EU and US Cybersecurity Strategies and Their Impact on Businesses and Consumers

By: Nir Kshetri

Kshetri, Nir and San Murugesan (2013). "EU and US Cybersecurity Strategies and Their Impact on Businesses and Consumers", IEEE *Computer,* 46(10), October, 84-88.

Made available courtesy of IEEE Computer Society:
http://dx.doi.org/10.1109/MC.2013.350

Abstract:

To secure information systems and protect vital national and global infrastructure, IT professionals need to understand key elements of national cybersecurity strategies and their impact and coordinate their efforts at local, national, and global levels.

Keywords: security | cybersecurity strategy | EU Data Protection Directive | cyberattacks | cyberespionage

Article:

The UK's 2010 National Security Strategy warned that cyberattacks are one of the four highest-priority risks facing the nation. According to US President Barack Obama, cybersecurity is one of the most serious economic and national security challenges the US currently faces (http://tinyurl.com/yexjyz8). Cybersecurity issues now receive greater attention from all stakeholders and are a major force driving the development and implementation of national cyberdefense strategies (http://tinyurl.com/boys7dj).

In February 2013, both the European Commission and the US government released their long-awaited cybersecurity strategies. The European Commission's cybersecurity strategy (http://tinyurl.com/cdejw3a) and its proposed directive on network and information security (http://tinyurl.com/ctkcfhu) represent the EU's comprehensive vision on how best to prevent and respond to cyber disruptions and attacks. Obama issued an executive order (EO), "Improving Critical Infrastructure Cybersecurity" (http://tinyurl.com/b7ag5fr), aimed at increasing cybersecurity for critical infrastructure vital to the US's economy, security, and daily life such as financial, transportation, power, and communication systems.

These strategic directives, despite their arguable incompleteness and lack of full legal stature, have the potential to bring significant improvements to the cybersecurity landscapes of not only these two regions but also the world at large. Moreover, as our experience with other legislative directives such as data privacy standards and regulations indicate, these two important regions and their associated economies could serve as role models for other regions and nations in formulating strong national cybersecurity frameworks and strategies.

To protect information systems and IT infrastructure, IT professionals, information system developers, information security specialists, CIOs, CTOs, and business executives need an informed understanding of key elements of these strategies and their impact.

EU and US Cybersecurity Strategies

The cybersecurity strategies of the EU and US are driven by somewhat different visions and priorities.

The EU strategy builds on the EU data privacy regulations, which are based on the 1995 EU Data Protection Directive and rely on a principle-based framework that provides a model for good practice, which many privacy advocates consider defensible and preferable to models of privacy protection promoted by other countries.

The US cybersecurity strategy places an emphasis on combating cybersecurity threats. For example, according to US-based Fox News, in light of the cyberespionage activities associated with the Chinese government, the US government levied fines and other trade penalties against countries found guilty of engaging in cyberattacks against it (http://tinyurl.com/cq4sxxy).

Table 1 presents a brief summary of EU and US cybersecurity strategies.

In the EU context, the proposed strategy is expected to harmonize cybersecurity-related laws and enforcement in the 28 member states. Although a 1995 directive mandated a uniform data protection standard across member states, the EU is still far from achieving this goal. There have been issues related to substantial heterogeneity in the standard's implementation and interpretation.

To some extent, this problem is also present in the US. There are reportedly 47 different state laws in the US regarding how people should be notified in case of data breaches involving personal information (http://tinyurl.com/cjujzgl). That said, the interstate differences in cybersecurity laws and enforcement are relatively insignificant across the US.

Impact on Businesses and Consumers

As noted earlier, the EU approach is more effective for protecting consumer privacy. Privacy protection in the US faces a substantial Democrat-Republican political party divide. Although they emphasize national security and information sharing, Republican elected officials are against imposing regulations that would increase costs to private firms and require the firms to follow government-set security standards. Democratic officials, on the other hand, like to limit

states' power to access citizens' data held by Internet firms but are less worried about regulatory burden on the private sector (http://tinyurl.com/cnflnbz).

The American Civil Liberties Union is concerned that the Cyber Intelligence Sharing and Protection Act (CISPA) would allow companies to hand over sensitive information to government agencies such as the National Security Agency and the Defense Department without making a reasonable effort to protect privacy. In this regard, compared to CISPA, Obama's EO performs better in protecting privacy and security interests of consumers.

Table 2 compares the impact of the EU and US cyberstrategies on the private sector and consumers.

The EU and US strategies will affect local as well as foreign businesses operating in these economies. The EU directive, which is stricter than US regulations, is likely to have more wide-ranging impact affecting all types of businesses. For instance, it would require more than 42,000 firms in the EU banking, transportation, energy, and healthcare sectors as well as Internet and public administrations to inform their respective national network and information security (NIS) authorities if their networks are attacked (http://tinyurl.com/aommfc2). US companies, on the other hand, are required to publicly disclose security breaches only if sensitive personal information—such as credit card or Social Security numbers—is involved.

It's important to weigh the short- and long-term effects of regulations on firms' cybersecurity practices and performances. In the US, the EO is likely to have a heterogeneous impact on cybersecurity performance in various sectors. For instance, Obama's EO excludes commercial information technology products and consumer information technology services from critical infrastructures, so firms in those sectors are less likely to be affected.

Hence, for firms in sectors outside of critical infrastructure such as media, legal, engineering, consulting, and manufacturing, the EO does little to enhance cybersecurity. In fact, in the long run, the EO is likely to place such companies at a disadvantage because these companies will need to manage cybersecurity in their own way ("US Cyber Security Executive Order Falls Short for the Private Sector," *Financial Times*, 15 Feb. 2013). For instance, although personnel in critical infrastructure sectors might be encouraged to get security clearances, those in noncritical infrastructures might not be in a position to take advantage of such an opportunity (http://tinyurl.com/aqu8cmf).

Some examples of standards envisioned by the EO include ensuring up-to-date antivirus programs, knowing all the points where a company's networks are connected to the Internet, and making sure that employees without proper authorization and potentially insecure devices don't have access to the company networks (http://tinyurl.com/d45fh98). In this way, the proposed standards would force companies to take measures to be more secure.

Some argue that as an increasing number of companies participate in the standards, meeting or exceeding standards could translate into lower premiums charged by insurance companies (http://tinyurl.com/d45fh98). In addition, should there be a security breach, companies complying with voluntary standards are likely to have some liability protection

(http://tinyurl.com/d46amme). Because not all companies will participate in adopting the voluntary standards and procedures, differences in cybersecurity orientation and behaviors among participating and nonparticipating companies could be observable in terms of the cybersecurity-related pressures they face and potential benefits they receive for participating. In this way, the degree of cybersecurity will vary among the sectors depending on adoption level of the voluntary standards and procedures described in the EO.

There are major differences between the US and EU in reporting requirements in cases of cyberattacks on businesses. In the EU, any company offering services online must report incidents of cyberattack on their networks. This means that companies such as Apple, Google, Amazon, Sony, Microsoft, Facebook, Twitter, LinkedIn, DropBox, Flicker, Picasa, and WordPress are not required to report most security breaches in the US, but for their EU operations, reporting is required.

The EO will offer businesses less protection than would be available under CISPA, which would have legally protected businesses from prosecution if they had shared information with intelligence agencies about their customers' or employees' online activities. On the plus side, however, information about cyberthreats that businesses receive from government intelligence is likely to help them enhance their cybersecurity.

The EU cyberspace policy, which is included in the vision and priority of the EU cybersecurity strategy, is a favorable development for cloud providers operating in the EU (N. Kshetri and S. Murugesan, "Cloud Computing and EU Data Privacy Regulations," *Computer*, Mar. 2013, pp. 18-21). That said, some member states are concerned about the compliance costs associated with the EU approach. Newer EU members in particular—owing to a lack of national administrative, economic, and technical capacity—are likely to face higher burdens to comply with the EU regulations. For instance, in an October 2012 questionnaire addressed to the national parliaments of the EU, Romania's Committee for Information Technologies and Communications described financial burdens on private data controllers and argued that further analysis of proposed obligations should be completed to examine the possibility of reducing these additional burdens (http://tinyurl.com/bf5u6bd).

Cybersecurity Strategy Limitations

Both the EU and US cybersecurity strategies are incomplete in some ways—currently lacking teeth and legitimacy. As noted earlier, unlike legislation, the EO cannot compel US firms to comply. Likewise, the member states have not yet adopted the EU directive on network and information security. EU member states will have 18 months to incorporate the directive into their national legislation, once it's approved by the European Parliament.

Likewise, in the US, there are many constraints that will make it difficult for the government to achieve a cybersecurity goal by relying only on an EO. Senior White House officials pointed out that an EO cannot create incentives for companies to share cyberthreat information with the government, eliminate barriers for companies to share cyberthreat information with other companies, impose higher penalties for cybercriminals, and unify and harmonize state laws

governing notification to consumers in case of a data breach at a company (http://tinyurl.com/cax6yoz).

In light of recent survey findings that indicate companies' fail to devote sufficient resources and effort to protect their networks, stronger regulations could force companies to increase spending on cybersecurity. For instance, according to a Bloomberg Government study, in order to prevent 95 percent of potential cyberattacks, 172 organizations in critical sectors need to spend US$46.6 billion, which is 774 percent higher than their current level of spending (http://tinyurl.com/d46amme). Without legal requirements to meet standards and regulations in the cybersecurity space, there is no penalty for companies who put consumers at risk as a result of their lax security.

Both the EU and US cybersecurity strategies fail to explicitly acknowledge key aspects that have long-term cybersecurity implications. Both regions face a severe lack of cybersecurity professionals, and their cybersecurity strategies have no special provisions for dealing with this shortage. For instance, according to the UK's National Audit Office, which has responsibility to make sure the nation spends money wisely, it would take 20 years to bridge the country's cybersecurity skills gap (http://tinyurl.com/cnflnbz). Likewise, according to the National Institute of Standards and Technology (NIST), the US will need more than 700,000 new cybersecurity professionals by 2015 (http://tinyurl.com/c6chf72).

Both economies' cybersecurity strategies are highly inward-oriented and exhibit a low degree of outward orientation: the strategies are largely silent regarding the need to work with key global economies in cybersecurity-related matters. Commenting on the EU directive, the Chinese telecommunications company Huawei emphasized the importance of working globally to deal with cyberattacks. The US-China Business Council, which represents about 230 US companies with operations in China, such as Boeing, Caterpillar, Citigroup, and JP Morgan Chase, have asked the US and Chinese governments to work together to address the growing problem of cyberattacks (D. Palmer, "Trade Group Wants U.S.-China Action on Cyber Security Threats," *Chicago Tribune*, 4 Feb. 2013; http://tinyurl.com/c7godjg). The absence of international cooperation has also insulated some countries and made them safe havens for criminals. For instance, the EU and US have no treaties or other forms of international agreements with Russia to deal with cyberattacks. This has allowed many Russia-based cybercriminals to operate from the country with impunity.

Overall, both the EU and US cybersecurity strategies can be viewed as positive steps that would enhance the general cybersecurity environments of the two economies and of the entire world. Other economies might wish to draw on these two economies' cybersecurity approaches to develop their national cybersecurity frameworks and policies.

Action Agenda for All Cyberspace Participants

Various cyberspace participants have distinct roles to play in making cyberspace safe and secure. Establishing a sound cybersecurity-related regulatory framework, by its very nature, involves cooperation among national governments as well as cooperation between political parties to establish policies and procedures beyond unilateral national or political interests.

As noted earlier, businesses differ in terms of the cybersecurity-related regulations they face. Businesses that don't belong to critical infrastructures can benefit from implementing the standards suggested by the framework even if they are not mandated to do so. Complying with suggested guidelines could shield these companies from cyberattacks, while also possibly lowering their insurance premiums. Finally, consumers can also benefit from adopting some elements of the standards, such as the deployment of up-to-date antivirus programs and firewalls.

We—and generations to come—will use cyberspace more than ever before for a variety of critical and noncritical applications. The increasing usage, however, makes cyberspace a more attractive target for cyberculprits and cyberthreats. Cyberattacks aren't going away—in fact, they will increase, intensify, and become increasingly sophisticated. We must deploy coordinated, multipronged efforts at local, national, and global levels. With active participation from governments, businesses, the IT industry, legal and enforcement agencies, and the public, we can make progress on the common goal of making cyber-physical systems safer and more secure, while setting personal and political differences aside.

Nir Kshetri *is a professor at the University of North Carolina at Greensboro and a research fellow at the Research Institute for Economics and Business Administration at Kobe University. Contact him at nbkshetr@uncg.edu.*

San Murugesan*,* Computer*'s Cloud Cover column editor, is the director of BRITE Professional Services and an adjunct professor at the University of Western Sydney. Contact him at san1@internode.net or follow him on Twitter @santweets.*