AIG®

# Is Cyber Risk Systemic?

## In December 2016, AIG surveyed cyber security and risk experts to gain a deeper understanding of their views of the likelihood and impact of a systemic cyber-attack.

While the question, *Is cyber risk systemic?*, is simple in form, we believe that the details are highly nuanced. Can a single attack affect tens, hundreds, or even thousands of institutions at the same time? Is the event size inversely proportional to the likelihood that it will occur? Are certain industries more exposed to systemic risk than others? These questions and more frame the research presented in this paper. The data may be useful for sizing up systemic cyber risk and preparing for systemic attacks, important topics for all companies living in the cyber security ecosystem. Moreover, for cyber insurers, answers to these questions are essential for proper modeling and management of accumulation risk.

While our research question, *Is cyber risk systemic?*, is simple in form, we believe that the details are highly nuanced.

# Key Findings

## A Resounding Yes: Cyber Risk is Systemic

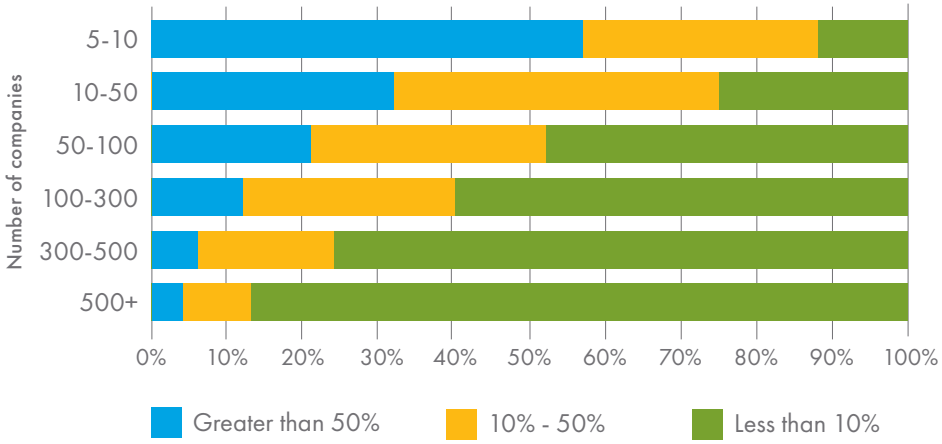
More than 90 percent of respondents believe that cyber risk is systemic, i.e., capable of impacting many companies at the same time. This has widespread implications for everything from cyber security and insurance to risk management practices. Businesses, cities, and people need to start thinking differently about their cyber security vulnerabilities as hiring vendors, placing data on the cloud, and using interconnected machinery and devices may materially change their risk profile. At the same time, insurance carriers, brokers, and service providers need to work together to improve the physical, virtual, and financial protection and support provided to clients to help mitigate this expanding risk.

More than 90 percent of respondents believe that cyber risk is systemic, i.e., capable of impacting many companies at the same time.

## How Big is "Big"?

Identifying systemic risk potential is a start. Yet, it is also important to understand the likelihood and scale of a systemic attack. When asked to rank the likelihood of different-sized attacks occurring within the next twelve months, a large majority of respondents replied that they believe a systemic cyber event impacting between five and ten companies is more likely to occur than one impacting 100 or significantly more companies. Nevertheless, recent incidents, e.g. the MongoDB ransom, Dyn distributed denial-of-service (DDoS), and SWIFT banking attacks highlight the very real threat of larger systemic events. In the DDoS attack against Dyn, a web traffic manager, hackers targeted an Internet infrastructure service, causing intermittent delays to high-traffic websites across multiple industries.

How likely is it that one systemic attack will impact multiple companies in the next 12 months? (n=68)



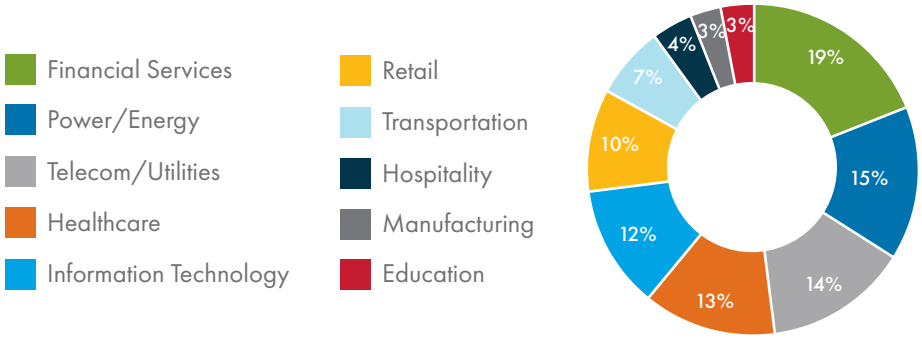
In late 2016 and early 2017, hackers launched an extortion campaign on customers of a widely used open-source database platform, MongoDB. Apparently the hackers targeted older versions with default security settings that made it easier to access, view, edit, or delete data. Security researchers suggest that between 50,000 and 100,000 databases were exposed globally. Flashpoint, a cyber security firm, estimates that at least 20,000 databases were perhaps permanently deleted.[1]

An ethical hacker investigating the issue has reported that companies across many sectors may have been impacted, including healthcare, financial services, education, and travel.[2] The fallout from lost databases is difficult to quantify, but likely quite large. One prominent healthcare institution is reported to have lost three years of research data when its database was deleted in the attack.

## First in Line? The Financial Services Industry

A majority of respondents (85 percent) think that certain industry sectors are more susceptible to systemic attacks than others. The financial services (19 percent), power/energy (15 percent), telecommunications/utilities (14 percent), healthcare (13 percent), and information technology sectors (12 percent) ranked as those most likely to be part of a systemic attack in the next twelve months. This paints a picture of large systemic events we might see including disruption to financial networks or transaction systems, internet infrastructure, the power grid, and the healthcare system. Information technology companies, including software and hardware providers that support the backbone of our digital economy, were also seen as particularly susceptible. Our highly-networked economy relies on secure, expedient, and constant data flow and electronic communication. Disruptions to the flow and security of data can have cascading impacts and negatively impact institutions that rely on such data.

**You have $100 to bet. Allocate your money based on which industries will be part of a systemic attack in the next 12 months (n=70) (Total Allocated = $7,000)**




[1]https://krebsonsecurity.com/2017/01/extortionists-wipe-thousands-of-databases-victims-who-pay-up-get-stiffed/#more-37597
[2]http://www.securityweek.com/33000-databases-fall-mongodb-massacre

## The Greatest Threat: Mass DDoS

When asked to weigh the likelihood of the most severe scenarios (e.g., single events impacting 500 or more companies) respondents ranked a mass distributed Denial-of-Service (DDoS) attack on a major cloud provider as the most likely cross-sector mega event. This is particularly important in light of brisk cloud computing growth and the proliferation of IoT devices which have been used to launch large DDoS attacks. The scenario ranking also suggested that systemic financial services, healthcare, and retail incidents are viewed as most likely. In data theft or destruction scenarios, flaws in hardware or software widely used by the industry were most concerning.

Attacks on critical infrastructure that could cause significant loss of life and bodily injury ranked lowest on the list of scenarios. Executing large-scale attacks on infrastructure (e.g., utilities, aviation, or transportation) would likely require a high degree of sophistication that may limit the pool of capable actors, though the specter of such a threat remains.

| Rank the following scenarios in order from most to least likely to occur in the next 12 months. Most Likely = 1, Least Likely = 10 (n=66) | Average Ranking |
|---|---|
| Financial Services. 15 breached. Mass business interruption. Mass DDoS coordinated against financial institutions. | 4.1 |
| Healthcare. 10 breached (e.g., hospital, pharmacy, insurer). Mass data theft. Flaw in commonly used electronic medical record software. | 4.1 |
| Retail/Hospitality. 25 breached. Mass data theft. Flaw in widely used payment processing software/hardware. | 4.3 |
| Multi-industry. 350 breached. Mass business interruption. Mass DDoS on large cloud provider. | 4.5 |
| Financial Services. 15 breached. Mass data theft. Flaw in widely used payment clearing system. | 4.7 |
| Multi-industry. 350 breached. Mass business interuption. Flaw in commonly used software (e.g., Plesk, BIND) running on Linux machines. | 6.2 |
| Multi-industry. 350 breached. Mass data theft. Flaw in commonly used software (e.g., Plesk, BIND) running on Linux machines. | 6.3 |
| Utility/Power. 35 utilities. Mass business interruption. Flaw in commonly used industrial control system. | 6.3 |
| Utility/Power. 10 utilities. Mass physical property damage, bodily injury, business interruption. Flaw in commonly used industrial control system. | 6.8 |
| Aviation. 10 airlines/airports. Mass physical property damage, bodily injury, business interruption. Flaw in control tower and on-board navigation software. | 8.0 |

**Respondents ranked a mass distributed Denial-of-Service (DDoS) attack on a major cloud provider as the most likely cross-sector mega event.**

# Conclusion

Technological progress moves societies forward. Vaccination, electricity, mass transit, and advanced chemistry have all fundamentally changed the world for the better. With each change however, comes risk and the potential to deviate from our established norms and expectations. Electronic commerce – possibly more than any other social factor – is shaping the risk profile of our modern economy.

But, as previous examples demonstrate, the risk can be managed as the majority of respondents largely agreed that systemic cyber exposure can be mitigated with proper cyber security investments. Along with security software and hardware, investments should include careful vendor vetting and management, training on proper security practices (e.g., back-ups of mission-critical data), and insurance to help mitigate the impact of a systemic cyber event. While cyber threats will continue to advance and expand, defenses must keep pace.

## Worst Case Scenarios Span Industries, Geographies, and Cyber Warfare

Respondents considered a wide range of scenarios that 'scare them most,' from cyber war games to casualty-causing attacks on critical infrastructure. Below are some specific scenarios cited:

- A power grid attack during times of system stress with widespread impact on the population.
- Cyber cat-and-mouse war games, retaliation, and escalation to conventional battle between prominent nation states.
- A significant attack on telecommunications and utilities infrastructure that has a widespread impact on essential services.
- Hacks that manipulate or destroy data (rather than stealing it or a DDoS). Medical, utility, or financial records that are altered so that system users are unable to trust what they see.
- Exploitation of security flaws in IoT devices broadly used in critical infrastructure resulting in large-scale disruption or bodily injury.

## Methodology

To collect data for this survey, in December 2016, AIG sent electronic surveys to over 100 cyber security, technology, and insurance professionals in the United States, United Kingdom, and Continental Europe. Recipients included chief information security officers, technology experts, and forensic investigators as well as cyber researchers, academics, insurance brokers, underwriters, and risk modelers.

## Contacts

For more information on AIG's available cyber liability underwriting, claims, and loss prevention service capabilities, email CyberEdge@aig.com, or contact your local AIG office or broker.

**www.aig.com**


Bring on tomorrow®