MARSH

Marsh Risk Management Research | Briefing

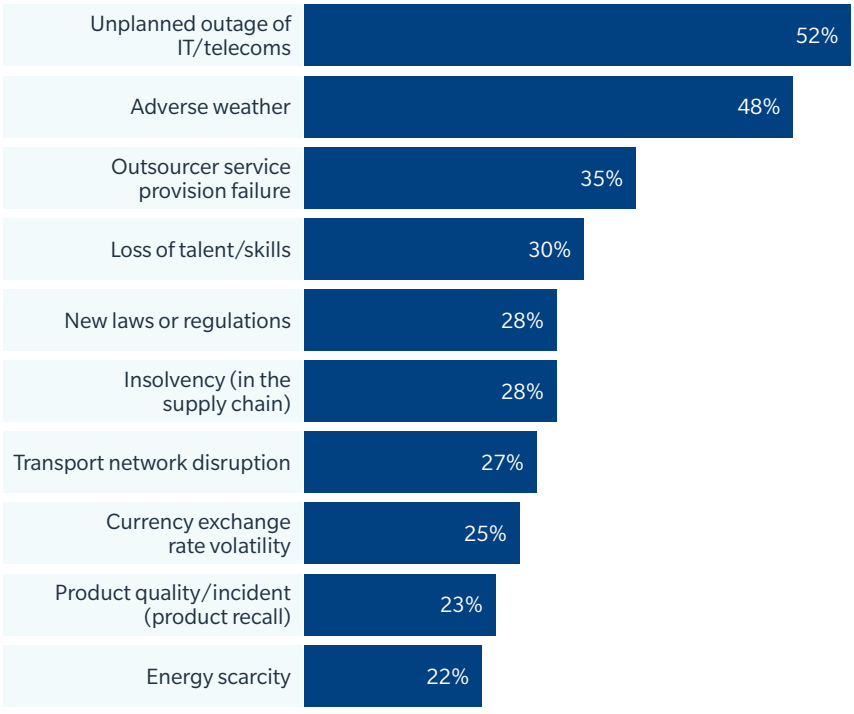
CYBER RISKS EXTEND BEYOND DATA AND PRIVACY EXPOSURES

SEPTEMBER 2013

Although data privacy issues may be top of mind for many organizations in managing cyber risks, they may be overlooking a potentially more severe threat: the impact of technology failures on supply chains and general operations. Technology outages and software failures resulting in supply chain and operational disruptions can cause significant loss of income, increase operating expenses, and damage an organization's reputation.

In fact, unplanned information technology (IT) or telecom outages are the most debilitating source of supply chain disruption, affecting 52% of companies, according to the Business Continuity Institute's (BCI) *Supply Chain Resilience 2012* report. Telecom and IT outages outpace a range of potential sources of disruption, including adverse weather, earthquakes, product contamination, and transportation disruptions. Even the relatively smaller subset of technology failures as a result of data breaches and cyber attacks has the potential to cause as much harm to a business as fire and civil unrest, according to BCI's research.

PERCENTAGE OF COMPANIES AFFECTED BY LEADING CAUSES OF SUPPLY CHAIN DISRUPTIONS



Source: Supply Chain Resilience 2012, Business Continuity Institute (November 2012)

HIGHLIGHTS

- Unplanned information technology (IT) or telecom outages are the most debilitating source of supply chain disruption, outpacing adverse weather, earthquakes, product contamination, and transportation disruptions.
- Although cyber insurance policies have historically been triggered primarily by data breaches and hacking attacks, many now provide coverage for a broad range of technology failures and outages.
- The purchase of cyber insurance should be just one part of a well-planned and effective risk management program that also includes policies and protocols to prevent and mitigate technology risks.

These technology failures can affect a variety of applications used by companies' employees and customers. For example:

- Frequent trading software glitches have struck securities exchanges globally over the last several years, costing exchange operators, securities firms, and investors hundreds of millions of dollars.
- In February 2013, customers at a major US bank could not access their accounts via the internet, automated phone systems, or mobile banks for 10 hours.
- In April 2013, a reservation software crash forced an airline to delay or cancel nearly 2,000 flights. Periodic crashes of the same software, used by more than 300 airlines globally, have affected other airlines on a smaller scale.
- In August 2013, the website of a major US newspaper was unavailable to readers for several hours. Although a cyber attack was initially suspected, the source was later determined to be a server failure during regularly scheduled maintenance.
- Each year, businesses are disrupted by outages in their email and phone systems, a particularly troublesome event now that so many businesses rely on voice over IP (VoIP) technology.

Such IT disruptions can be costly. The average business loses 545 person-hours each year in employee productivity due to IT downtime, according to a 2011 survey published by CA Technologies. And a March 2012 report published by Aberdeen Group found that data center downtime cost businesses $138,000 per hour, up from $98,000 per hour in 2010. Businesses can also suffer loss of revenue and reputational damage, particularly from extended or repeated outages.

THE EVOLUTION OF CYBER INSURANCE

Cyber insurance coverage is increasingly being seen as a must-have by organizations. Historically, coverage was triggered when insureds were the victims of data breaches or hacking attacks. But as cyber insurance policies have evolved, many now provide coverage for a broad range of technology failures and outages.

Given recent SEC guidance related to cyber risks, risk managers need to be prepared to answer questions from their directors and officers about whether the firm's insurance coverage provides adequate protection in the event an incident occurs. It will be important for risk managers to explain that the rapid evolution of privacy and security risks means that many traditional forms of insurance may not be able to adequately respond to these exposures. For example:

- General liability policies often do not provide coverage for damage to electronic data, criminal or intentional acts of insureds or their employees, or pre-claim expenses.
- Property policies typically limit coverage to damage to and/or loss of use of tangible physical property resulting from a physical peril, and to damage to tangible property only at specific locations. Several insurers expressly exclude coverage for any damage to data.
- Fidelity/crime policies generally limit coverage to direct loss from employee theft of money, securities, or other tangible property. Even broadened coverage under a computer crime extension often limits coverage to the cost of re-collecting or restoring the damaged or corrupted data. Often these policies will expressly exclude coverage for actual theft of data or information.
- Errors and omissions policies often limit coverage to claims arising from negligence in performing specifically defined services and exclude coverage for criminal or intentional acts of insureds or their employees and pre-claim expenses associated with a privacy breach.

Current cyber insurance policies can provide reimbursement for lost revenue, including forensic costs and extra expense, as a result of a failure of technology, computer system outage, or cyber attack. This coverage can in many cases be expanded to include contingent business interruption due to a failure of a vendor, such as a cloud computing service provider. Policies can also be customized to fund public relations and crisis management services in connection with an IT failure.

Cyber insurance policies can fill many of the gaps in traditional insurance and provide direct loss and liability protection for risks created by the use of technology and data in an organization's day-to-day operations. Policies can be customized to include any or all of the following coverages:

- Privacy and computer security.
- Information asset.
- Business interruption, including extra expense.
- Cyber crime.
- Cyber extortion.
- Criminal reward fund.
- Crisis management.

MANAGING IT OUTAGES

Any business that assumes its technology is impervious to any failure — especially as businesses increasingly rely on technology to conduct business operations — is ignoring a critical risk. But insurance alone is not an alternative to solid risk management. Instead, it should be just one part of a well-planned and effective risk management program that also includes policies and protocols to prevent and mitigate technology risks.

Before an IT outage occurs, businesses can take several steps to prepare for disruptions and mitigate their potential business impact, including:

- Determine the criticality of various IT systems to ongoing operations and whether alternatives are available or enhanced protection is possible. For example, if a company-owned email server fails, determine whether another can be purchased or rented. Also, assess the vulnerability of critical IT equipment locations to natural hazard events, such as flooding, and take appropriate steps, such as moving equipment to a higher floor or raising it off the floor.
- Develop and test business continuity and crisis management plans. Such plans should specifically address IT outages; communication with employees, customers, partners, and other stakeholders; and steps to protect the company's reputation. Businesses should also verify the plans and capabilities of key IT vendors.
- Evaluate claims preparation and management plans. Review and update procedures and responsibilities for gathering and processing claims information in the event of a loss. It is essential for insureds to document all IT interruptions and notify insurers of an event as soon as possible.

Risk managers should ensure that their companies' IT departments are included in each of these actions. Frequent communication between risk and IT professionals can help both functions to better understand their organization's risks, and to respond quickly and effectively when technology fails.

No business can inoculate itself against all risk of technology failure. But with effective planning inside a comprehensive risk management program, businesses can better prepare for IT outages and minimize their impact on business operations, revenues, and reputations.

ABOUT THIS BRIEFING

This report was prepared by Marsh's US FINPRO Practice, which specializes in financial and professional risks facing Marsh clients, including directors and officers liability, errors and omissions, privacy and cyber liability, and more. Marsh's Network Security & Privacy Practice — with dedicated practitioners in the United States, United Kingdom, and Bermuda — assists clients in evaluating their cyber risks through coverage gap analyses and scalable risk assessments, and in building the right insurance programs to meet their data and privacy needs.

FOR FURTHER INFORMATION, PLEASE CONTACT:

Bob Parisi
Network Security & Privacy Practice Leader
+1 212 345 5924
robert.parisi@marsh.com

ABOUT MARSH

Marsh is a global leader in insurance broking and risk management. We help clients succeed by defining, designing, and delivering innovative industry-specific solutions that help them effectively manage risk. We have approximately 27,000 colleagues working together to serve clients in more than 100 countries. Marsh is a wholly owned subsidiary of Marsh & McLennan Companies (NYSE: MMC), a global team of professional services companies offering clients advice and solutions in the areas of risk, strategy, and human capital. With more than 54,000 employees worldwide and approximately $12 billion in annual revenue, Marsh & McLennan Companies is also the parent company of Guy Carpenter, a global leader in providing risk and reinsurance intermediary services; Mercer, a global leader in talent, health, retirement, and investment consulting; and Oliver Wyman, a global leader in management consulting. Follow Marsh on Twitter @Marsh_Inc.