*Note*

# Zurich identifies seven cyber risks that threaten systemic shock

**Research from Zurich Insurance Group shows that organizations must improve their response to cyber risks to avoid a global shock similar to the 2008 financial crisis. The research reveals that even cyber security professionals are not clear on how the failure of an organization or of technology could develop to become a system-wide risk. The reliance on information technology has also created a complex web of interconnected risks.**

Zurich, April 22, 2014 – The recently published Zurich Cyber Risk Report, created in collaboration with the international think tank Atlantic Council, argues that cyber-risk management professionals need to look beyond their internal information technology safeguards to interconnected risks which can build up relating to counterparties, outsourced suppliers, supply chains, disruptive technologies, upstream infrastructure and external shocks.

Zurich warns that a build-up in these risks could create a failure on a similar scale to the 2008 financial crisis. Such interconnected risks are compounded when a company outsources the management of its servers, information technology and cyber security to focus on its core activities. Little information may be known about the third party's information security or business continuity safeguards and it may also in turn outsource activities to other companies.

The report calls for organisations to incorporate the best ideas from financial governance such as creating a G20+20 Cyber Stability Board to enhance cyber risk management and identifying and improving the governance of G-SIIOs (Global Significantly Important Internet Organizations).

Axel Lehmann, Group Chief Risk Officer and Regional Chairman Euope at Zurich Insurance Group, said: "The internet is the most complex system humanity has ever devised. Although it has been incredibly resilient for the past few decades, the risk is the complexity which has made cyberspace relatively risk-free can – and likely will – backfire.

"Organizations are unknowingly exposed to risks outside their organisation, having outsourced, interconnected or exposed themselves to an increasingly complex and unknowable web of networks.

"Few people truly understand their own computers or the internet, or the cloud to which they connect, just as few truly understood the financial system as a whole or the parts to which they are most directly exposed."

The report identifies the following seven interconnected risks

| | **Description** | **Examples** |
|---|---|---|
| **Internal IT enterprise:** | Risk associated with the cumulative set of an organization's (mostly internal) IT | Hardware; software; servers; and related people and processes |
| **Counterparties and partners:** | Risk from dependence on, or direct interconnection (usually non-contractual) with an outside organization | University research partnerships; relationship between competing/cooperating banks; corporate joint ventures; industry associations |
| **Outsourced and contract:** | Risk usually from a contractual relationship with external suppliers of services, HR, legal or IT and cloud provider | IT and cloud providers; HR, legal, accounting, and consultancy; contract manufacturing |

| | | |
|---|---|---|
| **Supply chain:** | Both risks to supply chains for the IT sector and cyber risks to traditional supply chains and logistics | Exposure to a single country; counterfeit or tampered products; risks of disrupted supply chain |
| **Disruptive technologies:** | Risks from unseen effects of or disruptions either to or from new technologies, either those already existing but poorly understood, or those due soon | Internet of things; smart grid; embedded medical devices; driverless cars; the largely automatic digital economy |
| **Upstream infrastructure:** | Risks from disruptions to infrastructure relied on by economies and societies, especially electricity, financial systems, and telecommunications | Internet infrastructure like internet exchange points, and submarine cables; some key companies and protocols used to run the internet (BGP and Domain Name System); internet governance |
| **External shocks:** | Risks from incidents outside the system, outside of the control of most organizations and likely to cascade | Major international conflicts; malware pandemic |

## Further information

To get instant access to Zurich's news releases, calendar and other corporate publications on your iPad, iPhone or Android phone please go to your App Store and get the free Zurich Investors and Media App.

**For broadcast-standard and streaming-quality video** and/or **high resolution pictures** supporting this news release, please visit our Multimedia Pressroom.

**Zurich Insurance Group (Zurich)** is a leading multi-line insurer that serves its customers in global and local markets. With more than 55,000 employees, it provides a wide range of general insurance and life insurance products and services. Zurich's customers include individuals, small

businesses, and mid-sized and large companies, including multinational corporations, in more than 170 countries. The Group is headquartered in Zurich, Switzerland, where it was founded in 1872. The holding company, Zurich Insurance Group Ltd (ZURN), is listed on the SIX Swiss Exchange and has a level I American Depositary Receipt (ZURVY) program, which is traded over-the-counter on OTCQX. Further information about Zurich is available at www.zurich.com.

**Contact**
Zurich Insurance Group Ltd
Mythenquai 2, 8022 Zurich, Switzerland
www.zurich.com
SIX Swiss Exchange/SMI: ZURN, Valor: 001107539

**Media Relations**
phone +41 (0)44 625 21 00, fax +41 (0)44 625 26 41
twitter @Zurich
media@zurich.com

**Disclaimer and cautionary statement**

The information in this publication was compiled from sources believed to be reliable for informational purposes only. All sample policies and procedures herein should serve as a guideline, which you can use to create your own policies and procedures. We trust that you will customize these samples to reflect your own operations and believe that these samples may serve as a helpful platform for this endeavor. Any and all information contained herein is not intended to constitute legal advice and accordingly, you should consult with your own attorneys when developing programs and policies. We do not guarantee the accuracy of this information or any results and further assume no liability in connection with this publication and sample policies and procedures, including any information, methods or safety suggestions contained herein. Moreover, Zurich reminds you that this cannot be assumed to contain every acceptable safety and compliance procedure or that additional procedures might not be appropriate under the circumstances. The subject matter of this publication is not tied to any specific insurance product nor will adopting these policies and procedures ensure coverage under any insurance policy.