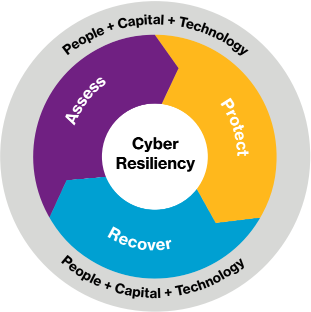

Decode risk transfer.

Software as a service, 'Internet of things' supercharge risk for technology companies

by Jeff Schermerhorn

The role of technology companies is rapidly shifting from being the primary provider of hardware and software to becoming the very backbone of many businesses, creating new and more threatening risk management challenges for technology companies.

From smart-phone-operated thermostats to cloud storage and software, technology companies have evolved to become on-demand service providers. This evolution has benefited consumers and businesses alike. But with technology companies' growing role, however, comes a high degree of risk associated with data aggregation, security and system availability, both for the technology provider as well as their customers.

Cloud shift + IoT = increased risk

According to Gartner research, there will be 20.4 billion Internet of Things (IoT) devices deployed globally by 2020. [1] These large-scale implementations, many of them unsecured, are a major factor driving the increase in distributed Denial-of-Service (DDoS) attacks. (In 2017, these attacks grew 91% from Q1 to Q3. [2]) Moreover, experts predict that by 2020, there will be a $1 trillion shift in IT spending from traditional solutions to the cloud. [3]

This "cloud shift" and dramatic expansion of IoT devices present greater financial challenges to technology companies, due to the risk of mishandled data and the potential for network interruptions for their customers. This enhanced risk was apparent in Willis Towers Watson's 2017 Reported Cyber Claims Index, which found that 63% of claims against technology companies resulted from threats that either impacted network and/or business operations for their customers, or had the potential to do so.

Technology Industry	
Accidental	26%
Hack	21%
Social Engineering	21%
Denial of Service	10%
Rogue Employee	10%
Other	5%
Unknown	5%

*Percentages may not equal 100% due to rounding.

The case for enhanced risk mitigation

Ten years ago, an electronic medical records (EMR) company would sell its software to a health care organization to be installed on that customer's servers and systems. Today, the same technology company is likely to sell a subscription to a service (known as Software as a Service, or SaaS) to the same health care organization. The distinction between the two? Data storage.

[1] http://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/
[2] http://www.techrepublic.com/article/ddos-attacks-increased-91-in-2017-thanks-to-iot/
[3] https://www.gartner.com/newsroom/id/3384720

When data was stored on the servers of the health care organization, the organization would retain the risk associated with that data. Today, the data and its associated risk shifts to the technology company. This heightened risk creates a data aggregation concern when this single entity is holding protected and sensitive information for several other customers. The aggregation of this data inherently creates an aggregation of the risk as well. If the data is compromised, the sheer magnitude could potentially reach beyond the core event, potentially leading to regulatory action as well as civil litigation, including class actions from multiple parties.

Reining in the risk

In light of the changing risk profile associated with data aggregation and system availability, technology companies may want to consider employing the following risk management strategies:

Quantify the risk to customers

Examine the risks of the services provided to customers by asking these key questions:

- What data is collected, stored and maintained for our customers?
- If these services fail for 24, 48 or 72 hours, what is the likely financial loss for our customers?
- Who is responsible for a failure or the mishandling of that data?

The answer to these questions will reveal a key metric for evaluating the technology company's risk: the degree of potential financial losses for customers. Even if customer agreements contain enforceable limitations of liability, these answers will assist in understanding whether customers are likely to sue following an outage or breach.

Compare contractual limitations of liability against the insurance program

Evaluate the limitation of liability provisions of standard customer contracts (and any modified contracts of large clients). Assuming that the contractual limitation of liability is enforceable, consider its applicability in the case of a catastrophic cyber event. Should a service error or software failure impact a large number of clients simultaneously, consider whether the limits of your current insurance program are adequate to cover a potential loss from the event.

Require customers to maintain cyberinsurance

A compulsory requirement that customers maintain cyberinsurance covering first-party losses, including those resulting from a dependent network business interruption, helps reduce the likelihood of a claim being made against the technology company responsible for the outage. Requiring customers to purchase cyberinsurance designed to make them whole in the event of a data breach or network outage will reduce their risk as well as that of the technology company. If the customer's insurer indemnifies its policyholder for the loss, there would be no need for the customer to pursue indemnification from the technology company.

Protect against subrogation

Under the terms of most cyber policies, insurers have the right to subrogate against a third-party responsible for the losses sustained by the policyholder, meaning they can transfer any rights or duties resulting from a claim to another party. Insurers typically weigh various factors in deciding whether subrogation is worthwhile; the expected net recovery being the most material factor. A loss affecting one policyholder for a nominal amount is not one an insurer is likely to subrogate.

On the other hand, a loss affecting dozens of that insurer's policyholders, even if not significant on an individual basis, could nevertheless constitute a major loss to the insurer when aggregated, posing a unique risk to technology companies. To mitigate this risk, it is common for technology companies to have their customers seek a provision in their policies waiving their subrogation rights against their company. However, this must be approved by the underwriter and is typically evaluated on a case-by-case basis.

Realignment of risk is key

The expansion of IoT and the efficiencies derived from the cloud have the potential to improve productivity, simplify daily activities and, in the very near future, revolutionize our lives. Proactive realignment of risk management strategies to match the new potential threats inherent in this productivity burst will enable technology companies to withstand future challenges to their growth and profitability. In this scenario, tech companies, customers, and the everyday people most impacted by these services, will continue to thrive.

Contact

Jeff Schermerhorn
Willis Towers Watson
213 607 6280
jeffrey.schermerhorn@willistowerswatson.com

willistowerswatson.com

Willis Towers Watson