Perspectives on Cybersecurity and Its Legal Implications

A 2015 SURVEY OF CORPORATE EXECUTIVES
The National Institute of Standards and Technology (NIST), a non-regulatory agency of the US Department of Commerce, released its “cybersecurity framework” in February 2014 to help regulators and businesses identify and mitigate cyber risks that could affect national and economic security. The need was urgent. According to the Ponemon Institute’s 2014 Cost of Data Breach Study: Global Analysis, the total average cost per data breach for US businesses was in excess of $5.85 million. Unsure of Congress’ ability to respond quickly with effective legislation to address the myriad issues surrounding cybersecurity, companies are developing their own cyber risk management protocols.

Survey Background and Participants

In an effort to gauge industry concerns and measure corporate responses to these significant privacy and security threats, Mayer Brown conducted an informal survey of key executives and corporate counsel in 15 industry sectors between mid-November 2014 and mid-February 2015. The majority of the companies were from finance and financial institutions, professional services (law, medicine, accounting, architecture and design), utilities and energy (including extraction), health care and pharmaceuticals. While two-thirds (70%) of the respondents’ companies have a chief information officer (CIO) or both a CIO and a chief privacy officer, one-fifth (21%) of the companies had neither.

Summary Analysis and Outlook

Survey respondents overwhelmingly considered the disclosure of personally identifiable information as the biggest cyber-related threat to their companies (63%). Concern about interruption of business operations such as system sabotage ranked second (24%). Less than 10% of the respondents considered theft of trade secrets as the most serious threat. Most respondents (63%) considered cyber issues to be just one more cost of doing business or that these problems can be overcome. Well over half (57%) of the respondents estimated that litigation risk posed by cybersecurity issues has a relatively modest impact on their cybersecurity planning. For some, pessimism reigns. Around 29% of respondents have a negative outlook on cyber-related issues, believing that cybercrime will always be one step ahead of legislative protections and enforcement.

The survey revealed that respondents’ concern about the adverse impact of regulatory enforcement appreciably affects their willingness to share incident information with the government. Liability protection is a critical component of a voluntary cyber information-sharing program. Without meaningful liability protection, companies will be hesitant to participate because any act or omission made by a participant based upon cyberthreat information received by that entity could subject it to liability. This concern may also explain why only 23% of respondents said that their company had built a close working relationship with either a government enforcement agency (FBI, US Secret Service) or a prosecutorial agency (DOJ or state attorneys general) on cyber issues. An equivalent percentage (23%) reported working closely with industry regulatory (FTC, FCC, FDIC, CFPB). Over 40% said “no, they have no such relationship,” while approximately 24% did not know.

The survey showed that 84% of respondents expect clear national standards on data breach notification to emerge within the next five years. Smaller numbers expected national standards for securing personally identifiable information, investor disclosures and liability protection for information sharing.

This may reflect a growing recognition in Congress that having 47 different reporting standards does not make sense. Given the number of breaches that have occurred in recent years, it makes sense to instead have a clear set of standards, not just for notification but for information security as well.

Nearly 50% of respondents weren’t sure if the NIST Cybersecurity Framework has been helpful to their company in managing cybersecurity risk. This may indicate that it is premature to judge the NIST Framework, or that companies are not sufficiently aware of how it is meant to be helpful. Mayer Brown has published an informative overview which can be found at: http://www.mayerbrown.com/The-NIST-Cybersecurity-Framework-Overview-and-Potential-Impacts/.
Full Survey Results

Question 1:
Does your organization have a Chief Privacy Officer ("CPO," or equivalent) or a Chief Information Officer ("CIO," or equivalent) who is accountable for developing, implementing and maintaining an organization-wide governance and privacy/cybersecurity program?

- Chief Privacy Officer ("CPO" or equivalent): 33%
- Chief Information Officer ("CIO" or equivalent): 37%
- Both a CPO and a CIO: 4%
- Neither a CPO or a CIO: 21%
- Don’t know the answer: 4%

Question 2:
How would you describe your outlook on cybersecurity issues? For this survey, “cybersecurity issues” could include breaches, attacks, denial of service, loss of data, and/or damage to cyber infrastructure.

- Optimistic, we’re catching up with or getting ahead of the problem(s): 27%
- Pessimistic, the problem(s) will always be one step ahead: 29%
- Neutral, cyber-related issues are a cost of doing business: 36%
- Don’t know the answer: 9%
Question 3:
Which do you consider the biggest threat to your company?

- Breach of confidential personally identifiable information: 63%
- Theft of trade secrets: 9%
- Loss of availability or sabotage of systems: 9%
- Don’t know the answer: 4%

Question 4:
Has the NIST Cybersecurity Framework been helpful to your company in managing cybersecurity risk?

- Yes: 36%
- No: 17%
- Don’t know: 47%
Question 5:
Has your company built a close working relationship with a government entity on cybersecurity issues (more than one answer could have been selected)?

- **20%** Yes, a law enforcement agency (e.g., FBI, US Secret Service)
- **23%** Yes, an industry regulator (e.g., FTC, FCC, FDIC, CFPB)
- **41%** No
- **3%** Yes, a prosecutorial agency (e.g., State AG, DOJ)
- **7%** Yes, an incident response agency (e.g., US-CERT)
- **24%** Don’t know the answer

Question 6:
Which of the following percentage ranges best represents the estimated amount that litigation risk associated with cybersecurity issues influences your company’s cybersecurity planning?

- **34%** 0% - 20%
- **23%** 20% - 40%
- **10%** 40% - 60%
- **6%** 60% - 80%
- **0%** 80% - 100%

*Don’t know the answer - 27%*
Question 7:
Does concern about regulatory enforcement actions or other adverse regulatory action impact your company’s willingness to share incident information with the government?

1. (no impact) 14%
2. 11%
3. 27%
4. 13%
5. (significant impact) 4%

*Don’t know the answer - 30%

Question 8:
Do you expect clear national standards to emerge in the next five years in the following areas (more than one answer could have been selected)?

- Data breach notification: 84%
- Security of personally identifiable information: 54%
- Investor disclosures: 41%
- Cybersecurity of third-party service providers: 34%
- Liability protection for information sharing: 30%
Question 9:
Has your company developed a global strategy to meet the differing cybersecurity and data privacy legal requirements of the countries in which you operate?

- Yes: 46%
- No, we handle compliance on an individual country basis: 27%
- Not applicable: 17%
- Don’t know the answer: 10%

Question 10:
Does your company have a separate cyber insurance policy?

- Yes, for liability: 27%
- Yes, for remediation costs: 7%
- Yes, for penalties or fines: 0%
- No, but considering in the next 12 months: 14%
- No, but might down the road: 14%
- No interest: 4%
- *Don’t know the answer - 33%
Question 11:
Does your organization have a written data protection plan? If so, how was the plan prepared (more than one answer could have been selected)?

- 30% We retained an outside IT expert or outside counsel to assist in preparing the plan
- 30% We consulted the PCI, NIST and or ISO standards in preparing the plan
- 49% Don’t know the answer

Question 12:
If your company suspected that a cyber-related incident had occurred, which two external entities on the following list do you believe your company would contact first?

- IT security company: 19%
- Consulting firm with cybersecurity advisory: 21%
- Law firm: 28%
- Insurance company: 7%
- Law enforcement (any level): 13%
- Some other external entity not listed here: 4%

*Don’t know the answer 8%
About Mayer Brown

Mayer Brown is a global legal services provider advising clients across the Americas, Asia and Europe. Our geographic strength means we can offer local market knowledge combined with global reach.

We are noted for our commitment to client service and our ability to assist clients with their most complex and demanding legal and business challenges worldwide. We serve many of the world’s largest companies, including a significant proportion of the Fortune 100, FTSE 100, DAX and Hang Seng Index companies and more than half of the world’s largest banks. We provide legal services in areas such as banking and finance; corporate and securities; litigation and dispute resolution; antitrust and competition; US Supreme Court and appellate matters; employment and benefits; environmental; financial services regulatory and enforcement; government and global trade; intellectual property; real estate; tax; restructuring, bankruptcy and insolvency; and wealth management.

Please visit www.mayerbrown.com for comprehensive contact information for all Mayer Brown offices.

Mayer Brown is a global legal services provider comprising legal practices that are separate entities (the “Mayer Brown Practices”). The Mayer Brown Practices are: Mayer Brown LLP and Mayer Brown Europe-Brussels LLP, both limited liability partnerships established in Illinois USA; Mayer Brown International LLP, a limited liability partnership incorporated in England and Wales (authorized and regulated by the Solicitors Regulation Authority and registered in England and Wales number OC 303359); Mayer Brown, a SELAS established in France; Mayer Brown JSM, a Hong Kong partnership and its associated legal practices in Asia; and Tauil & Chequer Advogados, a Brazilian law partnership with which Mayer Brown is associated. Mayer Brown Consulting (Singapore) Pte. Ltd and its subsidiary, which are affiliated with Mayer Brown, provide customs and trade advisory and consultancy services, not legal services.

“Mayer Brown” and the Mayer Brown logo are the trademarks of the Mayer Brown Practices in their respective jurisdictions.

© 2015 The Mayer Brown Practices. All rights reserved.
Attorney advertising