ZURICH

Risk Nexus

Global interconnections of cyber risk: impact on healthcare companies

April 2014

The world is likely to suffer internet failures for reasons similar to those that put the global financial system at risk in 2008: these included a nearly absolute dependence on an interconnected system so complex as to be unknowable. Healthcare companies face increased burdens arising from connecting medical devices to the internet and due to their reliance on a network of partners and outsourced providers.

Complex systems, unexpected risks

The internet has proved to be incredibly resilient. This is due in large part to a stable technology platform and dedicated, even heroic technicians who work behind the scenes to keep things running reliably. This has allowed healthcare companies to rely on new technologies that both enhance the quality of care and also reduce the cost of administration and treatment.

But this type of reliance exposes companies to significant risks that they tend to overlook; not just those posed by data breaches or theft of trade secrets, but larger global shocks.

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

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

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

Atlantic Council

Healthcare
continued

mundane comes to depend on distant digital perfection," in the words of Dan Geer, a noted internet risk expert.

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

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

Recommendations for healthcare companies

Embrace new technologies but carefully manage the risk:
The healthcare industry must embrace new IT-driven technologies to drive innovation for drugs and devices; improve health with embedded or internet-connected medical devices; streamline storage and sharing of medical records; and rationalize hospital and medical office operations. Tightly coupling technologies with human health allows incredible efficiencies and health outcomes, but this heavy reliance on "distant digital perfection" introduces significant new risks when cyber shocks strike with increasing frequency. The coupling of poorly understood technologies means intellectual property can be stolen with regularity, even from well-protected companies.

Each new technology drastically increases the 'surface area' that can be exposed to attacks, failure or disruption. But these technologies will likely prove to be riskier than currently assumed: even when one system may be well understood, its interaction with all the others is not, especially in the face of increased cyber disruptions and attackers.

The companies that best understand and manage these new technology-driven risks will have a significant advantage with ultimately higher profits and fewer disruptions, negative media attention, or recalls of medical devices.

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

Shift from protection toward resilience:
Unfortunately, a single set of principles alone will be insufficient. Organizations can no more 'secure' themselves against these interconnected and complex cyber shocks than they can hope to forever stack sandbags to protect from the damage caused by more frequent and severe hurricanes. The main hope for companies, therefore, is to be agile and resilient, and able to bounce back from disruptions through redundant systems and processes, under the leadership of meaningful corporate governance.

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

Healthcare
continued

Push out the risk horizon:
Companies are ever-more reliant on external providers, from outsourced business functions to cloud providers or IT vendors and so must look beyond their own four walls to better understand how upstream and downstream relationships increase their own exposure to disruptions or intrusions by those looking to steal patient records or intellectual property.

Larger or more advanced companies should extend their risk management horizon to include counterparties, contract and outsourcing agreements, and upstream infrastructure. Each of these risks can be at least partially controlled through contracts, service-level agreements, or in-depth site visits and audits. For example, one financial institution implemented a complete vendor security management plan that reviewed every contract and outsourcing agreement to assess the impact of disruptions or data breaches.

Board-level risk management:
Some boards might lack knowledge about their information assets, the impact of disruption or loss, or which third parties have access to sensitive corporate data. Boards may hold executives to account and become smarter on cyber risks by taking a broader view of global interconnections, while continuing to focus on issues related to compliance and auditing.

About this report

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

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

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

Disclaimer and cautionary statement

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

Zurich Insurance Company Ltd

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

www.zurich.com

Atlantic Council

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

www.atlanticcouncil.org