Data Protection Masterclass: Cybersecurity & Data Protection Concerns – Current and Upcoming Risks

2 December 2014
Data Protection Masterclass: Cybersecurity & Data Protection Concerns – Current and Upcoming Risks

Table of Contents

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

DP Masterclass:

Cybersecurity & Data Protection Concerns – Current and Upcoming Risks
Data Protection Masterclass:
Cybersecurity & Data Protection
Concerns – Current and Upcoming Risks

2 December 2014
Karin Retzer
Andrew Serwin
Hanno Timner
Miriam Wugmeister
U.S. Rules on Data Security and Data Breaches
Data Security/Destruction Laws

- There are a number of federal and state requirements, which include:
  - GLB Safeguards Rule
  - FTC Act and enforcement cases
  - HIPAA
  - California
  - Massachusetts
  - Minnesota (includes new liability shifting provision)
  - Montana
  - Nevada (encryption requirements)
  - New Jersey
  - New York
  - North Carolina
  - Oregon
  - Rhode Island
  - Tennessee
  - Texas
  - Utah
  - Vermont
  - Washington
  - Wisconsin
Security Breaches Are on the Rise

- Security breaches are becoming more common and reported on more frequently.
Cybersecurity--Threats

- Cyber-terrorism;
- Organized crime;
- Hactivists; and
- Industrial espionage.
Examples of Information

- Your company creates, gathers, and processes a significant amount of information:
  - Financial information;
  - Information regarding individuals (employees, customers, or both);
  - Proprietary/confidential information
    - Undisclosed M&A activity;
    - Business and marketing plans; and
    - Pricing;
  - IP;
  - Information regarding businesses processes, including process improvements;
  - Information regarding business trends;
  - Social data/user generated content;
  - Machine data; and
  - Many other forms of information.
Executive Order

• Executive Order 13636 — Improving Critical Infrastructure Cybersecurity.
• The Framework is supposed to provide a “prioritized, flexible, repeatable, performance-based, and cost effective approach” for cybersecurity risk for critical infrastructure.
U.S. Legal Considerations

• 47 states have data breach laws.
• Certain federal laws also require notice.
• There are other regulators agencies that require notice as well.
Data Breach Laws Vary by State

- 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.

- The requirements of these laws vary and sometimes conflict.
Notice of Security Breach Issues — U.S.

Common issues:

- When must notice be given;
- The form of the notice;
- Who notice must be given to;
- Risk of harm;
- Physical versus electronic data;
- The scope of federal preemption;
- The effect of existing security policies; and
- Emerging issues due to the expansion of data breach laws.
Strategy for Compliance

- Review and comply with the breach notifications laws for each relevant state (i.e., those states where individuals whose personal information is held by the company reside), as well as any other requirements.
- Time is often of the essence.
- Determine whether other entities need to be contacted (state attorney general, office of consumer affairs, FTC, consumer credit reporting agencies).
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 data breach doesn’t mean consumers injured.

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

Asia
Rules on Data Security and Data Breaches
Asia/South Asia: Data Security

• Reasonable organizational, technical, and administrative measures to protect data

• More detailed rules in:
  • India
  • Japan
  • Korea
  • Taiwan
India: Data Security

- Reasonable security practices and procedures
  - Comprehensive documented program and policies
- In the event of a security breach, Government may require the organization to demonstrate that measures in the documented program have been implemented.
- Organizations that have implemented IS/ISO/IEC 27001 standard or an approved code of best practices are deemed to have complied with reasonable security practices and procedures.
  - Such standard or codes must be certified or audited on an annual basis by independent auditors approved by the Central Government.
Japan: Data Security

- Appoint data protection officer
- Perform Risk Assessment
- Supervise service provider and contract
- Implement technical and organizational measures to protect data
- Implement access controls
- Provide secure disposal of PI
Japan (cont’)

• Financial organizations must establish security regulations for:
  • acquisition and input; use and processing; storing and saving; transfer and transmission; deletion and abandonment; and responding to data breaches

• Financial organizations must also encrypt biometric data and save and store separately from other personal data
Korea : Data Security

• Technical, administrative, and physical security measures are required
• Encryption for selected data in transit and certain data at rest (unless mitigating controls in place)
• Internal administrative plan
• “Exert active efforts” to conduct the impact assessment if there is concern that personal data have been infringed
• Training at least twice a year for employees, outsourcing contractors, and developers
Korea (cont’)

- Policy to prevent illegal or unauthorized use of software
- Block access from unauthorized IP addresses
- Separate from the network an administrator’s PC access to a database server
- Change access passwords of Data Managers and other people at least every 3 months
- Perform vulnerability test against new and well-known vulnerabilities at least once per year
Taiwan: Data Security

- Central competent authority for the specified industry sector may require and specify the standards for a security maintenance plan or method of disposal of personal data
- Supervision of service providers required; periodic compliance checks; maintain supervision records
Asian Countries with Breach Notification Laws

- Japan
- Korea
- Philippines
- Taiwan
Japan Breach Notification Rules

• METI
  • Recommended but not mandatory
  • Loss of any unencrypted personal data
  • Regulator or APIPO to be notified about all breaches
  • Notice to individuals in some cases
  • Public announcement (in certain circumstances)
  • Immediate notice when sensitive data involved

• FSA
  • Mandatory
  • Loss of any personal data
  • Immediate notice to regulator
  • “Prompt” notice to individuals
  • “Prompt” public announcement
Korea Breach Notification Rules

- Any leak of Personal Data
- Notice to affected individuals
- Notice to government authorities for leaks involving 10,000 or more individuals
Philippines

- Sensitive personal information or other information that might lead to identity fraud
- Notice to individuals required
- Notice to regulators required
Latin America Rules on Data Security and Data Breaches
Latin America: Data Security

- Detailed rules in:
  - Argentina
  - Costa Rica
  - Mexico
  - Peru
  - Uruguay
- Nicaragua expected to issue additional regulations
Argentina: Data Security

- Three levels of security: High, Medium, Low
- Establish a written security program
- Encryption for transfers of sensitive data
- Supervise service provider and contract
- Implement access controls
- Provide secure disposal of PI
- Employee training
Costa Rica: Data Security

- DPA Registration of Security “Performance Protocol”
- Risk assessment
- Minimum reference security protocol for service providers
  - Requires binding and enforceable privacy and security policies, training manuals, audit procedures, procedures for receiving and responding to access, correction, consent revocation requests and complaints
- At least yearly updates to security measures for sensitive data
- Detailed inventories of data types, infrastructure, licenses, and processing and storage systems
- Documented procedures to supplement, preserve, modify, block, and suppress personal data onsite or in the cloud
Mexico: Data Security

- Administrative, physical, and technical security measures
  - Internal supervision and monitoring system
  - External inspections or audit to check compliance with privacy policies.
  - Analyze causes of any violations and implement corrective, preventive, and improvement actions

- Data Controller must consider taking the following actions:
  - Prepare inventory of personal data and processing systems;
  - Conduct risk analysis
  - Analyze possible security deficiencies
  - Conduct audits
  - Record the means used to store personal data

- Personnel training program to educate and generate awareness about obligations to protect personal data.
Peru: Data Security

- DPA to issue additional requirements
- Data encryption, digital signatures, and checksum verification to prevent unauthorized access, loss, or corruption during data transfers
Uruguay: Data Security

- Regular compliance audits required
- Different security levels assigned to users according to function
- Documented data access and processing procedures
- Restricted access for support, maintenance and testing activities; entry and exit control of support personnel
Data Breach in Latin America

Mandatory obligations in

- Colombia
- Costa Rica
- Mexico
- Peru
- Uruguay
Colombia breach notification rules

- When there has been a violation of security codes or where there are any risks in the administration of information of Data Subjects.
- All Personal Data contained in Databases covered by the Law
- No obligation to notify individuals
- Obligation to notify regulators
Mexico Breach Notification Rules

- Breaches of any Personal Data that “significantly affect” an Individual’s property or moral rights
- Covers a Personal Data
- Notice to individuals required
- No notice to regulators
Uruguay breach notification rules

- The obligation to give notice is triggered by the knowledge of a data security breach that could affect the Individuals’ rights in a significant way.

  - Not clear to whom notice must be given
  - No exceptions
  - No content requirements
Europe
Rules on Data Security and Data Breaches
Europe: Data Security

- EU Countries: Reasonable organizational, technical, and administrative measures to protect data
- Very little guidance in most countries
- More detailed rules in:
  - Germany
  - Italy
  - Norway
  - Poland
  - Spain
  - Russia
Spain: Data Security

• Three Tiered System depending on the sensitivity of the data
  • Appoint Information Security Officer
  • Establish a written security program
  • Supervise service provider and contract
  • Implement technical and organizational measures to protect PI
  • Encryption of sensitive PI in transit
  • Implement access controls
  • Provide secure disposal of PI
Poland: Data Security

- Appoint Information Security Officer
- Establish a written security program
- Supervise service provider and contract
- Implement technical and organizational measures to protect data
- Implement access controls
- Provide secure disposal of PI
Germany: Data Security

- Physical Security Controls
- Access Control
- Authorization Process
- Transmission Control
- Input Control
- Monitoring of External Parties
- Availability Control
- Data Segregation
Germany: Draft IT Security Act

- Extend competencies of Federal Office for Information Security (BSI)
  - Information of public in case of data breaches
  - Competence to inspect operators of “critical infrastructure”
  - Serve as central point of contact in case of data security incidents
  - Provide counsel on IT security measures
- “Critical infrastructure” subject to new rules will belong to operators in the areas energy, IT, telecoms, transport, public health, water, food supply, banks, and insurances. Precise definition subject of separate ordinance
- Additional notification obligations of telecoms and tele-media companies in case of severe incidents
- Right of telecoms and tele-media companies to collect and process user data to cure technical defects
- Possibility to restrict cross-border sale of telecoms companies potentially involved in interception activities of police authorities (change of Foreign Trade and payments Act – AWG) – under discussion
Draft Cybersecurity Directive

- Aim is to streamline information sharing about cybersecurity threats to ensure high level of common network and information security (NIS) across Europe
- EP version: Operators of critical infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health will be required (per Chapter IV) to:
  - Assess the risks they face and adopt appropriate and proportionate measures to ensure NIS (in particular, prevent and minimize impact of incidents affecting core services and ensure continuity of services)
  - Report to competent authorities about incidents with a “significant impact” on core services provided
- Competent national authority may require that public be informed
- Hardware manufacturers and software developers may be exempt from Chapter IV obligations
- Unclear whether providers of e-commerce platforms, online payment gateways, social networks, search engines, cloud computing services and app stores may still be covered by Chapter IV (removed by EP)
Draft Cybersecurity Directive (cont’d)

- Factors to determine “significant impact” of an incident
  - Number of users whose core service is affected by the incident
  - Duration of the incident
  - Geographic area affected by the incident
- Sector-specific criteria/NIS relevant standards and/or specifications will be developed to give further guidance and ensure consistent reporting across Member States
- When core services affected are located in several Member States, authority notified will pass notification to authorities in other Member States where services are affected
- Member States must ensure that competent authorities have the power to issue binding instructions to market operators and require them to:
  - Provide information needed to assess security of their networks and information systems, including documented security policies
  - Undergo a security audit carried out by a qualified independent body or national authority and make results thereof available to competent authority
Europe - Security Breach Notification

- No pan-European general breach notification requirements
- Some Member States have statutory breach notification requirements
  - Austria, Germany, and Norway (+ bill in the Netherlands)
- In others, breach notification is based on DPA guidance
  - Denmark, Ireland, Italy, and the UK
- Breach notification mandatory under ePrivacy Directive but limited to ISPs and telecommunication operators
  - Notification is triggered by any breach (no thresholds and no limitations as to data types covered)
  - DPAs must be notified without undue delay
    - Regulation 611/2013: within 24 hours after detection
    - Exception for notifying individuals when breached data are encryptedhashed
  - Regulation 611/2013: but only if (i) adequate measures to prevent, detect, and block breaches were implemented, and (ii) the key was not compromised
Germany Breach Notification Rules

- Notification provisions
  - Loss of sensitive and financial data that may lead to “serious impediments for privacy and other interests” (§ 42 a Federal Data Protection Act; § 109 a Telecoms Act)
  - Immediate notice to individuals
  - Immediate notice to regulators
  - Public announcement may substitute for individual notice when breach affects a broad public
UK Breach Notification Rules

• Data Protection Act 1988 ("DPA")
  ➢ No legal obligation on data controllers to report security breaches, which result in loss, release, or corruption of personal data, but ICO believes that serious breaches should be brought to its attention
  ➢ “Serious breach” is not defined, but should consider:
    ▪ The potential detriment to data subjects
    ▪ The volume of personal data lost/released/corrupted
    ▪ The sensitivity of the data lost/released/corrupted
  ➢ Serious breaches should be notified to the ICO using a specific DPA security breach notification form
  ➢ No set time limit for notifying ICO, although practically the sooner the better
Enforcement Examples

- U.S.: Enforcement via the FTC, State AGs, the SEC, the OCR, and other government regulators, as well as consumer class actions and payment card litigation can result
- Japan: regulatory actions have occurred against several financial institutions as well as against Sony following data breaches
- Korea: there have been several high profile enforcement actions and court cases including the maximum aware of $98,000 (which is the cap). The cap was removed as of November 29th. In addition court can now award up to KRW 3 million (US $2,700) per person as a result of a breach
- UK: FSA fined HSBC Life £1,610,000, HSBC Actuaries £875,000 and HSBC Insurance Brokers £700,000 for losing unencrypted data disks
- UK: ICO fined NHS Trust £325,000 following data security breach affecting thousands of patients and staff
Thank you!

Karin Retzer  
KRetzer@mofo.com  
Brussels

Andrew Serwin  
ASerwin@mofo.com  
San Diego

Hanno Timner  
HTimner@mofo.com  
Berlin

Miriam Wugmeister  
MWugmeister@mofo.com  
New York
Speaker Biographies

DP Masterclass:
Cybersecurity & Data Protection Concerns – Current and Upcoming Risks
Karin Retzer’s practice focuses on the legal aspects of data protection and security, direct marketing, and electronic commerce.

Ms. Retzer assists clients with privacy and data security compliance and risk management, involving both national and international multi-jurisdictional dimensions. She advises on questions regarding data transfers, the handling of information in shared service centers and sourcing transactions, e-discovery, breach notification, and the use of email and the Internet in the workplace. She has drafted privacy policies and guidelines, notices, agreements for data list management, and data transfer and processing contracts for dozens of multinational clients. She also assists clients in their dealings with data protection authorities, developing appropriate responses to requests for information and complaints, and provides legislative and policy advice to clients. Additionally, Ms. Retzer assists clients with privacy audits and data protection complaints and litigation.

Ms. Retzer has particular expertise regarding the implications of legislative restrictions for online tracking, analytics, personalization of Internet content, behavioral advertising, and direct marketing communications. She regularly advises clients on the use of location data gathered through smart phones and location-based services.

In addition, Ms. Retzer advises clients on issues relating to electronic commerce, such as online terms of use, the requirements for online contracts, disclosure obligations, liability for website content, and the legal aspects of online auction sites. She has developed template agreements and negotiated complex commercial agreements for many clients, counseling them not only with respect to legal ramifications, but also taking into account applicable business and technical considerations. Ms. Retzer is listed as a key individual in The International Who’s Who of Information Technology Lawyers 2013.

Her work spans a wide range of industry sectors. Clients include internationally renowned consumer product companies, financial services organizations, technology and telecommunications providers as well as clients in the advertising, hospitality, media and entertainment, healthcare, pharmaceutical, and retail industries.

Prior to joining Morrison & Foerster, Ms. Retzer worked in Paris at the European headquarters of Sterling Commerce, a U.S. supplier of e-commerce products. From 1997 to 1998, Ms. Retzer worked at the European Commission, where she was involved mainly with examining and monitoring Member States’ implementation of European Community directives.

Ms. Retzer regularly writes for a wide variety of publications. She is a member of the IAPP Publications Advisory Board and a contributing author in the publication, Employee Privacy: Guide to US and International Law. She is a member of the Munich bar and the Brussels EU bar, after studies in Regensburg (Germany), Utrecht (The Netherlands), and Munich (Germany). Ms. Retzer is fluent in German, English, and French and has a working knowledge of Dutch. She is a member of the International Association of Privacy Professionals, the German Association for Data Protection and Data Security, the Licensing Executives Society, and the Association for Industrial Property and Copyright Law.
Andrew B. Serwin is a partner in the Global Privacy and Data Security Practice Group at Morrison & Foerster's San Diego and Washington, D.C. offices. Mr. Serwin is internationally recognized as one of the leading consumer protection and privacy lawyers, as well as a thought leader regarding information, and its role in society and the economy. Mr. Serwin also serves as the CEO and Executive Director of the Lares Institute, a think tank focused on information management issues, and is also a member of the advisory team of the Naval Postgraduate School’s Center for Asymmetric Warfare.

Mr. Serwin advises a number of Fortune 500 and emerging companies regarding global privacy compliance and technology transactions, with particular emphasis on incident response and data breaches; international compliance; health care; mobile communications; behavioral advertising; information sharing concerns; cybersecurity; Electronic Communications Privacy Act (ECPA) and wiretap issues; electronic marketing concerns; information security; social media; and compliance with state and federal laws impacting the collection and use of information. Mr. Serwin also has unique experience in representing emerging companies because he founded an online political magazine and serves on the advisory boards of a number of emerging companies.

Mr. Serwin also has extensive litigation and enforcement experience, having served as lead counsel in numerous high-profile Federal Trade Commission (FTC) matters, matters before the Office of Civil Rights, class actions and enforcement matters brought by state attorneys general.

Security magazine named Mr. Serwin to its list of the “25 Most Influential Industry Thought Leaders” for 2009 – he is the only law firm lawyer ever to receive this award, and was ranked second in the 2010 Computerworld survey of top global privacy advisors.

He is recognized by Chambers USA as one of the top privacy and data security attorneys nationwide (2009–2013). 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 recognized Mr. Serwin as a Leading Lawyer in data protection and privacy (2010–2012); clients stated that he “understands business concerns and provides practical, to-the-point advice.” He is recognized by Martindale Hubbell as an AV® Preeminent™ ranked attorney, the highest performance rating available to any individual lawyer. He was selected for inclusion in the San Diego Super Lawyers® lists (2007–2013), including being ranked in the Top 50 lawyers of 2012. Mr. Serwin was selected by his peers for inclusion in The Best Lawyers in America® in the field of information technology law (2010–2015). He is also recognized as a leading lawyer by the San Diego Daily Transcript (2013), and he received the 2012 Securing Our E-City Business Focus Awareness Award.

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.” It was cited by *Ostergren v. Cuccinelli*, 615 F.3d 263 (4th Cir. 2010), and the international title was named one of Thomson-Reuters’s Best Selling Books for 2010.


Mr. Serwin serves as general counsel of the RIM Council of the Ponemon Institute, LLC; a member of the International Advisory Council of APCO Worldwide (a group of more than 60 recognized global leaders and policy experts); the University of San Diego School of Law Alumni Board; the Law Practice Management and Technology Section of the State Bar of California; and the Data Privacy Day Advisory Committee. He previously served as co-chair of the Survey Committee of the American National Standards Institute’s report on PHI, as well as the privacy and the legal subcommittees of the Public Service Accounting Board (PSAB) of the California Health and Human Services Agency. He also previously served as co-chair of the California State Bar’s Cyberspace Law Committee, as a member of the Committee of Administration of Justice, and as a member of the San Diego County Bar Association’s delegation to the Conference of Delegates to the State Bar of California. Mr. Serwin served as a member of the Publications Board for the Business Law Section of the American Bar Association, as well as on the San Diego Venture Group’s PitchFest Board. He is a member of the editorial board of the Cyberspace Lawyer.

Mr. Serwin received his J.D. cum laude from the University of San Diego School of Law in 1995, where he was a member of the Order of the Coif. He earned his B.A. in political science cum laude from the University of California, San Diego in 1992, where he was a member of the Provost's List (1988–1992). He is admitted to practice law in California, New York, and the District of Columbia.
Hanno Timner is the co-managing partner of the Berlin office and head of the Employment and Labor practice group in Germany. He advises and represents national and international employers in all labor law issues and disputes.

His practice focuses on the advising of national and international companies in connection with the labor law ramifications of corporate restructuring, legal consultation on the acquisition of German firms, and on negotiations for the reconciliation of interests and/or social benefit plans, as well as on the employment of management board members, managing directors, and chief executives.

A further main focus is on the advising of national and international firms concerning all data protection issues and compliance issues (especially on the implementation of compliance systems, corporate policies, and whistleblowing systems).

Hanno Timner has extensive experience in the conducting of internal investigations on behalf of companies.

During the period from 1989 to 1990 Hanno Timner worked in London. Mr. Timner has since acquired the official title Fachanwalt für Arbeitsrecht (Specialist in Labor and Employment Law).
Miriam H. Wugmeister
Partner
New York
(212) 506-7213
mwugmeister@mofo.com

Few lawyers in the world have Miriam Wugmeister’s breadth and understanding of privacy and data security laws, obligations, and practices. In the words of her clients, she is “extremely practical and phenomenally smart. Just about one of the best privacy advisers there is” (Chambers USA 2011). Chair of Morrison & Foerster’s market-leading Global Privacy and Data Security Group and ranked among the top in the profession by all major directories, Ms. Wugmeister is regularly called upon by some of the world’s largest and most complex multinational organizations to confront their most difficult U.S. and international privacy challenges. She develops cutting-edge solutions for clients that marry legal compliance with business realities.

Ms. Wugmeister advises organizations on the planning and execution of complex global compliance efforts, assists in the negotiation of strategic deals, and defends regulatory and litigation matters relating to privacy and data security in the U.S. and internationally. She regularly provides advice on data security breach issues; the global collection, use, sharing of employee, customer, vendor, and consumer personal information; ediscovery and monitoring conflicts; social media issues; and cloud computing deals, as well as on developing data security policies and procedures and cybersecurity preparedness and response plans.

As leader of the Global Privacy Alliance (GPA), Ms. Wugmeister encourages the rational development of privacy laws around the world and monitors privacy practices, laws, and regulations globally. On behalf of the GPA’s members, she takes an active role in anticipating upcoming privacy legislation and educating regulators on the commercial implications of proposed regulations. Ms. Wugmeister developed the firm's Privacy Library and the MoFoNotes subscription database so that organizations can keep apprised of privacy and data security compliance requirements in jurisdictions around the world. She is also co-editor of Global Employee Privacy and Data Security Law, Second Edition (BNA Books, 2011).

Chambers USA 2014 and Chambers Global 2014 recommend Ms. Wugmeister in the top tier of U.S. privacy and data security lawyers, and Legal 500 US 2013 recognizes her as a leading lawyer for her “professionalism and strong international presence.” Ethisphere listed her as one of its 2012 “Attorneys Who Matter,” and BTI named her a 2012 Client Service All-Star. Ms. Wugmeister was also noted by Best Lawyers in America 2015.
About Morrison & Foerster

DP Masterclass:
Cybersecurity & Data Protection Concerns – Current and Upcoming Risks
Privacy + Data Security

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 winners of Chambers USA’s award for excellence in the field of Privacy and Data Security 2008 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 lifecycle 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
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 90 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.
Privacy + Data Security

EUROPEAN DATA PROTECTION

We help our clients navigate Europe’s complex patchwork of data protection laws at the EU and individual country level, providing advice on international data transfers and processing of personal data in the employment context and online. We bring years of experience to the complex jurisdictional issues encountered by multinational companies operating in Europe and work with our long-established network of privacy experts to provide in-depth, tailored advice. In particular, we provide advice on the implementation of EU laws in the individual EU Member States, and provide our clients with regular updates, analysis, and practical compliance solutions.

Our privacy group consults and negotiates extensively with European data protection authorities, such as the French Commission Nationale de l’Informatique et des Libertés, the various German Länder Data Protection Commissioners and the UK Information Commissioner’s Office, as well as the European Commission. Our work handling both compliance and advocacy projects gives us an advantage. We are able to translate and clarify high-level policy guidance into concrete compliance actions and, at the same time, use our practical compliance experience to advise government policymakers on how to craft policy in ways that can be translated into sensible compliance actions.

Recent Representative Engagements

- **Consumer Products Company.** We provided advice on global whistleblowing hotlines and codes of conduct, including registration obligations across the EU. We also drafted appropriate communications with employees, internal protocols and procedures, and crafted language to include in contracts with service providers.

- **Several clients – Implementation of ePrivacy Directive.** We have assisted a number of clients in comprehensively tracking and analyzing implementation of the EU ePrivacy Directive in all 30 EEA Member States. The ePrivacy Directive introduced new requirements for data security breach notification, spam and electronic marketing, and the use of cookies and online tracking technologies. We provided and continue to provide our clients with practical advice on how to deal with these legal changes cost effectively across the jurisdictions.

- **Multinational Pharmaceuticals Company.** We advised our client on the choice, adoption, and implementation of Binding Corporate Rules as the global cross-border data handling strategy. We drafted the BCRs, inter-affiliate agreement, and provided comprehensive assistance and advice.

Clients value our “extensive network of attorneys around the world since privacy legal issues are becoming more global every day.”

- Legal 500 US

PARTNER
Karin Retzer
Boulevard Louis Schmidt 29
1040 Brussels, Belgium
+322 340 7364
kretzer@mofo.com

Clients value our “extensive network of attorneys around the world since privacy legal issues are becoming more global every day.”

- Legal 500 US
including preparing presentations to management, drafting communications, and establishing standard operating procedures and complaint handling procedures.

- **Global Health Care Company.** We advised on the adoption and implementation of a global framework agreement. We advised on the approach to consultations with works councils, drafted communications to management, human resources, sales, marketing and clinical research departments, conducted training for the procurement and legal functions globally, and prepared employee notice and consent forms. We also advised on and handled registration requirements in all EEA countries and relevant Latin-American countries, and handled all aspects of data transfer authorizations with regulatory authorities.
Selected Articles & Alerts

DP Masterclass:
Cybersecurity & Data Protection Concerns – Current and Upcoming Risks
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)?

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,
February 19, 2013

Cybersecurity Developments in the U.S. and the EU

By Nathan D. Taylor and Miriam H. Wugmeister

Everyone is talking about cybersecurity. Articles appear almost daily regarding significant cybersecurity events. And over the past two years, the drumbeat for action on the issue of cybersecurity and the protection of the nation’s critical infrastructure has grown louder and louder. In the context of the current debate on cybersecurity, virtually everyone agrees that cyber threats are real, as evidenced by highly publicized cyber events, such as the recent denial of service attacks on banks. Virtually everyone also agrees that protecting critical infrastructure is an important goal. Nonetheless, little consensus has been reached, particularly in the U.S. Congress, on the “appropriate” approach to protecting the nation’s critical infrastructure from cyber threats.

The U.S. Executive Branch and the EU Commission, however, have both now weighed in on the issue. President Obama’s long-awaited and highly anticipated cybersecurity Executive Order (“Executive Order”) was released on February 12, 2013, directing the U.S. government to take various steps to protect the nation’s critical infrastructure from cyber threats.1 Similarly, on February 7, 2013, the European Commission published a proposed Directive on network and information security for “market operators” (the “EU Directive”).2 The EU Directive, once finalized and transposed into Member State legislation, would apply to all “market operators” providing a service in the EU/EEA, including operators of critical infrastructure in the energy, transport, banking, finance, and health sectors, as well as “information society” service providers, such as e-commerce platforms, payment gateways, social networks, search engines, and cloud providers.

1 The Order is available here. The President also released a related presidential policy directive establishing the nation’s policy for the protection of critical infrastructure from all types of threats, which is available here.

While neither the Order nor the EU Directive are immediately or directly applicable to companies, they are indicative of the fact that legislation is likely coming around the world, and companies should begin to prepare now to comply with the key components of possible cybersecurity legislation.

THE EXECUTIVE ORDER

The Executive Order’s clear purpose is to “enhance the security and resilience of the Nation’s critical infrastructure.” It attempts to do so by directing various federal agencies, including principally the Department of Homeland Security (DHS), to take a number of important steps designed to further this goal. In so doing, the Executive Order includes several important principles that were widely supported by the private sector, including provisions designed to improve the sharing of cyber threat information between the U.S. government and the private sector and improvements to the private-sector security clearance process. The Executive Order, however, also creates a regulatory-like process involving the development of cybersecurity standards and the creation of a “voluntary” program to encourage companies to follow these standards. Although the Executive Order does not create new legal obligations for companies, the Order could result in a federal agency responsible for a given sector issuing security requirements for companies within that sector.

Critical Infrastructure Defined

Potentially the most prominent question raised by companies considering the Executive Order is “who will be covered?” Because the ultimate goal of the Executive Order is the protection of the nation’s “critical infrastructure,” the definition of this term largely defines the Order’s scope. In this regard, the term “critical infrastructure” is defined as the “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” While virtually all companies are subject to at least some cybersecurity risks, most companies likely do not maintain the types of systems and assets the destruction of which could lead to a “cyber Pearl Harbor,” in the words of U.S. Defense Secretary Panetta. Nonetheless, the definition provides limited practical guidance, particularly for large companies.

The responsibility to address the complex issue of what infrastructure is critical, at least with respect to infrastructure “at greatest risk,” is left to the Secretary of DHS. Specifically, the Executive Order directs the Secretary of DHS, within 150 days, to conduct a risk-based assessment to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. If a company is identified as the owner and operator of such critical infrastructure, the Secretary of DHS, in coordination with the company’s sector-specific agency, is directed to “confidentially notify” the company and provide the company with the basis for such determination. As a result, ultimately the federal government will decide who is “covered” and who is not. But many companies likely will not be viewed as owners and operators of “critical infrastructure.”

Although critical infrastructure conceptually could be maintained in a wide spectrum of sectors, the Executive Order is largely focused on 16 specific sectors: (1) Chemical; (2) Commercial Facilities; (3) Communications;

---

3 Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City (October 11, 2012), available here.
(4) Critical Manufacturing; (5) Dams; (6) Defense Industrial Base; (7) Emergency Services; (8) Energy; (9) Financial Services; (10) Food and Agriculture; (11) Government Facilities; (12) Healthcare and Public Health; (13) Information Technology; (14) Nuclear Reactors, Materials, and Waste; (15) Transportation Systems; and (16) Water and Wastewater Systems. For companies that do not operate in one of these sectors, the likelihood that DHS would identify that company as owning or operating critical infrastructure may be low.

**Information Sharing**

The issue of information sharing has been a critical one for the private sector throughout the current debate on cybersecurity. Specifically, the private sector has largely supported any effort that would improve the private sector’s access to valuable cyber intelligence that the federal government obtains. For example, if the federal government knows of a specific cyber threat to a company, knowledge about that threat information may significantly assist the company in taking steps to prevent or mitigate the threat. Importantly, the Executive Order directs the Secretary of DHS, the Attorney General and the Director of National Intelligence to each issue instructions to ensure the timely production of declassified reports of cyber threats that identify a specific targeted entity. In turn, the Secretary of DHS and the Attorney General are directed to establish a process to rapidly disseminate declassified cyber threat reports to the targeted entity.

The concept of the federal government sharing cyber threat information with the private sector, however, has raised privacy and civil liberty concerns for some. Historically, the type of information shared between the private sector and the federal government has focused on cyber threat signatures and other technical information (e.g., the signature of a denial of service attack, which ports it is aimed at, where is it coming from, and how), and not personally identifiable information relating to individuals. Nonetheless, the Executive Order attempts to alleviate privacy concerns associated with the contemplated information sharing by directing the federal government to ensure that privacy and civil liberty protections based on the Fair Information Practice Principles are incorporated into its activities to implement the Order.

**Security Clearances**

Another critical issue for the private sector has been the availability of security clearances. Specifically, the private sector has supported efforts to improve private-sector access to security clearances to allow companies to receive critical classified cyber threat information. To address this point, the Executive Order directs the Secretary of DHS to expedite the processing of security clearances to appropriate personnel of owners and operators of critical infrastructure, with priority being provided to those companies notified by DHS that they maintain critical infrastructure. If properly effectuated, this aspect of the Executive Order should prove valuable for companies that own or operate critical infrastructure. But for those companies that do not own or operate critical infrastructure, access to security clearances may be unlikely, at least as a result of the Order.

**The Cybersecurity Standards and the Voluntary Program**

To assist companies in determining the actual security practices to employ to protect their critical infrastructure, the National Institute of Standards and Technology (NIST) will issue (and periodically update) a “Cybersecurity...
Client Alert.

Framework” that includes a set of standards, methodologies, procedures, and processes to address cyber risks.\(^4\) This Framework will identify specific information security measures and controls to help owners and operators of critical infrastructure identify, assess and manage their cyber risks. Importantly, the Cybersecurity Framework is to be developed through “an open public review and comment process.” Companies should have an opportunity to comment on the Framework and could potentially have a meaningful impact on the resulting standards.

In addition, the Secretary of DHS, in coordination with the sector-specific agencies, will encourage companies to implement the Cybersecurity Framework by establishing “a voluntary program to support the adoption of the” Framework (“Voluntary Program”). Because the President cannot directly impose legal obligations on companies, the Executive Order establishes the Voluntary Program to encourage (but not require) the adoption of the Cybersecurity Framework. Of course, this begs the question of why a company would elect to participate in the Program and agree to follow the security standards identified in the Framework. As a result, the Secretary of DHS is directed to establish “a set of incentives” that are designed to encourage companies to participate in this Voluntary Program and to make recommendations to the President as to whether these incentives can be provided under existing law or require new law. It is far from clear that DHS has the legal authority necessary to provide truly meaningful incentives to encourage participation in the Voluntary Program.

Adoption of the Cybersecurity Framework by Federal Agencies

Ultimately, companies in some sectors may find that the Cybersecurity Framework is not entirely “voluntary.” For example, the Executive Order directs the various sector-specific agencies to review the Framework and, where necessary, develop implementation guidance or supplemental materials to address sector-specific risks. To the extent that a sector-specific agency does issue guidance, the guidance could apply broadly to companies within that sector, even potentially those that do not participate in the Voluntary Program or even those that do not own or operate covered critical infrastructure.

Also, the Executive Order directs executive-branch agencies that have responsibility for regulating the security of critical infrastructure to conduct risk assessments comparing existing regulatory requirements with the preliminary Framework issued by NIST.\(^5\) Specifically, these agencies will be charged with determining if existing regulatory requirements are sufficient to address cybersecurity risk. If an agency determines that existing regulatory requirements are not sufficient, it must, within 90 days of the final Framework being issued, propose “prioritized, risk-based, efficient, and coordinated actions” to mitigate cyber risk. The phrase “prioritized, risk-based, efficient, and coordinated actions” is terribly vague. If an executive-branch agency finds that existing cybersecurity requirements for entities subject to its authority are insufficient and that agency also has statutory authority to issue regulations or guidance relating to cybersecurity, the agency may issue regulations. As a result, when the dust settles, some companies could find themselves with new regulatory requirements or guidance directing or expecting them to implement the types of security measures identified in the Cybersecurity Framework.

\(^4\) The Executive Order includes an optimistic timeframe for the development of the Framework: 240 days for a preliminary version and one year for a final version.

\(^5\) An Executive Order cannot direct an independent federal agency to act. Independent agencies include, for example, the Federal Reserve Board, the Federal Communications Commission, and the Bureau of Consumer Financial Protection. See 44 U.S.C. § 3502(5). Nonetheless, the Order “encourage[s]” these independent agencies to consider prioritized actions to mitigate cyber risks for critical infrastructure, consistent with their authorities.
Client Alert.

THE EU DIRECTIVE

The draft EU Directive is designed to protect network and information systems (“NIS”), encourage information sharing among the EU Member States and protect critical infrastructure. As a result, the definition of companies that may be covered by the EU Directive is substantially broader than that proposed by the Executive Order. As currently drafted, the companies covered by the EU Directive would include:

1. Providers of information society services, including e-commerce platforms, Internet payment gateways, social networks, search engines, cloud service providers, and application stores; and

2. Operators of critical infrastructure in the following sectors:
   a. Energy (the non-exhaustive list refers to electricity and gas);
   b. Transport (such as air and maritime carriers, railways, airports, ports, and auxiliary logistics services, including warehousing and storage, cargo handling, and other transportation support activities);
   c. Banking (including savings and mortgage banks and electronic payment providers);
   d. Stock exchanges; and
   e. Health (including hospitals and private clinics and other health care providers).

The main obligations under the EU Directive would be for the covered entities to implement appropriate technical and organizational measures to minimize the risks to “network and information systems on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems.” This would include an obligation to notify the competent national regulator (to be designated by each Member State) about “incidents having a significant impact” on the continuity of the service. The national authority then may decide to notify the broader public when it deems that disclosure is in the public interest. In addition, the European Commission as well as the Member States may issue legislation to specify what security measures must be implemented, as well as how, when, and under what circumstances security incidents must be disclosed to the new national regulator.

New Regulatory Authorities and Goals

Each EU Member State would be obligated to adopt a NIS strategy that would include: (1) a risk assessment; (2) “general measures on preparedness, response and recovery;” (3) a strategy for sharing between the public and private sector; and (4) an education, training, and awareness program. Each Member State would be required to determine which authority within the country would be responsible for implementing and enforcing this EU Directive and to establish a Computer Emergency Response Team (CERT). One key component of the

---

6 The proposed EU Directive would not apply to public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services.

7 The EU Directive would define a Network and Information System as an electronic communications network, a device used to perform automatic processing of computer data, or computer data. Computer data is not defined.

8 Article 7 of the proposed EU Directive states that a “well-functioning” CERT must be established in each Member State under the supervision of the competent authority, to ensure effective capabilities to deal with cybersecurity incidents and ensure effective cooperation across the EU. Annex I to the EU Directive sets out detailed requirements for the CERT, which must be supported by national policy and/or legislation.
Client Alert.

draft EU Directive would be to encourage cooperation among the EU Member State regulators and the CERTs that are to be established. Thus, the EU Directive calls for the appropriate authorities to regularly publish non-confidential information on early warnings on a common website, and share information regarding specific threats and responses to those threats.

Given that it is a proposed Directive (as opposed to a Regulation), each EU Member State would be obligated to implement the EU Directive into its own country’s laws in order for it to have any effect on a company. At this stage, the EU Directive is simply a draft and must first be formally adopted at the EU level. Once adopted at the EU level, Member States will have 18 months to implement that EU Directive into national law. Thus, the earliest implementation of the rules likely would be January 2016.

PRACTICAL IMPLICATIONS

Many companies do not maintain the types of systems and assets that are deemed “critical infrastructure” for purposes of the Executive Order. Nonetheless, the U.S. government (and not companies themselves) will ultimately make the determination of which infrastructure is critical. It is inevitable that DHS will identify some companies as owning and operating critical infrastructure, even though those companies do not believe such identification is appropriate. No company wants to be caught off guard if this occurs. It is important that companies (particularly those in the 16 sectors identified in the Executive Order and the companies identified in the EU Directive) consider the scope and the extent to which new proposed rules may apply to them.

Moreover, even though the Executive Order and EU Directive do not directly create new legal obligations for companies, there are various ways in which the Order or Directive could result in new legal requirements being created. This is true even for companies that do not own or operate the type of infrastructure that is deemed critical. At a minimum, expectations regarding cybersecurity and preparedness will certainly be raised. It is critical that companies not focus on the “voluntary” or broad nature of the Executive Order and the EU Directive and work to improve their data security practices. Also, once the EU Directive is transposed into national law, these Member State laws will apply directly to companies,

While many of the time frames for implementation of the Executive Order are optimistic, it is important to keep in mind that NIST, DHS, and others have already begun their implementation activities. If the Order’s deadlines are met, this year DHS will identify critical infrastructure “at greatest risk” and notify the companies that own and operate that infrastructure, and NIST will issue its preliminary Cybersecurity Framework. Particularly for those companies that believe there may be a risk that certain systems or assets maintained by them may be deemed critical, it is important to engage now. For example, these companies should consider the types of information security measures that may be appropriate in the Framework, any potential practical or technical issues raised by the Executive Order (including with respect to information sharing and the security clearance process), and the types of incentives that would meaningfully encourage participation in the Voluntary Program. When the opportunity arises to contribute to the implementation of the Executive Order, including through the public comment process associated with the development of the Framework, a company should be prepared to do so.
Client Alert.

About Morrison & Foerster:

We are Morrison & Foerster — a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We’ve been included on The American Lawyer’s A-List for nine straight years, and Fortune named us one of the “100 Best Companies to Work For.” Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by Chambers and Legal 500 as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "Global Employee Privacy and Data Security Law," or our free online Privacy Library, please visit: http://www.mofo.com/privacy-data-security-services/ and "like" us on Facebook at http://www.facebook.com/MoFoPrivacy.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.
Beware the Botnets:
Cyber-Security is a Board Level Issue

By Sue McLean

Today, you would be hard pressed to find an organisation that does not use IT systems and the internet to conduct its business. While technology offers great benefits, it also brings risk. As technology becomes ever more complex, the scope and scale of cyber-risks is increasing at an unprecedented rate. Because responsibility to manage cyber-risks rests with each organisation, it needs to be high on each board’s agenda. It’s clear that this is no longer just an issue for the IT department.

Governments around the world are trying to educate businesses about the risk of cyber-crime, while at the same time equipping law enforcement authorities with the tools to prosecute offenders. The EU in particular is seeking to take a lead in efforts to raise the bar in cyber-crime prevention and enforcement and the UK has identified cyber-crime as a ‘Tier 1’ threat to national security alongside terrorism.

Although it will never be possible for cyber-risks to be eradicated entirely, there are many steps that companies can take to address and mitigate cyber-risks and to respond appropriately when an attack occurs. But evidence suggests that many companies are still not putting in place adequate measures to address cyber-security. According to the UK government, "about 80% of known attacks would be defeated by embedding basic information security practices for your people, processes and technology". Indeed, KPMG recently announced that it had been able to collect employee user names, email addresses and sensitive internal file location information about every UK FTSE 350 company using data publicly available on the internet. This kind of data could be used to carry out fraud or obtain companies’ intellectual property. The research also indicated that more than half of the FTSE 350 companies demonstrated potential vulnerabilities to attack because they did not have up-to-date security patches and/or were using old server software. As the Director of GCHQ (the UK’s communications intelligence agency) said in guidance published last year, “Value, Revenue and Credibility are at stake. Don’t let cyber security become the agenda – put it on the agenda.”

BACKGROUND

Cyber-attacks can be conducted using a variety of different methods and technologies, including botnets, denial of service attacks, spamming, pharming, spoofing, malware (e.g., viruses, worms, Trojan horses, etc.), phishing, and ID theft.

Such attacks may be instigated by a wide variety of players for different reasons (e.g., employees accidentally, through negligence or maliciously, competitors conducting industrial espionage, sabotage or intellectual property theft, state sponsored actors such as foreign intelligence services, organized crime gangs, terrorists, cyber criminals intent on fraud and hackers and hacktivists, etc.).
Client Alert

Cyber incidents can be caused by a variety of factors including vulnerable IT systems and networks, insecure email, lost and stolen devices, social engineering, etc. The inside factor cannot be underestimated. According to Symantec’s recent annual Cost of a Data Breach Report, employee actions and system errors were the cause of nearly two thirds of all data security breaches.

Cyber incidents can result in damage to infrastructure, downtime and business interruption, loss of commercially sensitive data, theft of intellectual property, fraud and liability to third parties. Accordingly, the potential harm that can be caused to businesses by cyber incidents is substantial and may include:

- financial losses (e.g., loss of money, the cost of remediating and rectifying damage, impact on share value, loss of revenue, etc.);
- reputational damage (damage to brand, loss of trust with customers, etc.);
- damage to business interests (e.g., loss of business/clients, impact on potential merger/corporate transaction, reduced competitive advantage, etc.);
- legal and regulatory penalties (e.g., fines, etc.); and
- compensation to affected third parties.

LATEST DEVELOPMENTS: UK

Cyber-security is high on the UK government’s agenda. A Cyber Security Strategy was published in November 2011 and various initiatives have since been launched to deal with the issue. Latest developments include the following.

- In September 2012, the UK government published cyber-security guidance for UK businesses explaining what cyber-risks are and providing a 10-step plan for the management of cyber-risks. However, according to a recent survey, although almost all of the companies surveyed thought that their company’s specific exposure to cyber risk was increasing, almost 50% of company boards had not discussed this guidance and 28% of boards had not even seen it.
- In March 2013, the government launched the Cyber Security Information Sharing Partnership (CSIP) to help government and industry share information and intelligence on cyber security threats. The kind of information to be shared includes technical details of an attack, methods used in planning an attack and how to mitigate and deal with an attack. The initiative will initially involve 160 private sector organisations.
- In April 2013, the government published further guidance on cyber security specifically for small businesses.
- In April 2013, the government published its detailed 2013 Information Security Breaches Survey. The survey identified that 93% of large organisations and 87% of small businesses had experienced at least one security breach in 2012. This was an increase of roughly 50% on 2011 figures. The average worst security breach cost large organisations between £450,000 and £850,000 and small businesses £35,000 to £65,000. 81% of respondents briefed their board or senior management on cyber-risk, but the frequency of such briefings varied considerably.
- In May 2013, the government published guidance outlining the required criteria for a cyber-security standard for companies. Businesses have until 14 October 2013 to submit views.
Client Alert

- It has been recently reported that the UK’s intelligence agencies MI5 and GCHQ have written to FTSE 350 companies urging them to carry out cyber-security health checks. The companies have been asked to complete a questionnaire identifying how they protect intellectual property and customer data. The data will then be aggregated anonymously to enable companies to see how they rank compared with their peers. The companies will then be contacted to discuss where the company may be vulnerable under a second stage of the initiative.

Other industry-specific initiatives have been launched. For example, in February 2013 it was reported in the UK parliament that the Financial Services Authority (the UK’s financial regulator prior its replacement by the FCA and PRA in April 2013) is reviewing the cyber practices of 30 major financial institutions. When the review is concluded, the regulator intends to publish an updated version of its Business Continuity Management Practice Guide and a discussion paper.

LATEST DEVELOPMENTS: EUROPE

Pursuant to the EU’s cyber-security strategy, in June 2013 the EU’s cyber-security agency ENISA was formally granted a seven-year mandate with an expanded set of duties and in July 2013 the Cyber-Crime Directive was adopted. In addition, the draft Network and Information Security Directive and the draft Data Protection Regulation continues to make progress through the legislative process.

Cyber-Crime Directive


The new Directive aims to tackle the increasingly sophisticated and large-scale forms of attacks on information systems (including increased use of botnets) that have emerged since the Framework Decision and is intended to enlarge the scope of criminal offences, increase the level of sanctions and provide a reinforced framework for cooperation between the relevant EU agencies and bodies, such as Eurojust, Europol, the European Cybercrime Centre, and the European Network and Information Security Agency (ENISA).

Following the Directive’s publication in the Official Journal, EU member states will have two years to implement the Directive into national law (except for Denmark, which has decided to opt out of the Directive.) Although the Directive has been broadly welcomed, commentators have noted that tracking down the perpetrators of cyber-crime will remain a huge challenge for authorities.

The Directive establishes the following criminal offences, where committed intentionally and without authorization or otherwise permitted by law:

- **Illegal access to information systems**: it will be an offence to access the whole or part of any information system by infringing a security measure.

- **Illegal system interference**: it will be an offence to seriously hinder or interrupt the function of an information system inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible. It will also be an offence to attempt to commit this offence.
Client Alert

- **Illegal data interference**: it will be an offence to delete, damage, deteriorate, alter or suppress computer data on an information system, or render such data inaccessible. It will also be an offence to attempt to commit this offence.

- **Illegal interception**: it will be an offence to intercept, by technical means, non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data.

It will also be an offence to intentionally produce, sell, procure for use, import, distribute or otherwise make available: (i) a computer program designed or adapted primarily for the purpose of committing an offence or (ii) a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed ("prohibited tool"), without authorization or otherwise permitted by law and with the intention that such tool be used to commit one of the offences. In addition to penalizing commission of the offences, it will be an offence to incite, or aid and abet, another to commit any of the offences. The offences only apply in ‘cases that are not minor’. Member States will have the freedom to define what constitutes a minor case (but could include, for example, where the damage caused, or risk to legal interests, is insignificant or is of such a nature that the imposition of a criminal penalty or liability is not necessary, *e.g.*, the activities of ‘ethical hackers’, *etc.*).

Note that the Directive does not impose criminal liability where the acts are committed without criminal intent (*e.g.*, where the person does not know that access is unauthorized or where a person is engaged by an organisation to carry out penetration testing, *etc.*). Also, if a user breaches Terms of Use or an employee breaches a user security policy although this may be considered unauthorized access, this would not attract criminal liability under the Directive (although may be caught by other national law).

The Directive increases the level of criminal penalties to a maximum term of imprisonment of at least two years.

In addition, when committed intentionally, the illegal system and illegal data interference offences will be subject to a maximum term of imprisonment of: (i) at least three years, where a significant number of information systems have been affected through the use of a prohibited tool that was designed or adapted primarily for that purpose; or (ii) at least five years, where the offence is committed within the framework of a criminal organisation, causes serious damage, or is committed against critical infrastructure. Also, where these offences are committed using an innocent party’s personal data this may be regarded as aggravating circumstances.

As we mentioned above, companies may perpetrate cyber-attacks for the purpose of corporate espionage or sabotage or intellectual property theft and the Directive addresses this issue by introducing liability for legal persons. Organisations can be criminally held liable for a cyber-crime offence if: (a) the offence is committed for the organisation’s benefit by any person having a leading position within the organisation; and/or (ii) the lack of supervision or control of a person allows the commission, by a person under the organisation’s authority, of the offence for the benefit of that organisation.

The Directive requires that sanctions for organisations should include fines and may include other sanctions, such as: (i) exclusion from entitlement to public benefits or aid, (ii) temporary or permanent disqualification from the practice of commercial activities; (iii) placing under judicial supervision, (iv) judicial winding-up; and (v) temporary
or permanent closure of establishments which have been used for committing the offence.

**Update on the Network and Information Security Directive**

As we reported in February, a draft EU Directive on network and information security has been introduced that would require a range of organisations that provide critical infrastructure (including key internet enablers and financial institutions) to meet certain security measures in relation to their IT systems and notify regulators of any significant cyber breaches. The draft Directive is currently being scrutinised by EU Member States. The UK government ran a consultation on the draft Directive between 22 May 2013 and 21 June 2013 and will publish its report on the consultation in due course. On 4 July 2013, the UK's privacy regulator, the ICO, published its response to the Directive. The ICO broadly welcomes the objectives of the Directive, but raises a number of concerns. In particular, the ICO makes clear that: (i) it does not wish to take on responsibility for security breaches which do not involve personal data, (ii) it would like to see the removal or minimisation of any personal data disclosed as part of a breach notification, and (iii) it considers the proposals relating to sharing information on risks and incidents to be too vague. The European Parliament is expected to begin consideration of the draft Directive in February 2014.

**Update on the Data Protection Regulation**

Data breaches remain a key cyber-security risk. In the UK, for example, data security breaches account for the vast majority of all enforcement actions brought by the ICO, the UK's privacy regulator. Currently, within the EU, except for personal data breaches involving telcos and ISPs, personal data breach reporting is not generally mandatory\(^1\). However, with the introduction of the Data Protection Regulation, that is set to change. As we have reported previously, the draft Data Protection Regulation, which is intended to replace the existing Data Protection Directive (95/46/EC), introduces broad personal data breach notification requirements. Authorities must be notified without undue delay within 24 hours of the controller becoming aware of the breach. In addition, following notification to the authorities, affected individuals must be notified without undue delay (unless the controller can demonstrate that it applied appropriate measures to protect the data).

Since its publication the draft Regulation has been the subject of extensive negotiations and on 31 May 2013, the Council of the European Union released a draft compromise text. The compromise outlines a more relaxed data breach notification regime, increasing the time period from 24 to 72 hours and requiring only significant breaches resulting in severe material or moral harm to be notified. The European Parliament and Council of the European Union are expected to begin negotiations on the final text of the Regulation in September 2013.

**MANAGING CYBER-RISKS**

In order to deal with cyber-risks, organisations need to put in place a multi-layered strategy that covers prevention, mitigation and reaction and that takes a holistic approach, focusing on people, processes and systems. Organisations should consider the following best practice steps.

\(^1\) See our article [Dealing with Data Breaches in Europe and Beyond](#) for more details.
Client Alert

- Treat cyber-risks as strategic business risks as opposed to purely IT risks and consider what level of risk the organisation is prepared to accept.

- Ensure that you have board and senior stakeholder ownership of the cyber-security strategy. To help non-technical management understand the extent and nature of the potential cyber-security risks, create cyber-security risk metrics and communications that can be easily understood (i.e., avoid technical jargon wherever possible).

- Carry out a thorough risk assessment across the whole business (don’t just focus on the IT department) - identify the company’s key information assets and services, assess their vulnerability to attack and from whom and consider the potential impact if an incident took place. People are often the weakest link, so consider the risks posed by suppliers, employees and other users, in addition to technical risks.

- Ensure that you understand your legal and regulatory obligations (and recourse) with respect to cyber-attacks. Become familiar with any available government, regulatory and industry guidance.

- Establish a governance framework that enables and supports cyber-security management across the organisation.

- Allocate responsibility for cyber-risks appropriately. Use risk registers and other tools to document and monitor risks.

- Consider working with third parties (including other companies in your sector) in order to benchmark, learn from others and help identify emerging threats.

- In terms of employees and other users:
  - implement clear security policies and procedures (including in respect of new technologies and practices which can compound security risks e.g., BYOD, social media, etc.);
  - promote a risk management and incident reporting culture and carry out regularly training to educate users as to the possible security risks and the importance of compliance with your security policies and procedures;
  - carry out appropriate background checks and ensure that third party providers do the same;
  - carry out effective privilege management to ensure that users only have access to the files, systems and data that they need; and
  - monitor compliance with security policies and procedures and investigate and consider disciplinary action in respect of abuse.

- In terms of users of websites, mobile apps and social media networks, etc., put in place appropriate terms of use, security policies, takedown procedures, etc.

- Ensure that security is carefully considered when designing, developing and implementing all IT systems. Implement appropriate malware protection software, ensure that security patches are implemented, ensure secure configurations for all IT equipment and disable unnecessary devices and removable media access. (With systems becoming increasingly complex vulnerabilities are becoming more difficult to identify. New

---

2 See our previous Alert on Bring Your Own Device Challenges for more details.
Client Alert

technology leads to new types of risks. For example, companies must not overlook mobile apps – it has been reported that many apps are currently unprotected against reverse engineering and tampering attacks. And commentators have also acknowledged the potential for security risks posed by disruptive technologies such as the ‘Internet of things’ and ‘Big Data’.

- Keep up-to-date and meet good industry practice and recognized standards in terms of security management (e.g., BSI’s PASS 555:2013 which was published in May 2013, ISO/IEC 27001, etc. Note that ISO/IEC 27001 is currently being revised and is due to be formally published in November 2013. It is expected to include a requirement for senior management commitment).

- Put in place appropriate disaster recovery and business continuity procedures and test those procedures regularly. Ensure that those procedures include clear cyber-security incident response plans covering all appropriate steps (including notification to regulators where required, managing media and communications, etc.).

- Carry out regular monitoring and conduct regular security audits, risk assessments and testing (including penetration testing).

- Check insurance cover and, where appropriate, put in place specific insurance to cover cyber-risks. (Earlier this year, Marsh reported that the number of clients purchasing cyber insurance policies increased by 33% from 2011 to 2012 and also that those companies buying cyber insurance are buying higher limits of cover.)

- Put in place appropriate security measures with all relevant third party providers of goods and services, including appropriate contractual provisions dealing with all relevant aspects of security. Check existing contracts and amend where appropriate to ensure that it is clear what your rights and remedies will be if security requirements are breached (including in terms of notification, indemnification and liability, audit, step-in rights, termination, etc.). Note that certain types of services (e.g., cloud computing) may raise particular security concerns that will need to be addressed.

Contact:

Sue McLean
44 20 7920 4045
smclean@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We’ve been included on The American Lawyer’s A-List for 10 straight years, and Fortune named us one of the “100 Best Companies to Work For.” Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.