ZURICH

Risk Nexus

Beyond data breaches: executive summary

April 2014

The internet and associated information technology (IT), which often go by the name 'cyberspace,' give modern societies, economies and lives benefits that are too numerous to count. But the dark side of our dependence on the internet goes far beyond the day-to-day headlines of cyber crime, identity theft or concerns about online espionage or loss of privacy.

While our society's reliance on the internet grows exponentially, our control of it only grows linearly, limited by outdated government procedures and ineffective governance. "As society becomes more technologic, even the mundane comes to depend on distant digital perfection," according to Dan Geer, a noted internet risk expert.[1]

Yet modern cyber risk management does not give much thought to 'distant digital perfection,' the aggregations of cyber risk, which lie sometimes far outside an organization's own server and firewalls.

In financial markets in the run-up to the 2008 crisis, these aggregations of risk included inflated U.S. real estate prices, over-leveraged households and companies, fragile banks, and implicit public guarantees to large parts of the financial sector. The seven aggregations of cyber risk begin with the internal corporate network and security practices, and expand outward to counterparties and affiliates, supply chain and outsourcing agreements, upstream infrastructure, external shocks and other risks.

Companies may use leverage to maximize their gains, taking on debt to make investments in a company or positions in the market. While this leverage increases potential upside in good times, it also can intensify the impact of any sharp downside events. Similarly, the aggregations of cyber risk listed above can likewise be considered areas of technology leverage; organizations rely on technology solutions and technology-enabled business plans (such as outsourcing and just-in-time logistics) to increase efficiency and lower costs, making it possible to increase profitability while deploying fewer resources.

The way in which the complexity of interconnected risks is assessed is painfully similar to how financial risks were assessed prior to the 2008 crash.

> *"Just imagine if a major cloud service provider had a 'Lehman moment,' with everyone's data there on Friday, and gone on Monday."*

[1] Dan Geer, We Are All Intelligence Officers Now, 28 February 2014, http://geer.tinho.net/geer.rsa.28ii14.txt, (Accessed 11 March 2014).

Atlantic Council

Executive summary
continued

Risks were considered one at a time, each organization largely assuming these risks to be all local and not highly correlated with one another. Indeed, pre-2008, many experts insisted that due to its own complexity, correlations had been engineered out of the system, though in the end, it was this very complexity which helped bring the system down.

In a parallel to how the many elements of the financial system created an extended period of prosperity, a combination of factors has led to the internet being incredibly resilient. Stable technology, dedicated technicians and resistance to random outages have been the bedrock of this resilience. But the same added complexity which has made it relatively risk-free can, and likely will, backfire at some time.

There are a number of reasons to believe the internet of tomorrow will almost certainly be less resilient, available, and robust than today. It will also be more likely to initiate and cascade 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. The internet is highly interconnected and tightly coupled with society, meaning that (as in other such systems) a small failure or series of them in one place can cascade, producing an outsized impact elsewhere.

Just imagine if a major cloud service provider had a 'Lehman moment,' with everyone's data there on Friday, and gone on Monday. If that failure cascaded to a major logistics provider or company running critical infrastructure, it could magnify a catastrophic ripple running throughout the real economy in ways difficult to understand, model or predict beforehand. Especially if this incident coincided with another, the interaction could cause a crash or collapse of much larger scope, duration and intensity than would seem possible – similar to the series of events that struck the financial system in 2008.

On the internet, it has been easier to attack than defend for decades. The original architecture of the internet was founded on trust, not security, software is still poorly written and secured, and the system is so complex that it is difficult to defend. Systems in which one set or participants have asymmetric advantages, year after year and decade after decade, must hit a tipping point when there are more predators than prey. Attackers could have not just a local advantage, but superiority with strategic consequences for the internet's availability and resilience.

This increasingly tight coupling of the internet with the real economy and society means a full-scale cyber shock is far more likely to occur than some risk managers (and internet professionals) care to admit: internet failures could cascade directly to internet-connected banks, water systems, cars, medical devices, hydroelectric dams, transformers, and power stations.

Past internet incidents and attacks have only made ones out of zeros, and broken software or things made of silicon. All of these can be recreated or replaced with relative ease. But as the internet connects increasingly with real life, in places like the smart grid interconnection with the electrical power infrastructure, this will no longer be true: cyber incidents will break things made not of silicon but of concrete and steel.

Risk managers, regulators, and organizations with system-wide responsibility all need to focus more on resilience and agility rather than simply prevention. In an increasingly interconnected world, risks can strike quickly and from any direction – so, too, is it equally critical that those affected are able to respond rapidly to ride out the shocks.

All the report's recommendations are summarized in the box below. The full report is available on www.zurich.com

About Risk Nexus

Risk Nexus is a series of reports and other communications about risk-related topics from Zurich.

For more information on this issue please go:

www.zurich.com

Recommendations

System-wide risk: recommendations for governments and organizations with systemic responsibilities	
Expand horizon of cyber risk management to system-wide resilience and response	1. Improve system-wide risk management, resilience and incident response 2. Cautiously use existing regulatory authority to expand risk management to third-party providers and affiliates 3. Pursue a private-sector-centric approach to work at needed scale 4. Provide targeted grants for non-government groups
Borrow ideas from finance-sector governance	1. Expand and fortify internet governance with a G20+20 Cyber Stability Board 2. Consider recognition of Global Significantly Important Internet organizations 3. Address 'Too Big to Fail'

Local risk: recommendations for individual organizations	
Basic: regardless of the size of the organization, there are a relatively small set of actions to protect from the most cyber risks:	1. Provide application whitelisting 2. Use standard secure system configurations 3. Patch application software within 48 hours 4. Patch system software within 48 hours 5. Reduce the number of users with administrative privileges
Advanced: larger, more sophisticated organizations should certainly implement the 20 Critical Security Controls, but they also have the capability to engage in far more advanced cyber risk management.	1. Push out risk horizon 2. Cyber insurance 3. Demand more resilient and secure standards and products 4. More effective board-level risk management
Resilience: for all organizations, and in some ways, perhaps the most effective.	1. Redundancy 2. Incident response and business continuity planning 3. Scenario planning and exercises

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