BRINK
The Edge of Risk

TECHNOLOGY Cybersecurity

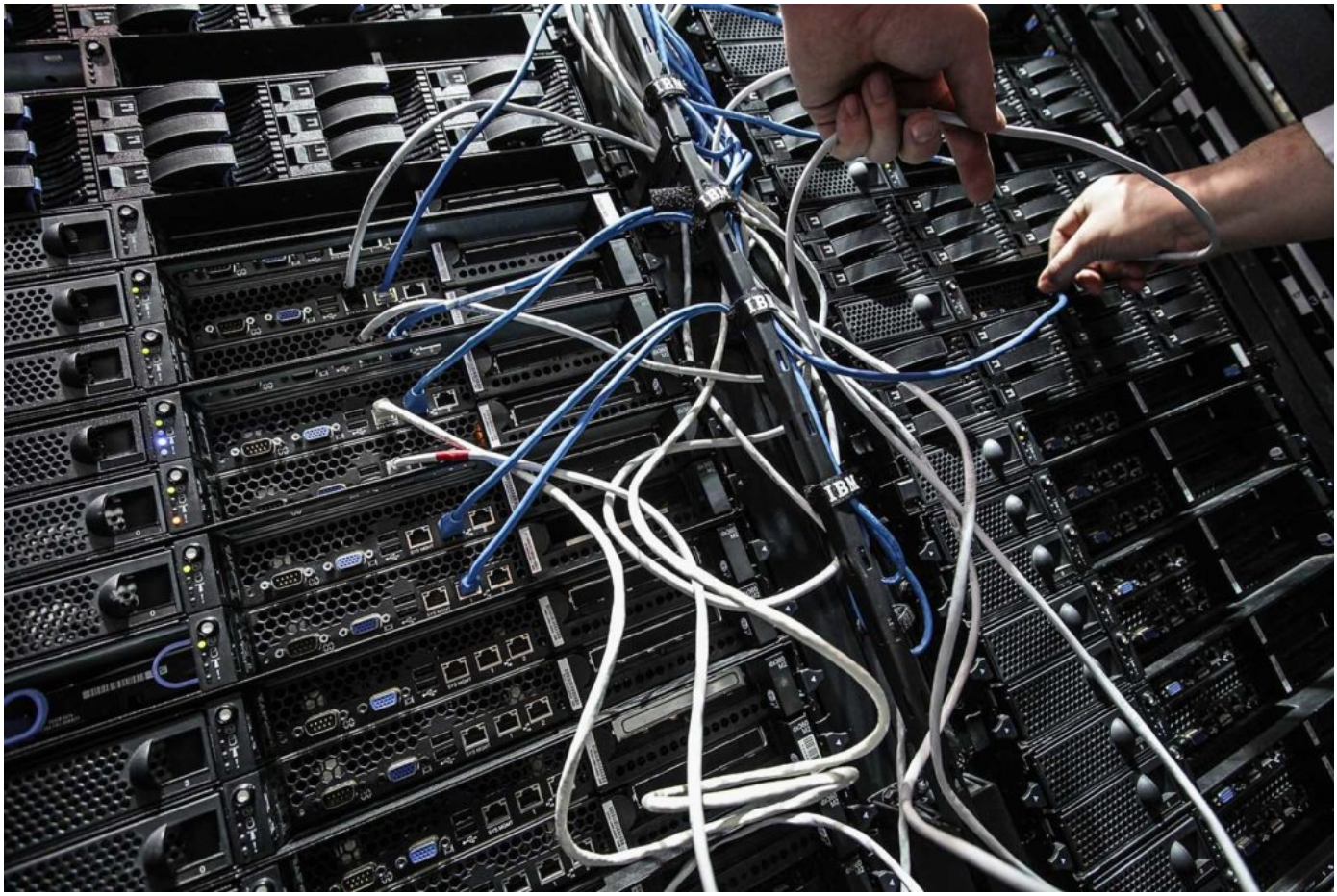
Cybersecurity Regulation on the Rise: Is Your Company Prepared?

May 27, 2016

http://www.brinknews.com/cybersecurity-regulation-on-the-rise-is-your-company-prepared/

Pamela Passman

President and CEO of Center for Responsible Enterprise and Trade



Data breaches and other cyber incidents are on the rise and on the agenda for corporate boards and the C-suite, and for good reason: Loss of customer information, trade secrets or other confidential assets can significantly diminish a corporate reputation, financial standing and competitive advantage.

However, these aren’t the only risks for companies. The diversity and complexity of cybersecurity risks, and their evolving character, have caused governments to respond in many different ways. Some have taken action directly to require the cybersecurity of various public and private networks and systems, while others have encouraged the development of voluntary frameworks and best

practices that industries can choose to adopt.

This rising tide of cybersecurity regulation and recommendations further complicates the landscape for companies. These new requirements are often inconsistent among different governments, between agencies of the same government and from industry to industry. One of the major unknowns for companies is whether they can embrace one overall information security framework, or whether they will face a splintered environment with an unmanageable number of different corporate, industry and government requirements, standards and practices.

New and Expanded Cybersecurity Regulation

Governments around the world have adopted or are considering legislation that would specifically impose cybersecurity requirements on industry in various ways. For example, more than 240 bills, amendments and other legislative proposals dealing with cybersecurity have been introduced in the U.S. Congress in the past three years.

Requirements fall in a variety of categories. Some are direct requirements to implement cybersecurity protections. For example, companies in the critical infrastructure sector now face regulation in the U.S. and similar requirements in Europe and Asia. Government departments are also seeing a rise in cybersecurity requirements, such as risk assessments, training and controls. Trade secret protection laws also require “reasonable steps” be taken to keep information

confidential from cyber threats.

For publicly traded companies, securities laws and shareholder expectations are increasingly demanding that those companies safeguard their confidential information and reputation against cyber-attacks—or face administrative penalties and civil damage remedies. This is particularly true in the U.S., where shareholder litigation and some Securities and Exchange Commission guidance and enforcement have already been launched.

Governments around the world are also increasingly insisting that contractors and suppliers that wish to do business with the government also closely manage cybersecurity risks at their own firms and among subcontractors and suppliers.

The shared view among governments and industry is that cybersecurity is an important and growing problem, and that many existing practices are inadequate or inconsistent. Yet, while there is a common appreciation of cyber risks, at least at a high level, there is little coherence in these efforts, even within national borders, and even less coordination internationally.

The rising tide of cybersecurity regulation and recommendations complicates the landscape for companies.

Growing Use and Importance of Cybersecurity Frameworks and Standards

With cybersecurity regulation on the rise, how can a company prepare? To help companies seeking to address these new requirements, governments and the private sector are working together to develop security frameworks and guidance designed to protect confidential information more effectively from cyber risks.

The voluntary Framework for Improving Critical Infrastructure Cybersecurity, developed by the National Institute of Standards and Technology (NIST) unit of the U.S. Department of Commerce, is to-date the most comprehensive, risk-based tool for managing information security. U.S. federal government agencies are enthusiastically embracing the NIST Framework. One recent survey of 150 federal government IT and security professionals found that 82 percent are using the NIST Framework to improve their security, while 74 percent say it serves as a foundation for their own cybersecurity roadmap.

The NIST Framework is also being reviewed and considered by governments and the private sector internationally. NIST itself has been meeting with European and other governments and information security bodies, including the European Commission, the UK, Italy, Poland, Romania and others, to discuss how the NIST Framework and other approaches could be aligned on a global scale.

To date, use of the NIST Framework is voluntary. Compliance with the Framework is neither mandatory as a condition for government contracting nor is NIST the formal standard against which information security practices have been measured in litigation following data breaches. However, the landscape is changing. The trend to promote such guidelines—and in particular the NIST Framework—seems likely to develop into more mandatory requirements, to which other cybersecurity measures will be mapped.

The NIST Framework could very well be the guideline that courts and regulators will use to determine whether companies are managing data security adequately in a range of legal contexts.

Other information and cybersecurity standards are also proliferating. The principal information security standard at the international level is ISO 27001, which many companies are implementing and are seeking certification of their compliance. The NIST Framework—although structured quite differently than this ISO standard—includes and makes numerous references to particular ISO 27001 requirements.

Implementing Leading Practices

Cybersecurity tools and standards such as the NIST Framework and ISO 27001 are proving useful to companies and other organizations. Use of a risk management program, such as the NIST Framework, provides the opportunity to bring some uniformity and cost-effectiveness to the varying cybersecurity efforts and requirements that have been developing to date. Such an approach can also help organizations assess, manage and respond to their particular cyber risks more effectively, both internally and down the supply chain**.**

The bottom line for agencies in the public sector, government contractors, the U.S. and multinational companies: Given the flood of new cybersecurity regulation, the use of leading practices such as the NIST Framework may become virtually, or actually, mandatory. Thus, taking steps now to implement protections will position organizations to proactively meet these ever-evolving cybersecurity requirements.

Pamela Passman

Pamela Passman is President and CEO of the Center for Responsible Enterprise and Trade (CREATe.org), a global nongovernmental organization dedicated to helping companies and supply chain members prevent corruption and protect intellectual property. Prior to founding CREATe.org, Passman was Corporate Vice President and Deputy General Counsel, Global Corporate and Regulatory Affairs, Microsoft Corporation.