MOFO SEMINAR SERIES

Data Protection Masterclass: Managing Data Breach Incident Response

22 July 2015
MoFo Webinar.

Data Protection Masterclass: 
Managing Data Breach Incident Response

Table of Contents

Presentation ................................................................................. 1
Speaker Biographies .................................................................... 2
About Morrison & Foerster ....................................................... 3
Selected Articles and Alerts ...................................................... 4
Presentation

DP Masterclass: Managing Data Breach Incident Response
Data Protection Masterclass:
Managing Data Breach Incident Response

July 22, 2015
Speakers

Korin Neff  
Senior Vice President and Corporate Compliance Officer  
Wyndham Worldwide Corporation

Ron Plesco  
Principal and National Lead Cyber Investigations, Intelligence & Analytics  
KPMG LLP

Andy Serwin  
Partner  
Morrison & Foerster LLP
Agenda

- What is at stake, and how should we think of these issues?
- Who are the threat actors, and how have they changed?
- How can you prepare?
- How do you respond?
Cyber security is an area of focus for the government, given its potential impact on the economy and national security.

"We know hackers steal people’s identities and infiltrate private email. We know foreign countries and companies swipe our corporate secrets. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions and our air traffic control systems...

...we cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy...

...the “cyber threat is one of the most serious economic and national security challenges we face as a nation...America’s economic prosperity in the 21st century will depend on cyber security.”

– President Obama
State of the Union – February 2013
Key Stakeholder Analysis

Understanding of how attackers work is crucial and technology needs to follow process – however, process often follows technology

Proactive (possibly in time)

T0 - X weeks

Attacker recon and preparation

Company notices the attacker and learns tactics, techniques and procedures

Company tunes the security measures, incl. security monitoring

Threat Management Process

Detection and reactive (still too late)

T0

Attack

Attacker gains persistent control and continues attack

Right-hand side of hack

T0 + X weeks

Attack is detected by Company or gets informed by others

Incident Management Process

Vulnerability Management Process

No detection and reactive (too late)
Identifying and finding sensitive data which needs to be protected is the first step in understanding the potential impact of a breach.

### Overview of Information

<table>
<thead>
<tr>
<th>What’s at Stake?</th>
<th>Whose Data and What Information?</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Valuable IP assets, proprietary information, business, transaction and negotiating records, financial data, electronic funds, business functionality and continuity</td>
<td>▪ Consumers</td>
</tr>
<tr>
<td>▪ Account information; personal information; access to accounts</td>
<td>▪ Employees</td>
</tr>
<tr>
<td>▪ Disruption of business; denial of service; cyber-extortion</td>
<td>▪ Account holders</td>
</tr>
<tr>
<td>▪ Derailed acquisition (e.g., deal team at law firm is hacked)</td>
<td>▪ “Patients”</td>
</tr>
<tr>
<td>▪ Debilitating impact on critical infrastructure and essential services</td>
<td>▪ Online advertising and e-commerce data</td>
</tr>
<tr>
<td>▪ Communication systems, supply chain management, etc.</td>
<td>▪ Credit cards</td>
</tr>
<tr>
<td>▪ SCADA (supervisory control and data acquisition):</td>
<td>▪ Company IP, secrets and networks</td>
</tr>
<tr>
<td>▪ Industrial control systems (ICS): computer systems that monitor and control industrial, infrastructure, or facility-based processes</td>
<td>▪ Transactional, negotiations and corporate records</td>
</tr>
<tr>
<td></td>
<td>▪ Cross-border data</td>
</tr>
<tr>
<td></td>
<td>▪ Corporate reputation</td>
</tr>
</tbody>
</table>
Impacts....

The business impacts are financial and reputational – including loss of competitive advantage in accessing new fields, losing deals and disputes (or winning them on unfavorable terms), regulatory fines, share price drops, and negative international media coverage.

Organized crime
(i.e. stealing credit card numbers)

State sponsored & corporate espionage
(i.e. Night Dragon)

Hacktivists
(i.e. Wikipedia, Anonymous, LutzSec)

Malicious users
(i.e. Bradley Manning and the U.S. Department of State memos)

Information Assets

Seismic Data

Personal Data
(i.e. addresses, DOB)

Merger & Acquisition Transaction Information

Senior Executive Emails
(i.e. CEO)

Quarterly & Annual Financials

Legal Disputes

Process Control Networks
(supports exploration & production activity)
Given the rapidly evolving sophistication of bad “actors,” corporate concern over cyber threats is accelerating.

YESTERDAY...

Bad “Actors”
- Isolated criminals
- “Script Kiddies”

Targets
- Identity Theft
- Self Promotion Opportunities
- Theft of Services

“Target of Opportunity”

TODAY...

Bad “Actors”
- Organized criminals
- Foreign States
- Hacktivists

Targets
- Intellectual Property
- Financial Information
- Strategic Access

“Target of Choice”
Three key trends reinforce each other making cyber risk “a perfect storm”

**Growing Threat Level**
*Cyber security is becoming more and more of an important C-level suite agenda item*

**Changing Technology Landscape**
*Consumerization of IT, Cloud and ‘eroding perimeter’*

**Compliance Pressure**
*Compliant does not necessarily mean sustainably (cyber) resilient*
Preparedness: The Program

Governance

Create governance structure for all aspects of the program

• “Tone at the Top”
• Established Structure
• Accountability
• Charters
• Up the ladder reporting
Preparedness: The Program

Policy Development

*Develop policies commensurate with local law, regulation and business standards*

- Policy Governance
- Policies, Standards commensurate with local law (e.g., Information Security, Privacy, Business Systems and Facilities Monitoring)
Preparedness: The Program

Key Processes

Maintain process review of various risk programs

- Process Review of Risk Legal Developments
- Tracking Laws, Contractual Obligations, Regulations
- Impact Statements
- PCI Assessment
- Vendor Security
Preparedness: The Program

Training and Awareness

*Establish a program appropriate for the audience*

- Training
- Everyone, everywhere
- Role Based
- Awareness
- Kiosk events
- Newsletters
- Flyers
Preparedness: The Program

Investigations, Monitoring and Reporting

Assess, track and report on program to measure compliance with policy

- Metrics
- Assessments
- Audit
- Disciplinary action
- Senior Leadership reports
- Incident Response
Preparedness: Incident Response Plan

**Purpose**

- To effectively manage security incidents with the objective of minimizing impact, maintaining or restoring normal operations, and manage breach of personal or company confidential information.

**Incident Management Team**

- Provides services that help detect, respond to, and recover from potential information security incidents in a timely, efficient and effective manner.
Preparedness: Incident Response Plan

Roles & Responsibilities

- Internal (e.g., Legal, Information Security, Physical Security, IT, Communications, Investor Relations, Human Resources, Business Teams, C-Suite, Board of Directors)
- External (e.g., law firms, forensic firms, credit monitoring agencies, communication firms)

Incident Categories (e.g., breach, malware)

- Who to engage
- Metrics
Preparedness: Incident Response Plan

**Incident Priority Levels**
- Containment
- Upwards Reporting

**Sample Documents**
- Consumer notification letters
- Regulatory notification letters
- Talking Points (e.g., call center, employees, business partners)
- FAQs
- Media Statement
Response

Discovery of the Incident:

- IT
- Company Hotline
- Legal Department
- Information Security
- Customer Service
Investigation of the Incident:

- How pervasive is the incident?
- What systems and/or processes were affected?
- How did the company learn of the incident?
- What caused (or allowed) it to occur?
- Has the company addressed the cause, and, if not, what actions must be taken to do so?
- What actions need to be taken to prevent this incident from reoccurring?
In the U.S., most states have enacted data breach notification laws requiring businesses and other entities to notify affected individuals when a data breach involving their personally-identifiable information occurs. Globally, there are a number of different considerations. The requirements of these laws vary and sometimes conflict.
Response

Notification

- Individual
- Governmental Agency
- Law enforcement
- Business Partners
- Board of Directors
- Senior Leadership
- Insurance carriers
Response

Closing Documents

• Steps followed
• Timeline
• Interview notes
• Decisions reached
• Actions taken
• Business records
What If I Fail to Notify?

• Failure to notify could result in enforcement action, penalties, or lawsuits brought by affected consumers.
Class Action Risk for Data Breach

- Class action bar has targeted companies that are victims of data breaches.
- File multiple “copycat” class actions across the country.
- Brought on behalf of nationwide and state classes.
Legal Theories

• Violation of state consumer protection laws.
• Negligence.
• Breach of contract.
• Invasion of privacy.
• Violations of state data security regulations (e.g. Mass. Data Security Reg.).
• Violations of federal data compliance/security regulations (e.g. FCRA, ECPA, CFAA, etc.).
• Civil RICO.
Where’s the Injury?

- Just because a breach happens doesn’t mean consumers were injured.

- Significant issue is actual harm versus risk of future harm.

Working with Law Enforcement

- How should companies think about these issues?
- When should companies call law enforcement?
- Who should they call?
Best Practice Take-Aways

• What can you do to prepare before an event?
• What can you do during the event?
  • The first 24 hours.
  • The first 48 hours.
  • The first 72 hours.
Questions
Data Protection Masterclass:
Managing Data Breach Incident Response

July 22, 2015
Speaker Biographies

DP Masterclass: Managing Data Breach Incident Response
Andrew B. Serwin is an internationally recognized thought leader in the fields of privacy, cybersecurity, information governance, and information sharing. As co-chair of Morrison & Foerster’s market-leading Global Privacy and Data Security Group, he provides global advice to a number of emerging and Fortune 500 companies, and handles some of the highest-profile data security incidents and privacy enforcement and litigation matters. He has a unique understanding of cybersecurity through his role in several organizations. Mr. Serwin serves on the Board of Directors of the private sector of federally funded National Cyber Forensic Training Alliance (NCFTA), an entity that functions as a conduit between private industry and law enforcement, with a core mission to identify, mitigate and neutralize cybercrime. In addition, he serves as an advisor to the Naval Postgraduate School’s Center for Asymmetric Warfare, and is the CEO and Executive Director of the Lares Institute, a think-tank focused on privacy, information superiority, and national security issues.

Mr. Serwin provides global regulatory advice regarding privacy, security, and technology transactions, with particular emphasis on: international compliance; health care; security incidents; forensic investigations; remediation of security issues; government requests for information; COPPA; CAN-SPAM; mobile; behavioral advertising; ECPA and wiretap issues; electronic marketing concerns; social media; HIPAA; and compliance with FTC requirements. He has provided advice to companies in a diverse set of industries, including: technology; social media; financial services; health; retail; data brokers; online businesses; hospitality; utilities; and insurance. Mr. Serwin also has extensive global enforcement experience, having handled numerous high-profile enforcement matters. He also frequently represents companies in consumer protection and privacy litigation matters.

**Recognitions**

Mr. Serwin was the only law firm lawyer ever to be named to Security Magazine’s prestigious “25 Most Influential Industry Thought Leaders.” He was also ranked second in the most-recent Computerworld survey of top global privacy advisors. He is also recognized by Chambers USA and Chambers Global as one of the top privacy and data security attorneys. Chambers USA 2013 notes that Mr. Serwin “attracts praise for his consultative and strategic approach to complex matters.” He was described by clients as “a tireless worker, holding onto the ever-shifting puzzle pieces of the law in this area in a way that other privacy lawyers cannot,” and noted as “an excellent privacy lawyer, a real expert in the field,” by Chambers Global 2012. The Legal 500 has recognized him as a Leading Lawyer in data protection and privacy and cyber-crime, and clients stated that he “understands business concerns and provides practical, to-the-point advice.”

**Selected Publications**

The treatise has been called “the best privacy sourcebook,” “an indispensable resource for privacy professionals at all levels” and “a book that everybody in the information privacy field should have on their desk.”
Korin A. Neff

Senior Vice President and Corporate Compliance Officer
Wyndham Worldwide

Korin Neff is the senior vice president and corporate compliance officer at Wyndham Worldwide, and is responsible for managing the compliance, ethics, information management and privacy programs across the global hospitality company. Prior to her current role, Korin held various positions within Wyndham Worldwide.

Prior to the spin off that created Wyndham Worldwide, Korin served as litigation counsel for Cendant Corporation. Earlier in her career, Korin worked in private practice focusing on general commercial litigation.

Korin graduated with a Bachelor of Arts from Emory University, Atlanta, Ga., and received her Juris Doctor from The American University Washington College of Law in Washington DC.
Ron Plesco

Principal and National Lead, Cyber Investigations, Intelligence & Analytics
KPMG

Ron is an internationally known information security and privacy attorney with 16 years experience in cyber investigations, information assurance, privacy, identity management, computer crime and emerging cyber threats and technology solutions. Ron is the National Lead of the KPMG Cyber Investigations, Intelligence and Analytics practice. Ron joined KPMG in 2012 after a distinguished career in the private and sectors and is a frequent speaker nationally. Prior to joining KPMG, Ron was the CEO of the National Cyber Forensics and Training Alliance (NCFTA), where he managed the development of intelligence that led to over 400 worldwide cyber crime arrests in four years and prevented over $2 billion in fraud. Notable NCFTA intelligence-led arrests include Ghost Click, Anonymous, Coreflood and multiple online frauds.

rpleesco@kpmg.com
About Morrison & Foerster

DP Masterclass: Managing Data Breach Incident Response
Morrison & Foerster has a world-class privacy and information security practice with more than 60 lawyers from across our global offices actively counseling, litigating cases, and representing clients before regulators around the world on privacy and security of information issues.

Our practical approach to privacy and data security challenges is what truly distinguishes our practice. We believe that it is our job to find innovative and realistic solutions for clients that balance legal compliance with the commercial realities of running their businesses.

We have been recognized by Chambers and Legal 500 as one of the best domestic and global practices in this area. We were named the 2015 Cyber Crime Firm of the Year by Legal 500 US and were named Privacy & Consumer Protection Practice Group of the Year by Law360. Chambers Global ranks the practice Tier 1 in its “Data Protection: Global” category. Clients have commented that our group comprises: “incredibly thoughtful, smart and responsive lawyers, who work seamlessly across different continents,” Chambers Global; and is “the best at giving practical advice by applying the law to the situation at issue,” Legal 500 US.

Our approach has made us the privacy counsel of choice for some of the world’s largest and best-known corporations, as well as a host of smaller organizations. Our skills are particularly valued by companies that operate in highly regulated sectors (such as financial services, healthcare, and pharmaceuticals), those with an online presence, those operating internationally and companies facing regulatory scrutiny or litigation. Our clients face multiple layers of regulation and appreciate the timely, knowledgeable, and realistic advice our attorneys are trained to provide.

We take a big picture view of how organizations handle information during its life cycle and help our clients find practical solutions to seemingly complex problems. From big data to cybersecurity to online behavior advertising, our lawyers work on cutting-edge issues that cover every aspect of privacy and data security.

**We Advise On:**

- U.S. and international privacy compliance
- Privacy litigation
- Regulatory investigations and inquiries
- Cross-border data transfers
- Cybersecurity and information security

“Incredibly thoughtful, smart and responsive lawyers, who work seamlessly across different continents.”

— Chambers Global
Practice Group Description

“Data breach notification globally
• Healthcare privacy
• Privacy and data security issues in commercial transactions
• Online privacy and behavioral advertising
• Employee/HR privacy, including employee monitoring
• Cloud Computing deals
• Data protection and privacy policies, procedures, and training
• E-discovery and disclosure issues in internal investigations and litigation

The changing nature of technology has been a driving factor in data protection regulation in recent years, including issues such as the increased emphasis on technological means to secure data, how we use social media, user-generated content, the adoption of Cloud Computing, and sophisticated advertising and marketing techniques, including behavioral targeting. Our privacy and data security lawyers are as comfortable with technological innovation as they are with complex and evolving regulation. Because of wide experience with technology, we are at ease speaking with the general counsel, the chief privacy officer or the chief information officer regarding technical and non-technical issues relating to privacy and data security.

In addition to our transactional, regulatory and counseling practice, our lawyers are just as much at ease in the court room or with regulatory authorities in contentious situations. Our global team is able to help with virtually any privacy or data security issue anywhere in the world.

Resources

We offer important resources to support our clients in their privacy compliance and data security efforts.

• Legal Resources: The privacy team writes extensively on privacy and data security matters, including Global Employee Privacy and Data Security Law, setting out the U.S. and international legal landscape related to workplace privacy and data security; Information Security and Privacy: A Guide to Federal and State Law and Compliance and Information Security and Privacy: A Guide to International Law and Compliance, which compose a 4,300-page, three-volume treatise that examines all aspects of privacy and security laws, published by Thomson-West; and The Law of Financial Privacy, covering the Fair Credit Reporting Act, Financial Privacy Act, Bank Secrecy Act, and Internal Revenue Code requirements, including discussions of state financial privacy laws, use of technology, and use and protection of confidential information. The team has also written Health Care Privacy and Security, West’s Corporate Counsel’s Primer on International Privacy and Security and Internet Marketing and Consumer Protection.”
- **Privacy Library**: Our Privacy Library (www.mofoprivacy.com) is an online resource which provides links to privacy laws, regulations, reports, multilateral agreements, and government authorities of more than 100 countries around the world, including the United States. The Privacy Library is the most comprehensive collection of privacy laws and regulations ever assembled—the result of years of research and experience working with clients around the world.

- **MoFoNotes**: Morrison & Foerster provides content to Nymity (www.nymity.com) for its MoFoNotes product, a subscription-based database that helps organizations determine local compliance requirements in jurisdictions around the world, spot potential compliance issues, and simplify the development of global privacy approaches.
Selected Articles & Alerts

DPMasterclass: Managing Data Breach Incident Response
Cybersecurity has rapidly emerged as a top-of-mind issue for many Boards of Directors in the wake of recent large-scale data security incidents. Boards are engaging with management teams in new ways in order to assess cybersecurity risks and the company’s readiness to respond to emerging threats.

These threats have placed additional pressure on Boards in part due to the level of attention and adverse scrutiny directed at other data security incidents. This includes scrutiny from shareholder advisory service firms as well as a number of government agencies, including the FTC, the SEC, and state Attorneys General, who routinely investigate data security incidents. While the “business judgment rule” can be expected in most circumstances to provide protection to the Board in the event of shareholder litigation regarding data security issues, a careful review and assessment of the company’s level of preparedness for cybersecurity risks is a helpful step in mitigating risks to the business.

Although there is no simple solution to this set of issues, there are three broad topics that many Boards of Directors are examining as they review and assess these issues:

• how important cybersecurity is to the company;
• what steps the company has taken to evaluate and mitigate cybersecurity risks; and
• what public disclosures the company has made.

How Important Is Cybersecurity to Your Company?

• What is the scope of information regarding individuals—customers, vendors, or employees?
  – Almost every company has some personal information regarding individuals.
  – In general, companies which are consumer facing or for whom information is the primary asset, as well as those with large numbers of employees, have more pronounced cybersecurity risk.

• How important is information security to your brand?
  – If your company had a cybersecurity incident, would it make it more difficult to sell your products or services?
  – Is maintaining customer trust regarding information important to your business?
  – If the answer to any of these questions is “yes,” then your company has a higher cybersecurity risk.

• Does your company have valuable or sensitive proprietary data that someone might seek to steal?
  – While theft of personal information and credit cards is in the news, there is a great deal of other cybercrime, including attacks directed continued on page 2
at proprietary information, trade secrets, business processes, and other corporate assets including cash.

— Whether or not your company is consumer facing, if your organization has sensitive proprietary information, it may be a more attractive target to cybercriminals than you think.

• Is your company “critical infrastructure,” or are you a supplier/vendor for the government, or for critical infrastructure?
  — Companies deemed to be critical infrastructure or that provide services to the government face special considerations.
  — For example, these businesses are likely to be regulated on cybersecurity matters sooner rather than later.

Has Your Company Taken Steps to Evaluate, Mitigate, and Govern the Risks?

• What organizational structures exist to measure, govern, and assess data and information risk and how are threat assessments managed and reported?
  — Companies with cybersecurity risk need to understand the risks they face and should consider formalized governance structures or processes to measure, assess and mitigate that risk.

• Is responsibility for all aspects of protecting your company’s information assets allocated appropriately?
  — Having a clear chain of command and a specific allocation of duties for those charged with information protection can both mitigate cybersecurity risks and prepare the organization better to respond to a security incident.
  — Has a comprehensive risk assessment regarding information security been completed recently and what is the status of addressing issues identified in such a risk assessment?

— A good place to start a risk assessment is to:
  » complete a high level data inventory of the company’s information assets so that you have an understanding of what information you have and generally where it is located; and
  » do a thorough review of policies and procedures to ensure that they comply with the relevant data security laws and are consistent with industry best practice.

• Has the company assessed the impact of global privacy and data security laws on the business?
  — While there a number of different U.S. laws dealing with cybersecurity and data protection, there are also more than 90 other countries that have data protection laws.
  — If your company is operating outside of the U.S. it is important to take the global laws into account when designing a cybersecurity program.

• Does the company have an incident response plan, and are the appropriate business leaders identified in it?
  — For many companies, it is not a question of if you will have a security incident so much as when.
  — Having a clear written incident response plan can help companies effectively respond to a security incident.

• Have the company’s security processes and systems been reviewed by a third-party assessor?
  — Third-party review of cybersecurity readiness can be a crucial factor in defending the company after a security incident as well as helping a company to take reasonable steps to prepare for and defend against a cyberattack.
  — Consider the following kinds of questions:
    » Does the company have a Security Operations Center, or other similar group in the company, and if so, have its activities been reviewed by a third-party to ensure they are adequate?
Has the level of penetration testing, software patching, and other similar activities been reviewed by a third-party to ensure it is adequate for your company?

Has the company benchmarked its cybersecurity risk posture against other similar businesses?

Many Boards of Directors are taking additional steps in order to establish that they are exercising appropriate oversight of cybersecurity.

One crucial question that may be asked in the wake of significant information security breaches is “was the Board engaged?”

To assure that you will be able to answer that question with confidence, consider: when was the last time the Audit Committee or other responsible committee of the Board received a report regarding information security and when was the last time the Board received such a report?

Does the company carry insurance that covers cyber risk?

Cyber risk insurance is becoming much more common in recent years and is one tool that can be used to help the company to manage risk.

What Public Disclosures Has the Company Made?

Do the company’s public disclosures on information risk adequately describe its current risk posture?

In October 2011, the SEC’s Division of Corporation Finance issued guidance regarding disclosure obligations related to cybersecurity risks and cyber incidents. http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Generally speaking, that guidance discourages “boilerplate” disclosures related to cybersecurity issues, and outlines issues to consider when a company is drafting the risk factors, MD&A, business description, legal proceedings, and financial statement portions of its public filings.

The Chair of the SEC, along with various staff members, has been publicly asking questions about whether companies are being sufficiently transparent in their disclosures about cybersecurity and cyber incidents.

In addition, Target has publicly disclosed that it is under investigation by the SEC for its disclosures related to cybersecurity.

Closely reviewing the company’s data security policies, prior cyber incidents, and material information concerning cybersecurity risks in connection with drafting periodic filings is important as long as this issue is a priority for the SEC and its staff.

Assess the company’s internal and external privacy and information security policies and statements to confirm they appropriately and adequately describe its information practices.

Read the publicly facing privacy statements on the company’s website or in the literature the company provides to customers.

Ask whether it is consistent with the company’s actual practices and what methods are used to ensure that the company upholds the promises that it makes.

For more information on these issues, please contact:

Andrew Serwin  (858) 720-5134 aserwin@mofo.com
Miriam Wugmeister  (212) 506-7213 mwugmeister@mofo.com
YOUR PRE-BREACH CHECKLIST

Is your company prepared to respond to a security breach?

For many companies, even reading this question causes some anxiety. However, being prepared for what seems like the inevitable—a security breach—can be the difference between successfully navigating the event, or not. While we still hear some companies say, “That would never happen to our company!,” a significant breach can happen to any company. In light of this, and the significant scrutiny that the high-profile breaches reported in the past year have received, many companies have taken the opportunity to consider their preparedness and ability to respond quickly and decisively to such an incident. We have prepared the following “checklist” that highlights some steps we have been helping companies take so that they can be better prepared in the event that a significant incident occurs.

1. Make Friends with Your IT/IS Department. As attorneys, we frequently focus on compliance and litigation. But you need to be familiar with your company’s risk tolerance and approach to information security to develop an understanding of your company’s security posture. The time to ask these questions isn’t after a breach has happened, so ask your colleagues in your company’s Information Technology or Information Security Departments the basic questions (e.g., What’s DLP?) and the tough questions (e.g., Why haven’t we addressed data security concerns raised in last year’s audit)? You would rather learn, for example, that your company does not encrypt its laptops before one is stolen.

2. Have a Plan. Many companies have an incident response plan. If your company does, dust it off. Does it need to be updated based on the current breach environment? Would it actually be helpful in responding to a high-profile nationwide data security breach? Does it have a list of key contacts and contact information? Also, make sure you have a copy printed out in case the breach impacts your company’s electronic system. If you don’t have a plan, draft one, and follow it!

3. Practice. Practice! Although practice may not make perfect when it comes to data breach response, you do not want your response team working together for the first time in the middle of an actual high-stress incident. Gather your response team and relevant stakeholders and do a fire drill or breach tabletop (and consider bringing your outside counsel). This will be valuable training and an investment in your company’s preparedness.

4. Decisions, Decisions, Decisions. Someone has to make the tough calls. A high-profile breach incident is a series of tough calls (e.g., when will you go public, how will you respond to the media,
will you offer credit monitoring). We continue to see incidents where there are competing views within a company about the “right” decision and incidents where difficult decisions have to be made based on limited facts. You should give thought to whom within your organization will be responsible for making the tough calls, and making sure the key decision-makers understand the broader issues that have to be considered.

5. **Know the Law.** Notice is driven by federal and state law. There are federal breach requirements (e.g., HIPAA), and there are state requirements in 51 states and jurisdictions. Needless to say, notice in a nationwide incident can be complicated. And, the laws have been rapidly changing over the last several years. You should make an effort to stay abreast of the current landscape of breach-related requirements (e.g., requirements for the content of consumer notices and requirements to notify state regulators). In addition, breaches that affect individuals outside the U.S. are even more complicated. Be aware that the number of jurisdictions with breach notification obligations is growing and in many instances includes the unauthorized disclosure of any type of personal information.

6. **Go Outside.** Outside counsel who have a deep practice in this area will have worked on countless incidents both large and small and can advise on how other companies respond to similar incidents and how regulators have reacted. This is invaluable insight when the tough calls have to be made. See (4) above.

7. **Engage Vendors.** In a significant breach incident, a company’s resources can be stretched thin. Many companies would not have the capability to produce and mail 500,000 breach letters in just a few days. Similarly, many companies are not prepared to handle dramatically increased call center volumes after an incident becomes public. There are a wide variety of vendors that can help companies respond to a breach incident, including forensic investigators, crisis communication experts and mail houses to name a few. Consider your capabilities and engage vendors before an incident occurs.

8. **In Case of Emergency, Call.** The list of individuals and entities that you may need to contact in the case of a significant breach is probably longer than you think. For example, you may need to contact members of your response team, members of senior management, your merchant acquirer, payment card networks, a wide variety of vendors, the press, your regulators, outside counsel and others. While it seems simple, it can reduce stress in the heat of the moment if you have a comprehensive contact list. See (2) above.

9. **Consider Coverage.** Cyberinsurance is one of the fastest growing areas of insurance today. It’s quite possible that your company already has a policy that would provide at least some coverage in the case of a data security breach. If so, you should review the policy to get a sense of the breadth of the coverage and consider whether that coverage is appropriate for your company’s needs. If your company does not have a policy, you can consider the costs and benefits of obtaining coverage. This is a risk-based decision, but one that of course needs to be thought about before a breach occurs.

10. **Don’t Delay.** Although you can’t control whether a breach occurs, you can control how your company responds. Most companies with whom we work with find that there is more that they can do to prepare for a potential breach event. In light of the public, regulatory and internal scrutiny that a high-profile breach brings, don’t delay in considering your preparedness to respond to such an event.

For more information on these issues, please contact:

**Andrew Serwin**  
(858) 720-5134  
aserwin@mofo.com

**Miriam Wugmeister**  
(212) 506-7213  
mwugmeister@mofo.com

**Nathan Taylor**  
(202) 778-1644  
ndtaylor@mofo.com
Cybersecurity—Emerging Trends and Regulatory Guidance

By Fernanda Schmid, Robert B. Hubbell, Nathan D. Taylor and Daniel A. Nathan

Cyberthreats are ever-present. The US Office of the Director of National Intelligence identified cyberthreats as the top threat in 2014, surpassing terrorism. There has been a 10,000-fold increase in the number of new digital threats over the past 12 years. Hacking attacks increased 62 percent in 2014 alone. As the assistant director of the FBI’s Cyber Division stated in April 2011, Cyberthreats have “reached the point that given enough time, motivation and funding, a determined adversary will likely be able to penetrate any system that is accessible directly from the Internet.” But if you think data security is only an issue for Fortune 500 companies, you are wrong. Any company that has confidential information or employee, customer or client data needs to think about cybersecurity.

A company cannot eradicate cyberthreats. But it can manage the threats and develop a plan to respond to an incident. This process requires cooperation and teamwork across company departments, including the active participation of in-house counsel, who play a critical role in this process. Recent guidance from industry groups and regulators provides a framework for in-house counsel to answer two key questions: What should my company do to prepare for a data breach, and how can I help?
The challenges: an ever-present threat and the absence of national regulation

There is no simple fix and no single solution to cyberthreats. Each company must examine its own structure, its own systems and its own data to determine what needs to be protected and how best to protect it. Data security threats exist not just at the enterprise level but at other points of entry as well, such as point-of-sale (POS) registers, employee smartphones, social media, personal email accounts, Wi-Fi printers and the "Internet of Things." In addition, a company cannot focus only on its own information systems to identify vulnerabilities but must consider the systems of critical third parties, including vendors. Threats exist not only from hackers but employees, independent contractors and third-party vendors.

Managing these risks involves multiple levels of a company. It requires knowledge at the board level of what the issues are and what your company is doing to address them. Some public companies have cyber-risk committees. On a daily operation level, managing the risk requires the input of multiple management groups in a company, including, for example, legal, IT, human resources, accounting, payroll and sales. It also requires a culture where every employee understands the importance of what is at stake and her role in maintaining security.

To add to this internal complexity, a patchwork of local, state and federal regulations governs data security issues. For example, 47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands require that companies notify individuals of security breaches of information involving personal information. Moreover, a number of states impose obligations on companies to safeguard personal information relating to consumers. In many instances, these obligations may be high level (i.e., maintain reasonable security procedures to protect data), but some states impose detailed security standards, including, for example, the Massachusetts data security regulations. In addition, depending on your company’s industry, the company may also be subject to federal regulation, such as the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, Sarbanes-Oxley, the Fair Credit Reporting Act, the Children’s Online Privacy Protection Act, the Privacy Act, the Electronic Signatures in Global and National Commerce Act, the Federal Information Security Management Act or the Homeland Security Act of 2002. Along with these acts, various federal agencies may also have oversight or input regarding how a company handles data, such as the Federal Trade Commission, the Department of Health and Human Services and the Office of the Comptroller of the Currency.

Trying to comply with all the applicable laws can be confusing and daunting. But ignoring data security can have far-reaching ramifications beyond the loss of critical data, including federal and state penalties, civil suits and reputational harm. A company’s legal group plays a critical role in the company’s security preparedness. For example, your legal department distills the regulatory framework to which your company is subject. And if your company does not have a separate risk or compliance department, then the legal department likely is responsible for assessing your company’s preparedness.

A framework for thinking about company information and cybersecurity threats

The first step in assessing your company’s exposure to a cybersecurity threat is to figure out what your company needs to protect. It is not possible to protect all data or every access point on your network. Prioritization is key. What data and systems are critical? What servers or other critical network systems does your company use? How are your systems segmented? How is access to your systems from the Internet controlled? What data are your company legally required to protect? What data are your company contractually or legally required to protect? What other data do your company want to protect? Does your...
company have personal information relating to employees or customers? What health information does your company possess? Does it have strategic or competitive information? Does it have market-sensitive information? What proprietary or trade-secret information does your company possess? What client information does it have?

Making this assessment requires input from all the stakeholders who have data or systems at issue. Who these actors are depends on what your company does. In fact, every business line or department may have meaningful input. At a minimum, it will likely involve your IT, facilities, audit, human resources and accounting departments. It could also involve your sales department or other client or customer-facing groups within your company.

Then your company needs to identify where vulnerabilities exist. This is a complex and multilayered issue. Examples of questions to ask: Who handles or has access to the data or systems that need to be protected? How do the data enter your company? Where are the data stored? How are the data handled within your company? Where are the critical systems kept? What security is already being deployed to protect those systems? Related questions include thinking about how your company handles access to these data and these systems, including not only internal access but external access by third parties such as vendors. Another way to approach this facet of the issue is to consider what threats exist regarding these data or these systems. Potential threats include access to your systems by hackers, destruction or loss of the data by internal or external parties, external disruptions such as a denial of service or distributed denial-of-service attack or intentional or unintentional disclosure of the data by internal or external parties.

Your company also needs to consider who will watch the watchers. What systems, controls and processes are in place to make sure that the parties who have day-to-day oversight of these issues are doing what they are supposed to be doing? Technology and company processes play a vital role here. Another aspect of this issue is the board’s knowledge of and input into these systems, controls and processes. As cyberthreat issues become more prominent, it becomes increasingly important for a board to, at a minimum, have knowledge of who has responsibility for cyberissues, what the issues are and what your company is doing to address them. Beyond this, the specific role the board plays in cybersecurity depends on the size

<table>
<thead>
<tr>
<th>TIER</th>
<th>Risk Management Processes/Policies</th>
<th>Cyberincidents</th>
<th>External Participation</th>
</tr>
</thead>
<tbody>
<tr>
<td>IV Adaptive</td>
<td>Continuous updating of practices based on lessons learned</td>
<td>Implemented across enterprise, part of culture</td>
<td>Actively shares information with partners</td>
</tr>
<tr>
<td>III Repeatable</td>
<td>Formally approved and regularly updated</td>
<td>Companywide approach implemented</td>
<td>Received information from partners and collaborates</td>
</tr>
<tr>
<td>II Risk Informed</td>
<td>Approved, not implemented</td>
<td>Awareness by management, not implemented fully</td>
<td>Aware of role in ecosystem, no formal interaction</td>
</tr>
<tr>
<td>I Partial</td>
<td>Ad hoc</td>
<td>Limited awareness</td>
<td>None</td>
</tr>
</tbody>
</table>

Your company also needs to consider who will watch the watchers. What systems, controls and processes are in place to make sure that the parties who have day-to-day oversight of these issues are doing what they are supposed to be doing?
To provide timely, comprehensive and accurate information to investors while not disclosing information that could serve as a roadmap to those who seek to exploit a company’s vulnerabilities.

Cybersecurity around the world

With the growing number of data-security breaches around the world, security remains a great concern. Seventeen countries have enacted mandatory breach-notification laws that require organizations to notify individuals and/or government regulators in the event of a data breach. Ten other countries have issued voluntary data-breach-notification guidelines. With respect to data safeguards, there is a broad range of data security obligations. Some countries, such as those in the United Kingdom, simply require that companies use reasonable organization and technical measures to protect personal information. Other countries have detailed security obligations such as South Korea (which requires encryption of certain types of data at rest) and Argentina (which requires encryption of sensitive data over the Internet).

With respect to privacy, more than 90 countries now have comprehensive privacy statutes. Most privacy laws outside the United States are broader than US law, covering any personally identifiable information, not only customer or consumer information. Generally, these laws require that the existence of databases be publicly disclosed and that the databases be registered with the government or with an independent data-protection authority. They also require that individuals whose personal information is maintained in these databases be given notice of, and in certain circumstances consent to, the collection, use and transfer of their personal information as well as the right to access and correct the information held about them.

Cybersecurity – Emerging Trends and Regulatory Guidance

The NIST framework: one alternative to a national approach

In the dynamic environment where cyberthreats are becoming more frequent, sophisticated and severe, having effective cyber-risk management policies and programs in place has become increasingly important. Like other risk-management policies and programs, those that address cybersecurity risk must be specifically tailored to the company’s business, risk tolerance and resources. But companies should assess their cyber-risk management policies and programs against conceptual frameworks, industry standards and best practices that have been developed to manage cybersecurity risk.

One conceptual framework, developed by the National Institute of Standards and Technology (NIST framework) in early 2014 in response to an executive order issued by President Barack Obama has garnered much attention as a standard of care for company readiness against cyberattacks. The NIST framework consists of three interrelated parts that can be used to identify, assess and manage risk: the framework core, the categories that address those risk-management activities, and the associated controls that implement those activities.
The framework core includes five functions that are performed concurrently and continually to create a culture that addresses the dynamic nature of cybersecurity risks:

- **Identify**—understand the business context, resources that support critical functions and the related cybersecurity risks to focus and prioritize efforts.
- **Protect**—develop and implement safeguards to limit or contain the impact of a potential cyberincident.
- **Detect**—develop and implement activities to detect a cyberincident in a timely manner.
- **Respond**—develop and implement activities to contain the impact of a potential cyberincident.
- **Recover**—develop and implement activities that support timely recovery to normal operations to reduce the impact of the cyberincident.

The framework-implementation tiers represent a lens through which the company can view the characteristics of its risk management approach. Implementation tiers range from partial (tier 1) to adaptive (tier 4), with increasing levels of rigor and sophistication of cybersecurity risk management at successive tiers. Companies select a tier based on current cybersecurity risk management practices; however, those companies in the partial implementation tier (tier 1) are encouraged to move toward risk informed (tier 2) or higher tiers. Figure X below summarizes the risk management processes, programs and external participation at each tier.

The final part of the NIST framework is the framework profile (profile). The profile is designed to meet the company’s unique needs. It should be aligned with the company’s goals, reflect risk-management priorities and should be developed in consideration of legal and/or regulatory requirements and industry best practices. A current profile identifies the outcomes that the company is achieving in the five core functions (identify, protect, detect, respond, recover).
respond and recover). A target profile can also be developed to identify the outcomes needed to achieve the company's goals. Gaps between the current and target profile can be used to create a prioritized action plan for continuous improvement of cyber-risk management policies and programs.

Companies should take seriously the self-assessment and continuous improvement concepts included in the NIST framework. Companies should also consider the importance of maintaining attorney-client privilege in conducting assessment and making recommendations for improvement.

SEC guidance regarding cybersecurity risk disclosures for public companies

Determining the information to disclose to investors about cybersecurity risks and incidents is complex and challenging for public companies. Of critical importance is balancing the need to provide timely, comprehensive and accurate information to investors while not disclosing information that could serve as a roadmap to those who seek to exploit a company’s vulnerabilities. Adding to the complexity is the potential for litigation, regulatory actions, and accurate information to investors needs to be disclosed.

A company may experience many circumstances rather than describe generic risks that apply to all companies or provide boilerplate disclosures. Companies should also review the adequacy of cybersecurity-related disclosures on an ongoing basis.

The importance of timeliness and an on-the-shelf response plan

"The primary distinction between a cyberattack and other crises that a company may face is the speed with which the company must respond to contain the rapid spread of damage. Companies need to be prepared to respond within hours, if not minutes, of a cyberevent to detect the cyberevent, analyze the event, prevent further damage from being done and prepare a response to the event." Whether to disclose the event, what and how your company discloses of the breach and what it does to address it depends in part on your industry, how the cyberincident occurred and what data were compromised. Depending on the nature of the cyberattack, a timely response and the time available to respond can be dictated by regulations or even contractual obligations. Failure to disclose a loss of data can expose your company to a regulatory investigation by state and even federal authorities.

The key to being able to respond in a timely manner is having an incident response, crisis management, disaster recovery or business continuity plan that addresses these issues. At a minimum, the plan should include identifying and grading risks. What internal response and escalation is required for which sort of incident? A company may experience many
Your plan should also include guidance on a potential media response by your company. For example, when a media response is required, who should be involved in drafting the response, and who should give the response?

3 The Internet of things is the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure that could be clearer. The Internet of things refers to everyday devices like refrigerators, chips in pets, thermostats and gas meters that can now connect to the Internet, and these devices are also susceptible to cyberhacks.

4 For a discussion of relevant state laws as well as key court cases, see the Morrison & Foerster Privacy Library, www.mofo.com/privacylibrary/privacylibrarylanding.


7 In a June 2014 speech at the New York Stock Exchange, SEC Commissioner Luis Aguilar stated: “While the [NIST] framework is voluntary guidance for any company, some commentators have already suggested that it will likely become a baseline for best practices by companies, including in assessing legal or regulatory exposure to these issues or for insurance purposes…. At a minimum, boards should work with management to assess their corporate policies to ensure how they match up to the framework’s guidelines—and whether more may be needed.” (“Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus,” Commissioner Luis A. Aguilar, June 10, 2014, emphasis added (www.sec.gov/News/Speech/Detail/Speech/1370542057946#).VKNf5CvF98E.

8 Recognizing the need for flexibility in establishing a profile as a roadmap for reducing a company’s specific cybersecurity risk, the NIST framework does not prescribe a template for the profile.


10 CF Disclosure Guidance: Topic No. 2 Cybersecurity, available at www.sec.gov/divisions/corpfin/guidance/cf-guidance-topic2.htm. Commissioner Aguilar, in his March 26, 2014, public statement at the SEC’s Cybersecurity Roundtable, noted that “Some have suggested that such disclosures fail to fully inform investors about the true costs and benefits of companies’ cybersecurity practices and argue that the commission (and not the staff) should issue further guidance regarding issuers’ disclosure obligations.” See letter from U.S. Senator John D. Rockefeller IV to chair White (Apr. 9, 2013), available at www.commerce.senate.gov/public/?a=Files.Serve&File_id=49ac989b-bd16-4bdd-8d64-8c15ba0e4e51.” www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541287184#.


12 There are many publications that discuss what steps to take in the event of a breach, including what steps are mandated by the various laws that regulate the differing types of information that may be compromised, and so this topic will not be addressed in-depth in this article.

13 What each of these plans should include and what type of each of these plans is right for a company are subjects in their own right. Again, there are many publications regarding this topic and consultants who specialize in providing this guidance.

NOTES
3 The Internet of things is the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure that could be clearer. The Internet of things refers to everyday devices like refrigerators, chips in pets, thermostats and gas meters that can now connect to the Internet, and these devices are also susceptible to cyberhacks. For a discussion of relevant state laws as well as key court cases, see the Morrison & Foerster Privacy Library, www.mofo.com/privacylibrary/privacylibrarylanding.
7 In a June 2014 speech at the New York Stock Exchange, SEC Commissioner Luis Aguilar stated: “While the [NIST] framework is voluntary guidance for any company, some commentators have already suggested that it will likely become a baseline for best practices by companies, including in assessing legal or regulatory exposure to these issues or for insurance purposes…. At a minimum, boards should work with management to assess their corporate policies to ensure how they match up to the framework’s guidelines—and whether more may be needed.” (“Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus,” Commissioner Luis A. Aguilar, June 10, 2014, emphasis added (www.sec.gov/News/Speech/Detail/Speech/1370542057946#).VKNf5CvF98E.
8 Recognizing the need for flexibility in establishing a profile as a roadmap for reducing a company’s specific cybersecurity risk, the NIST framework does not prescribe a template for the profile.
10 CF Disclosure Guidance: Topic No. 2 Cybersecurity, available at www.sec.gov/divisions/corpfin/guidance/cf-guidance-topic2.htm. Commissioner Aguilar, in his March 26, 2014, public statement at the SEC’s Cybersecurity Roundtable, noted that “Some have suggested that such disclosures fail to fully inform investors about the true costs and benefits of companies’ cybersecurity practices and argue that the commission (and not the staff) should issue further guidance regarding issuers’ disclosure obligations.” See letter from U.S. Senator John D. Rockefeller IV to chair White (Apr. 9, 2013), available at www.commerce.senate.gov/public/?a=Files.Serve&File_id=49ac989b-bd16-4bdd-8d64-8c15ba0e4e51.” www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541287184#.
12 There are many publications that discuss what steps to take in the event of a breach, including what steps are mandated by the various laws that regulate the differing types of information that may be compromised, and so this topic will not be addressed in-depth in this article.
13 What each of these plans should include and what type of each of these plans is right for a company are subjects in their own right. Again, there are many publications regarding this topic and consultants who specialize in providing this guidance.
Chapter 1

Introduction

§ 1:1 The rise of information security and privacy
§ 1:2 General privacy principles
§ 1:3 Organisation for economic co-operation and development guidelines: a beginning
§ 1:4 Scope of OECD guidelines
§ 1:5 Collection limitation principle
§ 1:6 Data quality principle
§ 1:7 Purpose specification principle
§ 1:8 Security safeguards principle
§ 1:9 Openness principle
§ 1:10 Individual participation principle
§ 1:11 Accountability principle
§ 1:12 International application—Free flow and legitimate restrictions
§ 1:13 National implementation
§ 1:14 International cooperation
§ 1:15 Principles adopted by the Asia-Pacific Economic Cooperation
§ 1:16 APEC information privacy principles
§ 1:17 Privacy and security—The seven U.S. privacy principles

KeyCite*: Cases and other legal materials listed in KeyCite Scope can be researched through the KeyCite service on Westlaw®. Use KeyCite to check citations for form, parallel references, prior and later history, and comprehensive citator information, including citations to other decisions and secondary materials.

§ 1:1 The rise of information security and privacy

Information security and privacy issues are not new, but mass attention and compliance efforts are at an all time high, and appear only to be increasing, particularly as litigation and high-profile security breaches continue to draw attention to these issues. That privacy and information security concerns have been a societal problem for a long time is demonstrated by the fact that many wiretapping laws are called “eavesdropping” laws, referring to people standing in the so-called eavesdrop of a house listening to conversations before telephones were invented.
Current hot issues in information security and privacy include:

- Big Data;
- Managing differing international standards;
- Financial privacy;
- Privacy litigation;
- Outsourcing to foreign countries;
- Electronic health records and personal health records; and
- Social networking.

Issues that have arrived, but without complete impact on the privacy landscape include interoperability of medical records, non-HIPAA covered medical information, genetic privacy, and increased concerns over computer crimes and controlling one’s identity. Just a few years ago, there were a limited number of privacy and security laws in the United States and they generally applied only to companies in certain industries (such as health care and financial institutions). Now, the number of laws is staggering. Many new laws apply, or will apply, to companies in all industries, not just certain industries. Moreover, though there is no federal law that generally requires information security, certain Federal Trade Commission (“FTC”) actions indicate that the FTC is imposing a generalized duty to impose information security via the Federal Trade Commission Act. As this trend continues, many companies may face a situation where data security issues must be directly and quickly addressed, or they will incur extensive FTC mandated administrative costs and burdens.

Compliance with these laws is not only a legal reality, but it is also a business reality as the frequent and well publicized data security incidents demonstrate. These days the newspapers are full of stories about the high-profile data security incidents that usually involve numerous consumers. This in large part results from the 46 states, plus Puerto Rico, New York City, and Washington D.C., that have enacted laws that require notice of security breach incidents. These laws have increased the publicity that is received when these incidents occur and heighten consumer awareness of incidents. Security breach is now a concern under HIPAA due to the recent changes to HIPAA that have not fully gone into effect and now many foreign countries are beginning to enact security breach laws as well.

Notice of security breach laws are just one of the categories of laws that are being enacted. Identity theft is also an area of great legislative concern and numerous states have enacted privacy and security laws that cover a variety of information categories. Generally these laws cover:

- Internet privacy restrictions;
Financial privacy;
Unauthorized access to networks and information;
Wiretapping and privacy in electronic communications;
Identity theft;
Data security and data destruction;
Notice of data security breaches;
Spyware and phishing;
Restrictions upon the use of Social Security numbers;
Video and cable privacy;
Genetic privacy;
Pretexting;
Telecom privacy; and
Restrictions upon government entities.

As this book demonstrates, these general categories represent just the beginning of the regulatory and administrative hurdles. Within these and other categories, there are an extensive number of laws and regulations that must be complied with and considered if a company intends upon complying with these requirements. Moreover, there are laws, including laws regarding wiretapping, that are becoming more important as electronic communications become the preferred mechanism for business communication. Also, contrary to popular belief, many of these laws apply to all companies, not just companies in the health or financial industries, or companies that collect data regarding children.

Now, with more and more companies exploring international markets, the laws of the European Union ("EU") and other countries are becoming more relevant. These laws differ in many ways from the laws in the United States and compliance with one standard, even the generally higher EU standard, will not guarantee U.S. compliance. Moreover, other nations, including Japan and Argentina, have also enacted broad privacy laws. The laws of these jurisdictions are the subject of Information Security and Privacy: A Guide to International Law and Compliance.

The cost of failing to comply with these requirements is high. In addition to the regulatory fines and penalties, companies face litigation costs defending suits by individuals, as well as in some cases class action suits, alleging violations of these laws. The direct costs of remedying non-compliance after an incident can be staggering—some companies have disclosed costs that reach into the millions of dollars. And these costs do not include the potential loss of business that can result from consumer trepidation created by a company permitting the wrongful acquisition of a consumer's data.
§ 1:2 General privacy principles

Laws that regulate privacy and security typically involve restrictions on the collection of data (usually information that identifies a person, particularly if coupled with other sensitive information), the transfer, or dissemination, of information, the security of the information, as well as the accuracy of the information that is collected and stored. As the discussion below demonstrates, certain organizations have expressed these principles in different ways, but all of these laws involve the application of these principles.

§ 1:3 Organisation for economic co-operation and development guidelines: a beginning

The Organisation for Economic Co-operation and Development (“OECD”) is a group of 30 member countries, including the United States, that wish to foster democratic government and the market economy. The OECD was one of the first organizations to recognize the issues that privacy could create in a global economy and to generate what was, in essence, a model for member countries to follow regarding privacy practices. This occurred on September 23, 1980, when the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (“OECD Guidelines” or “Guidelines”) were adopted. If there is one document that served as the basis of the privacy laws that are in existence today, particularly the EU Data Directive, it is the OECD Guidelines. While these guidelines are not binding, even on the member countries, they are useful in providing a framework for later privacy legislation.

The principles in the OECD Guidelines are the:
- Collection limitation principle;
- Data quality principle;
- Purpose specification principle;
- Security safeguards principle;
- Openness principle;
- Individual participation principle;
- Accountability principle; and

[Section 1:3]

1See, generally, http://www.oecd.org/document/58/0,2340,en_2649_201185_1889402_1_1_1_1,00.html (last visited May 5, 2009).

2Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1_1,00.html (last visited May 5, 2009).
International application principles.

§ 1:4 Scope of OECD guidelines

The Guidelines apply to personal data,\(^1\) in both the public or private sectors, which, because of the manner in which it is processed, or because of the nature or the context in which it is used, poses a danger to privacy and individual liberties.\(^2\) The Guidelines do not prevent the application to different categories of personal data of different protective measures depending upon the nature and the context in which the data was collected, stored, processed or disseminated; the exclusion from the application of the Guidelines of personal data which obviously does not contain any risk to privacy and individual liberties; or the application of the Guidelines only to automatic processing of personal data.\(^3\)

Exceptions to the Guidelines, set forth in Sections 2 and 3 of the Guidelines, including those that are related to national sovereignty, national security and public policy, were to be as few as possible and made known to the public.\(^4\) Ultimately, these Guidelines were to be considered minimum standards which were to be supplemented by additional measures for the protection of privacy and individual liberties.\(^5\)

§ 1:5 Collection limitation principle

The OECD Guidelines call for limits to the collection of personal data and any such data should be obtained by lawful and fair

---

\(^1\)“Personal data” means any information relating to an identified or identifiable individual (data subject). Guidelines Governing the Protection of Privacy and Transborder Flows of Persona Data, Part 1, Section 1(b).

\(^2\)Guidelines Governing the Protection of Privacy and Transborder Flows of Persona Data, Part 1, Section 2.

\(^3\)Guidelines Governing the Protection of Privacy and Transborder Flows of Persona Data, Part 1, Section 3(a) to (c).

\(^4\)Guidelines Governing the Protection of Privacy and Transborder Flows of Persona Data, Part 1, Section 4(a) to (b).

§ 1:5 Information Security and Privacy

means and, where appropriate, with the knowledge or consent of the data subject.¹

§ 1:6 Data quality principle

Personal data should also be relevant to the purposes for which it is to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.¹

§ 1:7 Purpose specification principle

The purpose for which personal data is collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of these purposes or others that are not incompatible with those purposes and as are specified on each occasion of change of purpose.¹ Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with this requirement except with the consent of the data subject, or by the authority of law.²

§ 1:8 Security safeguards principle

Personal data should be protected by reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification or disclosure of data.¹

§ 1:9 Openness principle

The Guidelines suggest that there should be a general policy of openness about developments, practices and policies with respect

[Section 1:5]
¹Guidelines Governing the Protection of Privacy and Transborder Flows of Persona Data, Part 2, Section 7.

[Section 1:6]
¹Guidelines Governing the Protection of Privacy and Transborder Flows of Persona Data, Part 2, Section 8.

[Section 1:7]
¹Guidelines Governing the Protection of Privacy and Transborder Flows of Persona Data, Part 2, Section 9.
²Guidelines Governing the Protection of Privacy and Transborder Flows of Persona Data, Part 2, Section 10(a) to (b).

[Section 1:8]
¹Guidelines Governing the Protection of Privacy and Transborder Flows of Persona Data, Part 2, Section 11.
to personal data. Readily available means should exist to establish the existence and nature of personal data, and the main purposes of its use, as well as the identity and usual residence of the data controller.¹

§ 1:10 Individual participation principle

The Guidelines suggest that individuals should have the right to: obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; have communicated to him, data relating to him within a reasonable time, at a charge, if any, that is not excessive, in a reasonable manner, and in a form that is readily intelligible to him; be given reasons if a request is denied, and to be able to challenge a denial; and challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.¹

§ 1:11 Accountability principle

A data controller should be accountable for complying with measures which give effect to these principles.¹

§ 1:12 International application—Free flow and legitimate restrictions

The Guidelines also encourage member countries to consider the implications for other member countries of domestic processing and re-export of personal data.¹ Member countries were also encouraged to take all reasonable and appropriate steps to ensure

---

¹“Data controller” means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf. Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Part 1, Section 1(a).

Part 2, Section 12.

¹Guidelines Governing the Protection of Privacy and Transborder Flows of Persona Data, Part 2, Section 13(a) to (d).

¹Guidelines Governing the Protection of Privacy and Transborder Flows of Persona Data, Part 2, Section 14.

¹Guidelines Governing the Protection of Privacy and Transborder Flows of Persona Data, Part 3, Section 15.
that transborder flows of personal data, including transit through a member country, are uninterrupted and secure. A member country was also cautioned to refrain from restricting transborder flows of personal data between itself and another member country except where the other country does not substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A member country may also impose restrictions regarding certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of the data and for which the other member country provides no equivalent protection.

Member countries were also encouraged to avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for these protections.

§ 1:13 National implementation

In implementing the principles set forth in above, member countries were encouraged to establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries were particularly encouraged to: adopt appropriate domestic legislation; encourage and support self-regulation, whether in the form of codes of conduct or otherwise; provide for reasonable means for individuals to exercise their rights; provide for adequate sanctions and remedies in case of failures to comply with

2"Transborder flows of personal data" means movements of personal data across national borders. Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Part 1, Section 1(c).

3Guidelines Governing the Protection of Privacy and Transborder Flows of Persona Data, Part 3, Section 16.


5Guidelines Governing the Protection of Privacy and Transborder Flows of Persona Data, Part 3, Section 17.


[Section 1:13]

1Guidelines Governing the Protection of Privacy and Transborder Flows of Persona Data, Part 4, Section 19.
measures which implement these principles; and ensure that there is no unfair discrimination against data subjects.²

§ 1:14 International cooperation

Member countries were also encouraged, where requested, to make known to other Member countries details of the observance of the principles set forth in these Guidelines.¹ Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other member countries which comply with these Guidelines.² Member countries were also encouraged to establish procedures to facilitate information exchange related to these Guidelines, and mutual assistance in the procedural and investigative matters involved.³

Member countries were also encouraged to work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.⁴

§ 1:15 Principles adopted by the Asia-Pacific Economic Cooperation

The Asia-Pacific Economic Cooperation ("APEC") is an organization similar to the OECD, but for the Pacific Rim.¹ It too has adopted privacy principles that are supposed to serve as the basis for legislation for member countries, APEC Privacy Framework 2004 ("Framework").² As with the OECD guidelines, these are high-level principles that do not provide significant detail regarding legislation, but certain provide a direction for member

²Guidelines Governing the Protection of Privacy and Transborder Flows of Persona Data, Part 4, Section 19(a) to (e).

¹Guidelines Governing the Protection of Privacy and Transborder Flows of Persona Data, Part 5, Section 20.


⁴Guidelines Governing the Protection of Privacy and Transborder Flows of Persona Data, Part 5, Section 22.


countries. These Principles are contained in a Framework that was adopted in 2004.

As a general matter, exceptions to these Principles contained in the Framework, including those relating to national sovereignty, national security, public safety, and public policy should be limited and proportional to meeting the objectives to which the exceptions relate, and made known to the public, or in accordance with law.

§ 1:16 APEC information privacy principles

Preventing Harm

Personal information protection should be designed to prevent the misuse of information, in light of the interests of the individual to legitimate expectations of privacy.\(^1\) Specific obligations should factor in this risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.\(^2\)

Notice

Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that should include: the fact that personal information is being collected; the purposes for which personal information is collected; the types of persons or organizations to whom personal information might be disclosed; the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information; and the choices and means the personal information controller offers individuals for limiting the use and disclosure of, and for accessing and correcting, their personal information.\(^3\)

Additionally, all reasonably practicable steps should be taken to ensure that notice is provided either before or at the time of collection of personal information.\(^4\) Otherwise, notice should be provided as soon after as is practicable.\(^5\) It should be noted that under the Guidelines, it may not be appropriate for personal in-

\(^3\) APEC Privacy Framework 2004, Principle II, Section 15(a) to (e).
\(^4\) APEC Privacy Framework 2004, Principle II, Section 16.
formation controllers to provide notice regarding the collection and use of publicly available information.  

Collection Limitation

The collection of personal information should be limited to information that is relevant to the purpose for which it is collected. The information should be proportional and collected through lawful and fair means, and, if appropriate, with notice given to the individual.

Uses of Personal Information

Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except: with the consent of the individual whose personal information is collected; when necessary to provide a service or product requested by the individual; or by the authority of law and other legal instruments, proclamations and pronouncements of legal effect.

Choice

Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. It may not be appropriate for personal information controllers to provide choice when collecting publicly available information.

Integrity of Personal Information

Personal information should be accurate, complete and kept up-to date to the extent necessary for the purposes of use.

Security Safeguards

Personal information controllers are to protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of infor-

---

The safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment.

**Access and Correction**

The APEC Framework suggests that individuals should be able to: obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them; have communicated to them, after having provided sufficient proof of their identity, personal information about them within a reasonable time, at a charge, if any, that is not excessive, in a reasonable manner, in a form that is generally understandable; and, challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted. Access and opportunity for correction should be provided except where: the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question; the information should not be disclosed due to legal or security reasons or to protect confidential commercial information; or the information privacy of persons other than the individual would be violated. If a request or a challenge is denied, the individual should be provided with reasons why and be able to challenge the denial.

**Accountability**

A personal information controller should be accountable for complying with measures that give effect to these Principles. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to

---

15APEC Privacy Framework 2004, Principle VIII, Section 23(a) to (c).
16“Confidential commercial information” is information that an organization has taken steps to protect from disclosure, where such disclosure would facilitate a competitor in the market to use or exploit the information against the business interest of the organization causing significant financial loss.
ensure that the recipient person or organization will protect the information consistently with these Principles. 20

§ 1:17 Privacy and security—The seven U.S. privacy principles

In the United States, the principles are expressed slightly differently, but also in a form that is non-binding on many companies. There are a variety of state and federal privacy statutes that identify different duties and obligations regarding the level of privacy afforded to consumers’ information. As a general principal the differences relate to the type of information in question, the type of business involved, as well as what jurisdiction the consumer resides in. All of these laws in essence address the privacy principles in different ways. 1

These seven U.S. privacy principles are:

Notice. Companies can be required to give individuals notice about the purpose for which private information was gathered, as well as how information collected by a company will be used. A company can also be required to provide users with information regarding how they can register complaints and inquire regarding privacy issues, whether a company discloses information to third parties, and what the methods and standards are for limiting and using information.

Choice. Companies can be required to give users the option of not disclosing their personal information to a third party and requesting that their information not be utilized for purposes other than those originally disclosed at the time of collection. For certain sensitive information, Companies must receive explicit permission from the user before the information is disclosed to third parties or used for purposes other than that for which it was originally collected.

Onward Transfer. Before a company discloses any information to a third party, it can be required to apply the above-referenced notice and choice principles. If a third party is acting as an agent for a company, the third party in some circumstances can be required to comply with the privacy principles as well.

Access. Companies typically are required to permit users to have access to their personal information. A company can also be required to afford users the opportunity to amend, delete or alter personal information when it is inaccurate, with the caveat that ac-


[Section 1:17]

These principles have been expressed in the EU Safe Harbor principles, which are not applicable to many U.S.-based businesses. They represent general principles regarding privacy and not all of these have been adopted or codified by U.S. law at this time.
cess need not be provided when the cost of providing access would be disproportionate compared to the risk of violation of the individual's privacy, or to provide access would violate another's privacy.

Security. A bedrock principle of many privacy laws is information security. While absolute security is not required, a company can be required to take reasonable precautions to protect private information from misuse, disclosure, unauthorized access or alteration, particularly if affirmative representations regarding data security are made.

Data Integrity. Ensuring the accuracy and completeness of the data can also be required. One of the main principals is that private information collected by a company must be relevant to the purposes for which it was collected.

Enforcement. Companies can also be required to provide some enforcement mechanism to protect an individual's privacy rights, including a reasonably affordable and accessible dispute-resolution system. They can also be obligated to self-remedy problems arising out of its failure to meet the requirements of the principles.
Chapter 10

DATA SECURITY: MAINTAINING AN INFORMATION SECURITY PROGRAM

Morrison & Foerster LLP

Editors
Miriam H. Wugmeister
Morrison & Foerster LLP
New York, NY

Christine E. Lyon
Morrison & Foerster LLP
Palo Alto, CA
Library of Congress Cataloging-in-Publication Data

Global employee privacy and data security law / Morrison & Foerster LLP ; editors Miriam H. Wugmeister, Christine E. Lyon. -- 2nd ed.
  p.cm.
  Includes bibliographical references and index.


K3264.C65G578 2011
342.0858--dc23

2011027106

All rights reserved. Photocopying any portion of this publication is strictly prohibited unless express written authorization is first obtained from the copyright holder.

Published by BNA Books
1801 S. Bell Street, Arlington, VA 22202
bnabooks.com

Printed in the United States of America
I. Introduction

Traditionally, many data security laws focused on protecting specific types of information or information relating to specific types of individuals, such as the federal Gramm-Leach-Bliley Act (GLBA) protections for information relating to customers of financial institutions. Today, however, data security laws tend to focus on personal information generally, without regard to the categories of individuals to whom such information may relate (e.g., requirements relating to any Social Security number (SSN) maintained by a company, as opposed to SSNs relating to its customers).
Accordingly, a company may be required to protect all personal information that it handles, including personal information that relates to prospective, existing, and past customers, employees, vendors, and other individuals. Nonetheless, many companies still tend to focus their information security efforts on maintaining the security of information relating to customers. All companies, however, maintain sensitive personal information relating to their employees, such as national identification numbers that are collected for tax reporting purposes and financial account information that is used for payroll direct deposit purposes. As a result, companies must ensure that they protect sensitive personal information relating to their employees, not only because it is a best practice and will help maintain employee trust, but also because it is often required by applicable law.

In recent years, the issue of data security has received heightened legislative scrutiny, both internationally and within the United States. The principal focus of this scrutiny has been the extent to which companies maintain the security of sensitive personal information relating to individuals. Initially, data security laws tended to focus on how to respond to an information security incident, which is the topic of Chapter 9. More recently, however, the growing trend in data security law is to prescribe substantive requirements for how companies should protect information. That is, data security laws also are now prophylactic in nature and designed to prevent, as opposed to respond to, information security incidents. As a result, the varied data security laws have begun to regulate how and when organizations must safeguard personal information to avoid its unintended access or disclosure. As will become evident in this chapter, the data security obligations have a great deal in common and seem to be coalescing around a common set of practices for protecting personal information that requires input from, among others, the human resources group and the technology services organization within a company.

Not long ago, a company’s human resources department would handle all matters related to the company’s employees, while the company’s information technology (IT) department would handle its IT issues, with little overlap or interaction between the departments. Today, however, a number of factors compel a different approach, including the growing risk of information security inci-
idents and a common understanding that many of these incidents are rooted in a company’s internal processes. A company must take precautions against both inadvertent and intentional breaches and/or disclosures of the company’s data by its own employees and also by contractors and vendors. At the same time, a company must train and empower its employees to protect the information that provides the company’s livelihood. Only by capitalizing on its investment in its employees, as well as in appropriate technological solutions, can a company successfully protect its data against the growing array of internal and external threats to the security and confidentiality of that data. A company should foster a culture of information security as a core value. This is most readily accomplished when the entire company (e.g., the human resources, IT, physical security and legal departments, and the business owners) works in concert to address and promote information security.

A company must appreciate that sound information security practices are essential for conducting its business. As more countries and more states within the United States impose information security requirements, more and more companies will need to adopt information security programs and practices in order to comply with those obligations. As a result, this chapter describes the key elements of an information security program that a company may need to develop in order to comply with the growing array of laws that impose requirements with respect to the company’s information security practices.

In connection with describing the key elements of an information security program, this chapter provides an overview and sampling of data security laws throughout the world. With respect to the United States, this chapter focuses on detailed information security regulations issued by the Massachusetts Office of Consumer Affairs and Business Regulations (Massachusetts Security Regulation). The Massachusetts Security Regulation, which required compliance by March 1, 2010, is the most comprehensive state effort in the United States to regulate the information security practices of companies. In addition, this chapter describes important international data security requirements by highlighting

---

1201 Mass. Code Regs. §§17.01–17.05.
obligations in Argentina, Italy, Japan, Norway, Poland, and Spain. As a result, this chapter should assist a company in its efforts to strengthen its information security program by highlighting key steps that the company can take to protect data and, in the process, comply with some of the more restrictive data security laws.\(^2\)

### II. Overview of Data Security Laws and Regulations

Within the United States, various laws and regulations require that employers protect personal information relating to their employees. Some of these laws are targeted specifically at employee information. For example, New York law prohibits an employer from communicating an employee’s “personal identifying information” to the general public. The New York law further provides that it is presumptive evidence of a “knowing violation” of the law, which may result in a civil penalty, “if the employer has not put in place any policies or procedures to safeguard against such violation.”\(^3\) In addition, as discussed in Chapter 8, a number of state laws impose data security requirements on employers with respect to employee SSNs.

The vast majority of data security laws that require employers to protect employee information, however, are focused more generally on personal information that relates to any individual, not simply employees. For example, California and Texas have enacted laws that require companies that own or license personal information about residents of those states, including employees, to implement reasonable security procedures to protect that information from unauthorized use or disclosure.\(^4\) Apart from state laws that impose general mandates to protect personal information, some companies may be subject to laws or rules that require the implementation of a comprehensive information security program. For

\(^2\)For clarity, this chapter does not attempt to provide an overview of all international laws on data security, or an overview of any particular international law on data security. Rather, this chapter notes certain obligations required by some of the more restrictive international data security laws—those of Argentina, Italy, Japan, Norway, Poland and Spain—as guidelines for a company’s international data security practices.

\(^3\)N.Y. Lab. Law §230-d.

example, the Massachusetts Security Regulation requires “[e]very person that owns, licenses, stores or maintains personal information about [a Massachusetts] resident [to] develop, implement, maintain and monitor a comprehensive, written information security program applicable to any records containing such personal information.”

In addition, the Federal Trade Commission (FTC) has adopted rules under the GLBA (the Safeguards Rule) that require a financial institution to implement a written, comprehensive information security program that, in general, is designed to protect customer information against anticipated threats or hazards to the security of the information, as well as to guard against unauthorized access to, or use of, the information that could result in substantial harm or inconvenience to any customer. At first blush, it appears that the Safeguards Rule does not apply to most companies because the Safeguards Rule applies only to financial institutions subject to the FTC’s jurisdiction under the GLBA and only with respect to financial information relating to financial institutions’ customers. Nonetheless, the Safeguards Rule is important for all companies. The FTC, and even state attorneys general, frequently use the Safeguards Rule as a general benchmark or standard when bringing data security enforcement actions against companies and have taken the position informally that the Safeguards Rule is a “best practice” that should be adopted by all companies. It is also worth noting that, in many respects, the Massachusetts Security Regulation is modeled after the Safeguards Rule.

If a company also operates outside of the United States, it is likely subject to additional data security obligations with respect to personal information relating to its employees. Many foreign

---

5201 Mass. Code Regs. §17.03(1).
616 C.F.R. pt. 314. The federal banking agencies have adopted substantially similar regulations under the GLBA, which apply to the financial institutions subject to each agency’s respective jurisdiction. See, e.g., 12 C.F.R. pt. 364, app. B (FDIC). For the sake of clarity, however, this chapter focuses on the FTC’s Safeguards Rule. However, companies that act as service providers to financial institutions should be mindful of the information security requirements that apply to their financial institution customers and, indirectly, to their service providers. Accordingly, a company acting as a service provider should be prepared to enter into an agreement with a financial institution that, in relevant part, requires the company to use appropriate security controls to protect the institution’s customer information.
laws, including laws in Argentina, Italy, Japan, Norway, Poland, and Spain, require companies to implement written information security programs to protect the security and confidentiality of personal information, including personal information relating to employees.

III. CREATING AN INFORMATION SECURITY PROGRAM

As described above, many laws, both foreign and domestic, require a company to implement a written information security program to protect personal information, including personal information relating to its employees. In developing an information security program, it is important for a company not to focus solely on the technological aspects of data protection, such as firewalls and encryption. While technology often forms the cornerstone of an information security program, many companies tend to neglect a critical component of any effective information security program, namely, their employees. A company’s investment in firewalls, encryption, password protection, and other security measures can be completely undermined, even accidentally, by a single employee. At the same time, employees can be one of the company’s strongest lines of defense against internal and external information security threats.

In order to comply with the myriad data security laws that are coming into force, companies need to create information security programs and practices that protect the company’s information from inadvertent as well as intentional misconduct. This task may seem daunting. Many of the key obligations in data security laws and regulations around the world, however, are in fact similar. Exhibit 10.1 provides a brief overview of some of the common obligations.
## EXHIBIT 10.1
### Selected Domestic and International Data Security Requirements

<table>
<thead>
<tr>
<th>Security Requirement</th>
<th>Safeguards Rule</th>
<th>Massachusetts</th>
<th>Spain</th>
<th>Poland</th>
<th>Japan(^1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Written Security Program</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes [METI &amp; MHLW]</td>
</tr>
<tr>
<td>Security Program Coordinator</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes [MHLW] Desirable [METI]</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
<td>Yes [METI]</td>
</tr>
<tr>
<td>Document Security Breach Responses</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>Desirable [METI]</td>
</tr>
<tr>
<td>Oversight of Service Providers</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes [METI &amp; MHLW]</td>
</tr>
<tr>
<td>Employee Training</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes [METI &amp; MHLW]</td>
</tr>
<tr>
<td>Authentication</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes [METI] Desirable [MHLW]</td>
</tr>
<tr>
<td>Access Controls</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes [METI &amp; MHLW]</td>
</tr>
<tr>
<td>Password Requirements</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Desirable [METI &amp; MHLW]</td>
</tr>
<tr>
<td>Unauthorized Use</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Desirable [METI] Yes [MHLW]</td>
</tr>
<tr>
<td>Malware Controls</td>
<td>N/A</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes [METI]</td>
</tr>
<tr>
<td>Encryption of Data Communicated via Public Network</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Desirable [METI]</td>
</tr>
<tr>
<td>Physical Access Controls</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes [METI]</td>
</tr>
<tr>
<td>Controls on Portable Devices</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Data Destruction/Retention Limits</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Desirable [METI]</td>
</tr>
<tr>
<td>Internal Audits/Reviews</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>Desirable [METI]</td>
</tr>
<tr>
<td>Back-ups</td>
<td>N/A</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td>Desirable [METI]</td>
</tr>
</tbody>
</table>

\(^1\) Guidelines issued by the Ministry of Economy, Trade and Industry (METI) and by the Ministry of Health, Labor, and Welfare (MHLW). The guidelines use the term “desirable” to refer to actions that are not required, but that, if not followed, require the company to articulate the alternative method used.
A. Personal Information

Before discussing the steps that a company should take to develop a robust information security program, it is important to discuss in greater detail the types of information covered by data security laws and regulations. While some data security laws apply broadly to any type of personal information about an individual, many of these laws (particularly in the United States) apply only to narrow categories of personal information.

For example, the Massachusetts Security Regulation applies only to a narrow subset of personal information. Specifically, the Massachusetts Security Regulation applies to an individual’s

first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such [individual]: (a) Social Security number; (b) driver’s license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident’s financial account.7

On the other hand, many foreign data security laws tend to apply quite broadly to any form or type of personal information. For example, Spain’s data security law applies with respect to any “personal data,” which is defined as “any information concerning identified or identifiable natural persons.”8

Notwithstanding the differing scope of the personal information that is covered under the various data security laws, a company may elect to apply many aspects of its information security program broadly to most types of personal information that it maintains. The growing trend in data security regulation is clearly moving toward more detailed and prescriptive requirements for information security programs that protect personal information.

7 201 Mass. Code Regs. §17.02. Under the Massachusetts Security Regulation, the term “personal information” does “not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.” Id.

8 Spanish Organic Law 15/1999 of 13 December on the Protection of Personal Data, Article 3(a).
generally. For a company that operates in multiple jurisdictions, developing a robust information security program that applies broadly to various types of personal information may reduce future compliance costs when new jurisdictions adopt comprehensive data security regulations. Moreover, it may simply be more efficient and less costly for a company to apply its information security program to personal information beyond that which is required, as opposed to attempting to apply various procedures to some types of personal information and not others. Nonetheless, a company may want to limit the scope of some information security controls that may be particularly costly or unduly burdensome (e.g., encryption) to only those types of personal information subject to specific legal obligations.

B. Written Security Program

As discussed above, any company with personal information relating to individuals, including employees, should develop a comprehensive information security program that covers risks arising from both technical failures and human foibles. For companies operating solely or primarily in the United States, the requirements of the Massachusetts Security Regulation provide a particularly useful roadmap for developing comprehensive information security programs.

The Massachusetts Security Regulation requires a company to implement, maintain, and update from time to time a comprehensive, written information security program that is appropriate to the size, complexity, nature, and scope of the company’s activities. Although the data security laws in Argentina, Italy, Japan, Norway, Poland, and Spain impose similar requirements, companies that operate outside the U.S. may need to modify their policies to satisfy specific jurisdictional requirements. For example,
in Poland, a company must maintain a data security policy and instructions on computer system management. The policy should be prepared in Polish, as it must be provided to employees and, in case of inspection, to the data protection authority.\footnote{Polish Regulation, §4.} Under Argentinean law, a company must implement a written information security program that specifies the security measures and procedures that must be followed for information systems that contain personal information, and must update and revise its program when any changes are made to the underlying information systems.\footnote{Argentinean Regulation, Annex 1, Basic Level, paras. 1–10. To facilitate the creation of this program, the data protection agency of Argentina has enacted Disposition 9/2008, which contains in an annex a “model security document” with a sample list of matters that should be included in the information security program. This document, once completed, has to be signed by both the security officer of the company and someone with power of attorney over, or power to represent, the company, e.g., an attorney, a general counsel or someone who can bind the company. This is just a model, and the company does not have to follow this scheme and is free to draft its own security program.} Spanish law requires a company to develop an internal security document, which must be binding on employees who access the information systems.\footnote{Spanish Royal Decree, Art. 88.}

The steps described below should assist any company in developing a comprehensive, written information security program that strikes a workable balance between a company’s security needs and its operational requirements. Information security policies are of little use if the policies would prevent employees from having access to the information that they need to perform their jobs. As a result, the policies, as well as the particular technological controls, must be tailored to the company’s individual needs and practices.\footnote{See 16 CFR §314.3(a).}

To begin, a company should ensure that the relevant policies and procedures that make up its information security program are memorialized in writing. This written information security pro-
gram should describe, among other things, the company’s data classification system; mandatory and recommended uses of access controls; and limitations on the access, use, and disclosure of personal information. The program also may address related issues, such as a requirement for each employee to sign a confidentiality agreement and required elements for agreements with vendors relating to information safeguards and nondisclosure. In addition, the program should identify the process owner and encourage employees to direct questions or concerns to the process owner or her delegate. Companies also may consider providing a means for employees to report concerns or assure employees that the company will not permit any reprisal against an employee for raising a good-faith concern about information security practices.

Moreover, a company should take steps to ensure its written program is followed in actual practice. An information security program should be a living, breathing document that is modified to reflect changes in technology, changes in business operations, and new threats to a company’s information. As described in more detail below, a company should regularly monitor its written program to ensure that its risk-based controls continue to be reasonably designed to prevent unauthorized access to, or unauthorized use of, personal information. A company should periodically and regularly revisit its existing security procedures and controls and upgrade its procedures and security controls as appropriate.

C. Risk Assessment

The foundation for any information security program is a company-specific risk assessment. A company’s information security program should take into account the reasonably foreseeable threats or risks to its data in light of the nature and scope of the company’s business and the sensitivity of the personal information contained in the data. In addition, the company must periodically modify its program, as appropriate, to address the changing nature of these threats and risks.

Moreover, many jurisdictions now require that a company perform a risk assessment. For example, the Massachusetts Security Regulation requires that a company identify and assess reasonably foreseeable internal and external risks to the security,
confidentiality, and integrity of its electronic, paper, and other records that contain personal information.\textsuperscript{15} Moreover, after completing this risk assessment, a company must evaluate and improve, where necessary, its safeguards in order to limit any identified risks.\textsuperscript{16} In sum, a company’s risk assessment should highlight for the company where the greatest threats to its information lie and allow the company to implement security controls to limit those risks.

Similarly, a number of foreign jurisdictions impose specific requirements for risk assessments that companies must perform. For example, Italy requires companies that process sensitive data to include in their security policy documents an analysis of risks applying to data and measures to be taken to ensure data integrity, availability, and protection.\textsuperscript{17} Under Norwegian law, a company must establish criteria for acceptable risks associated with the processing of personal information and carry out a risk assessment to determine the probability and consequences of information security incidents, followed by a comparison of the risk assessment to the established criteria for acceptable risk.\textsuperscript{18} Under Argentinian regulations, a company must perform internal and external audits in order to verify the application of the measures under the security policy.\textsuperscript{19} The relevant audit report has to be submitted to the person responsible for the database for the relevant correcting measures to be adopted. The regulations state that the data protection agency, when carrying out audits or inspections, may be able to consider, on a non-binding basis, the results of these internal and external audits, provided they were performed within the last year.

A company’s risk assessment need not take into account every conceivable threat or risk, only those that are reasonably foreseeable. To begin, a company should consider each aspect of its systems used to process, store, and transmit electronic and paper records containing personal information, including employee

\textsuperscript{15} 201 Mass. Code Regs. §17.03(2)(b).
\textsuperscript{16} Id.
\textsuperscript{17} Italian Code, Annex B, paras. 19.3–19.4.
\textsuperscript{18} Norwegian Regulations, §§2–4.
\textsuperscript{19} Argentinean Regulation: Disposition 11/2006, Annex 1, Medium Level measures, para. 2.
information. A company also must take care to assess the systems used by its service providers to perform these functions on the company’s behalf. To begin its risk assessment, a company could consider several basic questions:

- **what** types of personal information does the company handle;
- **who** has access to each of its systems used to process, store, and transmit personal information (e.g., employees, contractors, customers);
- **where** are the company’s systems located (e.g., at retail locations, the company’s domestic and foreign offices);
- **what** types of environmental hazards pose threats to those systems and how frequently do these hazards occur (e.g., fire, flood, or earthquake); and
- **what** types of existing safeguards has the company implemented to protect personal information (e.g., employee training, encryption, an information classification scheme).

In addition, this assessment should be based on the sensitivity of the data stored in the company’s information systems. For example, the company should assess the nature or severity of the threat or risk depending on whether the data contain personal information about individuals, including employees.

As part of its risk assessment, a company should assess the various forms in which data are maintained. It is not uncommon for information security policies to contain state-of-the-art protections for computerized data, while neglecting to address the creation or handling of paper copies of the same data. In addition, employees may transport data in other forms, such as files saved on the hard drives of their laptop computers or spreadsheets stored in their personal data assistants (PDAs). A company may find that its employees are storing and transporting data in new ways that have not been considered or approved by management. Unless these practices are identified and evaluated, there inevitably will be gaps in the coverage of the information security program. Accordingly, a company should review its information systems and paper records, including electronic databases, computing systems, and storage media, to identify where personal information is commonly maintained or processed. This identification should
assist a company in determining where its information security program should be applied.

After assessing the forms in which its data are maintained, the company should begin evaluating the level of confidentiality protection that should apply to each type of data. This classification process requires balancing the company’s goal of keeping all of its data confidential against its real-world operational needs. It does little good to classify all employee data as uniformly confidential if, in practice, the same confidentiality safeguards will not be followed. In fact, automatically classifying all data as confidential may be counterproductive because, for example, it may increase the difficulty of enforcing trade secret or confidentiality protections. In the event that a company does not comply with its own information security policy, an argument could be made that the company’s noncompliance is evidence that the company does not actually treat the data as secret or confidential. Consequently, a company needs to approach its confidentiality classifications in a realistic manner and avoid setting standards that the company itself cannot meet.

Moreover, a company should review its information collection procedures to assess whether personal information is collected only as reasonably necessary to accomplish the legitimate purposes for which it is collected. As discussed below, limiting the collection of personal information and, further, limiting access to the information to those persons (employees or service providers) who are reasonably required to know such information to carry out the company’s legitimate purposes are essential elements of the company’s program to protect personal information. In addition, a company should limit the amount of time the personal information is retained to periods that are anticipated as reasonably necessary for accomplishing the company’s legitimate purposes.

D. Security Program Coordinator

Establishing a comprehensive information security program is not a one-time project. Instead, a company must continually administer its program and, in light of the changing nature of the reasonably foreseeable threats and hazards to its data and information systems, periodically evaluate and update its program to
control these threats and hazards. As a result, a company generally should identify a particular individual or group as the “owner” of this ongoing process. The process owner should be responsible for ensuring that each category of data is appropriately classified and protected. Additionally, the process owner should take more long-term responsibility for proposing modifications to the information security program based on the company’s evolving business needs and practices.

Many jurisdictions actually require a company to designate a process owner to oversee its information security program. For example, the Massachusetts Security Regulation requires that a company “designat[e] one or more employees to maintain the [company’s] comprehensive information security program.”20 In addition, a number of foreign jurisdictions, including Japan, Poland, and Spain, have a similar requirement.21 Under Japanese law, a company must appoint a process owner who has the required knowledge and experience to be responsible for the protection of employment data.22 Under Argentinean law, the information security program has to identify and name the security officer of the company, and the document must be approved and signed by him.23

E. Employee Training and Awareness

In order to effectuate a company’s information security program, the company’s employees must be aware of, and familiar with, their underlying obligations to safeguard personal information. To begin, companies should consider creating a contractual

20 201 Mass. Code Regs. §17.03(2)(a); see also 16 C.F.R. §314.4(a) (FTC Safeguards Rule).
23 Argentinean Regulation: Disposition 9/2008 and Disposition 11/2006, Annex 1, Medium Level measures, par. 1. Medium level measures must be adopted by private companies performing public utilities and those companies that are subject to bank secrecy regulations or any other secrecy laws.
obligation for their employees to maintain the confidentiality of their data. In some countries, such as Japan, a contract with employees relating to the protection of personal information is part of the specific security requirements. In Norway, a company’s staff must be subject to a duty of confidentiality concerning personal data where confidentiality is necessary; the duty of confidentiality must also apply to other data of significance. This contractual protection can be created by requiring each employee to sign a confidentiality agreement (also known as a nondisclosure agreement). The confidentiality agreement can include a broad definition of information that is considered confidential and should provide specific examples of confidential data (such as formulas, inventions, and customer lists). Additionally, the company can bolster the confidentiality agreement by requiring new employees to sign new-hire certificates and requiring departing employees to sign termination certificates confirming their obligations to maintain the company’s data in confidence. The confidentiality obligations contained under these agreements create legal protections for the company’s data, even if it does not qualify for trade secret protection. Regardless of the particular legal status of the data, maintaining appropriate levels of confidentiality is integral for preserving any type of legal protection against disclosure of the data.

The ultimate purpose of the information security program is to improve and standardize security practices throughout the company. This will happen only if employees know about and understand the particular policies that apply to the company’s data and information systems. Generally, a company cannot sufficiently implement its program merely by distributing certain policies to its employees. Instead, a company should consider a variety of methods to educate its employees and other workers (including temporary and contract employees) about the security controls relevant to the data and information systems with which they work.

26 Many jurisdictions require that a business take steps to limit the access terminated employees have to personal information. For example, the Massachusetts Security Regulation requires that a company prevent terminated employees from accessing records containing personal information. 201 MASS. CODE REGS. §17.03(2)(e).
One of the best ways to reinforce the elements of a company’s program is to provide employees with training that covers both the basic and more advanced aspects of the relevant information security controls. For instance, employees should be periodically reminded of the importance of everyday precautions, such as deleting or shredding confidential information once it is no longer needed, password-protecting confidential files, and exercising caution in using the public Internet outside the company’s firewall.

Moreover, many jurisdictions require that a company regularly train its employees about relevant information security procedures. For example, the Massachusetts Security Regulation requires a company to train its employees, including temporary and contract employees, regarding the company’s information security program, including the proper use of the company’s computer security system and the importance of personal information security.27 Various foreign jurisdictions, including Italy and Japan, impose similar requirements.28 For example, under Japanese law, a company must provide education and training to those responsible for employee personal data management, as well as those who handle employee personal data.29 In Italy, a company must schedule training sessions for individuals on data management, liability in data processing, and continuous updating. A description of this training session must be included in the security policy document.30

Beyond the basics, employees should be trained about how to handle a worst-case scenario, such as an incident involving a potential breach of security or an environmental hazard that threatens part of the company’s information systems. All employees should know who to call if an information security incident is suspected, and employees with IT responsibilities also should be trained in taking actions to stop or minimize unauthorized access upon learning of a breach. In jurisdictions requiring notice of a security breach, management should be prepared to contact knowledgeable

---

29 Japanese Employment Management Guidelines, §III.3(5).
attorneys to discuss the company’s legal obligations and whether to involve law enforcement to respond to the incident. An information security incident requires a rapid response, and by the time such a breach occurs, it might be too late for this type of planning. Moreover, as discussed below, many jurisdictions require that a company document its response to information security incidents.

In addition, in order to lend credibility to its information security policies and procedures, a company should establish measures to enforce compliance with these policies and procedures. For example, a company should impose disciplinary measures for personnel and vendors that commit violations of the company’s program. In addition, this may be required under applicable law. The Massachusetts Security Regulation, for instance, requires a company to impose disciplinary measures on its employees for violations of the company’s information security program.31

The importance of informing and training employees about information security practices cannot be overstated. Without employees actively involved in fulfilling the company’s information security program, the policies themselves will be of limited value, if any. Moreover, in order to comply with its varied legal obligations, a company must have well-educated and well-trained employees who are prepared to implement and maintain all aspects of the company’s information security program. While employee training need not be conducted on a rigid time frame, a company should ensure that all relevant employees are in fact periodically trained. Moreover, a company should have flexibility in terms of how it provides such training (e.g., posting training modules on the company’s internal Web site and conducting formal training sessions alike should suffice, depending on the particular subject matter).

F. Access Controls

One of the most fundamental principles of information security is limiting internal and external access to sensitive information. While many companies take appropriate steps to limit external access to information, such as by protecting information systems

with firewalls and limiting the third parties with whom they share personal information, companies frequently fail to appropriately limit internal access to information. Simply stated, a company should permit employees to have access to personal information, including employee information, only if those employees need that information to perform their job duties.

Many jurisdictions expressly require companies to establish both external and internal access controls. As an example, the Massachusetts Security Regulation imposes a variety of access control requirements on companies, including limitations regarding physical access to personal information and internal access to company information outside of its business premises.\(^\text{32}\) Similarly, the Massachusetts Security Regulation requires that a company restrict electronic access to records and files containing personal information to those individuals who need such information to perform their job duties.\(^\text{33}\) The laws of many foreign jurisdictions, including those of Argentina, Italy, Japan, Norway, Poland, and Spain, also require companies to establish access controls.\(^\text{34}\) In Poland, for example, a company must apply access control mechanisms in computer systems that are used to process personal data.\(^\text{35}\) In Spain, a company must adopt adequate measures to limit employee access to personal data.\(^\text{36}\)

Aside from minimizing the risk of an information security incident, assigning different levels of confidentiality is essential in preserving the company’s trade secret or other applicable legal rights. Trade secret protection requires that a company prove that: (1) certain data are economically valuable because such data are not known to others; and (2) the company has taken reasonable measures to protect the secrecy of such data. The greater the number of employees with access to the alleged trade secret data, the greater the difficulty of proving that the company has taken

\(^{32}\)201 Mass. Code Regs. §§17.03(2)(c), (2)(e), (2)(g).


\(^{34}\)Argentinean Regulation, Annex 1, Medium Level, paras. 3–5.2; Italian Code, Annex B, paras. 1–11; Japanese METI Guidelines, §II.2(3)(2); Norwegian Regulations, §§2-10 to 2-12; Polish Regulation Appendix, Section II; Spanish Royal Decree, Article 83.

\(^{35}\)Polish Regulation Appendix, Section II.

\(^{36}\)Spanish Royal Decree, Article 83.
reasonable measures to maintain its secrecy. In other words, a company should maintain policies that, in general, support an inverse relationship between the value of certain data and the number of employees with access to that data. Otherwise, the company may not be able to proffer sufficient evidence that would authorize a court to recognize the data as a trade secret, and thus deprive the company of remedies available under the Uniform Trade Secrets Act or similar laws prohibiting the misappropriation of trade secrets. Nonetheless, a company should take measures to create and preserve legal protections for its confidential data, even if the data may not qualify as the company’s trade secret.

In classifying the level of confidentiality that should apply to each category of data, companies generally will find that different data fields or data sets within a single database require different levels of confidentiality and thus different levels of access. For instance, employee compensation is generally treated as confidential, but government identification numbers should be subject to an even greater degree of confidentiality because of the risk of identity theft to the individuals to whom those numbers relate. Thus, managers may be granted access to compensation data from the company’s payroll database, while not being allowed access to the SSNs contained in the same database. In fact, countries such as Argentina and Italy actually require different levels of security and access control for different types of data. In other words, simply because various types of data are stored or processed in the same systems does not mean that all such data should be accorded identical treatment under the company’s information security program.

Additionally, a company must not overlook the access controls necessary to guard against the risk of unauthorized access by former employees or vendors. A company should establish procedures and security controls designed to prevent terminated employees (or vendors whose service contracts have ended) from accessing records or computer systems used to store or transmit

---

37 Argentina requires a detailed access registry to be made available for databases that contain sensitive personal data. See Argentinean Regulation, Annex 1, Critical Level, para. 2. Italy requires access to archives containing sensitive or judicial data to be controlled. See Italian Code, Annex B, paras. 19–24.
personal information. This includes developing procedures to deactivate an employee’s user name and password for the company’s computer systems immediately when the employee is terminated.

G. Physical Access Controls

Companies frequently make the mistake of focusing solely on electronic access controls. While a company that predominately maintains and processes personal information in electronic form may reasonably determine that its most significant threat involves electronic access, all companies should implement controls to limit physical access to personal information as well. Simply stated, a company must develop policies and procedures to limit access to physical records containing personal information to those individuals who need such access to perform their job duties. In fact, the Massachusetts Security Regulation requires that a company establish reasonable restrictions upon physical access to personal information.\(^{38}\) For example, the Massachusetts Security Regulation further requires that a company store physical records containing personal information in locked facilities, storage areas, or containers.\(^{39}\) Similarly, under Spanish law, only personnel authorized in the written security document may have access to the physical equipment that supports the information systems.\(^{40}\)

Personal information, including employee information, should not be left in areas in which unauthorized individuals may access such information. Instead, personal information in paper form should be locked in filing cabinets, drawers, or other secure areas. Moreover, a company should implement physical controls over areas of its premises that frequently contain personal information or where personal information is processed. For example, a company should implement card key access to rooms or areas that contain personal information, such as rooms that house servers.

\(^{38}\)201 Mass. Code Regs. §17.03(2)(g).

\(^{39}\)Id.

\(^{40}\)Spanish Royal Decree, Art. 99.
H. Technical Security Controls

Technical security measures often form some of the most fundamental elements of an information security program. The growing trend in data security legislation is for jurisdictions to impose express and detailed requirements for technical controls that companies must adopt. For example, the Massachusetts Security Regulation requires a company to adopt security controls that are specifically tailored to its computer systems, including its wireless systems, such as detailed requirements for the authentication of users of its computer systems.\textsuperscript{41} The Massachusetts Security Regulation also includes various requirements for firewalls, malware, and virus protection.\textsuperscript{42} Moreover, the Massachusetts Security Regulation requires that a company monitor its computer systems for unauthorized use of, or access to, personal information.\textsuperscript{43} These technical security controls will play an important role in assuring that only authorized individuals have access to personal information. A number of foreign jurisdictions have similar provisions. For example, the laws of Spain and Italy also contain authentication requirements.\textsuperscript{44} In addition, in Poland, Norway, and Argentina, companies must take measures to secure their computer systems against malicious software.\textsuperscript{45}

In implementing technical security controls, a company should ensure that it does not overlook systems or devices used to store or transport personal information, including employee information. As discussed above, a company should develop appropriate controls to protect information stored both in electronic and paper form. In addition, a company should consider the various devices used to process, store, and transmit the company’s data. For example, smartphones are increasingly used to store information, and, among other risks, smartphones are easy to misplace or lose, owing to their small size and portable nature. At a minimum,

\textsuperscript{41} See 201 Mass. Code Regs. §17.04.
\textsuperscript{42} Id. §§17.04(6)–(7).
\textsuperscript{43} Id. §17.04(4).
\textsuperscript{44} Spanish Royal Decree, Art. 93; Italian Code, Annex B, paras. 1-11.
\textsuperscript{45} Polish Regulation, §5; Norwegian Regulations, §2-13; Argentinean Regulation, Annex 1, Basic Level, para. 9.
companies should place password protections on laptops, PDAs, and other devices containing confidential information.

Companies that allow employees to store confidential data on their personal or noncompany-managed devices, such as personal laptops, home computers, or PDAs, should reconsider this practice. Not only does a company face obstacles to ensure that personally owned (or noncompany-managed) devices are equipped with appropriate access controls, but a company can rarely ensure that all company data will be permanently deleted from the device when the employment relationship ends. In addition, in those instances in which the company needs access to documents stored on a computer (such as in response to a document request or subpoena), if the company does not own or control the computer or device, gaining access can be difficult. Ideally, the company should have ready access to all laptops, smartphones, and other devices used to store confidential company data. Passwords also should be used to protect individual files or documents containing highly confidential information. An organization should consider adopting a policy that any documents that contain highly sensitive information should be password-protected.

Encryption deserves special discussion because of the security breach notification laws enacted in most states in the United States and other jurisdictions (see Chapter 9). In general, these laws require any person or business conducting business in the relevant state to provide notice in the event of a security breach of computerized data containing unencrypted “personal information” relating to that state’s residents. Under these laws, “personal information” is generally defined as an individual’s name in combination with one or more specified data elements, such as an SSN, if either the name or the data element is unencrypted. If the company’s controls are breached and personal information is acquired by an unauthorized person, including by an employee under certain circumstances, the company must notify each of the individuals potentially affected by the breach. The costs of notifying individuals, particularly the company’s customers, about a security breach are not solely monetary but can include reputation and relationship damage as well. As a consequence, companies should reevaluate whether it is truly necessary to maintain SSNs or other sensitive data elements that may trigger a notice
Global Employee Privacy

I. Data Destruction/Retention Limits

A company can often limit its risk of harmful information security incidents simply by not retaining personal information, including employee information, beyond the time period for which

obligation. These security breach notification laws also provide a significant incentive for companies to encrypt the personal information that they do maintain, thus limiting or avoiding entirely notification obligations under these laws.

Notwithstanding these security breach notification laws, a likely growing trend in data security legislation is to prescribe explicit encryption requirements. For example, the Massachusetts Security Regulation prescribes several standards for the encryption of personal information that is stored and transmitted. Specifically, the Massachusetts Security Regulation requires the following types of encryption: (1) encryption of all personal information that is stored on laptops and other portable devices; and (2) encryption of all records and files containing personal information that is transmitted by the company and will travel across public networks or that will be transmitted wirelessly.\(^\text{46}\) In addition, Nevada has enacted a law that specifically prohibits a business in that state from “transfer[ring] any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of the electronic transmission.”\(^\text{47}\) Similarly, the laws of Argentina and Spain contain requirements that certain personal data that is “outside of the “system” be encrypted.\(^\text{48}\) In Argentina, sensitive personal data that are transmitted through communications networks must be encrypted or otherwise protected.\(^\text{49}\) In Spain, personal data that contain sensitive information must be encrypted or otherwise protected when transmitted via electronic communications, or public or wireless networks.\(^\text{50}\)

\(^{46}\) See, e.g., 201 Mass. Code Regs. §§17.04(3), 17.04(5).
\(^{48}\) Argentinean Regulation 11/2006; Spanish Royal Decree, Art. 101.
\(^{49}\) Argentinean Regulation, Annex 1, Critical Level, para. 4.
\(^{50}\) Spanish Royal Decree, Art. 104.
the company actually needs such information to conduct its business. If a company fails to dispose of personal information after it no longer needs such information, the damage of an information security event can often be magnified. For example, if a company collects government identification numbers from its employees for tax reporting purposes only, the company should not maintain numbers relating to past employees beyond the time period for which it will actually need them, for example, to respond to a tax audit. Many jurisdictions now impose express requirements that companies limit how long they retain personal information, including, for example, the European Union (EU) Member States.51

Companies must also take appropriate measures to protect data from unauthorized access during the disposal process. In fact, along with security breach notification, the disposal of information was part of the initial focus of U.S. data security legislation. Now, many jurisdictions impose disposal requirements. For example, under Connecticut law, a company must “destroy, erase or make unreadable” any data, computer files, and documents containing any information “capable of being associated with a particular individual” prior to its disposal.52 Moreover, the FTC has issued a rule regarding the disposal of information in the context of the Fair Credit Reporting Act, the federal statute regulating the use of consumer report information. Specifically, the FTC’s rule provides that any person in possession of a consumer report or information derived from a consumer report “must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.”53 While this rule expressly only applies with respect to consumer report and related information, the FTC has taken the position in the context of enforcement actions relating to unfair and deceptive acts and practices that all sensitive personal information, not just consumer report information, should be disposed of in accordance with this standard.

51 See, e.g., Norwegian Act of 14 April 2000 No. 31 Relating to the Processing of Personal Data, §28 (Norwegian Law); Polish Act, Art. 26.1.4.
52 Conn. Pub. Act No. 08-167, §§1(a), 1(c).
53 16 C.F.R. §682.3(a).
Similarly, many foreign jurisdictions with data security laws, including Argentina, Italy, Japan, Norway, Poland, and Spain, impose some form of disposal requirement.\textsuperscript{54} For example, under Argentinean law, a company must destroy personal data once it ceases to be necessary or relevant to the purposes for which it was collected.\textsuperscript{55} Similarly, under Spanish law, whenever a company intends to discard a document or medium containing personal information, the company must destroy or delete the document or medium by adopting measures to avoid access to the information contained therein or its subsequent recovery.\textsuperscript{56}

J. Documentation of Security Breach Responses

As discussed in the Chapter 9, a company’s comprehensive information security program should include a plan that is designed to facilitate its ability to respond in a timely manner to an information security incident. The response plan needs to involve key personnel from multiple departments within the company who are responsible for maintaining data systems and communicating with customers, as well as appropriate members from the company’s human resources and legal departments.

In any particular incident, there are three basic steps that every company should take as part of its response:

1. Assess the media and the categories of information potentially affected—namely, assess whether computerized data or paper records are affected and which items of information are involved—to determine whether the affected personal information is subject to notification laws;

\textsuperscript{54}Argentinean Personal Data Protection Act, Act 25,326, §4.7 (Argentinean Act); Italian Code, Annex B, para. 22; Japanese METI Guidelines, §II.2(3)(2); Norwegian Regulations, §2-11; Polish Regulation Appendix, §VI; Spanish Royal Decree, Arts. 92, 112.

\textsuperscript{55}Argentinean Act, §4.7. No regulations implementing this article of the act have been issued, however.

\textsuperscript{56}Spanish Royal Decree, Article 92.
2. Establish and document the facts and circumstances of the incident, and keep records of the investigation up to date; and

3. Determine the number of individuals potentially affected and where they reside so that the company can be sure to satisfy various statutory requirements that depend, in part, on the number of affected individuals.

Beyond these core elements of a response program, the specific circumstances of an incident will dictate the steps to be taken to determine whether to notify individuals or, if the company does not own or license the data, notify the data owner or licensee. Only after investigating an incident and assessing the crucial factors under notification laws will a company be able to determine: (1) whether a “breach of security,” within the meaning of these laws, has occurred; (2) the individuals, and possibly regulators, who must be notified; and (3) the appropriate methods and content of the notification.

In addition, a company should document the responsive actions taken in connection with any incident involving a security breach so that the company can make appropriate changes in its business practices, if any, relating to the protection of personal information. This step is actually required under the Massachusetts Security Regulation.57 The law of Spain requires similar documentation.58 In Japan, it is “desirable” for companies to: (1) establish a system for reporting incidents and contacting representatives or the like when personal data has been divulged or other accidents have occurred or there is high probability that they will occur; (2) establish a system for providing information and offering apologies to principals who may be impacted; (3) establish a system for providing reports to the Minister and authorized personal information protection groups; (4) make public announcements of factual relationships and measures to prevent reoccurrence following accidents and violations; (5) investigate the facts; (6) identify

58 Spanish Royal Decree, Art. 90.
the scope of impact; (7) examine the causes; and (8) examine and implement measures to prevent any recurrence.\(^{59}\)

K. Oversight of Service Providers

Companies that provide personal information, including employee information, to vendors or other third parties should implement appropriate policies that require these service providers to protect the information, such as by adhering to nondisclosure agreements. In Japan, companies are required to have contractors sign a nondisclosure agreement.\(^{60}\) At a minimum, a nondisclosure agreement should prohibit a vendor from disclosing the company’s data without written permission, or from using the data for any purpose other than performing the terms of the contract. Typically, companies require their vendors to represent that the vendors (as well as their subcontractors) will implement appropriate technological and procedural safeguards to protect the company’s data and that these safeguards will be at least equal to the safeguards that the company uses to protect its own data. Some companies also require vendors to represent that each of their employees has signed a confidentiality agreement that would cover the company’s data.

Additionally, a company may negotiate an indemnification provision that requires its vendor to reimburse the company for any losses or expenditures that result from a breach of security affecting the company’s data maintained by the vendor. This type of indemnification provision is likely to become more common owing to the potential expense of notifying individuals of a security breach under the various notification laws.

Many jurisdictions have imposed express requirements establishing how a company must oversee its service providers that have access to personal information. For example, under the Massachusetts Security Regulation, a company must take reasonable steps to select service providers that are capable of appropri-

\(^{59}\)Japanese METI Guidelines, §II.2(3)(2). The Guidelines use the term “desirable” to refer to actions that are not required, but that, if not followed, require the company to articulate the alternative method used.

\(^{60}\)Japanese METI Guidelines, §II.2(3)(2).
ately protecting the personal information to which they will have access.\textsuperscript{61} Moreover, the Rule requires that a company require its service provider by contract to implement and maintain appropriate security controls.\textsuperscript{62} Various countries impose similar requirements. In Norway, companies must make certain that service providers ensure data security and document the data system and security measures.\textsuperscript{63} Under Spanish law, a company must ensure that its service providers comply with the data protection regulations.\textsuperscript{64} In Japan, a company must engage in necessary and appropriate supervision of service providers to ensure compliance with required security control measures.\textsuperscript{65} Italy requires service providers to give a company contractual guarantees about data security and compliance with the Code.\textsuperscript{66} In Argentina, when personal data processing services are provided by service providers, the data cannot be used by the service providers for any purpose other than that appearing in the contract, nor can it be communicated to other parties, even for storage purposes.\textsuperscript{67}

L. Internal Audits/Reviews

An integral part of maintaining an effective information security program is ensuring that the program continues to operate in the manner in which it was designed. As a result, a company should regularly monitor its written program to ensure that its risk-based controls continue to be reasonably designed to prevent unauthorized access to, or unauthorized use of, personal information, including when the company experiences a material change in its business operations or when the nature of its needs for personal information change. Even if a company does not experience a material change in its operations, the company should periodically and regularly revisit its existing security procedures and controls. In fact, this is required in many jurisdictions. For example,

\begin{itemize}
  \item \textsuperscript{61}201 Mass. Code Regs. §17.03(2)(f)(1).
  \item \textsuperscript{62}Id. §17.03(2)(f)(2).
  \item \textsuperscript{63}Norwegian Law, §13.
  \item \textsuperscript{64}Spanish Royal Decree, Art. 20.
  \item \textsuperscript{65}Japanese METI Guidelines §II.2(3)(4).
  \item \textsuperscript{66}Italian Code, §29.
  \item \textsuperscript{67}Argentinean Act, §25.1.
\end{itemize}
under the Massachusetts Security Regulation, a company must regularly monitor its information security program to ensure that it is operating in a manner that is designed to prevent unauthorized access to, or use of, personal information and upgrade its information safeguards as necessary to limit these risks.\textsuperscript{68} In addition, under the Rule, a company must review the scope of its security measures at least annually or whenever there is a material change in the company’s business practices that may implicate the security or integrity of personal information.\textsuperscript{69}

Italy, Japan, Norway, and Spain, require companies to update their written information security programs on a regular or annual basis.\textsuperscript{70} For example, under Italian law, companies that process sensitive data must draft a security policy document each year that analyzes the risk to the company’s personal information and that describes the company’s measures to ensure data integrity, availability, and protection. In addition, the authorization profiles of persons in charge of processing must be verified on at least an annual basis.\textsuperscript{71} Moreover, under Norwegian law, a company must carry out regular security audits that are documented and that include an assessment of the company’s security measures.\textsuperscript{72} In Spain, data files must be audited at least every two years to verify compliance with the Royal Decree.\textsuperscript{73} Finally, in Japan, it is “desirable” to designate a person responsible for audits and establish a system for implementing audits.\textsuperscript{74}

\textsuperscript{68}201 Mass. Code Regs. §17.03(2)(h).
\textsuperscript{69}Id. §17.03(2)(i); \textit{see also} 16 C.F.R. §314.3(e) (FTC Safeguards Rule).
\textsuperscript{70}Italian Code, Annex B, paras. 19.3–19.4; Japanese METI Guidelines, §II.2(3)(2); Norwegian Regulations, Section 2-5; Spanish Royal Decree, Art. 88.
\textsuperscript{71}Italian Code, Annex B, paras. 19.3–19.4, 14.
\textsuperscript{72}Norwegian Regulations, Section 2-5.
\textsuperscript{73}Spanish Royal Decree, Art. 110.
\textsuperscript{74}Japanese METI Guidelines, §II.2(3)(2).