Skadden

PRIVACY & CYBERSECURITY UPDATE

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP & AFFILIATES

04.08.13

Flaming Worms, Stuxnets and Other Cyber Threats — The European Union's Response

The media is replete with reports of a botnet onslaught paralyzing Spamhaus, flaming worms usurping strategic information in the Middle East and a stuxnet super weapon wreaking physical damage to Iran's nuclear reactors. Behind these barbaric neologisms hides a real and serious threat to most corporations: cyberattacks. Given the importance and breadth of electronic data stored within corporations today, any unauthorized access could lead to serious consequences ranging from a public relations nightmare to actual, significant monetary damages. When it comes to cyber-attacks, recent examples demonstrate that no organization is too big or too sophisticated to be immune.

In light of the risks involved, corporations must take appropriate measures, while considering the ever-evolving global regulatory regime. In addition to U.S. efforts to address cybersecurity risks,[1] the European Commission published a proposed directive on network and information security.[2] If and when it passes, the directive shall trigger significant changes in the way European companies and those doing business in Europe use information technology.

Propagation and Costs of Cyber-Attacks

Increases in the number of hackers and in illegal infiltration into public and private information systems have caused governmental authorities and the private sector to focus on the exposure of critical information systems to cyber-attacks. As has been widely reported, the variety of cyber criminals include teenage hackers, opportunists attempting to steal money, "sophisticated" hackers who appear motivated by the desire to cripple corporate systems and state actors using cyber weapons as a means of extending real-world warfare and espionage into the digital realm. Economic cyber espionage is particularly pervasive. The French finance ministry was infiltrated at the end of 2010 and in 2012, and even the offices of former President Sarkozy were infected.[3]

As of 2012, only one out of every four companies in the European Union (EU) had an established and regularly reviewed information and communications technology security policy, leaving many Member States vulnerable and ill-prepared to stave off the growing number of sophisticated cyber-attacks.[4] Recognizing the risks facing its constituents, the Commission now seeks to implement new regulatory measures in an effort to enhance cybersecurity. The French and German governments are among those Member States echoing the need for decisive action.[5]

Cybersecurity Measures Taken in the EU

On February 7, 2013, the European Commission published a proposed directive on network and information security designed to further the Commission's cyber-defense strategy which calls for an open, safe and secure Internet. To meet these goals, the Commission stressed that all 27 Member States must work as a unit with common legislative objectives and requirements, concluding that the voluntary approach to network and information security employed to date is insufficient to provide the desired results.[6] The Commission noted that Member States are currently not operating on a level playing field — some Members have both greater capabilities and are better equipped to defend their network information systems than others.[7] This disparity in capabilities and preparedness is viewed by the Commission as an impediment to creating effective collaboration and cooperation among the Member States, without which EU-wide cyber-resilience may remain illusory.[8]

LEARN MORE

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or your regular Skadden contact.

Pierre Servan-Schreiber
Paris
+33.1.55.27.11.30
pierre.servan-schreiber@skadden.com

Stuart D. Levi
New York
+1.212.735.2750
stuart.levi@skadden.com

Shari L. Piré
Paris
+33.1.55.27.11.43
shari.pire@skadden.com

Joshua F. Gruenspecht
Washington, D.C.
+1.202.371.7316
joshua.gruenspecht@skadden.com

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

68, rue du Faubourg
Saint-Honoré
75008 Paris, France
Telephone: +33.1.55.27.11.00

Four Times Square
New York, NY 10036
Telephone: +1.212.735.3000

WWW.SKADDEN.COM

Under the current regulatory framework, only telecommunications companies are required to implement risk management strategies and report network information systems incidents,[9] while only data controllers[10] are required to implement security mechanisms to ensure the protection of personal information.[11] As such, current legislation leaves a void for addressing incidents in sectors other than telecommunications, such as transportation, stock exchanges, aeronautics, cryptology, media, energy and banking, all of which can be adversely affected by information and infrastructure breaches.[12] Absent a more comprehensive legal regime, the Commission determined that Member States may lack effective incentives to report or evaluate breaches, manage risks or design effective cyber-solutions.[13]

The Proposed Directive is aimed at, among other things, bridging this gap. Should it be adopted, the Proposed Directive will require public administrations and market operators to implement and maintain risk management strategies and to report significant network information security breaches to the applicable competent authorities.[14] The Commission will be vested with the authority to dictate the requisite formats and procedures for notification of such incidents.[15] In addition, public administrations and applicable market operators will be required to furnish information necessary to assess the security of their network and information systems and be subject to regular security audits, the results of which would be made available to the competent authorities.[16] Failure to meet security assessments could result in sanctions.[17]

What Companies Would Be Affected?

The Proposed Directive defines a market operator as including certain information society services providers and the operators of critical infrastructure "essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health."[18] An annex to the Proposed Directive provides a non-exhaustive list of market operators, which list includes social networks, search engines, cloud computing services, electricity and gas operators, businesses operating refineries or other treatment facilities, air carriers, railways and businesses in the logistics services sector, certain credit institutions, central counterparty clearing houses as well as hospitals and health care facilities.[19]

Differences in EU and U.S. Proposed Cybersecurity Regulation

The Proposed Directive is being debated in Europe at the same time as a nominally less prescriptive regulatory regime is taking shape in the United States. A recent U.S. executive order (the Cybersecurity Order) focuses on information sharing and regulation related to critical infrastructure cybersecurity. Such "critical infrastructure" includes those private sector assets whose loss, disability or destruction would adversely affect U.S. security, public health or economic prosperity.[20] The Presidential Directive accompanying the Cybersecurity Order makes clear that the same classes of market operators that would be covered by the Proposed Directive in the EU may ultimately face additional regulation in the U.S. under the Cybersecurity Order. The classes of entities covered in the proposed regulations are not, however, completely parallel. By contrast to the Proposed Directive, the Cybesecurity Order and Presidential Directive explicitly identify food and agriculture and critical manufacturing among the covered sectors, but carves out cloud computing applications, social media and search engines.[21]

The Cybersecurity Order establishes a process under which the Department of Homeland Security (DHS) would assess the need for regulation of cybersecurity measures taken at critical infrastructure businesses,[22] and tasks the National Institute of Standards and Technology (NIST) with developing a framework designed to provide critical infrastructure owners and operators with proposed measures and controls which, if implemented, may reduce cyber-risks.[23] While the Cybersecurity Order states that private sector implementation of the framework is voluntary, certain sector-specific regulatory agencies have been asked to address deficiencies found by DHS.[24] More specifically, the Cybersecurity Order requires each such agency to review the extent of its regulatory authority, together with the DHS findings. If regulations are found deficient to address cybersecurity risks, the agencies would be directed to take actions within each such agency's power to enforce compliance by such businesses with the recommendations provided in the NIST framework.[25] Accordingly, critical infrastructure businesses operating in the U.S. may deem it prudent to treat the NIST framework much like their counterparts operating in the EU may treat the Proposed Directive — as a compulsory regulatory regime.

As a result of the different approaches to regulating private sector networks and systems taken in the U.S. and EU, operators should not assume that security measures instituted to satisfy one regulatory or legislative regime will suffice under another. Those operators who may be subject to either regime should pay careful attention as both approaches continue to take shape over the next several months.

Next Steps

The Proposed Directive was submitted to the European Parliament and the European Council for review and adoption. If adopted, the Member States will have 18 months following adoption of the Proposed Directive to transpose or implement it into their respective national laws. In the interim, operators falling within the scope of the Proposed Directive should begin to assess the security of their current systems as if the Proposed Directive were adopted so that they can begin to see where they may have vulnerabilities to be addressed.

More generally, all private sector companies should continue to monitor this area closely and take appropriate steps to minimize the risks associated with cybersecurity threats.

END NOTES

1 *See* Antoinette C. Bush, Stuart D. Levi, Ivan A. Schlager, John M. Beahn and Joshua F. Gruenspecht, "Privacy and Cybersecurity Updated: President Issues Cybersecurity Executive Order," *Privacy & Cybersecurity Update*, Feb. 13, 2013 at http://www.skadden.com/newsletters/Privacy_and_Cybersecurity_President_Issues_Cybersecurity_Executive_Order.pdf; *see also* Antoinette C. Bush, Stuart D. Levi, Ivan A. Schlager, John M. Beahn and Joshua F. Gruenspecht, "Privacy & Cybersecurity Update: NIST Issues Request for Information on Critical Infrastructure Cybersecurity Practices," Mar. 5, 2013 at http://www.skadden.com/sites/default/files/publications/Privacy_Cybersecurity_Update_%20NIST_Issues_Request_for_Information_on_Critical_Infrastructure_Cybersecurity_Practices.pdf.

2 Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, Brussels (Proposed Directive), Feb. 7, 2013 at http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf.

3 Saskya Vandoorne, "Cyber attack hit French Finance Ministry," government says, CNN, Mar. 7, 2011 at http://www.cnn.com/2011/WORLD/europe/03/07/france.cyberattack/index.html?_s=PM:WORLD; Emmanuelle Paquette, "Cyberattaque contre l'Élysée: la défense de Washington," *L'Express*, Nov. 20, 2012 at http://lexpansion.lexpress.fr/high-tech/cyberattaque-contre-l-elysee-la-defense-de-washington_361245.html.

4 *See* Neelie Kroes' European Commission speech, "Towards a coherent international cyberspace policy for the EU," Jan. 30, 2013, delivered in connection with the Global Cyber Security Conference in Brussels, at http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=9568 (Commission Speech), p. 3; *see also* European Commission press release "EU Cybersecurity plan to protect open internet and online freedom and opportunity," Feb. 7, 2013 at http://europa.eu/rapid/press-release_IP-13-94_en.htm (EU Press Release).

5 The French government recommends strengthening security standards imposed on businesses operating in critical sectors, developing risk-management tools and making them available to small and mid-sized businesses and running, within the confines of the legal framework, tests on software security and the means of responding to attacks. Antton Achiary, Joël Hamelin and Dominique Auverlot, *La Note d'analyse*, nº324, *Centre d'analyse stratégique*, March 2013. The German Federal Ministry of the Interior published proposed amendments, which if adopted, would require critical infrastructure operators to disclose cybersecurity breaches to the German Federal office for Information Security. *See* First draft of the Federal Ministry of the Interior at http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_it-sicherheitsgesetz.pdf;jsessionid=B3769DFABA3DFAD5C7FE3DF0B59948F9.2_cid287?__blob=publicationFile.

6 Explanatory Memorandum to the Proposed Directive § 1.1 (Directive Memo).

7 *Id.*

8 *Id.*

9 *See* Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009, Art. 13a, amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorization of electronic communications networks and services. French regulations are broader. In France, telecommunications operators and internet service providers are

required to report data security breaches to French authorities (*Commission nationale de l'informatique et des libertés*). *See Ordonnace* nº2011-2012 du 24 *août 2011 relative aux communications électroniques*.

10 Data controllers are "any natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data". Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "Data Protection Directive"). Banks, airlines, railways, hospitals and hotels provide a few examples of data controllers. On January 25, 2012, the Commission published a proposed regulation designed to replace the Data Protection Directive. *See* Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on free movement of such data at http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf.

11 *See* Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

12 *See* Directive Memo.

13 *See* Cybersecurity Strategy of the European Union: *An Open, Safe and Secure Cyberspace*, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Feb. 7, 2013, p. 6 at http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.

14 Proposed Directive Art. 14. Microenterprises are exempt from risk-management and notification requirements under the Proposed Directive. *See Id.*, which defines microenterprises within the meaning established in Art. 3 of Commission Recommendation 2003/361/EC, May 6, 2003 at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:en:PDF.

15 *Id.*

16 *Id.*

17 *See* Proposed Directive Art. 17, which provides that Member States shall adopt rules on sanctions applicable to infringement of national provisions adopted pursuant to the Proposed Directive.

18 Proposed Directive Art. 3.

19 Proposed Directive Annex II.

20 The White House – Office of the Press Secretary, "Executive Order: Improving Critical Infrastructure Cybersecurity," Feb. 12, 2013, §2. The presidential directive accompanying the Cybersecurity Order defines critical infrastructure as including the following 16 sectors: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear services, transportation systems and water and waste water systems. *See Presidential Policy Directive PPD-21: Critical Infrastructure Security and Resilience*, Feb. 12, 2013 (Presidential Directive).

21 "The Secretary [of Homeland Security] shall not identify any commercial information technology products or consumer information technology services under this section." Cybersecurity Order § 9.

22 Cybersecurity Order §10.

23 Cybersecurity Order § 7a.

24 Cybersecurity Order §10.

25 *Id.*