FT.com
FINANCIAL TIMES

Published April 22, 2013

Cyber resilience on the executive agenda – a global community acting locally

By Eric Openshaw and Jolyon Barker
The Financial Times
http://www.ft.com/intl/cms/s/0/d4290d84-ab6d-11e2-ac71-00144feabdc0.html#axzz2RIGtuUdP

With the meeting of the World Economic Forum (WEF) in Davos in January 2013, cyber security is officially no longer solely a technology or IT department concern.

Perhaps the most striking thing about the WEF's Partnering for Cyber Resilience initiative, now signed by more than 90 leaders from 26 countries and representing 18 different sectors, was the signatories: not chief information officers or chief technology officers, not security experts or law enforcement entities. The participants were chief executives and their public sector counterparts.

This isn't to say that there aren't highly technical infrastructure challenges or technology-based solutions to cyber security. There are. But the problem of maintaining a robust, shared digital environment is too important, not just to individual firms but increasingly to society, to the smooth functioning of governments and markets, to bump down the chain of command.

The WEF initiative recognises that in today's hyper-connected business environment, the ability to trust in the systems and entities connecting the world is fundamental to the economy and the public good. Yet the increasing connectivity of people, processes and machines has created the conditions for global, systemic cyber risk.

The traditional boundaries of company and country are almost meaningless. Certainly neither proprietary information nor personal data knows to stop at those borders. Neither do viruses or hacker attacks acknowledge the physical and legal boundaries of states and institutions. No single organisation can take on the threat or wall itself off and still participate in the global economy.

The only way to make headway against the growing cyber threat is through a flexible, collaborative, ongoing approach based in cooperation - within the private sector and between the private and the public sectors - and guidance that allows each entity to tailor its own risk management strategy within a shared understanding of cyber risk and the goals of cyber resilience. The goal of cyber resilience is that each entity manage risk within the organisation such that, while 100 per cent prevention isn't possible, the entity is better able to survive and quickly recover from attacks.

For industries, mitigating cyber-related risk will soon become essential to the ongoing viability and performance of the institution. Sectors such as Financial Services have already had to face this new reality, but with increasing dependence on connectedness, other sectors will find that

cyber risk threatens their intellectual property, their customer data, their supply and distribution chains, their product and service delivery capabilities.

The executive management team - the chief executive and the board - have a responsibility to make cyber resilience a priority and set the tone by including cyber resilience as part of the broader risk management program. Such a program would take into account the current thinking in leading practices toward managing the known cyber risks to reduce harm to the organisation as well as to all of the connected entities the organisation shares information with.

Cyber resilience may soon be seen as a confidence-building measure for investors. One of the areas for further exploration by industry groups will be what types of reporting and measures will be most useful and informative for management and investors to assess the level of cyber risk for the organisation and to judge the quality of cyber resilience measures in place.

Similarly, given the expectation that the Board understand the organisation's risk and executive management's plans for action and communication in the event of significant failure or breaches of networked information, what types of tools or information can make the organisation's cyber activities more transparent to the Board?

Boards may want to add questions around education, investment, monitoring, collaboration efforts, current and foreseen threats to the standard discussions of risk management to better understand organisational strengths and weaknesses around cyber resilience.

Third-party risk cannot be underestimated. If it is important that a company develop a comprehensive cyber risk management program; it is equally important that the company's suppliers and partners do this also. The shared digital environment is only as strong as the weakest link. Think about all of the entities a company shares information with and how many it depends on to conduct day-to-day operations.

It is incumbent upon executives in every industry to lead the way not just by implementing effective cyber management programs within their own firms but to actively encourage the development of cyber resilience programs across the ecosystem, even among competitors.

The public sector also has a significant role to play. If the private sector can accept the criticality of taking action to become more cyber–resilient, the public sector's role doesn't have to be about creating massive regulation. Indeed, given the fast-moving nature of cyber threats, national models for information security will need to focus on adaptability and information-sharing rather than slower-moving regulatory and legislative action.

Some countries are trying to stimulate a different level of debate about cyber risk, but there isn't the consistency needed to address this as a global threat. The public sector can help catalyse industry communities to share data and discuss issues that enhance collaboration in face of the cyber threat. A number of governments are taking proactive positions to support private sector engagement by providing platforms and mechanisms for communities to share information on attacks and to improve businesses' prevention and response capabilities.

Much remains to be done. More chief executives and their public sector counterparts need to sign the WEF Principles for Cyber Resilience and begin taking action within their own organisations. Committing to engage with others in the industry and/or country is an important step to be both a

good corporate citizen and to benefit from, and help shape, information sharing, leading practices and regulations in cyber security. Industry communities will begin to identify performance measures, management solutions and other guidelines to allow organisations to evaluate the maturity of their cyber practices relative to others and chart a course for improvement.

Those that have signed the Principles need to engage in the global community and with cyber security experts to drive deeper discussion in the areas of information sharing, policy development and the protection of critical infrastructure.

About the authors:
Eric Openshaw is a vice chairman and the US Technology, Media and Telecommunications leader for Deloitte. Jolyon Barker is the global managing director of the Technology, Media and Telecommunications group for Deloitte Touche Tohmatsu.