10 Minutes
on the stark realities of cyber-risk

September 2014

Cyber-risk is more than an IT challenge—it's a business imperative

Highlights

Business leaders must recognize the exposure and business impact that comes from operating within an interconnected global ecosystem.

They need to appreciate the dynamic, targeted threats to their business model and the deep motivations and capabilities of their adversaries.

By evaluating the risk profile, capability including which information assets are the "crown jewels" of the business, companies can target investment in the right area.

The CEO and board are ultimately responsible for ensuring the company designs and implements an effective cyber-risk program.

Cyber-risk has consistently been identified by business and government leaders as one of the key emerging global risk which will need to be managed effectively. In addition, our own research with business leaders has revealed that cyber-risk is a growing concern. [1] However, many CEOs and boards have yet to truly appreciate the seriousness and magnitude of this critical business issue.

Just how crucial is cyber-risk? Industry analysts have drawn parallels to the sentiment before the financial crisis when risks were not properly identified, assessed, and managed. It took the crisis for business leaders to fully appreciate the extent of their exposure within the interconnected global financial system.

Today, cyber-risks are a clear and present danger to the global business ecosystem. Yet many enterprises place the responsibility for managing cyberthreats solely in the hands of their technology team.

It is time for business leaders to see cyber-threats for what they are—enterprise risk management issues that could severely impact their business objectives.

A changed business environment demands a new approach:

1. **A focus from enterprise to business ecosystems** Businesses are more interconnected, integrated, and interdependent—creating dynamic and evolving business ecosystems. Trusted business relationships and interactions with customers, service providers, suppliers, partners, and employees rely on securely sharing information assets and critical data.

2. **Cyberattacks are impairing businesses** In the ecosystem, businesses are completely dependent on technology and connectivity. This amplifies the business impact of cyberattacks, affecting intellectual property, competitive advantage, operational stability, regulatory compliance, and reputation.

3. **Not all information assets are equal** Information assets continue to proliferate at an extraordinary rate. Safeguarding *all* data at the highest level is just not realistic or possible. Loss of some types of data is troubling; loss of others can destroy key elements of your business.

[1] http://pwc.blogs.com/ceoinsights/2013/01/todays-ceos-worry-more-and-have-more-to-worry-about.html

At a glance

Cyberattacks are accelerating at an unprecedented rate—and your approach to cyber-risk must keep pace. Here's how businesses are adapting to the new reality:

	Historical IT Security Perspectives	Today's Leading Cyber-risk Insights
Scope of the challenge	• Limited to your "four walls" and the extended enterprise	• Spans your interconnected global business ecosystem
Ownership and accountability	• IT led and operated	• Business-aligned and owned; CEO and board accountable
Adversaries' characteristics	• One-off and opportunistic; motivated by notoriety, technical challenge, and individual gain	• Organized, funded, and targeted; motivated by economic, monetary, and political gain
Information asset protection	• One-size-fits-all approach	• Prioritize and protect your "crown jewels"
Defense posture	• Protect the perimeter; respond *if* attacked	• Plan, monitor, and rapidly respond for *when* attacked
Security intelligence and information sharing	• Keep to yourself	• Public/private partnerships; collaboration with industry working groups

01

Your business ecosystem creates both opportunity and risk

“When the financial crisis of 2008 hit, many shocked critics asked why markets, regulators, and financial experts failed to see it coming. Today, one might ask the same question about the global economy’s vulnerability to cyber-attack. Indeed, the parallels between financial crises and the threat of cyber meltdowns are striking.”

—Kenneth Rogoff, Harvard University professor and former chief economist at the International Monetary Fund[2]

In the last two decades, the technology revolution has transformed the way companies conduct business, serve clients and drive ever increasing efficiencies through IT. Traditional boundaries have shifted; with company and personal digital footprint and audit trails leaving a mass of data open to theft and exploitation if not protected. Your ecosystem includes not only employees, partners, and customers but other constituents like law firms, investment banks, service providers, government agencies, regulators, industry affiliations, and even competitors. The ecosystem is built around a model of open collaboration and trust—the very attributes being exploited by an increasing number of global adversaries.

Their risk is your risk

Constant information flow is the lifeblood of the business ecosystem. Your data is distributed and disbursed throughout the ecosystem, expanding the domain you need to protect. The integrity and stability of your business is now, more than ever, dependent on those internal and external to your organization’s ecosystem.

Adversaries actively target the vulnerabilities throughout the ecosystem—significantly increasing the exposure and impact on the business. For example, a professional services firm was specifically targeted in order to obtain strategic deal documents related to one of its clients. In another ecosystem breach, several international high-tech firms were hacked through a penetration within their supply chain.

Old security models are inadequate

While cybersecurity risks have dramatically evolved, the approach businesses use to manage them has not kept pace. The traditional information security model—one that is compliance-based, perimeter-oriented, and aimed at securing the back-office—does not address the realities of today.

When looking beyond the enterprise boundaries, companies need to re-evaluate security priorities and allocations. Cyber-risk management in the business ecosystem is a complex problem, requiring management engagement, sophisticated techniques, and new skills and capabilities.

A new approach for a new world

Company leaders and boards can no longer afford to view cyber-risk as a technology problem; the likelihood of a cyberattack is now an enterprise risk management issue. Senior executives who view cybersecurity as an integral part of the business agenda position their organizations to take fuller advantage of ecosystem opportunities. Knowledge is power; gaining ongoing insight into ecosystem vulnerabilities and threats helps them anticipate and plan for risks that might sideline others who are less informed.

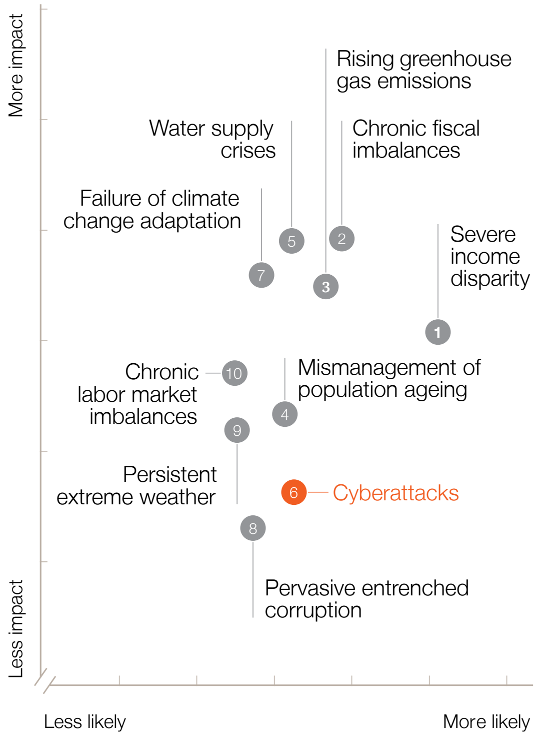
[2] “Will Governmental Folly Now Allow for a Cyber Crisis?” Project Syndicate, July 2012, http://www.project-syndicate.org/commentary/will-governmental-folly-now-allow-for-a-cyber-crisis-

02

Why cyberthreats have become business risks

World Economic Forum Global Risk Landscape Top 10

Cyberattacks were rated the sixth most likely global risk to occur—of 50 potential risks (top quadrant shown below)



Source: World Economic Forum Global Risk Landscape 2013

When CEOs and boards evaluated their market threats or competitors, few previously considered cyberthreats. Today, the sheer volume and concentration of data, coupled with easy global access throughout the business ecosystem, magnifies the exposure from cyberattack. The reward of a successful attack and the ability to remain anonymous and undetected presents an opportunity for anyone with a computer and Internet connection to infiltrate the business ecosystem. This is coupled with the shift to reduce the cost of IT and business processes through third-party outsourcing to service providers of Cloud Computing, Managed call centres etc., where securing, tracking, and controlling company data is critical.

Adversaries—motives, means, and methods

Nation states, organized crime, hacktivists, terrorists, and even employees are all potential adversaries. These adversaries are sophisticated, determined, and patient, and they will target individuals, companies, or industries to gain advantage. Their motives range from economic espionage, to rapid monetization of information, to advancing political agendas. Cultural convention and geographic or legal boundaries don't consistently apply in the global business ecosystem, leading to a low-risk, high-reward equation for your adversaries.

Numerous attack groups are backed by limitless resources, and in some cases are funded or informed by foreign intelligence services. Oftentimes, attack groups are able to devote highly talented individuals who are experts in technology, business process, and espionage tactics.

From our extensive experience working with a range of companies, we have witnessed adversaries use a wide array of methods and tactics to gain and maintain access while going undetected. Often the attack begins simply with an e-mail that contains an attachment or a link to a web site that compromises the victim's computer—and ultimately the core business.

Anticipating threats in your ecosystem

Organizations must establish an ongoing capability to provide insight and intelligence on the cyberthreats facing the business. Armed with this insight, business leaders can anticipate and dynamically react to changes in their companies' cyberthreat profile.

With cyberattacks posing a constant threat to the ecosystem, companies are beginning to understand that the real goal is to minimize, rather than eliminate, the damage and disruption they can do to the business. By considering threats now—instead of waiting until a breach is brought to light—they can limit the negative impact, such as lost revenue, competitive disadvantage, reputational damage, reduction of shareholder value, and eroding customer goodwill.

03

What information really matters—to your business and your adversaries

What's most at risk?

Technology and business information of most interest to cyberattackers

Information and communication technologies
Clean technologies
Military technologies
Advanced materials and manufacturing techniques
Healthcare, pharmaceuticals, and related technologies
Agricultural technologies
Business deals information
Macroeconomic information
Energy and other natural resources information

Source: Office of the National Counterintelligence Executive,*Report to Congress on the Foreign Economic Collection and Industrial Espionage, 2009-2011,* October 2011.

Organizations generate enormous amounts of data. Some of it is insignificant, but some is mission critical and will cripple the business if exposed. Putting equal priority on all of it is not practical, cost effective, or necessary.

What are your crown jewels?

Companies must determine what their most valuable information assets are, where they are located at any given time, and who has access to them. Crown jewels are those information assets or processes that, if stolen, compromised, or used inappropriately would render significant hardship to the business. Examples include product designs, hedge fund trading strategies, new market plans, and executive communications.

Too often, organizations apply a "one-size-fits-all" model to protecting information assets. This just doesn't work. Organizations must hold business executives accountable for protecting the crown jewels in the same manner as they are accountable for financial results and other key business management metrics.

The magnitude may not be felt for years

If R&D information, intellectual property, trade secrets, or other high-value information is compromised, the business impact may not be felt immediately. It may take months or years before the business feels the full effect on competitive advantage or degradation of cash flows.

In some cases, the fallout has been so severe that prominent companies ultimately went out of business. In fact, some public companies disclosed—after the fact—that they had been subjected to long-term hacking campaigns that destroyed the health of the business. One telecommunications CEO famously stated that he did not believe the hacking was a "real issue."[3] However, in retrospect, a senior security official at the company indicated that he had no doubt that extensive cyberattacks on the company contributed to its downfall.[4]

As adversaries continually evolve, so must businesses

Cyberattacks are about economic advantage. Attackers are constantly evolving their capability to exploit vulnerabilities inherent in the global business ecosystem. Yet companies have not adapted, investing billions of dollars on security products and services that are built on outdated security models. What's needed is an evolved approach in which businesses allocate and prioritize resources to effectively protect the crown jewels today and into the future.

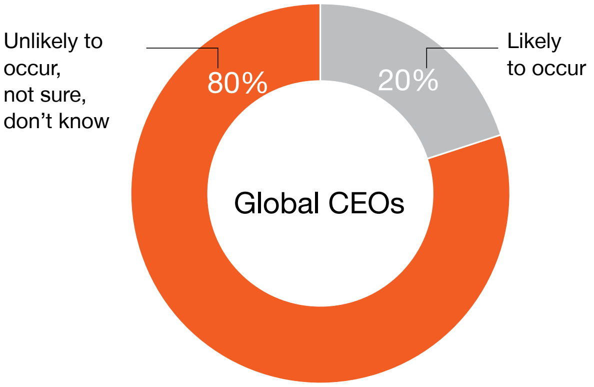
[3] http://articles.washingtonpost.com/2012-02-14/business/35442181_1_hackers-gmail-accounts-high-profile-hack

[4] http://www.cbc.ca/news/business/story/2012/02/15/nortel-hacking-shields-as-it-happens.html

Gaining advantage: Awareness to Action

The majority of CEOs would be blindsided by a cyberattack that could cripple the business

How likely is a cyberattack or major disruption of the Internet?



Base: Global 1,330
Source: PwC, 16th Annual Global CEO Survey, 2013

CEOs and boards that keep a sustained focus on cyber-risk do more than protect the business; they reap bottom-line benefits. We call this approach Awareness to Action, meaning that all activities and investments are driven by the best available knowledge about information assets, ecosystem threats, and vulnerabilities, and are evaluated within the context of business activity. Here are three areas to initially consider when assessing your cyber-risk posture.

1. Enhance your cyber-risk strategy and capability

- Is an integrated cyber-risk strategy a pivotal part of our business model? Does the strategy consider the full scope of security: technical, physical, process, and human capital? Have we applied the required resources and investments?
- Do we have the security capability to advise internal business leaders on critical threats, emerging technology, and strategic initiatives?
- Can we explain our cyber strategy to our stakeholders? Our investors? Our regulators? Our ecosystem partners?

2. Understand and adapt to changes in the security risk environment

- Is there clearly defined accountability and sponsorship for your organizations Cyber-risk policy, implementation, operation and ongoing posture monitoring?
- Do we know what information is most valuable to the business? Have we prioritized security to protect those assets accordingly? Have we quantified the business impact if the assets were impaired?
- Do we understand the significant changes in the threats facing our business? Who are our adversaries? What would they target? What techniques might they use?
- Are we actively acquiring and adapting to internal and external sources of intelligence? How are our controls and countermeasures responsive to events and activities? Are we actively involved in relevant public-private partnerships?

3. Advance your security posture through a shared vision and culture

- Does the chief information security officer role report, independent of IT, to the board or an executive leadership team committed to cybersecurity?
- Do employees understand their role in protecting information assets—have we provided the necessary tools and training?
- What assurances do we require from suppliers and service providers? Do we actively monitor, audit, and remediate our risk portfolio? Do we have standards in place to protect our assets throughout the ecosystem?

How PwC can help

To have a deeper discussion about cyber-risk, please contact:

Vincent Loy
Financial Crime & Cyber Leader Partner, PwC
+65 9088 6328
vincent.j.loy@sg.pwc.com

Shong Ye Tan
Cyber Security Partner, PwC
+65 6236 3262
shong.ye.tan@sg.pwc.com

Jimmy Sng
Cyber Security Partner, PwC
+65 6236 3808
jimmy.sng@sg.pwc.com

Ervin Jocson
Cyber Practice Director, PwC
+65 8261 7996
ervin.jocson@sg.pwc.com