Cyber-Risk Management

WHY HACKERS COULD CAUSE THE NEXT GLOBAL CRISIS

Leslie Chacko and Claus Herbolzheimer

In recent months, cyber terrorists have accessed the records of 21.5 million American public service employees, infiltrated the German parliament's network, and blocked a French national television broadcaster's 11 television channels for several hours. Last summer, a malware attack compromised the operations of more than 1,000 energy companies, giving hackers the ability to cripple wind turbines, gas pipelines, and power plants in 84 countries, including the United States, Spain, France, Italy, Germany, Turkey, and Poland at the click of a mouse.

For many years, the world has benefited from information technology advances that have improved the productivity of almost every industry – banking, healthcare, technology, retail, transportation, and energy. But we continue to underestimate the dark side of this equation: Greater dependence on information technology is resulting in an increasing and unprecedented number of cyberattacks.

More than 30 countries – including Germany, Italy, France, the United Kingdom, the United States, Japan, and Canada – have now rolled out cybersecurity strategies. Financial services regulators in the United Kingdom are working with top banks to improve their cyber-risk management. Germany is weighing a cybersecurity law that will require companies deemed critical to the nation's infrastructure to immediately report cyber incidents to the government. And on June 29, the Latvian Presidency of the Council of the European Union reached an understanding with the European Parliament on the main principles of what could become a unified cybersecurity directive for the European Union designed to protect critical infrastructure.

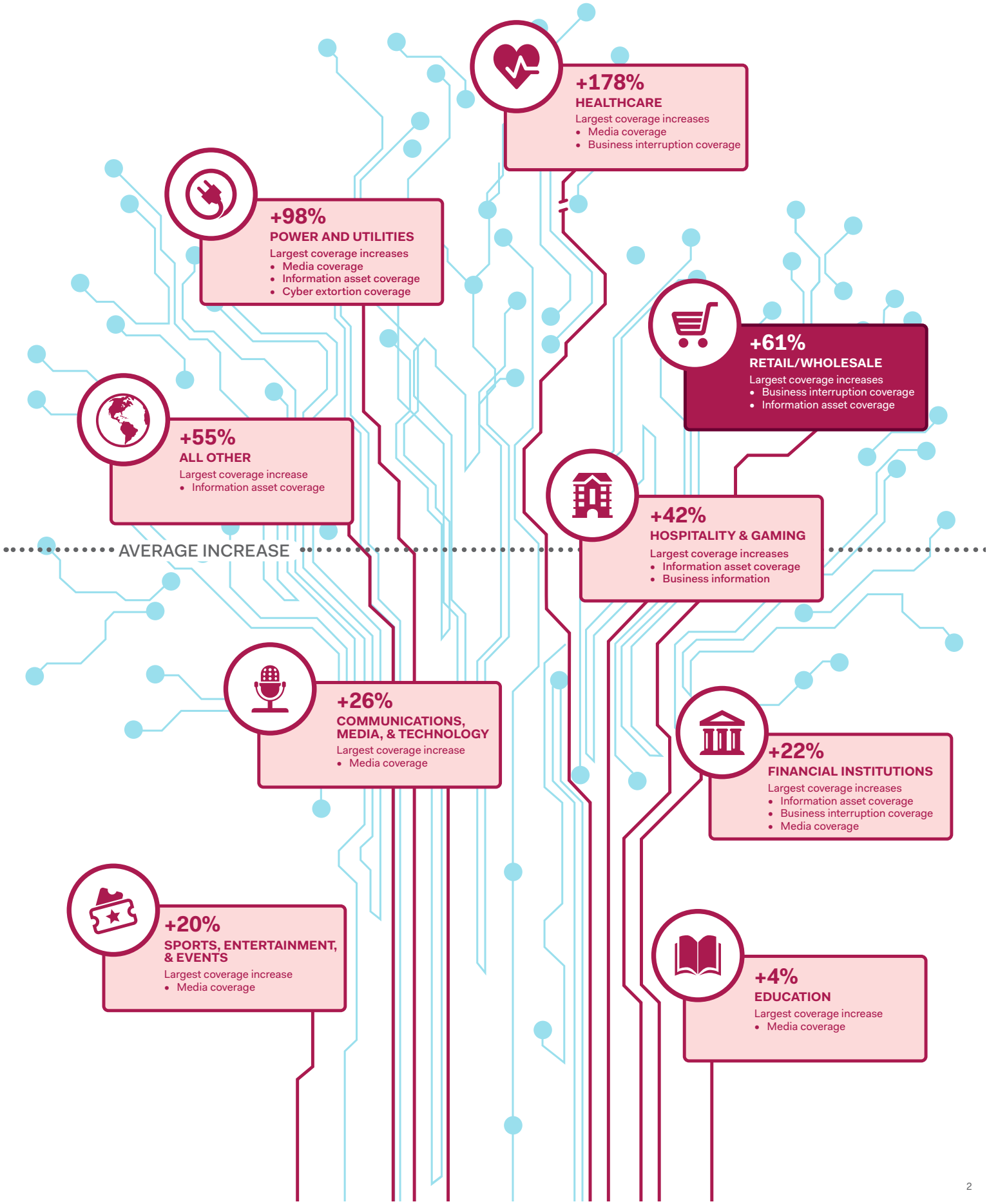
MOUNTING CYBER THREATS

But the searing reality is that both the growing strategic relevance of data and the potential impact of data breaches for companies are outpacing these initiatives. The most recent Global Risks report by the World Economic Forum and its partners (including our firm Oliver Wyman) ranks cyberattacks as one of the top 10 risks most likely to cause a global crisis. The World Energy Council, a forum for energy ministers and utilities, considers cyber threats as one of the top five risks to the world's energy infrastructure.

That's because the industrial control systems that support power utilities, oil and gas companies, and refiners are more exposed to external threats now that they increasingly rely on digital data networks. Digital blockchain collective ledgers of Bitcoin transactions and other new technologies are rapidly multiplying the potential points of intrusion in global banking systems. Manufacturing and machinery industries, too, are entering a new world of cyber product liability and data protection, as they share production facilities and introduce more devices produced elsewhere into their own products. In response, companies with revenues of more than $1 billion have increased their cyber insurance limits worldwide by 42 percent on average since 2012, according to Marsh Global Analytics estimates. Marsh, like Oliver Wyman, is a division of Marsh & McLennan Companies. Over the same time period, healthcare companies have bought 178 percent more cyber insurance and power, and utilities firms have expanded their coverage by 98 percent. (See Exhibit 1.)

Former director of the United States' National Security Agency, General Keith Alexander, has commented

Exhibit 1: Rising Cyber Crisis
Companies are spending more on cyber-risk insurance to protect themselves from an increasing number of cyber attacks



that countries need something like an integrated air-defense system for the energy sector to keep up with mounting cyber risks. The same is true for other industries. But recent clashes between the White House and Republicans over the establishment of a new Cyber Threat Intelligence Integration Center demonstrate that marshalling the resources required to protect companies more broadly will take time.

TREATING CYBER RISKS AS OPERATIONAL RISKS

So what else can be done? Above all, companies must treat cyber risks as permanent risks to their entire enterprise and not as isolated "information technology" events. Unlike strategic, operational, and financial risks, cyber risks are often mistakenly treated as lower priority and relegated to the information technology and communications departments.

As a result, the true cyber risk exposure of companies often goes unnoticed by top management and boards of directors, exposing companies to greater risk. Cyber risks are rarely quantified or linked with their potential impact on companies' financials, making it almost impossible to conduct cost-benefit analyses or make strategic choices. Information-technology departments introduce new technical solutions with minimal top-level direction and without any comprehensive understanding of the risk appetite of the organization. Companies adopt case-by-case reactive measures instead of a balanced portfolio of initiatives that involve their entire organization and align with their overall appetite for risk.

Companies, instead, should set a target level of cybersecurity for critical networks based on their importance to the firm's overall appetite for risk, much as they would with any other operational risk. This should be done quantitatively, perhaps in the form of financial exposure a company is willing to accept.

The company should then ensure that controls and processes address gaps that are accordingly prioritized, starting with those that are mission critical. For example, the potential economic loss associated with construction plans for a new, innovative product may be significantly higher than that of an older production line that is about to be retired.

MAKING CYBER-RISK MANAGEMENT SECOND NATURE

Top managers also need to develop a cyber-risk management culture to the point that it becomes second nature. Cyber-risk management goals, such as the protection of important customer data or the prevention of unauthorized access to mission-critical systems, should be baked into performance targets, incentives, regular reporting, and key executive discussions. When executives evaluate their tolerance for breaches that could impact their company's reputation or violate health, safety, and environmental standards, cyber incidents involving their industrial control systems should be front and center.

Otherwise, like other slow-building risks that people take for granted, ignoring the threat of increasing cyberattacks could drop unprepared companies into the middle of a full-blown crisis. Consider: 90 percent of large businesses in the United Kingdom suffered a cybersecurity breach during the past year and the average cost of breaches has nearly doubled since 2014, according to a recent report produced by the United Kingdom Department for Business, Energy and Industrial Strategy. This isn't a threat that is going away. Companies need to do the math and truly make cybersecurity a top priority.

14%

THE PERCENTAGE OF ORGANIZATIONS WHO HAVE NEVER BRIEFED THEIR BOARD ON CYBER SECURITY RISKS

90%

THE PERCENTAGE OF LARGE UK ORGANIZATIONS EXPERIENCING A SECURITY BREACH IN 2015