Sample Cybersecurity Legal Services

Initial Engagement	Scope of Review
Data Mapping and Determination of Applicable Law/Contractual Standards We will work with your in-house staff or an appropriate vendor to map your company's systems and data environments. Upon completion of this mapping, we can produce for you an applicable law chart per system.	For the initial engagement, we usually suggest an exploratory budget of up to $10,000* that will give us the opportunity to obtain a good understanding of what your company has done already in terms of systems and data mapping. Once we understand what additional work is needed, if any, we will be able to provide an estimate of the number of hours necessary to ensure the maps produced are thorough and to complete the applicable law charts.
Project Description	**Legal Work Anticipated**
Project 1: Internal Company Policies, Procedures, and Technical Practices Health Check We will review your IT privacy and security policies, including your vendor management program, to determine if they are adequate in accordance with legal requirements. Concurrent with this project, we could discuss your company's existing vulnerability scanning policies, and we may suggest that your company engage a vendor to conduct a vulnerability assessment scan that will help inform us of any needed policy changes. We have several vendors to recommend, but are pleased to work with a vendor selected by you or your team. For this type of project, we often arrange flat fees based on the size and complexity of the company.	1. Conduct interviews of only legal staff to determine the scope of your company's services and the scope of privacy-related contracts 2. Conduct legal research to determine applicable privacy laws and summarize legal requirements in a memo 3. Perform a detailed review of all IT policies and vendor management program for compliance 4. Draft policies as necessary to address observed gaps 5. Provide post-review memo detailing your company's privacy and data security health and vendor management program concerning privacy and data security

*As with all legal work, pricing depends on the size and complexity of the organization, as well as the budgets targeted to the issue.

Sample Cybersecurity Legal Services

<table>
<tr><th>Project Description</th><th>Legal Work Anticipated</th></tr>
<tr><td><b><u>Project 2</u>: Data Breach/Incident Response Check-up</b>

Many companies have existing data security and data incident response documentation. We will review the documentation (or draft anew) to make sure it is updated and takes into account your company's regulatory and contractual compliance obligations.</td><td>1. Review and revise your company's data incident response plan(s)

2. Draft additional data incident response policies, as necessary

3. Conduct post-data incident analysis of up to three selected incidents and recommend improvements</td></tr>
<tr><td colspan="2"><b><u>Project 3</u>: Cyber Liability Insurance Assessment</b>

We will review all existing insurance policies to determine which policies may be used and how much overall insurance coverage your company has at its disposal for data privacy, data security, and/or cyber liability events. We will produce a chart summarizing the available coverage. If procuring additional coverage is advisable, we will review data privacy, data security, and/or cyber liability policies with you and help you get that coverage into place with your regular insurance broker. We will also assist you with privacy and data security representations and warranties that must be answered for the policy underwriting and pricing process. Finally, we will work with you to identify and prioritize the amendment of key contracts to include more robust cyber liability policies. Our prices here will depend on the number of existing policies.</td></tr>
</table>

<u>Project 4</u>: Cybersecurity Policy Advocacy

We can assist with policy advocacy on Capitol Hill and before the administrative agencies on cybersecurity policy. We would like to discuss with you further the level of advocacy that would be helpful for your team. With more information, it may be possible for us to establish a flat monthly advocacy fee.

Below are some of our contacts that may be helpful to companies in the current cybersecurity debate. The current battles over the Cyber Intelligence Sharing and Protection Act (CISPA), the Cybersecurity and American Cyber Competitiveness Act of 2013, and similar legislation will be fought in the Senate. We have close contacts in the following Senate offices that will be helpful to advance cybersecurity legislation in that chamber:

- The Senate Commerce Committee (both majority and minority staff)
- The Senate Select Committee on Intelligence (both majority and minority staff)
- The Offices of Senator Dianne Feinstein
- The Offices of Senator John D. Rockefeller
- The Offices of Senator Barbara Mikulski
- The Offices of Senator Mark Warner
- The Offices of Senator Amy Klobuchar
- The Offices of Senator Saxby Chambliss
- The Offices of Senator Kelly Ayotte

We can provide more generally applicable House and Senate contacts upon request.

To lobby cybersecurity issues effectively within the federal agencies or obtain prosecutorial assistance when needed, we have helpful contacts at the following agencies and the White House:

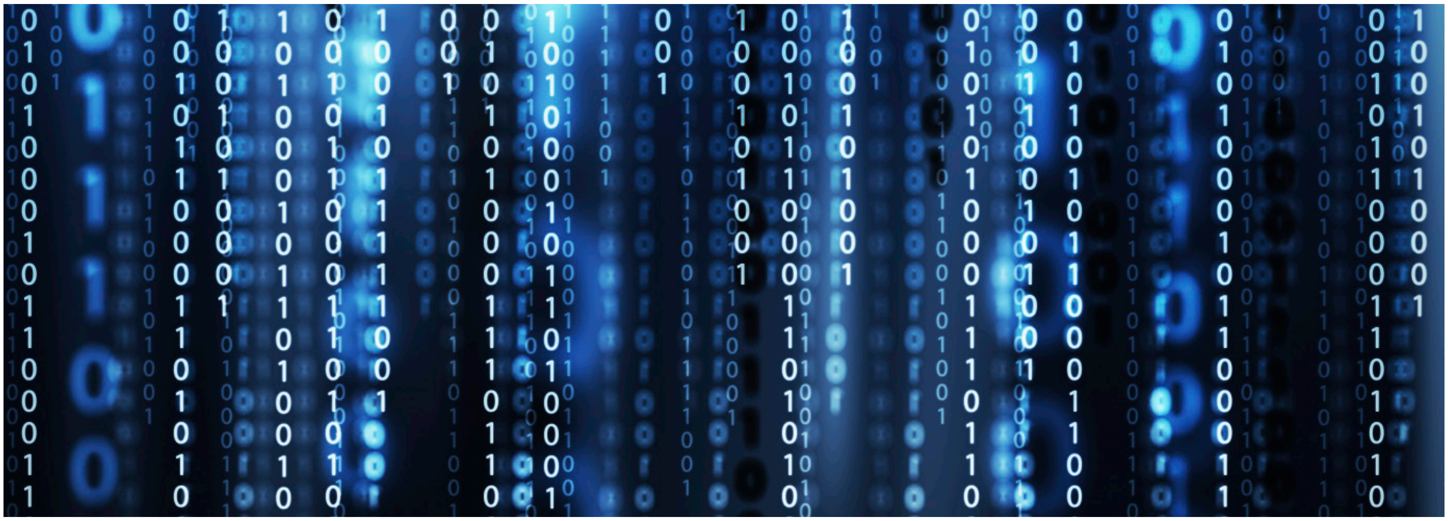
- U.S. Department of Commerce
- National Institute of Standards and Technology
- National Telecommunications Information Administration
- U.S. Department of Justice
- Federal Trade Commission
- Federal Communications Commission (advancing cybersecurity vis-à-vis telecommunications network hardening)
- U.S. Department of Homeland Security
- Federal Bureau of Investigation, Cyber Crime Division
- U.S. State Department
- U.S. Secret Service, Electronic Crimes Task Force
- White House, Office of Science and Technology Policy
- U.S. Department of the Treasury

Lastly, the cybersecurity issue has been heavily pushed by outside trade associations. We have helpful contacts at organizations that include the following:

- U.S. Chamber of Commerce Information Center
- Electronic Frontier Foundation (EFF)
- Electronic Privacy
- American Bankers Association

Ballard Spahr LLP

PRIVACY AND DATA SECURITY



Information Security Preparedness Checklist

Helping Your Organization Go Back to Basics with Information Risk Management

Financial services companies are under constant attack by cyber criminals to hack, skim, socially engineer, or even dumpster-dive consumer data. Given the virtually limitless ways that companies can be attacked, information security is no longer the responsibility of IT departments alone. Effective information risk management requires a top-driven, coordinated strategy implemented across the company.

We cannot emphasize enough the importance of a coordinated security strategy, as best evidenced by the Federal Trade Commission (FTC) settlement with CBR Systems, Inc. (CBR), the operator of a leading cord blood bank. CBR agreed to settle FTC charges that the cord blood bank failed to protect the security of customers' personal information, and that its inadequate security practices contributed to a breach that exposed Social Security numbers and credit/debit card numbers of nearly 300,000 consumers. The FTC used its Section 5 unfair and deceptive acts and practices jurisdiction to review CBR's security practices. The Commission's goal was to verify CBR's privacy policy claim that it took steps to ensure customer "information is treated securely."

According to the FTC, on December 9, 2010, a CBR employee removed four unencrypted backup tapes from a field office to bring them to the company headquarters. Four days later, the employee's car was broken into and a backpack containing the backup tapes and a number of other CBR materials holding consumer personal information (i.e., a CBR laptop, an external hard drive, and a flash drive) was stolen. None of the data on these devices was encrypted.

The FTC complaint listed a number of alleged security lapses of CBR, including:

- Transporting portable media in a way that made it vulnerable to theft
- Failing to take reasonable steps to make backup tapes unreadable in case of unauthorized access
- Not adequately restricting which employees had access to what information
- Failing to adequately supervise a vendor's work and require deletion of an unnecessary database
- Holding on to data when there was no longer a business reason to retain it

The CBR settlement—which included a 20-year FTC compliance plan—underscores how important it is for companies to honor the promises made in their privacy policies through comprehensive security planning. And yet even companies constantly subject to attacks, like financial services institutions, can find it difficult to have an internal dialogue regarding cyber security as a business process. This high-level checklist can be useful to help legal counsel and executives alike encourage such dialogue.

Data Mapping

All IT assets should be mapped to identify the fields of data available on each asset. If your organization's IT assets are mapped, this will increase your internal awareness of legacy systems and the systems coming into your organization via merger or other asset purchase. At a minimum, the inventory should include: name of system/platform, DNS names, type of device, operating system, IP address(es), MAC address(es), date of installation, vendor contact (if applicable), and data owner (with up-to-date contact information). In addition, you should make sure that your company regularly updates the mapping when systems are changed, acquired, or decommissioned.

Employee Permissions and Policies

Employees are your company's first line of defense to prevent a data security incident. Make sure your employees have the necessary tools to help the organization succeed, including:

- Effective access controls and user permissions to limit information access to those with a need to know; it is a good idea to periodically review individual access privileges
- Policies that are up to date, crisp, clear, and comprehensible to all members of your organization
- Policies that address the issues of employees bringing their own devices, remote-access employees, and social media
- Requirements for documented, signed employee agreements to your information security policies as well as privacy and confidentiality policies

Vendor Contracting Process

Given that vendors are a major source of information security headaches, the vendor contracting process is crucial. For each vendor with whom you do business and who has access to or collects personal consumer information on your company's behalf, ensure that appropriate contractual provisions are in place to address network security, application security, data security, data destruction, security breach notification, vendor data use, subcontractor data security requirements, and compliance audits you will conduct on such vendors. In addition, it is important to sensitize your marketing and procurement teams to the contractual risks related to free or low-cost Web services, since such providers often pose the greatest compliance risks.

Data Incident Response Plans

In the event that your company suffers a data incident, there is no time to learn on the fly. Companies must have a clearly defined and readily available data incident response plan in place. The plan should outline:

- The team representatives from the various operational groups within your organization, including staff from the IT, human resources, legal, and public relations departments, among others
- Up-to-date 24/7 contact information for all members of this team
- A standard conference line and notification procedure timeline
- A hierarchy for decision-making
- External forensics technical contacts
- Dos and don'ts for evidence preservation and general incident team e-mails

Disaster Recovery and Business Continuity Planning

In addition to planning for data incidents, companies should also be prepared for disruptive events. A disaster recovery plan is a blueprint for resuming operations if your organization needs to shut down or if it suffers a data loss, whereas a business continuity plan helps your employees determine within what parameters they can continue to make money and how to do so. Companies should conduct both types of planning.

Employee Training

Policies and procedures must be coupled with an effective organizational training program. Ensure your company is training employees on general security awareness and your internal corporate security policies. Consider which employees must receive mandatory training depending on the data that they handle and how that training will be documented and deployed by HR (with periodic retraining). Also consider voluntary "lunch and learns" on information security and organizational risk management to build a company culture of security.

Security by Design

Ongoing security dialogues are even more critical in the product development process. As an organization, do you build security into your IT and application development life cycles? If not, now is the time to implement a comprehensive development life-cycle process that, from the start, includes security planning, review, and testing, and then later touch points in the coding and deployment processes. Consider including these touch points as sign-off requirements of your company's standard development forms.

Develop an Internal Security/Data Governance Committee

Change is inevitable! Develop a team that is tasked with reviewing security governance practices. Establish a distribution list and a regular meeting schedule and agenda to ensure that all security policies are reviewed on an ongoing basis during appropriate times for the business units. When developing your review schedule, take into account the (1) IT audit schedule, (2) procurement/budgeting review period, and (3) business unit development black-out times, as well as any other company-specific timing considerations.

Become Part of the Outside Security Community

The financial services sector has one of the most robust security communities and information-sharing networks. Ask if your information security professionals are part of the broader financial services community networks, such as FS-ISAC or BITS (the Technology Policy Division of the Financial Services Roundtable), or general information security networks, such as the CISO Executive Network.

This checklist is by no means exhaustive, but it should be a good starting place for your internal conversations. We are available to help customize your approach to these issues and counsel you on developing all related policies, procedures, and processes.

For more information, contact:

Mercedes Kelley Tunstall
Practice Leader, Privacy and Data Security Group
Consumer Financial Services Group
202.661.2221 | tunstallm@ballardspahr.com

Amy S. Mushahwar
Privacy and Data Security Group
Consumer Financial Services Group
202.661.7644 | mushahwara@ballardspahr.com