ZURICH

Risk Nexus

Global interconnections of cyber risk: impact on small- and medium-sized enterprises

April 2014

The world is likely to suffer internet failures for reasons similar to those that put the global financial system at risk in 2008: these included a nearly absolute dependence on an interconnected system so complex as to be unknowable. Small- and medium-sized enterprises are particularly exposed to these risks, but there are solutions.

Complex systems, unexpected risks

The internet has proved to be incredibly resilient. This is due in large part to a stable technology platform and dedicated, even heroic technicians who work behind the scenes to keep things running reliably. This has provided small- and medium-sized enterprises (SMEs) with countless benefits, allowing them to handle more customers, provide superior service, and compete with far larger companies. But this type of reliance exposes companies to significant risks that they tend to overlook; not just those posed by data breaches or theft of trade secrets, but larger global shocks.

The internet is the most complex system humanity has ever devised, and our track record of successfully managing complex systems is far from perfect. We are rapidly connecting critical business functions and infrastructure systems to the internet, making us dependent on humankind's largest and most complex system, one that itself is very poorly understood.

Past internet incidents and attacks have only disrupted ones and zeros, or things made of silicon. All these can be recreated or replaced with relative ease. Future cyber incidents will break things made of concrete and steel as the internet increasingly connects with real life. As the trend continues, we are finding that there is no separate 'digital' economy, only a single economy where "even the mundane comes to depend on distant digital perfection," in the words of Dan Geer, a noted internet risk expert.

The internet of tomorrow will be both a source of global shocks, and a catalyst for other shocks; things for which risk managers, corporate executives, board directors, and government officials are not prepared. It will almost certainly be less resilient, available, and robust than today.

> *"Increasingly there is not a separate 'digital' economy but only a single economy where even the mundane comes to depend on distant digital perfection."*

Atlantic Council

SMEs
continued

Current cyber risk management ignores the risks arising from dependence on that "distant digital perfection" – aggregations of cyber risk that lie outside an organization's internal servers and firewalls: counterparties, outsourcing or contractual partners, supply chains, upstream infrastructure, disruptive new technologies, and external shocks.

Recommendations for SMEs

Embrace new technologies but carefully manage the risk:
New technologies such as cloud storage are game changers for SMEs but these companies' reliance on "distant digital perfection" introduces many new risks. Owners and CEOs should meet with line staff and managers periodically to examine how suppliers, outsourcing partners, cloud-service companies and others expose the company to risks. Each of these can be at least partially controlled through contracts, service-level agreements, or site visits. This process should include periodic drills to review how the company would detect cyber incidents, and how it should best respond to disruptions to ensure the least impact. Hackers will often target an SME not for its own value, but because a large client depends on that particular SME for a critical service. This is a significant business and reputational risk that can ruin an SME. Accordingly, owners and CEOs should lead a review of the access the company has to its client's systems, or what client information the company keeps in its systems.

Improve basic cyber security:
Regardless of the size of an organization, a relatively small set of actions can protect against most cyber risks. The Council on Cybersecurity maintains a list of critical security controls that presents the most important set of actions that can be undertaken for cyber defense: companies should especially rush to adopt the 'First Five Quick Wins.'[1]

Shift from protection toward resilience:
Unfortunately, a single set of principles alone will not suffice. Organizations can no more 'secure' themselves against these interconnected and complex cyber shocks than they can hope to forever stack sandbags to protect from the damage caused by more frequent and severe hurricanes. The main hope for companies, therefore, is to be agile and resilient, and able to bounce back from disruptions through redundant systems and processes, under the leadership of meaningful corporate governance. SMEs have an advantage here. Even though they may not be able to afford the redundant systems and processes of larger companies, their small size allows far greater agility in responding after cyber shocks occur.

Owner or CEO-level risk management:
Cyber risks are becoming significant enough that they can no longer be entrusted solely to the IT professionals. Owners or CEOs of SMEs will have to somehow find time to better understand the technologies upon which their company relies. They must determine how these disruptions could lead them to lose important clients, or even force them into bankruptcy.

[1] Critical Security Controls, Council on Cybersecurity, http://www.counciloncybersecurity.org/practice-areas/technology, (Accessed 16 February 2014).

About this report

This report is part of a series on global aggregations of cyber risk from Zurich Insurance Company Ltd and the Atlantic Council. A larger report more deeply examines aggregations of cyber risk and why the internet is likely to be less reliable in future. It includes recommendations for companies, governments and others. You can find these reports at www.zurich.com/insight/

For more information, please contact Zurich Insurance Group:
Lori Bailey, Global Head of Management & Professional Liability, Zurich General Insurance, lori.bailey@zurichna.com
+1 617 570 8847

Or visit the webpage of the Cyber Statecraft Initiative of the Atlantic Council, at http://www.atlanticcouncil.org.

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.

Zurich Insurance Company Ltd

Mythenquai 2
8002 Zurich, Switzerland
Phone +41 (0)44 625 25 25

www.zurich.com

Atlantic Council

1030 15th Street, NW, 12th Floor
Washington, DC 20005, United States

www.atlanticcouncil.org