

Mitigating cyber risk could make a difference of USD 120 trillion to global economy by 2030

New Atlantic Council / Zurich Insurance Group report uses economic modeling tools to examine how cyber risk costs and benefits affect national GDP under an array of complex scenarios. Building resilience remains a key factor.

Zurich, September 10, 2015 – A new report released today examines the economic impact of cyber costs versus the benefits of interconnectivity under an array of complex scenarios. The report [“Overcome By Cyber Risks? Economic benefits and costs of alternate cyber futures”](#) is a collaboration between Zurich Insurance Group (Zurich) and Atlantic Council, the international affairs think tank, and uses economic modeling tools of the Pardee Center at the University of Denver to gain an understanding of just how cyber costs and benefits affect national GDP over time – and what businesses and policy makers can do in the meantime. The report is the second from Zurich and the Atlantic Council and follows their 2014 [“Beyond Data Breaches: Global Aggregations of Cyber Risk”](#), which explored cascading and systemic cyber shocks, drawing parallels with the financial crisis of 2008.

“As far as we can tell, no one has ever examined the key question of how much the costs of cybersecurity problems compare to the economic benefits of being connected,” Jason Healey, author of the report and Senior Fellow at the Atlantic Council, noted. “Through research, modeling and thinking about how the future might be better, worse, or just different, we can now put answers to such questions.”

“This report does an excellent job at creating potential scenarios that provide multiple perspectives from which to view the future of cyber risk and its economic impact,” said Cecilia Reyes, Zurich’s Chief Risk officer. “It accurately

exhibits that the economic impact of technology is dynamic and its associated risks can be approximated and planned for – and reminds us of the importance of understanding those impacts and the actions we need to take.”

The unpredictable future of cyber development is unlikely to resemble past circumstances. In order to deal with this uncertainty, the report explores four alternate scenarios based on two major uncertainties: The dominance of governments versus the private sector in matters of cyber security; and whether risks will be largely manageable or become unmanageable to the point that stable and secure connectivity becomes a luxury good.

“Cyber Shangri-La,” a best case scenario outcome from the report details a possibility where technology booms are driven and supported by strong cybersecurity; and the subsequent annual economic benefits result in a potential cumulative net global gain of USD 190 trillion by the year 2030; about USD 30 trillion higher than that of the current projection case.

On the opposite end of the spectrum, the most undesirable future scenario, called “Clockwork Orange Internet,” envisions a state of perpetual cybercrime and cyber-warfare that ultimately creates a negative impact of 2.5 percent of global GDP. While this net loss is still not enough to drag down the cumulative benefits to a point where risks outweigh the benefits, if cybersecurity falls dramatically behind, leading to a future of non-stop nation-state cyber attacks and hacks against increasingly vulnerable critical infrastructure, the world could miss out on USD 90 trillion relative to its current trajectory.

Along with the potential future scenarios that the report outlines, it provides specific recommendations to executives who are responsible for creating their companies’ cybersecurity protocols, as well as policymakers that have a hand in shaping national cybersecurity laws.

Among the recommendations for businesses, the report calls for a continued focus on resilience, the ability to bounce back from disruptions to make them as short and

limited as possible. This includes measures such as building redundancy, incident response and business continuity plans; conducting scenario planning and exercises; and considering worst-case cyber futures when looking at business strategies.

“The focus for businesses in an interconnected world should be on how to bounce back from cyber risk events. It is very clear that businesses that want to protect themselves from cyber risks must adopt a mindset of resilience,” said Ms. Reyes.

For policy makers, the report recommends that governments work with the private sector for “next generation” solutions, with priority given to investments in overall stability, governance and resilience.

“Aim for what is realistically attainable – a relatively secure internet and a partnership between the state and private sector on control.” This is known in the report as “strategy of dynamic stability” and requires a collaborative approach between public and private sectors. For example, on systemic cyber risk, the earlier “Beyond Data Breaches” report by Atlantic Council and Zurich borrows an idea from Microsoft: a proposal for a G20+20 group to handle cyber security issues.

Reyes added: “To protect business and communities from cyber risks and leverage the benefits of the cyber world with confidence, the private and public sectors need to work together based on an in-depth understanding of the nature and evolution of the underlying risks.”

“The Atlantic Council, in conjunction with Zurich Insurance Group and the Frederick S. Pardee Center for International Futures, has done really groundbreaking work in examining how cyber costs and benefits might affect global economies in the years to come,” said Barry Pavel, Vice President, Arnold Kanter Chair, and Director of the Brent Scowcroft Center on International Security. “The report’s recommendations offer a useful road map for policymakers, the private sector, and the general public alike on how to reap the benefits of the global Internet and steer ourselves towards the most rewarding cyber futures.”



Further information

The report, summary and supporting materials are available [here](#).

Interested parties also can follow discussion of the report on Twitter at @Zurich, @ZurichNANews, and @AtlanticCouncil.

To get instant access to Zurich's news releases, calendar and other corporate publications on your iPad, iPhone or Android phone please go to your App Store and get the free [Zurich Investors and Media App](#).

For broadcast-standard and streaming-quality video and/or high resolution pictures supporting this news release, please visit our [Multimedia Pressroom](#).

Zurich Insurance Group (Zurich) is a leading multi-line insurer that serves its customers in global and local markets. With more than 55,000 employees, it provides a wide range of general insurance and life insurance products and services. Zurich's customers include individuals, small businesses, and mid-sized and large companies, including multinational corporations, in more than 170 countries. The Group is headquartered in Zurich, Switzerland, where it was founded in 1872. The holding company, Zurich Insurance Group Ltd (ZURN), is listed on the SIX Swiss Exchange and has a level I American Depositary Receipt (ZURVY) program, which is traded over-the-counter on OTCQX. Further information about Zurich is available at www.zurich.com.

Atlantic Council is a nonpartisan organization that promotes constructive U.S. leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges. For more information, please visit AtlanticCouncil.org and follow us on Twitter [@AtlanticCouncil](#).

Contact

Zurich Insurance Group Ltd
Mythenquai 2, 8022 Zurich, Switzerland
www.zurich.com

SIX Swiss Exchange/SMI: ZURN, Valor: 001107539



Media Relations

phone +41 (0)44 625 21 00, fax +41 (0)44 625 26 41

twitter [@Zurich](https://twitter.com/Zurich)

media@zurich.com