CYBER SÉCURITÉ

01

US v. EU: A Comparative Approach to Cybersecurity

Stéphane Grynwajc
avocat au barreau de Paris,
attorney at law (NY State)

Les cyberattaques sont une préoccupation à l'échelle mondiale. À ce titre, elles appellent des solutions elles-mêmes mondiales. Pour une entreprise qui fait de la détection, du contrôle, de la prévention et de la gestion des risques sécuritaires au niveau global ses priorités, l'existence de normes et de cadres législatifs et réglementaires différents d'une région à l'autre sont autant de facteurs de risques. Et pourtant, l'Europe et les États-Unis ont approché cette question globale de façon différente.

PE et Cons. UE, dir. 2013/40/UE, 12 août 2013 relative aux attaques contre les systèmes d'information : JOUE n° L 218, 14 août 2013
National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, February 12, 2014

After having introduced the respective approach adopted by the two regions (I), we will combine lessons learned from the two approaches to provide guidance to companies looking to build a global Compliance program that mitigates cross-jurisdictional gaps and risk areas (II).

I. The Legislative and Regulatory Framework

A. The EU Approach

When, on 30 April 2013, EU Home Affairs Commissioner Cecilia Malmström was offered the opportunity to introduce the EU cyberstrategy at a conference organized by the Homeland Security Policy Institute in Washington, DC., she explained that the such strategy is based around 3 main elements: (i) drastically reducing cybercrime; (ii) enhancing the EU cybersecurity and response capabilities; and (iii) supporting the use of the Internet as a freedom tool and for building capabilities around the world. She also explained that, in that area, the EU's preferred approach was to oblige companies to enhance security and report major attacks to governments[1].

The key elements of the draft Directive on Network and Information Security ("NIS Directive"), which was announced on 7 February 2013[2], were its security requirements and incident notification. In particular, it included an obligation to implement appropriate security measures and to report incidents having a "significant" impact on provided services. The proposed obligation was very wide in scope, as to the targeted actors, which included public administrations, providers of "critical infrastructure essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, financial markets and healthcare", and providers of information society services, including social network providers, search engines, application ("app") stores, e-commerce platforms and cloud computing services. As regards incident notification, incidents must be reported to the national competent authorities, which can then decide to disclose the incident to the public or require the companies or public administrations involved to do so.

On 13 March 2014, the European Parliament successfully voted through the draft NIS Directive, but with a number of amendments to the proposed text[3], including the removal of public administrations, software developers and hardware manufacturers, from the scope of the Directive, focusing instead on critical infrastructure providers. As relates to incident notification, the European Parliament has proposed a number of factors to determine the significance of the impact of the incident and whether it is reportable to the national competent authority, e.g. the number of affected users, the duration of the incident, and

1 *http://europa.eu/rapid/press-release_SPEECH-13-380_en.htm.*

2 *http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf.*

3 *http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0244+0+DOC+XML+V0//EN.*

its geographic reach. The amended text will now be examined by the Council of the EU, in the hope that it is adopted before the end of 2014.

B. The US Approach

The US legislative framework for cybersecurity is a complex interplay of more than 50 statutes addressing various aspects of it, without overarching legislation in place.

The latest effort to pass legislation at the federal level was aborted after the Cybersecurity Act of 2012 failed to move past a Republican filibuster, a battle of several months which ended on 2 August 2012 as the bill, which sought to protect computer networks running the power grid, gas pipelines and water supply and transportation systems from hackers fell 8 votes shy of the 60 votes needed.

In the wake of the delay caused by the legislative deadlock, on 12 February 2013, the President issued Executive Order 13636[4], which led to the release by the National Institute of Standards and Technology (NIST), of the "Framework for Improving Critical Infrastructure Cybersecurity"[5]. Such Framework does not have the force of law as much as it is meant to serve as a voluntary, risk-based set of existing standards, guidelines and practices to help organizations manage cyber-risks. The 3 main elements described in the document are the framework core, tiers and profiles. The core presents 5 functions - identify, protect, detect, respond and recover - that taken together, allow, in the words of NIST "any organization to understand and shape its cybersecurity program"[6]. The tiers describe the degree to which an organization's cybersecurity risk management meets goals set out in the framework and "range from informal, reactive responses to agile and risk-informed". The profiles help organizations progress from a current level of cybersecurity sophistication to a target improved state that is aimed at meeting business needs. NIST also released the same day a "Roadmap" document to accompany the framework, which document lays out a path toward future framework versions and ways to identify and address key areas for cybersecurity development, alignment and collaboration[7].

II. The Global Compliance Dilemma

So, legislation on the one hand; voluntary risk-based standards on the other hand: different paths that reflect a philosophical difference in approach to tackling issues faced by the industry. While EU law has grown over the years as a means to achieve harmonization in a coordinated way across all Member States, the US has traditionally favored self-regulation over legislation. And yet, in an area as critical as the protection of a country's critical infrastructure from cyber attacks, many in the US recognize the need for some level of federal regulation to accompany if not spur its adoption by the industry.

It is likely that new US federal legislation on the matter will be proposed in the near future. The EU draft NIS Directive itself won't become law in all of the EU until all Member States have adopted it into their national law, which may take up to 2 years from the adoption of the text at the EU level. Therefore, in both the US and the EU, there isn't at this time a compulsory framework that applies.

Meanwhile, the NIST Framework was adopted after the NIST had conducted 4 cybersecurity workshops and consulted with more than 3,000 individuals and organizations on best practices for securing IT infrastructure. That level of consultation, and the broad industry input, supports the notion that the framework will be recognized as an industry standard globally, not just in the US. If the framework is to be used as an industry standard in a legal proceeding, a company will have to be able to document its compliance with the framework in the language of the framework.

Companies with operations in both the EU and the US should therefore anticipate the probable adoption of the key elements of the NIS Directive while implementing the Framework recommendations as follows:

1. Revise their IT security policy documentation to adopt and reflect the language and vocabulary of the Framework;

2. Establish regular procedures for identifying and address new threats, and for testing security procedures;

3. Ensure that senior management is active in establishing a cybersecurity strategy for the company, and reviewing its implementation, as the framework places senior management at the top of the decision-making process and holds them responsible for complying with it;

4. Implement an Incident Response Plan, which includes setting up a Technical Incident Response Team to respond to an attack and implement the plan, in liaison with senior management, stakeholders, lawyers and independent cyber-experts as necessary; and

5. Comply with notification obligations in those EU countries and US States that already have obligations to notify data protection authorities, as well as affected users.

Whether mandated by law or simply recommended as industry standards, these measures are critical for any company to adopt in anticipation of a cyber-attack, with the dual objective of minimizing business disruption and maintaining consumer confidence. They also serve as a test of a company's readiness to be seen as one which has taken the full measure of the financial, reputational, and legal exposure of a risk cyber-attack on its IT systems, particularly in the wake of recent high profile security breaches[8].

4 *http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.*
5 *http://www.nist.gov/cyberframework/index.cfm.*
6 *http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm.*
7 *http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf.*
8 *http://globaledge.msu.edu/blog/post/6731/cyber-attacks-and-their-impact-on-business.*