Beyond Data Breaches: 7 Aggregations of Cyber Risk

May, 2014

Property Casualty 360

The Internet continues to be a driving source of connectivity, permeating all facets of society, and although we can benefit from it in so many ways, there is no denying the risks and shocks on a global level that risk managers, corporate executives, board directors and government officials may be not be prepared for. Though technological advancements and dedicated technicians have made the internet more resilient to attack, the potential for future attacks could be catastrophic, affecting globally interconnected systems.

Zurich Insurance Group and the Atlantic Council's latest report, "Risk Nexus: Beyond Data Breaches: Global Interconnections of Cyber Risk" explores new risk management insights on cyber risk, shocks and resilience.

Industry specific insights from the RIMS 2014 annual conference will help prepare risk managers to address future cyber shocks and build their resilience, and Zurich's report further details recommendations for managing risks, including a combination of the following sector-specific factors:

- Shift from protection to resilience
- Improve basic cyber security
- Embrace new technology while managing the risks involved
- Implement incident response and business continuity planning
- Focus on interconnection risk
- Push out of the risk horizon and look beyond their four walls
- Practice broad level risk management.

"To help protect the integrity and reliability of cyberspace and the bottom line for businesses, governments, the private sector and civil society must work closely together," said Dan Riordan, CEO Zurich Global Corporate North America. "We need a clear plan of what to do in the case of an event – both at the individual company level and also holistically and hopefully this report becomes a catalyst for developing such a plan."?? ??

The report is a result of a yearlong study by the Atlantic Council and Zurich on cyber hazards and underlying risks, and is designed to prepare governments and businesses for future cyber shocks.

?"The recent Heartbleed vulnerability demonstrates the main message of the report," according to report author Jason Healey, director of the Atlantic Council's Cyber Statecraft Initiative. "The Internet is so complex and tightly coupled to the real world, it turns out we were all gravely exposed to a cyber risk in an obscure technology that few understand and we didn't see coming. This time it was just passwords, but what happens once the internet is connected to the electrical grid or driverless cars?"

The report details system-wide and local-risk recommendations based on an analysis of the impact of possible shocks. But cyber risks are not self-contained within individual enterprises, so to understand the risks, managers must expand their horizons, and recognize the "cyberization" of risks, as organizations are unknowingly exposed to risks outside their own organizations, having outsourced, interconnected or otherwise exposed themselves to a complex, unknowable "network of networks."

Addressing this issue, the report identifies seven aggregations of risk that arise from the interconnectedness of different elements of technology in business.

1. Internal IT enterprise

Description: Risk associated with the cumulative set of an organization's (mostly internal) IT
Examples: Hardware; software; servers; and related people and processes

This may seem like the most obvious risk, but a Harvard Business Review Survey found that 20% of companies believe they have an inadequate security budget.

2. Counterparties and partners

Description: Risk from dependence on, or direct interconnection (usually non-contractual) with an outside organization
Examples: University research partnerships; relationship between competing/cooperating banks; corporate joint ventures; industry associations

This risk is specific to an individual organization, arising from dependence on or interconnection with an outside organization. The main cyber threat in this instance would be if one of the counterparties suffers a disruption that affects the others, regardless of internal security controls.

3. Outsourced and Contract

Description: Risk usually from a contractual relationship with external suppliers of services, HR, legal or IT and cloud provider **Examples:** IT and cloud providers; HR, legal, accounting, and consultancy; contract manufacturing

It is common for organizations to have contractual relationships with third-parities to handle certain business functions. However, behind words such as “cloud storage” or “software-as-service” lies a complex set of systems that could pose risk.

If the outsourcing provider has lax security controls or inadequate business community procedures, businesses that outsource, who may have thought that they have transferred their cyber risk responsibilities, could fall victim to a breach. The Target data breach in 2013 is a prime example, which was due, in part, because network credentials were stolen from a refrigeration, heating and air conditioning subcontractor.

4. Supply Chain

Description: Both risks to supply chains for the IT sector and cyber risks to traditional supply chains and logistics
Examples: Exposure to a single country; counterfeit or tampered products; risks of disrupted supply chain

5. Disruptive technologies:

Description: Risks from unseen effects of or disruptions either to or from new technologies, either those already existing but poorly understood, or those due soon
Examples: Internet of things; smart grid; embedded medical devices; driverless cars; the largely automatic digital economy

Disruptive technologies include the range of innovations that increase dependence. Though hyperconnectivity has its benefits, it also means that internet shocks could ripple through the system in countless ways, simply because the universe of unknown and unknowable dependencies. As systems get more complex and interdependent, coupled with fewer workarounds, the shocks could have an impact on the “normal” internet, the study claims.

6. Upstream infrastructure:

Description: Risks from disruptions to infrastructure relied on by economies and societies, especially electricity, financial systems, and telecommunications
Examples: 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

Upstream infrastructure failures are to be expected to cascade into cyber failures, the report indicates, as this happens anytime a desktop computer dies when the power goes out. At the same time, though, there are several important factors to consider. Not all upstream infrastructures are the same, and disruptions to finance, electricity and IT would have greater impacts as these different sectors become increasingly linked in the modern world of business operation, including the internet.

Disruptions to finance, electricity or telecommunications could cause possible failures in cyberspace, which are likely to magnify and reflect failures back into other infrastructures.

With the depth and interconnectedness of the infrastructures, these feedback loops can be difficult to identify. They can also be more difficult to isolate and mitigate.

7. External Shocks

Description: Risks from incidents outside the system, outside of the control of most organizations and likely to cascade
Examples: Major international conflicts; malware pandemic

The report indicates that external shocks are the most upstream of all cyber risk connections, affecting not only a single company or sector, but all of cyberspace, and have the potential to cascade to non-cyber systems. External shocks are also most outside the control of a single company or government agency, which often means that they are the most overlooked. They include cyber conflicts, large-scale disruptive attacks and failures or malware pandemics.