KAYE SCHOLER

Spring 2014

M&A and Corporate Governance Newsletter

The Need for a Holistic Approach to Global Cyber Issues

Adam M. Golodner Partner

As the issue sets in cyber become more complex and global, companies have to take a cross-cutting, holistic approach to understanding and dealing with the cyber issue. From a legal perspective, there are four broad categories of issues that leaders in companies need to think through and address: public policy, litigation, corporate governance and transactions. Often the issues are interconnected, and an action in one affects the other. In this piece, "cyber" refers to security and privacy issues that affect enterprise and network operations, information and treatment of information, and have an impact on governments, partners, customers and consumers, globally. This is a big and complex set of issues, and the intent here is not to delve deeply into each one, but to share a lexicon for thinking through these cross-cutting issues around policy, litigation, governance and transactions.

IN THIS ISSUE

Public Policy

Governments around the world are all trying to figure out what to do about the cyber issue. All at about the same time. In the US, the Director of National Intelligence has called cyber the number one national security threat. President Obama has talked about it as both a national security and economic security issue. With over 85 percent of the critical infrastructure (communications, IT, financial services, electricity, energy, transport, health care, etc.) of the country owned by the private sector, the government needs to, and is, working through the quintessential public policy question—what is the proper role of government vis-a-vis the private sector in cyber? How do we achieve national and economic security—and innovation?

More fundamentally, companies have to have a vision, a view, a policy, a true North for cyber that works globally.

But it's not just the US working through this issue set. At the same time, the European Union has legislation pending in the European Parliament (based on a European Commission proposal that would regulate all critical infrastructure for cyber); India has regulations pending on service provider networks and is working through other critical infrastructures; China has enacted its Multi-Level Protection Scheme of regulation for broad sectors of the economy; Korea is looking at cloud regulation, as is Brazil; and the whole issue of Internet governance and who should "own" or "control" the Internet into the future (essentially ICANN or the ITU) is one of the hottest and most important issues this year. And, of course, the developing Pacific and European trade agreements are looking at cross-border data flows and regulatory conformance.

All of this is happening with the backdrop of the reporting based on leaks related to Mr. Snowden, and significant government-to-government and industry-to-government discussions on the issues of security, privacy and trust—and what the global rules of the road look like going forward. Suffice it to say, a lot going on in cyber.

For companies, the solutions and their advocacy must be, by definition, global. The Internet, enterprise networks, business models, markets, technology, and the underlying standards and protocols (IETF, IEEE, ICANN, ISO, Common Criteria) are global. If, as Tom Friedman says about the broader economy, 'The World is Flat," and regardless about what lumpiness you might otherwise believe—the policy world really is flat. A proposal made in DC in the afternoon is noted and compared in Beijing in the morning. More fundamentally, companies have to have a vision, a view, a policy, a true North for cyber that works globally. You cannot advocate one thing in one capital and another a millisecond away in another. Nor should you.

If the issue is continuing to have the ability to drive innovation into your product sets and the network, or securing your global infrastructure or intellectual property, or providing secure services based on cloud and virtualization and big data, you need to advocate for and obtain global rules that allow you to do all these things, while at the same time understanding the security and privacy concerns of the governments globally. It is possible.

Perhaps not simple, but certainly achievable and critical to the future of global information technology and communications into the future.

The rules are being written now, and when written will likely have long-term effects. Leaders in companies would benefit from engaging in discussions about cyber, understanding what's core to them and their shareholders, employees and partners, and charting a strategic path and action plan to help ensure a global, interoperable, secure and innovation-driven future.

Litigation and Investigations

In addition to the policy issues corporate leaders need to think through, cyber has created a whole set of litigation issues as parties and governments set out to assign obligation and liability when things go wrong in cyberspace. The issues range from criminal (what was done to you, what can you do), to regulatory (FTC, FCC, DoJ, DoD, ITAR, Exports, HIPPA, SEC—and then to global and State equivalents), to US Constitutional (search and seizure, privacy, speech, association), and, of course, civil (tort, contract and loss of intellectual property). Some of these duties and obligations are being assigned in the ongoing global policy discussions. And some are the stuff of current headlines, like "data breaches" at retail chains, universities and hospitals, and governmental organizations ,that cause consumers to wonder about the security and privacy of their information on line. Given the wide-scale effects of data breaches and treatment of data, many of these cases are class actions, and we are starting to see shareholder derivative lawsuits against directors and officers.

In addition to the policy issues corporate leaders need to think through, cyber has created a whole set of litigation issues as parties and governments set out to assign obligation and liability when things go wrong in cyberspace.

In each of these categories of litigation, understanding technically what happened, the global and technical implications for the company for taking a particular legal position, the priorities and care-abouts of governmental actors, and what's the right application of new cyber facts to underlying laws and principles—are all quite important as many of the issues can be cases of first impression. In the cyber area, as in others, the use of internal investigations to understand what really happened, and how to redress and address issues can be helpful, particularly where the company's relations with governments, core customers and brand are involved. Action that indicates how seriously the company takes security and privacy is, in fact, meaningful. And, like in other areas, communication is key. When appropriate, like in publicly reported data breaches, explaining to the public, government leaders, employees and partners what happened and what the company's response and recovery plans are can be crucial to retain the value of the company's brand and confidence in its leaders. Deciding what to bring, how to defend and the interdependencies of the players and technologies is not simple, and requires a holistic understanding of the cyber playing field.

Corporate Governance and Compliance

Cyber is now recognized as a board-level issue. In part that's because of the intense governmental national and economic security issue globally. But it's more than that. At its core, cyber is about maintaining and driving competitive advantage. Given the integration of IT into core business processes, and the productivity gains, and transition of business models to IT-enabled services, the actual ability to deliver core services is also about IT and cyber risk. Further, for technology and many other types of companies, a company's competitive advantage is tied to innovation—and innovation is tied to its intellectual property, and the theft of intellectual property and innovation is a real, ongoing activity, and a top-level concern of companies, shareholders and governments. And, of course for technology companies making hardware and software products and services, cyber and security and trust in their products is core to the future of the business.

So what to do? First, companies clearly have to manage the cyber risk. Put in place best practices to secure systems, intellectual property, customer data and product assurance. Create and follow internal security and privacy and IPR polices, assign owners and leaders, and train employees. Ensure security-incident response, recovery, communications and escalation plans are in place and exercised. Understand who your partners, suppliers and distributors are. Put in place cyber threat information-sharing arrangements with others in your industry. Make sure the CIOs and CISOs have the resources they need, and frequent interactions with leadership. Understand the litigation risk (both as to loss of information, failure of service and theft of intellectual property), take steps and build compliance to demonstrate risks have been addressed. Insure against corporate, officer and director risk.

But in addition, and more than that, companies have to go through the hard work of identifying which assets and processes are core to its competitive advantage—are most valuable (intellectual property, customer data, ability to provide x service, brand) and prioritize those assets of highest value, and build out real security, mitigation, and response and recovery around those prioritized assets. You may not be able to secure everything, but you can prioritize, figure out what's of greatest value, and continually do your best to protect that core.

As in other cyber issues, given the complex global technology, legal, policy and geopolitical issues, an interdisciplinary approach with deep experts is key.

Transactions

There are five primary sets of cyber issues in transactions. First, governments and companies may care about the existence, treatment and security of hardware or software in cross-border deals, whether reportable or not under the rules for Committee on Foreign Investment in the United States, or Department of Commerce export controls and Department of State ITAR. Second, data today is a thing of value, and in any transaction—cloud, third-party vendor, mobile application, outsourcing—the security and privacy of data today and in the future should be understood, negotiated and agreed upon. Third, in any contract for essential services—communications, electricity, financial services, data center, supply chain, distribution—the security of the service provider needs to be understood and agreed upon. Fourth, in any merger or acquisition, the security posture, state of systems, contingent liabilities, culture, third-party agreements, governance and compliance need to be part of due diligence and undertaken by experts. And fifth, most cyber experts say, it's not "if" you've had a cyber issue, but "when" you've had it and if you "know" it. So, in transactions and agreements, it's important to agree on a process for dealing with the issue in case something happens, and then when and if something happens, the parties have a path forward for resolving or moving through the issues together.

Conclusion

Leaders in companies are faced with a wide range of interrelated cyber issues today. Given the global nature of networks, and the intense and important attention of government leaders and customers and consumers globally, leaders must view the issues holistically and understand that often seemingly disparate issues are interconnected and can take on a life of their own. This is a classic area where an interdisciplinary approach is called for. Often, policy merges into governance that can merge into litigation or a transaction. Seemingly disparate issues merge, where often there is a separate corporate owner. Leaders who think about these issues in holistic and interrelated ways will be able to understand them, seek proper counsel and move through the tough issues with a clear sense of direction and effect.

Adam M. Golodner
Partner
adam.golodner@kayescholer.com
+1 202 682 3575