the publishing of sensitive information. It is also about the state of the cybersecurity of entities—their networks, policies, procedures, culture, supply chains, preparedness and resiliency.

Cyber is, therefore, a core issue for M&A and M&A due diligence. In today's cyber world, you have to ask many questions, and then consider and understand the answers. For example:

- Does the target truly "own" the intellectual property key to its competitive advantage, or has a country or competitor already exfiltrated a copy?
- Does "marrying" the target's IT network make your company's technology infrastructure more vulnerable? If a new IT company is also involved in the merger, what's the security effect of integrating its hardware and software into your product set?
- What about the target's relations with governments? Will it affect your company's ability to sell your current products or the newly acquired products? And, seen through the global cyber lens, what will it mean to your company's reputation?

But the risk is manageable. Comprehensive cyber due diligence can help you understand the questions you need to ask, get answers, form opinions and narrow the risk aperture for the deal.

In short, today M&A players have to go into the deal with their cyber "Eyes Wide Open."

Road Map

To appreciate cyber risk, one must understand where the target and acquiring companies sit in the cyber ecosystem. Cyber is a global three-dimensional chess game with players from industry, governments, criminals and nongovernmental actors. Some products, services and markets matter for national and economic security

The areas you must investigate include the culture of the company, the state of their networks, the protection of their IPR, the assurance of their products in a tech deal, and their political and policy relationships.

(critical infrastructure and innovation industries), while some matter for consumer protection (retail and health and consumer finance). The adversaries of some companies may be governments, but for others they are criminals or hacktivists, and the techniques used by each can vary based on desired outcomes.

For any particular merger, one must first analyze this chess board in order to understand what really matters. The areas that require investigation include the culture of the company, the state of their networks, the protection of their IPR, the assurance of their products in a tech deal, and their political and policy relationships. Let's examine each of these in greater depth.

Culture

It's important to understand if the company has a "culture of security." Does security matter to it, and has it put in place people, processes and technology to manage cyber risk across its enterprise? If not, a hard slog may lie ahead.

The following questions will clarify the company's cyber culture:

- Is the board of directors involved in cybersecurity, and in what way? How about the CEO—does he/she stress its importance, and how does that manifest itself?
- Who "owns" cyber for the company? Is there a cross-functional team in place for risk management, enforcement and response?
- Has the company identified its "crown jewels," and what IP deserves priority protection?
- Are there security and privacy policies in place, and are they updated and enforced?
- Has the company experienced cyber threats in the past? What is the history of nontrivial cyber threats?
- What about employee training, communications and enforcement? Does the company prioritize cyber?
- Does the company have cyber insurance? What's covered, and is it sufficient?
- Is the company using existing best practices like the NIST Framework, ISO or some hybrid—if not, why not?
- Are business unit leaders responsible (and accountable) for cyber in their departments? When they plan new services or products or infrastructure, do they account for cyber risk? What are its current and past possible liabilities for cyber incidents?
- Does the company participate in public-private partnerships for cyber in their industry? What is its relationship with cyber law enforcement?
- Does the company understand cyber threats and their consequences on current and planned businesses—does the company "think like a bad guy?"

Although they are not "deal breakers," these and other enterprise-specific questions (and review of related documents and written and oral responses) can provide a sense of whether the company has a culture of security. Of course, the acquiring company will have its own culture of security—or not. Keep a keen eye on how these two approaches mesh. What will the merged company look like from a cyber culture perspective?

Networks

The merger of IT networks can have a profound impact on the success of an M&A transaction. One must understand the networks, topology, geography, service providers, vendors and cyber status and history. In essence, the question is "you will be connecting what to what?!"

Here, questions to ask include:

- What does the network topology look like? What kind of kit does the company use for what and why?
- Who are the service providers by geography?
- What are the points of ingress and egress?
- What is the history of cyber incidents? Of nontrivial incidents?

- What are the ongoing issues? How did the company find out? What did the company do when it found out? Has it done audits, assessments or PEN testing?
- What IT vendors does the company use and would you use them?
- Has the company classified its data sets and bases for priority?
- What do the practices look like for "crown jewel" protections? For non-"crown-jewel" protections?
- Where is the data?
- What are network configurations and conditions for the cloud and mobility?
- What are the company's top 5 new security initiatives?
- Will the two networks be interconnected? When and how?
- What changes will be needed to merge the networks securely?

In addition to the usual IT issue sets, understanding the network issues from a cyber perspective will provide a realistic view of the costs and benefits of the proposed transaction. A third-party review of the networks, which could be hands-off or -on will enhance this perspective, as will consulting with cyber services companies that may be able to provide a view about what company traffic or data is out on the net.

IPR

Often, intellectual property is the core motivator for a deal. To the extent pre-patented intellectual property, trade secrets, business methods, IPR that is otherwise not public, strategic plans and roadmaps, data and any other nonpublic assets really matter, it is important to understand the cyber risk, status, and history of this property.

Given the fact that it is very hard to stop a determined adversary—particularly a determined nation-state—it is important to know whether that IPR has already been compromised, in what way, and whether it matters. Even if some core IPR has been stolen (copied), it may not be a show stopper, but it might affect the value placed on those IP assets. Sometimes, even if a government, competitor or criminal had nonpublic or protected information, without other know-how the competitive value may be limited. In other cases, however, adversaries could put a company out of business, particularly if the new competitor is subsidized by a nation state.

Bottom line: if something would be a "crown jewel" post-acquisition, ask very pointed questions around its cyber status and history, and the methodologies (or not!) that have been used to protect that asset that is core to the deal's raison d'etre.

Products

If the deal is a technology transaction in which hardware or software is involved, there are an additional set of questions that are useful for due diligence. The questions will vary depending on whether the plan is to integrate the acquired technologies into existing products or sell them stand-alone. In either case, it is important to evaluate security of the hardware or software to be purchased, as well as any geographic sensitivities.

Although products contain vulnerabilities, the awareness by the target company about the state of product assurance, activities to address vulnerabilities and reduce instances of exploitation, and activities to achieve product certification can all form a view about the security of the product to be acquired.

Some questions to ask include:

- Does the company have secure development practices, and are they memorialized in writing?
- Is there a security review before shipping? How does this review impact the decision to ship product?
- Are there records of the internal product evaluation pre- and post-shipping? What tools do they use for product evaluation (e.g., static analysis, fuzz-testing, or certification)? What's the process for addressing the test results?
- Are the products' Common Criteria evaluated? Is the encryption FIPS validated?
- Is there a product security incident response team? What is the method for notifying customers? What is the backlog for bug fixes?

- Is the software proprietary? Open Source? If so, what's the method for updating OS fixes in code?
- What are the product (HW/SW) supply chain security protocols? What function does the HW/SW perform for customers? What other HW/SW does the product often interoperate with in a typical system architecture?

The answer to these and deal-specific questions about products will help inform the benefits and value of the deal and will help you unearth potential problems with specific customer sets. It will also provide a better understanding of additional engineering work that may be required to put your name on the product and integrate it into your own product development and incident response activities. In may also inform any decision to leave the acquired product under its own brand for a period of time.

> Bottom line: if something would be a "crown jewel" to you post acquisition, ask very pointed questions around its cyber status and history, and the methodologies (or not!) that have been used to protect that asset that is core to the deal's raison d'etre.

Geopolitics

With cyber as a top line issue, it is critical to consider how governments globally will perceive a merger or joint venture or other deal, as well as any potential spillover effects with both the government and enterprise customer base in those countries. This was true before Snowden, and it is even more important post-Snowden.

It is also critical to understand the relationships the target has with governments, which governments, and with regard to which issues. It is also important to understand how each government would perceive these relationships.

The networks, intellectual property and/or hardware and software implicated in any deal may be something governments care about, and the acquiring company has to understand the domestic and geopolitical implications and impacts of the deal for existing and potential customers.

To the extent there are concerns, there are often ways to structure deals to reduce the cyber risk of core care-abouts of government actors.

Operational-Security

In addition to the cyber due diligence required to understand and manage cyber risk in transactions today, parties have to employ good operational security to protect the deal or potential deal itself. To the extent a deal strategy was revealed to the other party, or another party bidding on the same deal, there would likely be an appreciable cost in loss of strategic advantage. Therefore, all the deal parties and advisors should put in place good operational security. Have an op-sec plan, and stick to it.

Conclusion

The value of companies, products and services are wrapped up in in the IT systems, data and information that allow the enterprises to run and gain competitive advantage. It is no longer safe to assume the cyber status of a target company or to understand it superficially. Governments, partners and customers all care about the cyber footing of companies in strategic and important industries. Perhaps most important in a proposed transaction is the value of the target asset. With superior cyber due diligence, one can move forward with "Eyes Wide Open" and understand the true value of the target now and after the transaction closes.