ZURICH

Risk Nexus

Global interconnections of cyber risk: impact on governments

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. Governments have the most capacity to ride out cyber shocks, but also a responsibility to take action that supports system-wide resiliency.

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 governments with countless benefits, allowing departments and agencies to handle more customers to provide superior service and improve internal productivity with fewer taxpayer dollars.

But this type of reliance exposes governments 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.

> *"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

Governments continued

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.

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 governments

Improve basic cyber security:
Regardless of the type of attack, 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 taken for cyber defense. In particular, each and every government agency should rush to adopt the 'First Five Quick Wins' and should be held accountable by legislatures or other watchdogs if it does not.[1]

Shift from protection toward resilience:
Unfortunately, cybersecurity on its own will be insufficient. Governments 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 governments, therefore, is to be agile and resilient, and able to bounce back from disruptions through redundant systems and processes, under the leadership of meaningful governance.

Focus on interconnection risks:
Governments will often assess their security one agency or department at a time along bureaucratic lines, ignoring the risks stemming from the interconnection of departments with each other and with the private sector. Each department might get a separate 'report card' for how it implements a checklist of security controls, with little focus on how government operations can be disrupted by cyber incidents which cause a cascading impact between departments or from outside companies.

A best practice among companies is to have a governance group at the COO level that can help cut across bureaucratic lines to focus on critical business functions and ensure end-to-end resilience and security for the process, regardless of the department in which any specific element resides. The same idea can be applied to a whole-of-government approach with an interagency committee reporting to ministers or the cabinet office and committed to reducing systemic risks.

Embrace new technologies but carefully manage the risk:
New technologies, such as cloud storage and services, are game changers, allowing governments to pool IT resources and concentrate scarce cyber defenders. But they do introduce new risks which governments are often poorly positioned to manage: even when one system may be well understood, its interaction with all the others is not, especially in the face of increased cyber disruptions and attackers.

The coupling of poorly understood technologies means disruptions will likely come with increasing frequency and intensity and sensitive information can be stolen regularly, even when this involves well-protected agencies of national-security critical sectors.

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

Governments continued

In the face of cyber disruptions, it is normally the private sector which is at the center of the response. Governments cannot scale as easily as the private sector, and lack its agility and subject-matter expertise. National response strategies should put the private sector at the center of efforts, not the periphery.

Incident response and business continuity planning:
One way governments can build resilience, which is often overlooked, is to develop their cyber incident response capabilities and traditional business continuity planning. The best-prepared examine the most likely and most dangerous cyber risks. They exercise their security and response teams, as well as their leaders and decision-makers to build 'muscle memory' for responding to incidents. Such processes need to be built into the governance of agencies and tied into any parallel private-sector response.

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