ZURICH

Risk Nexus

Beyond data breaches: global interconnections of cyber risk

April 2014

Atlantic Council

Contents

About Risk Nexus

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

Foreword

The growing number and sophistication of cyber attacks is threatening to outstrip our efforts to increase resiliency against them.

Data breaches are today's top concern and a serious risk: 2013 was the worst year thus far, with 740 million data files potentially viewed or stolen worldwide.[1] But governments and forward-looking organizations need to take a holistic view and look beyond these issues to broader risks, including the increasing danger of global shocks initiated and amplified by the interconnected nature of the internet.

The internet of tomorrow will both initiate and amplify global shocks in ways for which risk managers, corporate executives, board directors, and government officials may not be adequately prepared.

Early on, we nicknamed this project 'cyber sub-prime' because we intended it to expose the global aggregations of cyber risk as analogous to those risks that were overlooked in the U.S. sub-prime mortgage market. Problems in that segment spread far beyond the institutions that took the original risks, and proved severe enough to administer a shock that reverberated throughout the entire global economy. At first, the term 'cyber sub-prime' was just a quirky nickname, but it soon became a useful analogy, helping us to gain additional insights into cyber risks based on extended parallels with the financial sector.

For example, in assessing the risk of financial shocks, the sector (both banks and regulators) generally behaved as though every organization was self-contained with regard to its own risks. In a business that depended on securitizing risks, experts insisted that complexity helped make the system more secure, as risks were not correlated, and all risks found a home with those most able and willing to own them. Decades of moderation lulled nearly everyone into believing these theories to be iron-clad laws.

In hindsight, it was folly to examine risks one organization at a time, while ignoring the interconnections. Yet this is just how cyber risks are looked at today. Obviously the internet has been incredibly resilient (and generally safe) for the past few decades, but as with securitization, the added complexity that has made cyberspace relatively risk-free can – and likely will – backfire. Cyber-risk management needs to look beyond the internal information technology (IT) enterprise to other aggregations of risk, such as outsourcing and contractual agreements, supply chain, upstream infrastructure, and external shocks.

There are fortunately several prudent actions which will help now, not least to shift resources to resilience rather than prevention. Here again, the 'cyber sub-prime' analogy helps, since the systems share much in common and the lessons are so recent.

This report is the result of a year-long effort between Zurich Insurance Company Ltd and the Atlantic Council, a project which encompassed meetings on four continents and consultations with cyber experts and risk professionals across different industries.

Jason Healey, director of the Atlantic Council's Cyber Statecraft Initiative, wrote the report. Several individuals made key contributions to the project, especially Jason Thelen of the Atlantic Council; Neal Pollard and Gregory Rattray, both Senior Fellows of the Atlantic Council; Jeff Schmidt and Tom Bossert, Zurich Cyber Risk Fellows of the Atlantic Council; and Paul Twomey, board member of the Atlantic Council. Gib Sorebo and Bill Woodcock also gave important advice, particularly on the energy and telecommunications sectors, respectively.

At Zurich, Francis Bouchard and Benno Keller guided the project, while several individuals including Steven Wilson, John Scott, Catherine Mulligan, Lori Bailey, and Larry Collins provided expert advice.

For Zurich, this project added depth to existing work on a Group-wide focus aimed at taking a holistic view of risks in order to better protect against them. It also extends the Atlantic Council's project on Saving Cyberspace to ensure the internet is as free, secure, and resilient for future generations as it was for ours.

We hope you find these insights useful both for the goals outlined here, and as a valuable contribution to reducing risk that ultimately has implications for nearly everyone today.

Fred Kempe
President and CEO, Atlantic Council

Axel P. Lehmann
Group Chief Risk Officer and Regional Chairman Europe, Zurich Insurance Group

[1] Eric Chabrow, Records Exposed Hit New High in 2013, Data Breach Today, http://www.databreachtoday.com/interviews/records-exposed-hit-new-high-in-2013-i-2166#.Uv6U5uw_AI4.twitter, (Accessed 11 January 2014).

Executive summary

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.[2]

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. 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 have 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

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

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.

The box below summarizes all the recommendations of this report: but these are only a few main points. 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 quickly to ride out the shocks.

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

Introduction: cyber sub-prime

The horizon of risk management needs to be extended far beyond its current perimeters – beyond the local IT enterprise to all aggregations of cyber risk, and especially to outsourcing and contractual agreements, supply chains, upstream infrastructure, and other sources of external shocks.

The 2008 financial crisis demonstrated that general underlying causes of risks are camouflaged by excess complexity. As this paper emphasizes, the financial sector can be a unique source of ideas whose lessons are hard-won and still very fresh in the minds of many.

Our lives (and our infrastructure) are increasingly expected to be online, all the time. The World Economic Forum refers to this as 'hyperconnectivity,' something which "does not just allow us to do things more efficiently; it transforms how we do things and even what can be done."[3]

Obviously, the internet has been incredibly resilient (and generally safe) in the past, but the same features that have made it relatively risk-free can and likely will backfire at some point. The internet of tomorrow will be both the source of global shocks and amplify shocks from other areas in ways for which risk managers, corporate executives, board directors, and government officials may not be adequately preparing.

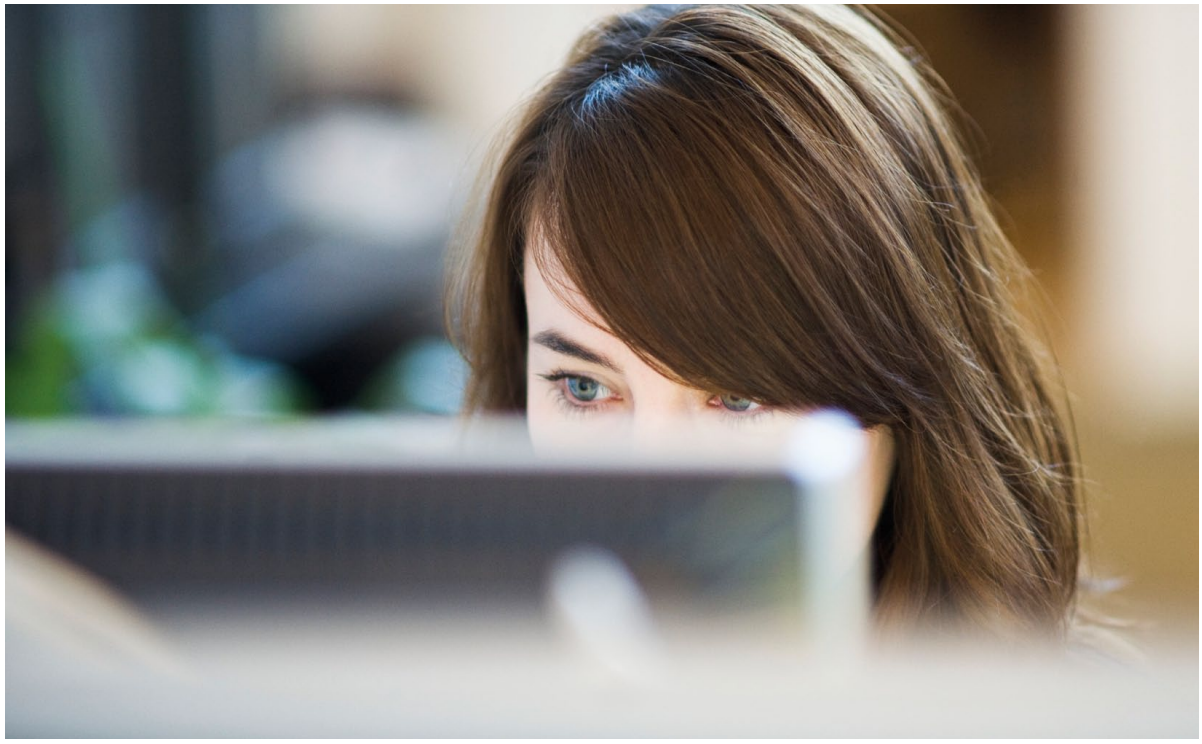
Global shocks are "cascading risks that become active threats as they spread across global systems." OECD [4]

The interconnected and amplifying nature of the global financial crisis bears striking resemblances to what could happen with an on-line crisis.

Shock to the financial system

Shock to the internet

The financial sector can be a unique source of ideas regarding cyber risks.



Cyber risk management today is essentially reductionist, assuming that the risk of each sector or nation is simply the aggregation of local technology and procedures in each organization. Risk managers in each organization focus mostly on what is going on inside their own four walls.

But cyber risks are not self-contained within individual enterprises, hence risk managers must expand their horizons. Connecting to the internet means exposure to nth-order effects – risks from interconnections with, and dependencies on, six other aggregations: counterparties and affiliates, contract and especially outsourcing, supply chain, new disruptive technologies, upstream infrastructure, and external shocks.

There have been disruptions to each of these aggregations. But until recently, societies have had only limited reliance on the internet. The magnitude of shocks resulting from incidents has not been amplified to the point of a global shock. With growing reliance on the internet, the volume of the shocks will likewise multiply.

And while society's reliance on the internet grows exponentially, control 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," as expressed by Dan Geer, the respected internet risk expert.[5]

These system-wide cyber risks have largely been ignored. In some ways, this is strikingly similar to the financial sector's disregard for similar system-wide risk prior to the 2008 financial crisis.

This report, a collaboration between the Atlantic Council and Zurich, examines the issue of global cyber shocks, focusing not on near-term losses or costs, but on long-term solutions to potentially catastrophic problems. The analysis starts with the seven aggregations of cyber risk, which are most likely to cause or amplify a cyber shock, followed by a discussion of why internet 'extreme events' – global shocks – are more likely in the future.

The report concludes with detailed recommendations to governments (and other organizations with internet-wide concerns) as to how they can make cyberspace more stable and sustainable, and to individual companies on how to survive in the face of severe cyber shocks.

[3] The Hyperconnected World, World Economic Forum, 2012, http://www3.weforum.org/docs/WEF_RRHW_Overview_2012.pdf, (Accessed 23 February 2014).

[4] OECD Report, Future Global Shocks: Improving Risk Governance, 2011, http://www.oecd.org/governance/48256382.pdf, (Accessed 11 January 2014).

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

Introduction: cyber sub-prime continued

What can cyber risk managers learn from the 2008 financial crisis?

Prior to the financial crisis, risks were assessed by financial institutions individually. For example, a bank with significant exposure to certain risks – such as those associated with a large portfolio of sub-prime mortgages – might have had to set aside a reserve and perhaps expect to have a bad quarter or two if the underlying risk led to a meltdown. There was little assessment by either regulators or the market participants themselves of the complex interconnections among the financial risks of different institutions. The resulting shock started with those who made the riskiest decisions, but soon cascaded to everyone, even those who had invested wisely and conservatively.

Not only were the chances for a cascading catastrophe widely ignored, but many experts insisted at the time that the system was sufficiently diversified so that linkages between risks were impossible. The system's very complexity allowed risk to be spread to those most willing and able to deal with it. But it was this complexity, magnified by attendant lack of transparency and limited understanding, which contributed to the ultimate crash of 2008. A failure in one small part of the U.S. mortgage market thus could lead to a global recession, the collapse of governments, a sovereign debt crisis requiring bailouts, and even fears for the future of the euro and European Union.

Unfortunately, cybersecurity professionals often approach risks in a similar fashion, relying on a reductionist analysis of risks, while assuming that the risk posed to the system as a whole is merely the sum of all the point risks. They analyze cyber vulnerabilities looking at one technology, one organization or one nation at a time, paying little attention to how risk might emerge from the interaction of those organizations or technologies. Just as sound, internally-focused risk management failed to protect companies from the collapse of the financial system, strong internal computer security controls won't shield even the best-protected companies from a 'cyber sub-prime' failure.

The similarities between the financial and cyber risk management methodologies go well beyond simple analogy.

In the financial crisis, banks, corporations, individuals and even nations became vulnerable because they were highly leveraged, taking on incredible financial debts. The same is true in cybersecurity, where modern economies and societies are perhaps even more heavily leveraged, but their leverage involves information technologies (IT), not borrowed dollars, yen or euros. Companies are feeling the pressure to

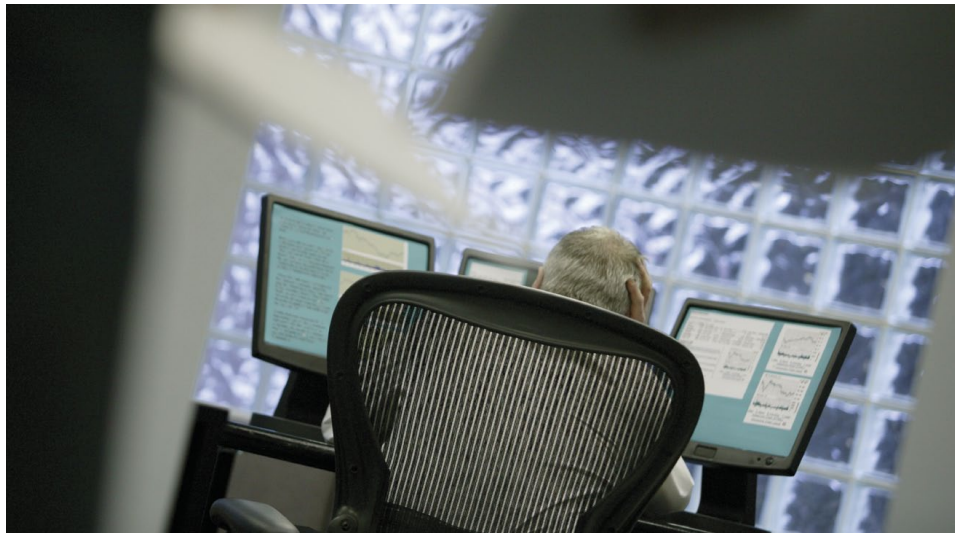
Upcoming cyber shocks

The number of man-made and natural disasters has tripled over the past 40 years, a trend not likely to diminish any time soon.[6] Reports by the OECD and World Economic Forum agree that global shocks will become increasingly more likely and frequent while the US National Intelligence Council believes the "risks of interstate conflict are increasing owing to changes in the international system."[7]

As summarized by PwC, "In short, improbable risks aren't so improbable now; they're becoming the norm in a more uncertain world."[8]

The internet will not be immune to these shocks and conflicts. As a highly connected and increasingly tightly coupled system, with extensive common-mode functions, and one on which societies and economies are so dependent, it is very likely to initiate and or amplify disruptions. These cascading cyber disruptions, where a series of local incidents (each perhaps unimportant on their own) will be passed along through connections to cause more widespread shocks.

Before the financial crisis, financial institutions assessed risks individually.



increase their IT leverage for the same reason that banks and other companies once increased their financial leverage: to keep pace with rivals that are all doing the same. IT leverage has just as much complexity, lack of transparency with regard to the risks, and lack of understanding of the underlying fundamentals as financial leverage. Few people truly understand their own computers or the internet, or the cloud to which they connect, just as few before the crisis truly understood the financial system as a whole or the parts to which they were most directly exposed.

A significant chain of disruptions to an interconnected system that only a few, if any, fully understand, could bring it all crashing down.

Complex systems, unexpected risks

Both the financial sector and cybersecurity risks are passed along to others to become concentrated – possibly toxically – in places far removed from the companies or entities where the risks originate. Because the system has been incredibly resilient for several decades, the underlying expectation is that it will stay safe indefinitely, a belief that is often most pronounced among professionals who are part of the system.

Worse, these risks get lost even to the system as a whole: the effects are so far removed from the source, and they are so complex and interconnected, that they are neither tracked nor easily modeled. Among those repackaging mortgage securities, these risks were obscured and concentrated when banks originated sub-prime mortgages and chopped the risk into securitized tranches that were sometimes re-combined. Ultimately no one fully foresaw where these risks would end up.

In cybersecurity a similar process occurs when companies outsource functions or information, allowing them to focus on core competencies, freeing them from the worries associated with managing servers, IT processes and security. All too often these companies know nothing of the information security or business continuity measures of the company to which they've outsourced. Worse, portions of the outsourced work often get further outsourced as each individual company focuses on its core competencies, and so on. Alternatively, a company might seek to mitigate risk by diversifying its outsourcing by, for example, working with four separate providers, only to find that in turn, they all rely on the same cloud service provider, on the same operating system, or on the same internet service providers.

With so many unknowns, it will be difficult or impossible to adequately measure the resulting risk of this hyperconnectivity and where it might be concentrated in places such as large cloud service providers. As one expert involved in this project put it, "the internet is an enabler of unknowable things."[9]

The financial sector, at least, had developed theories and formulas to try to understand the interconnected risks, developing models run by financial, physics and mathematics PhDs. The banking industry is also highly regulated with at least some system-wide, international governance and crisis management structures: the Basel Committee on Banking Supervision, International Monetary Fund, G8, and (later) the G20.

The world of the internet and cyber security lacks these advantages. Models are not nearly as well-developed or integrated into day-to-day risk management of companies or governments.

[6] Swiss Re Sigma, 2/2012, http://media.swissre.com/documents/sigma2_2012_en.pdf, (Accessed 16 February 2014).

[7] For OECD, see OECD Report, Future Global Shocks: Improving Risk Governance, 2011, http://www.oecd.org/governance/48256382.pdf, (Accessed 20 February 2014).

[8] PwC, Dealing with disruption: Adapting to survive and thrive, 16th Annual Global CEO Survey, January 2013, http://www.pwc.com/gx/en/ceo-survey/2013/assets/pwc-16th-global-ceo-survey_jan-2013.pdf, (Accessed 16 February 2014).

[9] Comment from expert (provided not for attribution), Atlantic Council workshop on global aggregation of cyber risks, 4 March 2014.

Cyberization: the seven aggregations of cyber risk

In the financial sector, risks became concentrated in part through securitization; risks were sliced and diced and sold to others, leading to the general assumption the risks had been successfully transferred to those who understood them best. But those firms that took on these risks continued the process of repackaging, eventually reaching the point where no one knew who owned the final risk, who was exposed to it, and where and how the risk was concentrated.

A similar process is happening for cyber risk – to use an ugly word, 'cyberization'– where organizations are unknowingly exposed to risks outside their own organization, having outsourced, interconnected, or otherwise exposed themselves to an increasingly complex, tightly-linked and unknowable network of networks.

Like securitization, cyberization of risk has been off to an exceptionally successful start. The internet so far has proved to be extremely resilient. Even major disasters such as 9/11 and Hurricane Katrina largely had only a direct local impact. Technical failures have lasted only a few hours, and congestion has had a sustained effect only where the infrastructure was inadequate.[10]

Table 1: Seven aggregations of cyber risk

	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

A Harvard Business Review survey found that 20 percent of companies believed they had an inadequate security budget.

But as with securitization, the risks to the cyber system may no longer be in-house. Risks in each case can concentrate in other places, in a system so complex that even in the U.S. military (widely assumed to be advanced cyber warriors), "commanders do not always know when they are accepting risk from cyber vulnerabilities."[11]

The aggregations of risk posed by the financial crisis included inflated U.S. real estate prices, over-leveraged households and companies, fragile banks, and implicit guarantees for public bailouts. For cyber risk, the aggregations start with the internal corporate network and security practices and expand outward to counterparties and affiliates, supply chains and outsourcing agreements, infrastructure, external shocks and others (see Table 1).

These aggregations of risk (explored in more depth in a separate paper released to accompany this report) are hazardous, but as discussed in the following sections of this report, risks arising from the interconnections between these elements are even more worrying.

On the list of the seven aggregations of risk, **internal IT enterprise** is the most obvious. A Harvard Business Review survey done in 2013 (supported in part by Zurich) found that 20 percent of companies queried believed they had an 'inadequate security budget' and that:

"Cyber risk comes in a bewildering variety of forms. More than one in four survey respondents mentioned each of the following as being among the most serious information security concerns for their organizations: malware and other viruses, administrative errors, incidents caused by data providers, malicious employee activity, attacks on web applications, theft or loss of mobile devices, and internal hackers."[12]

But nearly all of these risks listed here are essentially internal: even when the initial source is external (malware, attacks on web applications), these are expected to be controlled by IT departments, specifically the chief information security officer. The only truly external concentrations of risk mentioned are those "incidents caused by data providers." Other aggregations of cyber risk are not mentioned.

One positive trend has been the growing awareness of cyber risks among members of corporate boards. A 2013 survey of FTSE 350 companies' board chairs and audit committee chairs conducted by the UK government found general confidence among board members, with 64 percent believing that their colleagues took "cyber risks very seriously."[13]

Unfortunately, things are not as positive as this would suggest. The survey also found that:

- Only a third had a very clear understanding of their main information assets and 60 percent have merely a "basic understanding."
- 25 percent said the "main board has a poor understanding of where key information or data assets are shared with third parties."
- Less than half of FTSE board chairs "think their main board has a clear understanding of the potential impact of information and data losses."

In short, board members' confidence may be based on mistaken assumptions. They admit to not understanding the very information assets that are acknowledged to be at the heart of the success in the digital economy, and understand neither the impact of incidents involving these assets nor where that information leaves their organization (and their direct control).

[10] Inter-X: Resilience of the Internet Interconnection Ecosystem, Enisa, April 2011, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x/interx/report, (Accessed 20 February 2014).

[11] Testimony from VADM Mike Rogers to Senate Armed Services Committee, http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf?utm_content=buffer878a9&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer, (Accessed 15 March 2014).

[12] Harvard Business Review, Meeting the Cyber Challenge, 2013, http://www.zurichcorporateforum.com/news/2013/01/24/concerns-over-cyber-risks-grow, http://www.zurichcorporateforum.com media/2256/17873_zurich_ferma_white_paper_rev3.pdf, (Accessed 21 March 2014).

[13] HM Government, FTSE 350 Cyber Governance Health Check: Tracker Report, November 2013, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/268643/bis-13-1293-ftse-350-cyber-governance-health-check-tracker-report.pdf, (Accessed 10 January 2014).

Cyberization: the seven aggregations of cyber risk continued

The risk from **counterparties and partners** is specific to each organization and arises from some form of dependence on, or direct interconnection with an outside organization. For example, based on their activities in the interbank lending market, banks are dependent on each other as counterparties in thousands of transactions a day. This is the case even though they compete with each other to win new customers and business. The main cyber risk here would be if one of the counterparties suffers a disruption affecting the others regardless of internal security controls.

Other examples include university research departments that allow privileged access between networks, or a joint venture that allows some access to each of the partners' internal corporate networks. Here the risk is not just that one side will suffer a cascading disruption, but that the network interconnection might allow hazards like malicious software to spread directly between those with such access.

Outsourced and contract risks are one of the more easily understood concentrations. It is increasingly common for organizations to form a contractual relationship with others to handle even business-critical functions. Behind innocuous-sounding terms like 'software-as-service' or 'cloud storage,' a complex set of systems can operate; companies rely on others for software, hardware, ancillary business functions (HR or payroll), or functions that in earlier days would have been considered business critical (like order fulfillment, shipping, or even design or manufacturing).

Businesses that outsource can fall into the trap of thinking they have transferred cyber and other risks, when actually they have retained much of that risk. They may have added other risks if the outsourcing provider has lax security controls or inadequate business continuity procedures. U.S. retailer Target Corp. suffered a massive and embarrassing data breach intrusion in late 2013, apparently in part because of network credentials stolen from a refrigeration, heating and air conditioning subcontractor.[14] Even the best contract or service-level agreement will not prevent or mitigate a tarnished reputation.

The other obvious risk concentration occurs when a large number of companies, especially in the same sector, all use the same outsource provider. This herd mentality often sets in once an elite, trend-setting company chooses a particular provider. The same holds true in financial communities: once a major bank has agreed to outsource a service after considerable due diligence, its peers feel justified (or even compelled by cost pressure) to follow its lead. In such circumstances, a failure at the outsourcing company is far more likely to cascade to not just a few companies, but to large segments of a newly-dependent sector. And even the companies at the core of our critical infrastructure are all busy outsourcing increasingly critical functions.

A related concentration happens when the outsourcing partner decides to further outsource or source in another country, especially if this is done without telling the customer. Imagine a company hedging its outsourcing risk by using three providers in three separate locations. This diversity could be entirely undone if all three providers decided to rely on business-critical services from the same cloud service provider.

This cannot be an infinite regression – 'turtles all the way down,' as it were – with every company outsourcing to other companies, which then outsource to others, which in turn also outsource. At some point, the outsourcing stops and that point is a critical concentration of risk, capable of causing global cyber shocks. Disruptions here are doubly worrying, since not only will they ripple widely downstream, but few if any of the affected organizations would have factored this unknown dependency into their risk calculations.

Disruptive technologies generally include the range of innovations that increase our dependence in radical ways. The World Economic Forum calls this hyperconnectivity which "does not just allow us to do things more efficiently; it transforms how we do things and even what can be done."[15]

[14] Brian Krebs, Target Hackers Broke in Via HVAC Company, Krebs on Security blog, 14 February 2014, https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/, (Accessed 16 February 2014).

[15] World Economic Forum, Risk and Responsibility in a Hyperconnected World, June 2012.

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

[17] Dave Evans, CISCO paper, The Internet of Everything, 2012, http://www.cisco.com/web/about/ac79/docs/innov/IoE.pdf (Accessed 9 January 2014).

[18] Department of Energy webpage, SMART GRID, http://energy.gov/oe/technology-development/smart-grid (Accessed 9 January 2014)

[19] Taken from Jason Healey, Atlantic Council blog, Our Pre-industrial Cyber Future: Is the Smart Grid Setting Us Up For a 200-Year Crash?, and conversation with Scott Borg of the US Cyber Consequences Unit, http://www.usccu.us/

[20] For the DNS attacks, see Joris Evans, Internet backbone at center of suspected attack, CNET, 6 February 2007, http://news.cnet.com/Internet-backbone-at-center-of-suspected-attack/2100-7349_3-6156944.html, (Accessed 10 January 2014). For Spamhaus, see Matthew Prince, The DDoS That Almost Broke the Internet, CloudFlare blog, 27 March 2013, http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet, (Accessed 10 January 2014) and Lisa Vaas, Schoolboy arrested over Spamhaus DDoS, world's biggest cyber attack, Naked Security, 27 September 2013, http://nakedsecurity.sophos.com/2013/09/27/schoolboy-arrested-over-spamhaus-ddos-worlds-biggest-cyber-attack/, (Accessed 10 January 2014).

> The controlling factor, the root cause, of risk is dependence, particularly dependence on the expectation of a stable system state. Yet the more technologic the society becomes, the greater the dynamic range of possible failures.
>
> When you live in a technologic society where everybody and everything is optimized in some way akin to just-in-time delivery, the dynamic range of failures is incomprehensibly larger and largely incomprehensible."
>
> **Dan Geer, internet security and risk management specialist[16]**

The goals and implications are staggering, as "the internet now connects anywhere from 10 billion to 15 billion devices. Even so, less than one percent of things are connected to the internet today," a situation which companies like Cisco Systems Inc. would like to remedy.[17] When applied to the electrical grid, these technologies are referred to as the smart grid, a catch-all term for technologies to "to bring utility electricity delivery systems into the 21st century, using computer-based remote control and automation."[18]

Internet shocks could ripple through systems in countless ways, because of the universe of unknown and unknowable dependencies. As systems get more complex and interdependent, more tightly coupled and with fewer workarounds, the shocks from these systems will have an impact on, and echo in the 'normal' internet.

Upstream infrastructure failures would naturally be expected to cascade into cyber failures; indeed, this happens anytime your desktop computer dies when the power goes out.

But there are several other important factors to consider beyond this simple statement, starting with the fact that not all upstream infrastructures are the same. Disruptions to finance, electricity and IT would all have far more immediate and far-reaching impact as these sectors are increasingly tightly-linked to the whole of modern society and all business operations, including the internet.

According to an analysis by the U.S. Cyber Consequences unit, an independent non-profit research institute, if electrical power were out for over a week in a wide-enough area of the United States, upwards of 70 percent of that country's gross domestic product (GDP) would be 'frozen': people would have burned through their supply of candles and eaten the last food in the cupboards, while generators would be out of now-irreplaceable diesel.[19]

Such major disruptions to finance, electricity or telecommunications will cause failures in cyberspace, which are likely to magnify and reflect failures back into the other infrastructures. These feedback loops will be difficult to identify beforehand – due to the depth of interconnection and tight linkages – and since the failures will be novel and between specialists in different sectors that rarely talk, they will be all the more difficult to isolate and mitigate.

External shocks are the most upstream of all cyber risk concentrations and can affect not just a single company or sector, but all of cyberspace, potentially cascading to non-cyber systems. Moreover, external shocks tend to be mostly outside the control of any single company or government agency, which means they also tend to be the most overlooked.

If sufficiently severe, shocks can also 'reset' the entire system, providing wake-up calls to send alarms to citizens and policymakers that will echo for years or decades. The entire system enters a new state, as happened with American security policy after the 9/11 attacks. External shocks include cyber conflicts, large-scale disruptive attacks and failures, or malware pandemics.

- Cyber conflicts: This includes cyber incidents and campaigns with significant national security implications, such as high-end theft of a nation's corporate secrets, or the 2007 and 2008 attacks against Estonia and Georgia, respectively.

- Large-scale disruptive attacks: Whereas cyber conflicts tend to take place over weeks, months or even years, and in conjunction with real-world geopolitical crises, large-scale disruptive attacks tend to be one-off incidents that strike more quickly. Typically they are caused by groups operating outside of government, or individuals out for mischief, criminal gain, or pushing a political agenda. Examples include numerous deliberate and worrisome attacks on the Domain Name System (DNS) root servers, one of the most critical parts of the internet infrastructure, or the 2013 massive denial-of-service attack that generated 300 gigabits of traffic every second on the Spamhaus Project, an important international non-government group that tracks spam operations and sources to provide anti-spam protection, while blacklisting the worst spam offenders.[20]

Internet shocks could ripple through systems in countless ways.

Cyberization: the seven aggregations of cyber risk continued

- Large-scale disruptive accidents and failures: This category includes incidents that take out a significant portion of cyberspace, but which are not caused by human actions. The cause might be natural disasters, an accidental cable cut, or other mishaps. Perhaps the best example is the earthquake that struck in the narrow strait between southern Taiwan and the Philippines on December 26, 2006, destroying nearly all submarine cables in that part of the world.[21]

- Malware pandemics: For the past several years, the creators of malicious software (like worms) have been content to pursue profit, but this could change. Groups motivated by nationalism, anti-surveillance, anti-capitalism, or just plain anarchy could alter this dynamic overnight by deciding to take out the system rather than take it on.

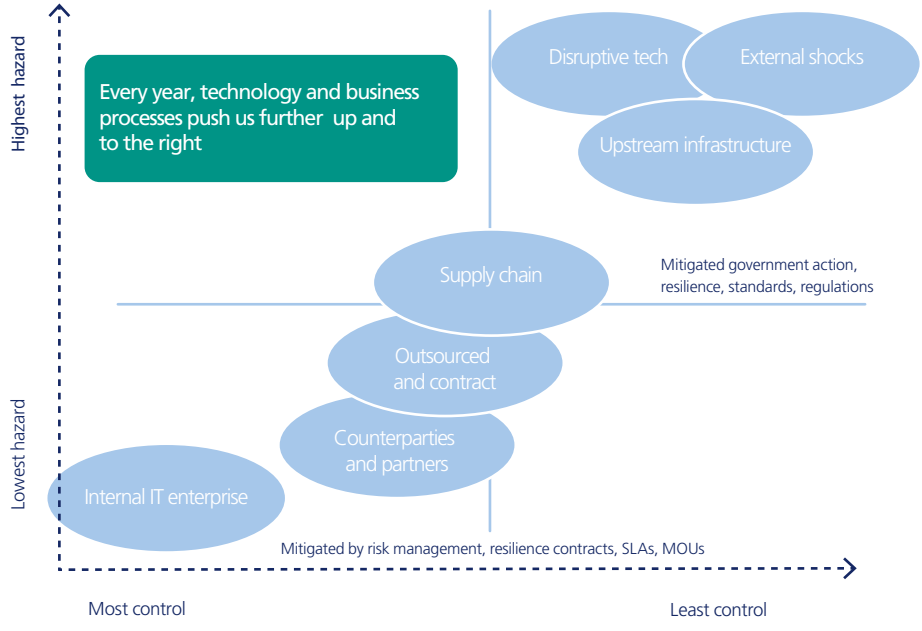
Understanding the seven aggregations of cyber risk

Companies use leverage to maximize gains, taking on debt to make investments in a company or take positions in the market. This leverage increases their upside in good times, but also intensifies the impact of a crash.

These seven aggregations 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.

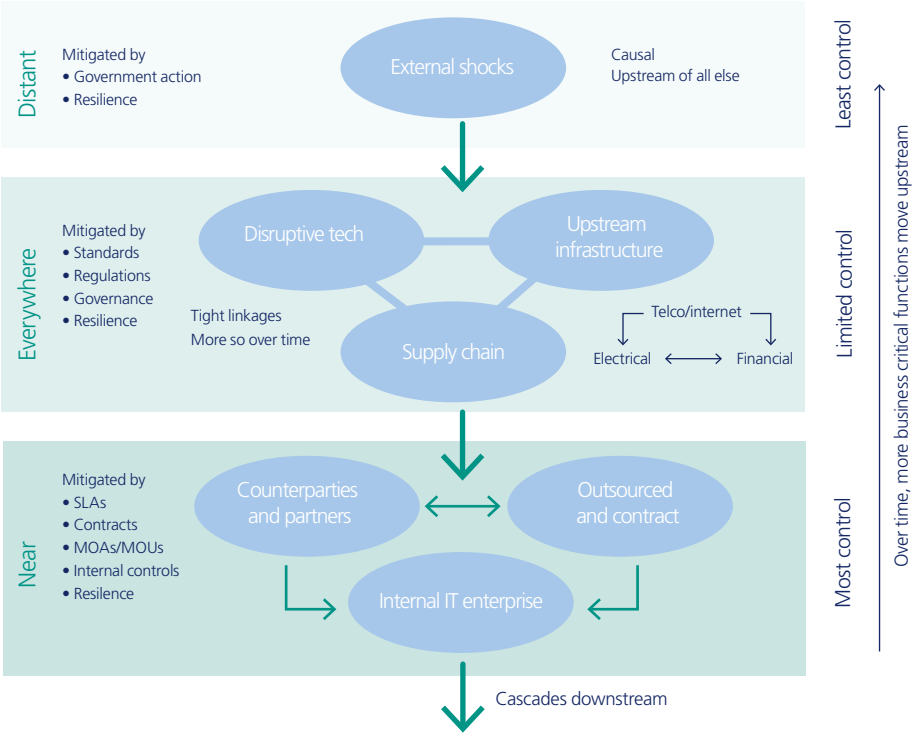
As discussed in the next section, this type of reliance makes global cyber shocks more likely and when they do occur, more intense. The internet is a highly-connected and increasingly tightly-coupled system, with extensive

Figure 1 Relationship of hazard and control



[21] Submarine Cables Cut after Taiwan Earthquake in Dec 2006, Submarine Cable Networks, 19 March 2011, http://submarinenetworks.com/news/cables-cut-after-taiwan-earthquake-2006, (Accessed 16 February 2014).

Figure 2 Zones of risk



common-mode functions. Societies and economies are so dependent on it that it is very likely to have cascading disruptions, where a series of local failures (each unimportant on its own) are passed along through connections to cause more widespread shocks.

The seven aggregations of risk are distinct, but, of course, each overlaps with (and reinforces) others. Looking at the seven together, some patterns can be discerned to help risk managers understand each one, and how they interact with each other.

The seven are listed in this report in rough order of how much control over them any individual organization might have: a corporate CEO or board chair can directly influence the internal IT enterprise of a company, and exert some influence on the outsource and contract, and supply chain aggregations, but have very little impact on upstream infrastructure aggregations, for example. Indeed, only governments and a few high-level organizations can hope to have much influence on external events.

Figure 1 shows the relationship between this element of local control and the overall implicit hazard of each concentration of cyber risk. The aggregations that are most upstream are the most hazardous, as their impact has the greatest chance of cascading downstream.

For risk managers it can be helpful to visualize the seven aggregations in three distinct zones: 'near,' 'everywhere' and 'distant' (see figure 2). A corporate risk manager can have the most impact on the near zone (internal IT enterprise, counterparties and partners, and outsourced and contract) using contracts, service level agreements, memoranda of understanding (MOUs) and memoranda of agreement (MOAs), and internal corporate controls and resilience.

The everywhere zone is so-named because it is all around us. A particular organization can have contractual relations with companies in the everywhere zone, of course, but upstream infrastructure, supply chain, and emerging disruptive technologies are becoming so ubiquitous and of such stunning complexity that the risks here are in a fundamentally different category. The risks arising from this category are generally controlled not by individual contracts, but by societies and governments through standards, regulations, global and national governance, and (as ever) by individual companies operating in this zone and their industry sectors.

The distant zone is for external shocks, risks beyond what any single company or group of companies can hope to meaningfully influence. Controlling risks from external shocks is almost entirely the purview of governments, intergovernmental and transnational organizations and the like.

Why more cyber global shocks are coming

Have no doubt, the internet of tomorrow will almost certainly be less resilient, available, and robust than today. It will be both the source of global shocks, and amplify shocks coming from other areas. As this section makes clear, the main concern is a failure of multiple local elements that leads to cascading global disruptions. The result is that organizations will suffer ever more frequent shocks that in their nature are like natural disasters...too severe and frequent to ever be able to sufficiently protect against.

Charles Perrow, an American professor and risk expert, has made a career studying failures of complex systems such as nuclear power plants and concludes that, "[W]e have produced designs so complicated that we cannot anticipate all the possible interactions of the inevitable failures."[22] And now we've taken these unknowable systems and we are rapidly connecting them to the internet, giving them an additional and critical dependence on humankind's largest and most complex artifact and one that itself is very poorly understood as a system.

The internet, however, seems incredibly stable to most of us. This section begins with an analysis of the 'glass half full' and reasons why there has not yet been a major Internet failure. The following section discusses the 'glass half empty' and why global cyber shocks are very likely to soon become more frequent.

Why no global cyber shocks yet?

Deliberately causing an internet catastrophe with a single attack would be extraordinarily difficult.

A history of cyber-attacks over the past 25 years shows that cyber incidents have so far tended to have effects that are either widespread but fleeting, or persistent but narrowly focused. No attacks thus far have resulted in both widespread and persistent disruption.[23]

Through a combination of **stable technology, dedicated technicians, proven resistance to random outages, and a relatively short history**, the OECD sees the internet as a less likely source of global shocks than pandemics, financial crises, food shortages, or even geomagnetic storms.[24]

The internet is extraordinarily resilient on a day-to-day or even year-to-year basis. It was designed to be so, with robust underlying standards (like TCP/IP), routers, cables and switches that are quite reliable, which have minor consequences when they do fail.

There are also legions of hard-working technicians for whom it is a matter of pride to keep their systems – and the internet – running, day in, day out. After the failure aboard the Apollo 13 spacecraft, NASA engineers did everything possible to bring it home. At the main telecommunications and internet service providers and at major software companies, indeed throughout the internet, there are similar technicians making 'Apollo 13 miracles' happen every week to ensure any internet disruptions are local and short.

Just as important, the internet is a specific kind of complex system, a scale-free network. All such networks (including the internet and the information on the World Wide Web) are extremely resilient to random loss of nodes, as a few very well-connected nodes are the most critical. Up to 80 percent of nodes can be lost without compromising the overall system's functioning, so it is little wonder the internet has not yet caused a global shock.[25]

In a different context, this openness to a large-scale failure, but resistance to a true catastrophe, can have devastating consequences. Charles Perrow, in his classic book on technological disasters wrote that, "It takes just the right combination of circumstances to cause a catastrophe," so that "accidents are rare...catastrophes are even rarer."[26]

[22] Charles Perrow, Normal Accidents: Living with High-Risk Technologies, 1984 and updated version, 1999, Princeton University Press, p10,11.

[23] Healey, *A Fierce Domain*, p21.

[24] See OECD's Future Global Shocks: Improving Risk Governance, 2011, for an overview of the subject.

[25] Scale-free research from Barabasi and Bonabeau, Scale-Free Networks, Scientific American, May 2003, available at http://www3.nd.edu/~networks/Publication%20Categories/01%20Review%20Articles/ScaleFree_Scientific%20Ameri%20288,%2060-69%20(2003).pdf, (Accessed 17 February 2014).

[26] Perrow, p356, 359.

[27] The language of failure->crash->collapse from Dick O'Neill, et al, ideas from the Forum on Collapse in Complex Systems, email to author, 12 March 2014.

[28] From Perrow, p274-275.

Dedicated technicians make miracles happen every week to ensure internet disruptions are local and short.

Lastly, the internet actually has a relatively short history of a few decades and it has only been tightly linked to the real economy and society for the past few years. This is actually quite a short period of interaction with such a system of such mind-bending sophistication and complexity. There have been serious incidents, but because societies' reliance on the internet has been relatively light until recently, the impact of these incidents was correspondingly modest.

Extrapolations based on this successful history lead many people to believe the internet will be stable over the long term. But in the increasingly hyperconnected present and future, the amplitude of the incidents should increase as well. As with other relatively new, but astoundingly complex systems, like nuclear power or securitization of financial risks, as time passes there will unfortunately be more opportunities for global cyber shocks.

Why cyber global shocks are likely

If the internet is so resilient, then how is it that cyber shocks are more likely in future?

As in most large-scale engineering works that have not had any major failures, experts often insist that such failures are impossible (or at least incredibly rare and astoundingly difficult to bring about). New technology, financial engineering, innovative processes, or other wizardry are said to have eliminated this risk from the system. Under this reasoning, complexity is a guarantor of resilience, not a threat.

Major engineering works are, sadly, rarely so immune to failures for several reasons, including those failures familiar to any complex system, as well as in the specific case of the internet.

The financial sector in the previous major crisis went through a transition from stable and resilient to incomprehensibly chaotic and volatile in a short period of time. But the deadwood of complexity had been building for several years, adding dry tinder ready to burst into flame at the first spark, which could have come from anywhere.

With so much complexity (and for the other reasons explained here) cyberspace might face such a phase transition, initiated by a single sudden shock analogous to the failure of Lehman Brothers. This is especially likely to be the case if the failure is mishandled by a feckless or overwhelmed governance structure, allowing a crisis to develop into a larger crash, bringing with it the risk of widespread collapse. The internet might not suffer loss of resilience in a blaze of heat, but instead face a more insidious transition over years. The failures and crashes could come at an increasing pace with shocks of ever-greater intensity until the internet becomes more a source of economic and societal angst than a contributor to innovation, prosperity or free speech.[27]

It is easy to be skeptical of warnings about shocks because of a tradeoff between specificity and plausibility. To be specific, shock scenarios usually include a list of things which have to fail in an exact sequence; accordingly they often end up sounding more like a bad disaster movie than a credible recipe for global shock.

Unfortunately, an implausible series of unlikely individual mishaps is just how many accidents occur. For example, the chief pilot of the Apollo 13 spacecraft said "nobody thought the spacecraft would lose two fuel cells and two oxygen tanks. It couldn't happen. If somebody had thrown that at us in the simulator, we'd have said, 'Come on, you're not being realistic.'"[28] Yet that is the exact disaster-movie scenario which nearly doomed the astronauts on that fateful flight.

Why more cyber global shocks are coming continued

> Very often… societies do reach a level where continued investment in complexity yields a declining marginal return. At that point, the society is investing heavily in an evolutionary course that has become less and less productive, where at increased cost it is able to do little more than maintain the status quo."
>
> **Joseph Tainter in Collapse of Complex Systems[31]**

The reasons that the threat of cyber crashes is increasing, as outlined in the following section, include both those properties common to complex systems in general, and to traits specific to the internet in particular.

Highly interconnected and tightly coupled: The internet is clearly a complex system, with few linear interactions, making it unlike, for example, a traditional automobile production line.

Cyberspace is highly interconnected, not just within itself, but with other systems on which it depends, or which depend on it. The complex interactions of internet systems (like the backbone routing system, corporate IT systems which connect to it, or even the arbitrary behavior of individual users and their governments) "are processes that can be described, but not really understood... often discovered through trial and error, and what passes for understanding is really only a description of something that works."[29]

The internet is also of course tightly coupled, possibly within itself, but certainly and increasingly to society as a whole, "a new era – the era of a global information society, characterized by increasing interdependency, interconnectivity and complexity, and a life in which the real and digital world can no longer be separated."[30]

Unfortunately, such highly interdependent systems-of-systems as the internet, with its tightly coupled and complex interactions "are vulnerable to failure at all scales [and] 'extreme events' [that] can be a result of the inherent system dynamics rather than of unexpected external events."[32] Failures may start as cyber shocks but will be quickly transmitted to the physical world and become 'shocks' without the 'cyber' modifier.

As with the financial sector, where previously trustworthy risk models and equations proved incapable of dealing with 'Black Swans,' the internet is so interconnected and complex we can't model it "as an infinite series of monsters under the bed," as Bill Woodcock, of the Packet Clearing House, notes.[33]

The internet, as stated in the previous section, is a scale-free network and therefore inherently resilient to random outages. But all scale-free networks turn out to be inherently vulnerable to selective attacks on the most connected hubs when "the simultaneous elimination of as few as five to 15 percent of all hubs can crash a system." [34] The internet is likely to be vulnerable to a sustained attack.

Presence of common-mode functions: Another feature of complex systems is that they have many common-mode functions – operations or components that serve more than one function – such as internet routers and packets, which not only relay user content, but control information for the system as a whole. The impacts of the failure of common-mode functions are particularly difficult to understand, since the failures affect multiple parts of the system simultaneously.

Indeed, now that society relies on the internet not just for emails, but global logistics, electrical generation and transmission, and other real-world functions, the internet has become the ultimate common-mode function.

Increasing global shocks: In addition, cyber shocks are more likely, because it appears that shocks of all kinds are more likely. According to the OECD:

"Extremely disruptive events, such as earthquakes, financial crises and political revolutions destabilize critical systems of supply, producing economic spillovers that reach far beyond their geographic point of origin. While such extreme events have been relatively rare in the past, they seem poised to occur with greater frequency in the future. Global interconnections accompanying economic integration enable some risks to propagate rapidly around the world."[35]

[29] Perrow, p85.

[30] Dirk Helbing, Globally networked risks and how to respond, Nature 497, 1 May 2013, p53.

[31] Joseph Tainter, Collapse of Complex Systems, Cambridge University Press, 1999, p117. Emphasis in the original.

[32] Helbing, p52, 53.

[33] Discussion with author, Bali, Indonesia, October 2013.

[34] Barabasi and Bonabeu, Scale-Free Networks.

[35] OECD Report, Future Global Shocks: Improving Risk Governance, 2011.

[36] Dan Geer, Tradeoffs in Cyber Security, http://geer.tinho.net/geer.uncc.9x13.txt, talk given to UNCC, 9 October 2013, (accessed 24 December 2013).

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

[38] OECD Report, Future Global Shocks: Improving Risk Governance, 2011, http://www.oecd.org/governance/48256382.pdf, (Accessed 11 January 2014).

> Systemic and cascading failures can be caused by a cyber or physical disruption but perhaps more important, is a hit to data integrity.
>
> If there is a manipulation of stock prices, a manipulation of the firmware on a medical device just before it is flashed on all the devices, or an alteration of GPS satellite data, the potential consequences could be disastrous with first the impacts before the problem is discovered and then the lack of confidence that the problem has been fixed and a re-infection has not occurred. An attack on integrity of data ultimately could mean a cascading loss of trust in the system."
>
> **Gib Sorebo, Chief Cybersecurity Technologist, Leidos**

The internet is the driving force behind global interconnections and economic integration, so it is natural these global shocks will have a heavy cyber component.

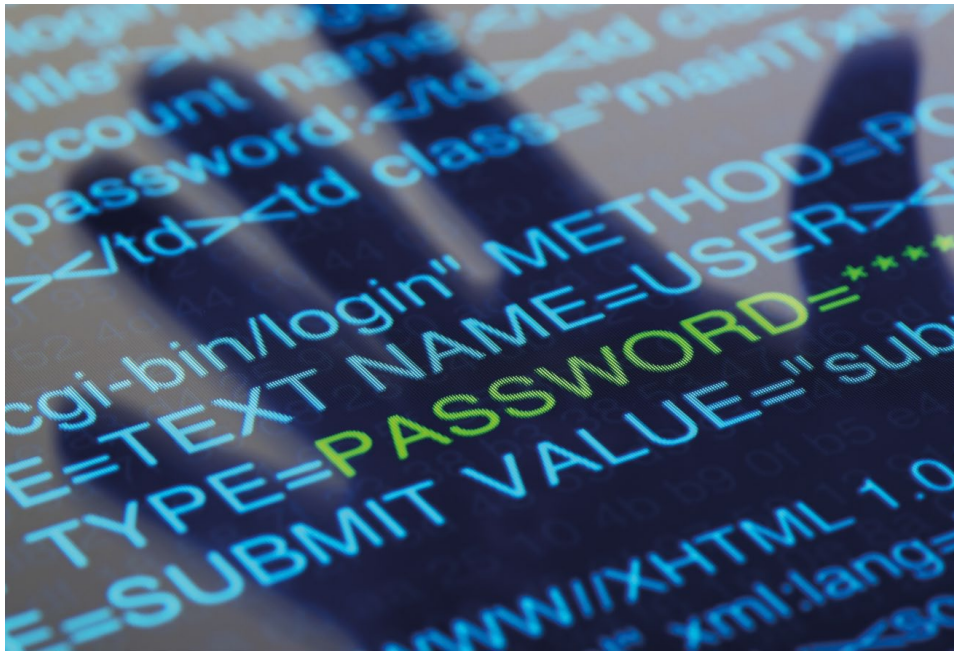
Attackers have the advantage: Offense is easier than defense because the original architecture of the internet was built on trust, software is still poorly written and poorly secured, and the system is so complex that it is difficult to defend. Dan Geer has described this fundamental strategic asymmetry thus:

"while the workfactor for the offender is the price of finding a new method of attack, the workfactor for the defender is the cumulative cost of forever defending against all attack methods yet discovered."[36]

Even though cyber defenses are obviously improving, they are not keeping pace with the attackers: "Whether in detection, control, or prevention, we are notching personal bests, but all the while the opposition is setting world records."[37] No system can have one side gain asymmetric advantages, year after year and decade after decade, and not expect to hit a tipping point. Attackers could someday have not just a local advantage, but superiority with strategic consequences for the internet's availability and resilience.

Ignored externalities: Beyond this fundamental asymmetry, it remains easy for those who use, create and maintain the internet to ignore important externalities. In its report on global shocks, the OECD noted:

"Most producers of [IT] do not have an incentive to make large-scale investments to improve security of their products as the cost generally outweighs the benefits, which include avoiding potential liabilities. Likewise, ISPs do not have incentives to root out malware from their networks despite being in the best position to detect infected machines. ISPs monitor systems for abnormally high email activity, which is most likely to be spam from a botnet, but there is no monetary incentive to notify individual users and help disinfect machines."[38]



Failures may start in cyber space, but will quickly be transmitted to the real world.

Why more cyber global shocks are coming continued

Software companies' strategy to 'release early, release often' worked well enough when the internet was only loosely coupled both internally and to the real world, but will be a contributing factor to future global cyber shocks.

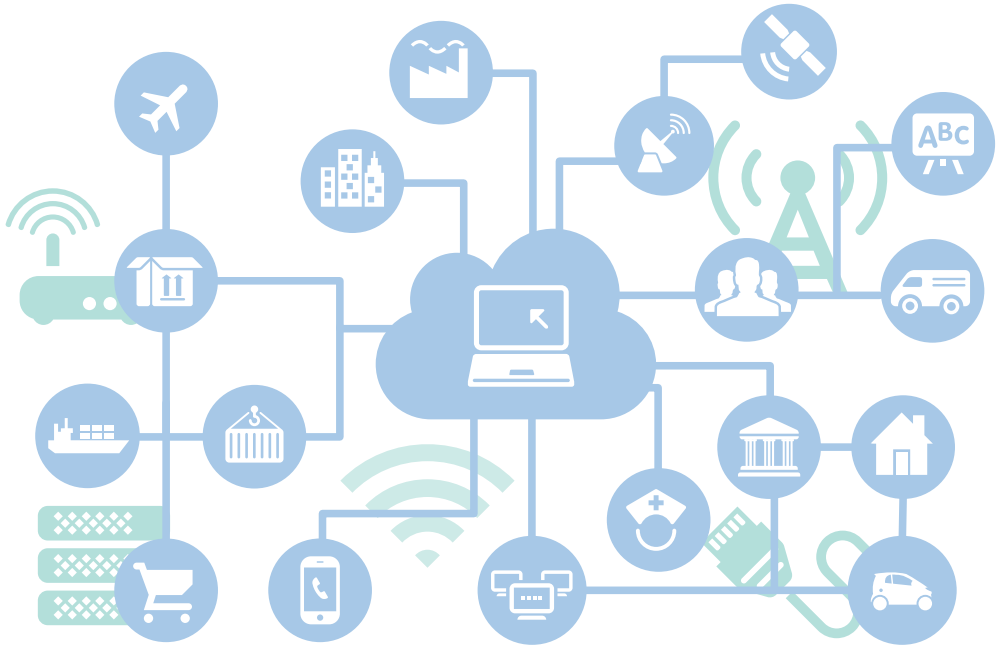
More tightly coupled with society: As the internet is getting more complex and interwoven with the real world, there are countless new connections and vulnerabilities formed every day. In practical terms, Rod Beckstrom breaks this down to three simple laws:

Law 1: Everything that is connected to the internet can be hacked.
Law 2: Everything is being connected to the internet.
Law 3: Everything else follows from the first two laws. [39]

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 most risk managers (and internet professionals) admit when failures are able to cascade directly to internet-connected banks, water systems, cars, medical devices, hydroelectric dams, transformers, and power stations.

As noted, past internet incidents and attacks have only disrupted software or wrecked things made of silicon. These can be recreated or replaced with relative ease. As the internet connects with real life, in places like the smart grid interconnection with the electrical power infrastructure, this will no longer be true: incidents will break things made not just of silicon but of concrete and steel.

The internet's increasingly tight coupling with all areas of the economy and society makes a full-scale cyber shock more likely.



The big risk is that there has been a marriage between a set of transmission and computational elements (of the internet) with essentially all elements of traditional monetary and commercial value. Efficiency has driven every system to rely on a monoculture of a single point of failure: the concentration of risk into online systems.

The value transaction system is accordingly no longer diverse. By pooling value you are actually pooling all the risk and very large markets could collapse because of failures (possibly trivial) at the technical level where all value is digitized.

There used to be ships, camels, and wagons. Increasingly there is only containers and bytes so the system is driven to global single points of failure."

Paul Twomey, Atlantic Council board member and former CEO of ICANN

Loss of diversity and ensuing monoculture: Over time, the internet has lost diversity as the software, hardware, and even chips tend to be the same or similar in every home, business, data center and country. This loss of diversity is as worrying in a computing environment as it is in the actual environment:

"Cascade failure is so very much easier to detonate in a monoculture – so very much easier when the attacker has only to write one bit of malware, not ten million [...] Put differently, when you deploy a computing monoculture you are making a fundamental risk management decision: That the downside risk of a Black Swan event is more tolerable than the downside risk of perpetual inconsistency."[40]

Breakdown of trust and governance: Internet governance – the global system which keeps cyberspace operating from day to day and agrees new technical standards for better Wi-Fi, for example – is in the midst of a tug-of-war over control of the future internet, which is likely to be determined in the next several years.

Each side claims it wants a more secure and resilient internet, though with very different views of what that future internet would look like. One group, largely composed of OECD and like-minded nations, argues for a more open internet based on a 'multi-stakeholder model' of a light government touch and respectively strong roles for companies, individuals, and civil society. Other governments, particularly those of the Russia- and China-led Shanghai Cooperation Organization, want sovereign nations to have a pre-eminent role as they do in other areas, including deciding what information should be allowed and what should be banned.

The worst-case scenario: Cybergeddon

A future in which attackers – whether hackers, organized crime or national militaries – have an overwhelming, dominant and lasting advantage over defenders could be just one disruptive technology away.

Attackers in the future could achieve a wide-ranging impact with little input, making large-scale, internet-wide disruptions easy and common. The internet would cease to be a trusted medium for communication or commerce, increasingly abandoned by consumers and enterprises. Cyberspace would no longer be divided between attackers and defenders, but between predators and prey.

Worse yet, this situation could become entrenched as the increasingly fragmented nature of the internet stymies attempts to reach global agreement on new, more secure technologies or standards. Cooperation among nations or non-governmental organizations would become similarly useless either because there is rampant mistrust in creating newer security standards or because attackers are ubiquitous, relentless and triumphant.

World Economic Forum, Global Risks Report 2014[41]

[39] From http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf.

[40] Dan Geer, Trends in Cybersecurity, 6 November 2013, http://geer.tinho.net/geer.nro.6xi13.txt (Accessed 10 January 2014).

[41] Digital Disintegration, WEF Global Risk Report 2014, http://reports.weforum.org/global-risks-2014/part-2-risks-in-focus/2-4-digital-disintegration/ (Accessed 16 February 2014). Cybergeddon taken originally from Jason Healey, The Five Futures of Cyber Conflict and Cooperation, 14 December 2011, http://www.atlanticcouncil.org/publications/issue-briefs/the-five-futures-of-cyber-conflict-and-cooperation, (Accessed 11 January 2014).

Why more cyber global shocks are coming continued

This decade-old debate is not only important because it represents different views of what the internet could or should be; more important than this simple dichotomy of views is the distraction and erosion of trust, which saps attention from other chronic and acute issues, such as capacity-building for resilience and security in developing countries, or improved internet standards.

Even without this split, governance is already falling behind when it comes to the internet. During the 2008 financial crisis, central banks were able to step in, and global coordination was possible through institutions such as the Bank for International Settlements and the G8. When the G8 alone was insufficient, still the base was there for an expanded G20 with more stakeholders.

Cyberspace and the internet have almost none of this governance structure. In the event of a similarly severe global cyber shock, it is simply not clear who would be in charge, or what levers could be used to mitigate the problems posed to the internet or society.

Most serious cyber conflicts have been expressions of traditional geopolitical tensions, so a growing likelihood of interstate tensions equates directly to a higher likelihood of cyber shocks.[42] If nations dig in behind defended digital frontiers, there may be little willingness to cooperate on stronger internet standards or work together to contain global shocks.

Scenarios for cyber shocks

Because of the historical reliability and underlying strengths of the internet, the OECD sees only two likely scenarios for a global cyber shock:

1. "[A]n attack would have to identify and exploit a hitherto unknown fundamental flaw in the critical technical protocols of the internet, and arrive under conditions where agreement for remedy could not be quickly reached."

2. "[A] succession of sustained, multiple zero-day cyber-attacks on key critical infrastructure sectors by perpetrators of great skill, determination and without concern that their actions might result in harm to themselves."[43]

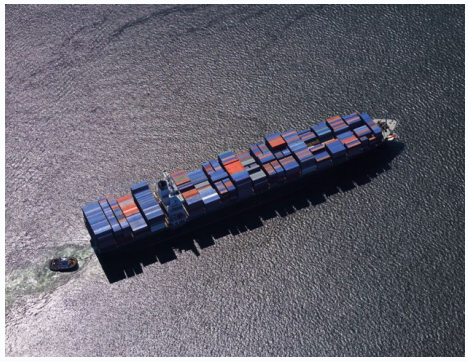
These scenarios are indeed worrisome but perhaps underestimate the risks of unfathomable complexity. Again and again, from Three Mile Island and the Fukushima nuclear disasters to Apollo 13 and the 2008 financial crisis, experts knew their complex systems to be immune to single-cause incidents, but overlooked the opportunities for disasters from multiple unrelated or cascading failures, problems which look obvious in hindsight.

[42] See Jason Healey, A Fierce Domain: Cyber Conflict, 1986 to 2013, for more details.

[43] OECD, Future Global Shocks, p34.

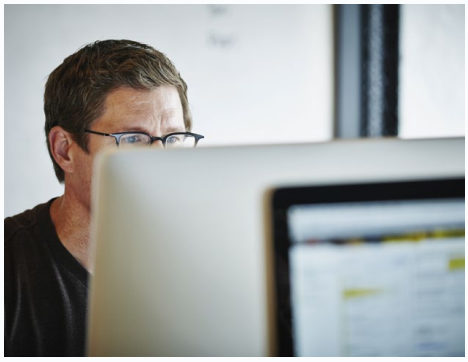
A number of shocks could cascade completely out of control, or multiple shocks might cascade and reinforce one another. Sometimes the initial incident is catastrophe enough, other times this sparks a cascading failure, or else the problem might be insidious and not obvious until it has quietly become a crisis:

- A conflict (cyber or otherwise) between China and the U.S. (or other national powers like China and Taiwan, India and Pakistan, or Iran and the U. S., Israel and Gulf allies) which disrupts the internet globally.
- An attack on Industrial Control Systems (e.g., SCADA) causes large-scale destruction of physical critical infrastructure especially the smart grid, electrical generators, dams or other disruptions which could take not hours but months to fix.
- A massive earthquake strikes the San Francisco Bay area, including Silicon Valley, causing massive downstream internet and IT disruption.



- A major cloud-security provider gives the world a 'Lehman moment.' The cascading impact could soon be just as hard to unwind as the financial chaos after Lehman's failure.
- A major attack on one of the protocols on which the internet depends, such as BGP or DNS.
- A major GPS outage or attack takes out global positioning, navigation and time signals, which would disrupt logistics, business and daily life, and rapidly cascade into innumerable other areas.
- A major outage or even dedicated attack on undersea cables. An even worse disruption would involve the cable repair ships, as there are a limited number of these globally and even fewer in any specific geographic region.
- A single destructive attack technology, which in itself creates the conditions for a shock. For example, a polymorphic malicious software which (like a living entity) can autonomously evolve itself to evade each new defense against it, could disrupt the internet for long periods.

- Balkanization of the internet forces every company to engineer separate web presences, far more intensely than today, in every country it wants to do business.
- Casual erosion of internet security, resilience and usability so that in ten years, only those old enough to remember believe the internet was once a place people shopped, made friends, or shared details of their private lives.



These hypothetical events are not predictions or warnings. They are simply intended to represent potential worst-case scenarios that could trigger the amplifying nature of the internet, and to sensitize risk managers to the aggregation of risks their institutions face in today's interconnected cyber world.

Recommendations

There are two broad sets of recommendations to address the global aggregation of cyber risks presented in this report.

The first set aims to improve the internet as a systemic whole, in effect, to reduce the chances of global cyber shocks and their impact. These recommendations are for governments, organizations (like ICANN) with a system-wide view, and select companies which have an especially critical role (such as major internet service providers, producers of routing equipment, or operating systems).

The second set of recommendations pertains to individual organizations, whether companies, government agencies, or even individual users of cyberspace. These recommendations will help insulate each from the larger dangers of global cyber shocks.

Recommendations

System-wide risk:

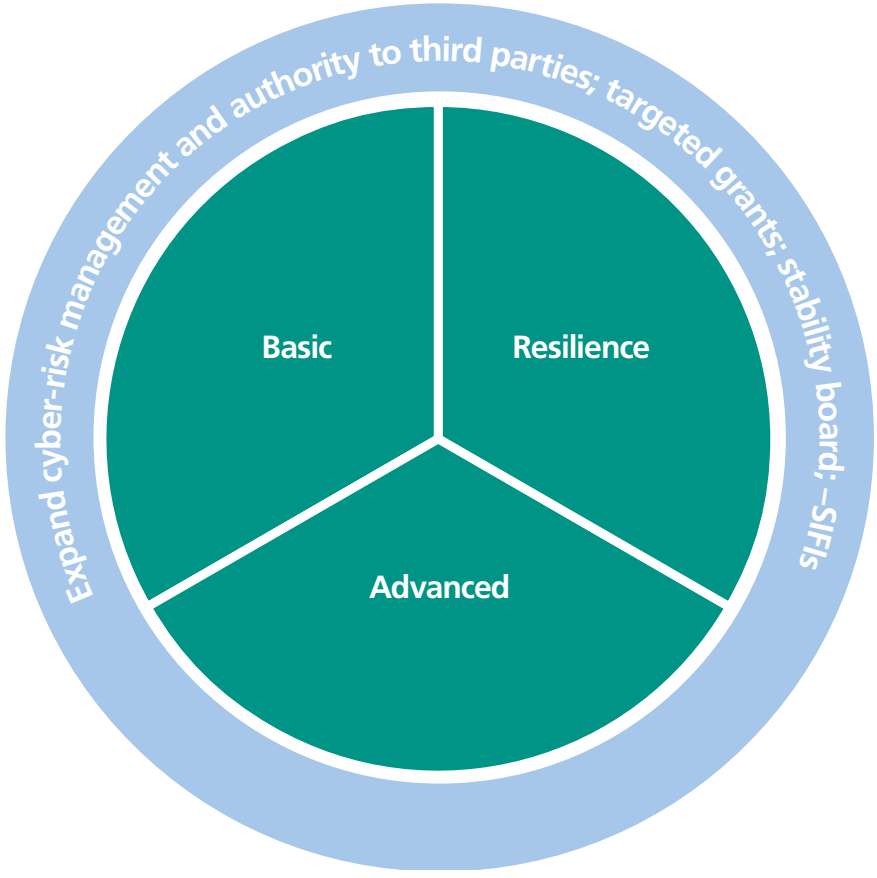
System-wide risk recommendations for governments and organizations with systemic impact:

- Expand cyber-risk management to make it system-wide, similar to financial markets, and improve system-wide resilience and incident response
- Cautiously expand authority to include third-party providers
- Provide targeted grants
- Consider other measures including 'Stability Board,' and recognition of 'G-SIFIs.'

Local risk:

Recommendations apply mainly to individual organizations:

- Basic actions are often simple but often ignored and relevant for everyone
- Advanced measures for more sophisticated companies include expanding their view of risk management
- Resilience to bounce back from disruptions and make them as short as possible offer the best defense.



System-wide risk: recommendations for governments and organizations with systemic responsibilities

The first set of recommendations is broad in scope to make the internet less prone to initiate and amplify shocks and reduce the intensity of those that do occur.

Expand horizon of cyber risk management to system-wide resilience and response:
As with the financial sector prior to 2008, there is too much focus on risks at individual organizations, and too little focus on the stability and resilience of the system as a whole. Governments and others with system-wide concerns (major telecommunications providers, ICANN and standards organizations, key IT vendors of software and hardware) must devote far more attention to systemic rather than organizational risk.

Improve system-wide risk management, resilience and incident response:
Just as surely as there will be more super storms and other natural disasters in the future, cyber shocks, too, are inevitable. Since they cannot be prevented, they must be endured. Organizations with system-wide responsibilities must shift more resources to resilience, ensuring any disruptions are as short and limited in scope as possible. Some governments have begun to look at mitigating risks from an increasingly interconnected and coupled world, such as the U.S. work on 'complex catastrophes.'[44] But risk management and response is still focused mainly on the risk and response carried out within individual organizations. National governments must shift attention to all seven aggregations of risk discussed in this report, developing scenarios, exercises and plans to respond to disruptions to any and all of them.

And while the internet crisis management community has been so far successful at ensuring failures do not develop into a full-scale collapse, the system will not be able to adequately address a truly global, cascading shock. The approach is largely ad hoc, centered on incident management rather than crisis response, and often staffed by poorly-funded organizations or individuals who have numerous other responsibilities.[45] To be ready for cyber shocks, internet stakeholders must conduct exercises, develop response playbooks, and increase funding and grants (see below) for such large-scale crisis management.

Cautiously use existing regulatory authority to expand risk management to third-party providers and affiliates:
In late 2013, the U.S. Office of the Comptroller of the Currency issued guidelines mandating national banks to increasingly look for risk outside their own perimeters, especially pertaining to 'critical activities.'[46] Other regulators can consider whether such a model – surely costly but which does address many of the aggregations of cyber risk – is appropriate for their sector. A regulatory focus on external aggregations of cyber risk can make sense for critical infrastructure sectors like finance, but probably not for retail or small- and medium-sized enterprises.

[44] Complex catastrophes: The 2011 Great Eastern Japan earthquake, tsunami, and nuclear reactor disaster created a complex catastrophe of immense scope. A similar convergence of a large-scale natural disaster and a resulting manmade crisis or technological failure could result in a complex catastrophe in the U.S., with cascading effects that overwhelm national response and recovery capabilities. See http://www.defense.gov/news/homelanddefensestrategy.pdf and other material.

[45] For a window into a successful (but ad hoc and stretched) crisis response, read the lessons learned from the group responding to the Conficker worm which spread in several waves in 2008 and 2009, available at http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf, (Accessed 16 March 2015).

[46] Office of the Comptroller of the Currency, OCC Bulletin 2013-09-29: Third-Party Relationships, 29 October 2013, http://www.occ.gov news-issuances/bulletins/2013/bulletin-2013-29.html (Accessed 20 February 2014).

Recommendations continued

Pursue a private-sector centric approach to work at needed scale:
Governments must understand their limitations when it comes to managing cyber risk. They cannot scale as easily as the private sector, and lack agility and subject matter expertise. Indeed, a study of past cyber conflicts shows that nearly every single one was resolved by the private sector and not government.[47] The private sector has far more agility than governments, an advantage that is highly important. This is especially true, given that the internet is so complex and embedded in society that cyber shocks might be initiated or amplified by any of the seven aggregations of cyber risk.

With that in mind, national cyber strategies should put the private sector at the center of efforts, not the periphery.

Targeted grants for non-government groups:
As one specific way to have a private-sector centric approach, governments and others with system-wide concerns should use monetary or in-kind grants to fund non-government groups already involved in minimizing the frequency and intensity of attacks. Groups like the Forum of Incident Response and Security Teams (FIRST), Spamhaus, and others like NSP-SEC are stopping and responding to attacks (far more effectively than governments) on a daily basis. But these are usually under-funded, lacking permanent staff and a secretariat. As a case in point, the group that coordinates the response to attacks on the financial industry, the Finance Sector Information Sharing and Analysis Center, was losing relevance until it received a USD 2 million grant from the U.S. Treasury. Ten years later, it won a prestigious award for 'excellence in information security.'[48]

Borrow ideas from finance-sector governance:
The banking and financial industry is perhaps the only other critical infrastructure sector that has global governance to deal with crises in real time.[49] Accordingly, the analogy of 'cyber sub-prime' need not be shallow, but should be extended to specific recommendations for cyber governance, borrowed from the finance sector.

Expand and fortify internet governance with a G20+20 Cyber Stability Board:
Prior to 2008 the financial sector had governance at the national level, especially regulators, as well as some international governance including the G8, International Monetary Fund and the Basel Committee on Banking Supervision at the Bank for International Settlements, which issues risk capital and risk management guidelines for banks. As the financial system faced a crisis, this system was expanded to a wider group, including more major developing economies.

Similar solutions can be considered for internet governance. The internet is dominated by the private sector companies which create and maintain it on a daily basis and fill it with content. But governments still have sovereign powers and responsibilities. Microsoft has therefore informally proposed the convening

[47] See Jason Healey, A Fierce Domain: Cyber Conflicts, 1986 to 2012, 2013.

[48] FS-ISAC press release, https://www.fsisac.com/sites/default/files/news/FS-ISAC-Receives-RSA-Award.pdf, (Accessed 15 March 2015).

[49] Other global sectors like maritime and air transportation have groups like the IMO and ICAO but these are very limited compared with financial sector and economic governance like G8, IMF, and the BIS.

[50] Matt Thomlinson, Microsoft announces Brussels Transparency Center at Munich Security Conference, http://blogs.technet.com/b/microsoft_on_the_issues/archive/2014/01/31/microsoft-announces-brussels-transparency-center-at-munich-security-conference.aspx, (Accessed 15 March 2014).

[51] For one way to implement this idea, see Franklin D. Kramer, Achieving Cyber Stability, Atlantic Council, September 2012, http://www.atlanticcouncil.org/images/files/publication_pdfs/403/kramer_cyber_final.pdf, (Accessed 17 February 2014).

of a G20+20 group, 20 governments and 20 global information and communications technology firms – to draft a set of principles for acceptable behavior in cyberspace.[50]

Such an idea could go beyond a single set of principles to a larger plan for risk management to deal with cyber shocks, with the financial sector as a model. Specifically, a G20+20 Cyber Stability Board could look across all aggregations of cyber risk to improve risk management, resilience, and response.[51] The number of IT organizations need not be limited to simply 20 and should not be limited to just companies, perhaps including also internet-critical non-governmental organizations like ICANN or the Internet Engineering Task Force.

Consider recognition of Global Significantly Important Internet:
About 30 'Global Systemically Important Financial Institutions' (or G-SIFIs) are so critical to the financial markets they are subject to additional requirements beyond what is set by their national regulators. This same concept could apply to G-SIIOs (Global Significantly Important Internet Organizations), which could be the same organizations invited to join the G20+20 Cyber Stability Board. Properly structured, this should not be a move towards added regulation, but better governance.

Recognition of G-SIIOs by the G20 or OECD would allow an organization to have a larger voice in the system with the tradeoff of higher expectations to participate in information sharing and incident response and major funding for resilience and stability projects.

Address Too Big to Fail:
A concept related to that of G-SIFIs and G-SIIOs is how to address companies that have become 'Too Big to Fail.' The internet provides many examples: Just imagine the repercussions to the real economy if a major cloud provider had a 'Lehman moment.' Internet companies are at least as vulnerable to disruption and bankruptcy as banks. Organizations invited to join the G20+20 might have some requirement to work together to plan how they fail gracefully.

Stress tests:
Banks and the financial system as a whole must submit to periodic stress tests to see how they would perform in various scenarios, ranging from troubling to horrific. The same concept could easily apply to G-SIIOs to determine if they have the capacity and plans to prevent or mitigate global cyber shocks.

Recommendations continued

Local risk: recommendations for individual organizations

There are three basic subsets of recommendations for those not operating at the systemic level: basic, advanced, and resilience. These recommendations not only make an organization better able to ride out cyber shocks, but as more organizations implement them, they will act as systemic dampeners, potentially reducing the magnitude of shocks.

Basic:
Regardless of the size of the organization, a relatively small set of actions can protect from most cyber risks. These actions are often quite simple and have not changed much in the last decades, but one reason why cyberspace remains so pervasively insecure is that so many organizations ignore them. Different groups of computer security experts have slightly different lists, but they generally overlap; the best known are the SANS 20 Critical Security Controls.[52] The Council on Cybersecurity is pushing these 20 controls, especially the 'First Five Quick Wins:'

- **Application whitelisting:** When organizations only allow computers to run a limited set of pre-approved programs, a hacker's malicious software is prevented from working, stopping intrusions in their tracks.

- **Use of standard secure system configurations:** Computers with only a few standard configurations are far less expensive and simpler to defend.

- **Patch application software within 48 hours:** A 'window of vulnerability' opens once new 'patches' are released by Microsoft, Apple or other to fix software. Dropping this window from weeks (in most organizations) to days (in the best) drastically reduces opportunities for hackers to find a fingerhold.

- **Patch system software within 48 hours:** As for application software, but even more critical as system software is used for more critical functions and with higher privileges.

- **Reduced number of users with administrative privileges:** Users with 'administrative privileges' have the keys to the kingdom, able to do nearly anything they want on a network, as Edward Snowden proved to the NSA. Yet many companies allow every employee such access to download and run any programs they want and have free access to anywhere on the corporate network.[53]

In addition, companies should strongly consider implementing the new Cybersecurity Framework which provides a comprehensive process for cyber risk management for organizations at different levels of risk-management maturity.[54]

Advanced:
Larger, more sophisticated organizations should go well beyond the 20 Critical Security Controls, as they have the capability to engage in more advanced cyber risk management.

- **Pushing out risk horizon:** Advanced organizations in particular should expand their view of risk management to take in the other aggregations of risk, particularly counterparties, contract and outsourcing agreements, and upstream infrastructure. Each of these can be at least partially controlled by contracts, service-level agreements, or in-depth site visits and audits.

  One financial institution reviewed every contract and outsourcing agreement, rating the criticality of each, and auditing those on which they had the most exposure. Some technical tools allow situational awareness outside of a company's own perimeters and give them insights into the networks of other companies to see which are riskiest, infected by malware or even owned by hackers.

[52] The Critical Security Controls, SANS, http://www.sans.org/critical-security-controls/, (Accessed 16 February 2014).

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

[54] National Institute of Standards and Technologies, Framework for Improving Critical Infrastructure Cybersecurity, 12 February 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf, (Accessed 15 March 2014).

[55] Memo from Bill Gates, Microsoft, http://www.microsoft.com/en-us/news/features/2012/jan12/gatesmemo.aspx, (Accessed 16 February 2014).

[56] Author's experience.

[57] For more read Ponemon Institute, Cyber Security Incident Response: Are We As Prepared As We Think, 2014, http://www.lancope.com/ponemon-incident-response/, (Accessed 15 March 2014).

– **Cyber insurance:** With cyber insurance, companies can transfer cyber risks, especially third-party risks associated with data breaches or business interruption. As more companies become involved, offering more products, this option is becoming more available as a recommendation for all companies, not just 'advanced' ones.

– **Demand more resilient and secure standards and products:** Organizations with particular heft can push key vendors and standards organizations to incorporate more security and resilience, which can have a significant impact: By 2002, Microsoft felt sufficient pressure from clients and others that Bill Gates prioritized security within Microsoft products.[55]

– **Board-level risk management:** As noted earlier, nearly two-thirds of boards thought they took cyber risks seriously even though most had little understanding of their information assets, which third parties had access to that data, or the impact of the loss of that data. Such poor board-level cyber risks gambles could ruin those companies not prepared for cyber-crime, much less cyber shocks. Accordingly, boards need to become smarter on cyber risks, include a broad view of global aggregations of cyber risk in their risk registers, hold executives to account, and move away from a checklist/audit perspective.

Resilience:
Unfortunately, these steps to protect against future global cyber shocks will be insufficient. These disruptions will be of such frequency and intensity most organizations will have to suffer through them as they do natural disasters. Organizations can no more 'secure' themselves against these risks than they can hope to forever stack sandbags to protect from a hurricane. Too much risk will be external, complex, and interdependent.

The main hope for companies therefore is resilience, the ability to bounce back from disruptions to make them as short and limited as possible.

– **Redundancy:** A resilient organization needs redundant power and telecommunications suppliers, alternate ISPs connected to different peering points, and work-arounds with little reliance on IT to provide alternatives during internet disruptions. When an earthquake took out nearly all of East Asia's undersea fiber-optic cables, one bank suffered hardly any loss because it had diverse pathways for each Asia office, each connecting to two regional hubs (Tokyo and Hong Kong) through separate cables, using different cable landing stations, and different telecommunications providers.[56]

– **Incident response and business continuity planning:** Having trained teams ready to respond when the worst happens is an overlooked strength.[57] Those teams should have defined standard operating procedures based and held to clear goals based on metrics such as how much time it takes to detect an incident or intrusion, how much time to eject the intruders from the system. The best teams comprehensively understand the organizations' various business lines and most business-critical and time-sensitive information and systems.

– **Scenario planning and exercises:** The best organizations examine the most likely and most dangerous cyber risks and exercise their security and response teams, as well as their corporate executives and boards, to build muscle memory for responding to incidents. Seize the opportunity of each crisis to create 'teachable moments' for responders and executives.

About the Atlantic Council:
The Atlantic Council promotes constructive leadership and engagement in international affairs based on the central role of the Atlantic Community in meeting global challenges. Founded in 1961, the Council provides an essential forum for navigating the dramatic shifts in economic and political influence that are shaping the twenty-first century by educating and galvanizing its uniquely influential, nonpartisan network of international political, business, and intellectual leaders. Through the papers we write, the ideas we promote, and the communities we build, the Council's 10 regional centers and functional programs shape today's policy choices and foster transatlantic strategies to advance international security and global economic prosperity.

About Zurich:
Zurich is a leading multi-line insurer that serves its customers in global and local markets in Europe, North America, Latin America, Asia-Pacific and the Middle East. It offers a wide range of general insurance and life insurance products and services for individuals, small businesses, mid-sized and large companies, including multinational corporations. Zurich employs over 55,000 people serving customers in more than 170 countries. The holding company, Zurich Insurance Group Ltd (ZURN), is listed on the SIX Swiss Exchange and has an American Depositary Receipt program.

About the author:
Jason Healey is the Director of the Cyber Statecraft Initiative of the Atlantic Council, focusing on international cooperation, competition and conflict in cyberspace, and the editor of the first history of conflict in cyberspace, A Fierce Domain: Cyber Conflict, 1986 to 2012. He has worked on cyber issues since the 1990s as a policy director at the White House, executive director at Goldman Sachs in Hong Kong and New York, vice chairman of the FS-ISAC (the information sharing and security organization for the finance sector) and a U.S. Air Force intelligence officer. He is a board member of the Cyber Conflict Studies Association, lecturer in cyber policy at Georgetown University and author of dozens of published essays and papers.

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