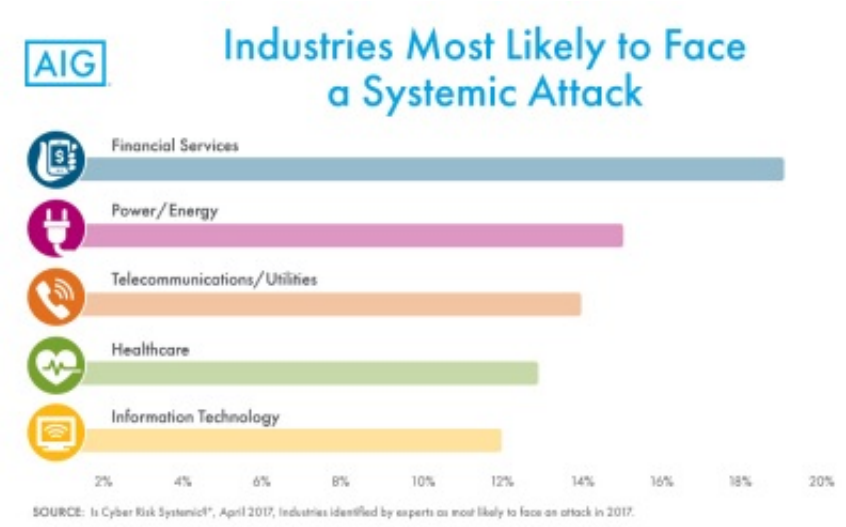
AIG Study: Systemic Cyber Attacks Likely in 2017; Financial Services, Power/Energy, International Cyber Conflicts Key Concerns
Wednesday, May 10, 2017 12:13:00 PM (GMT)

Nine in 10 global cyber security and risk experts believe that cyber risk is systemic and that simultaneous attacks on multiple companies are likely in 2017, according to a study issued today by American International Group, Inc. (NYSE: AIG).

This Smart News Release features multimedia. View the full release here: http://www.businesswire.com/news/home/20170510005781/en/



AIG Systemic Cyber Risk Study: Industries Most Likely to Face a Systemic Attack (Graphic: Business Wire)

More than half of survey respondents say a simultaneous attack on five to 10 companies is highly likely in the next year. More than one-third estimate the likelihood of a simultaneous attack on as many as 50 companies at greater than 50 percent. Twenty percent see an even greater threat, predicting a better than even chance that as many as 100 companies will be attacked.

AIG's survey of cyber security and risk experts was conducted to gain a deeper understanding of the likelihood and impact of a globally systemic cyber-attack. The survey follows several high profile systemic cyber events including the Dyn Denial-of-Service (DDoS) and MongoDB ransomware attacks.

Tracie Grella, Global Head of Cyber Risk Insurance, AIG said: "While data breaches and cyber related attacks have become more prevalent for individual businesses, concern about systemic cyber-attacks are on the minds of those in the very community dedicated to analyzing and preventing this threat."

The leading industries identified by experts as most likely to experience a systemic attack this year are:

- Financial Services (19 percent)
- Power/Energy (15 percent)
- Telecommunications/Utilities (14 percent)
- Healthcare (13 percent)
- Information Technology (12 percent)

Financial networks or transaction systems, internet infrastructure, the power grid, and the healthcare system would be vulnerable in attacks on these industries. Information technology companies, including software and hardware providers that support the backbone of the digital economy, were also seen as particularly susceptible.

"Our highly-networked economy relies on secure, expedient, and constant data flow and electronic communication," said Ms. Grella. "Disruptions to the flow and security of data can have cascading impacts

and negatively impact institutions that rely on such data."

Asked to rank specific scenarios, respondents selected a mass distributed DDoS attack on a major cloud provider as the most likely cross-sector mega event. For data theft or destruction scenarios, flaws in hardware or software widely used by the industry are most concerning.

The top three likely scenarios selected by experts are:

- Financial Services. 15 companies breached. Mass business interruption. Mass DDoS coordinated against financial institutions.
- Healthcare. 10 companies breached (e.g., hospital, pharmacy, insurer). Mass data theft. Flaw in commonly used electronic medical record software.
- Retail/Hospitality. 25 companies breached. Mass data theft. Flaw in widely used payment processing software/hardware.

The worst-case-scenarios that were of greatest concern include:

- Cyber cat-and-mouse war games, retaliation, and escalation to conventional battle between prominent nation states.
- A power grid attack during times of system stress with widespread impact on the population.
- A significant attack on telecommunications and utilities infrastructure that has a widespread impact on essential services.

To access the full study, please visit: http://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/aig-cyber-risk-systemic-final.pdf

Editor's Note: In December 2016, AIG surveyed 70 cyber security, technology and insurance professionals focused on cyber risk in the United States, United Kingdom and Continental Europe to gain a deeper understanding of their views on the likelihood and impact of a systemic cyber-attack. While the sample is small, it does represent a substantial set of key thought leaders and risk management experts in the cyber risk and cyber insurance fields. Recipients included chief information security officers, technology experts, and forensic investigators as well as cyber researchers, academics, insurance-brokers, underwriters, and risk modelers.

American International Group, Inc. (AIG) is a leading global insurance organization. Founded in 1919, today AIG member companies provide a wide range of property casualty insurance, life insurance, retirement products, and other financial services to customers in more than 80 countries and jurisdictions. These diverse offerings include products and services that help businesses and individuals protect their assets, manage risks and provide for retirement security. AIG's core businesses include Commercial Insurance and Consumer Insurance, as well as Other Operations. Commercial Insurance comprises two modules – Liability and Financial Lines, and Property and Special Risks. Consumer Insurance comprises four modules – Individual Retirement, Group Retirement, Life Insurance and Personal Insurance. AIG common stock is listed on the New York Stock Exchange and the Tokyo Stock Exchange.

Additional information about AIG can be found at www.aig.com and www.aig.com/strategyupdate | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance | LinkedIn: http://www.linkedin.com/company/aig. These references with additional information about AIG have been provided as a convenience, and the information contained on such websites is not incorporated by reference into this press release.

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. For additional information, please visit our website at www.aig.com. All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries, and coverage is subject to actual policy language. Non-insurance products and services may be provided by independent third parties. Certain property-casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds, and insureds are therefore not protected by such funds.

The data contained in the study is for general informational purposes only. The advice of a professional insurance broker and counsel should always be obtained before purchasing any insurance product or service. The information in the study has been compiled from sources believed to be reliable. No warranty, guarantee, or representation, either expressed or implied, is made as to the correctness or sufficiency of any representation contained therein.

View source version on businesswire.com: http://www.businesswire.com/news/home/20170510005781/en/

--30-- GA/NY

Contact:

AIG
Media:
Matt Gallagher, 212-458-3247
matthew.gallagher2@aig.com
or
Jessica McGinn, 212-458-4215
jessica.mcginn@aig.com
or
Investors:
Liz Werner, 212-770-7074
elizabeth.werner@aig.com

Industries: Technology, Data Management, Internet, Networks, Security, Professional Services, Insurance
Languages: English
Primary Identifiers: AIG-US
Related Identifiers: AIG-US, US026874784
Source: American International Group, Inc.
Subjects: Survey, Photo/Multimedia