CANADIAN UNDERWRITER.ca

Canada's Insurance and Risk Magazine

TABLE OF CONTENTS Mar 2015 - 0 comments

Over Exposed

The 2015 Allianz Risk Barometer makes clear that concerns over cyber risk are on the rise, both in Canada and around the world. In the wake of that accelerating ascent, what might be the value in taking a "think-tank" approach to addressing cyber risk exposures?

By: Thomas Varney, Regional Manager, North America, Allianz Risk Consulting, Allianz Global Corporate & Specialty North America
2015-03-01

The 2015 *Allianz Risk Barometer*, released in January, outlined the global exposures uppermost on the minds of risk managers. The top three risks not only globally, but within North America as well, were business interruption and supply chain, natural catastrophes and fire/explosion.

Looking specifically at North American results, though, there was a significant rise in concern as it relates to cyber risk exposures, with cyber risk moving into the number four slot. Cited by 25% of respondents, cyber was only 2% lower than the 27% for the number three slot, fire/explosion. In Canada, the results showed cyber risk was tied for the number two slot with reputational risk, behind the number one concern, business interruption and supply chain, the top risk at the global level.

Cyber risk did not even crack the Top 10 concerns of risk managers in the 2013 *Allianz Risk Barometer*. This exposure has risen globally from number 15 to number five since 2013. Currently at number two in Canada, the majority of concern here seems to be with financial institutions and retail, which are the sectors where most data breaches have been experienced.

DATA BREACHES

Data breaches exposing customer and client information, consistent hacking exposures, and mergers creating interconnected systems exposures with different interfaces and platforms, places companies at constant risk. And the increased use of mobile devices will only serve to increase the exposure levels.

Loss of reputation was a major factor in the reason why cyber risk has created such a critical concern for those taking part in the survey. The Canada Risk Barometer survey results reflect a significant concern with both cyber risk and reputational risk, the results show.

The Edelman Privacy Risk Index, for example, indicates 71% of customers would leave an organization after a data breach. The almost-automatic blow to a company's reputation can significantly hit the balance sheet. How can this exposure, with such potentially devastating bottom-line impact, be addressed?

In order to better address any exposure, first the key issues or concerns must be understood. The 2015 *Allianz Risk Barometer* survey broke out in detail the four major concerns, namely economic loss, most feared exposures, most important areas to be protected and, finally, what is preventing companies from being better prepared. Each of those concerns demands a deeper dive to determine some potential solutions.

WHAT MAJOR CAUSES OF ECONOMIC LOSS WERE CITED?

Survey respondents listed the number one potential for an economic loss to be loss of reputation at 61%. Clearly, as outlined in the Edelman Privacy Risk Index, the realization that the economic health of a company is tied to its reputation will have an impact in the marketplace. The loss of reputation through a data breach or other loss of customer data will lead to a potentially significant economic loss.

The second two highest exposures of concern involved potential business interruption exposures (noted by 53% of respondents) and the loss of production capabilities (45%) from some sort of a cyber event. The largest economic fears involve how customers and clients view a business, as well as the ability of a company to continue at proper production, potentially exposing a company to the economic downturn of failing to get products and/or services to market.

WHAT CYBER RISKS ARE MOST FEARED BY RESPONDENTS?

Data theft and manipulation topped respondent fears at 64%. Being responsible for client or customer data and then having it stolen, or in some way changed, would clearly place any company's bottom line at risk.

This concern was followed by loss of reputation (48%) and the increased threat of persistent hacking at (44%).

The top three respondent concerns reflect the overall interconnectivity of this type of exposure. The overall safety of client or customer data or information, coupled with the impact on reputation and the constant hacking atmosphere, supports these top three feared risks.

WHAT IS PREVENTING COMPANIES FROM BEING BETTER PREPARED?Lack of preparation

The barometer found that 73% of those surveyed listed underestimating the impact that a business may encounter from a cyber attack as the reason companies are not better prepared. Knowledge silos and the overall difficulty of identifying threat scenarios are the main reasons.

Clearly, cyber is not an IT issue alone. Involving a think-tank approach across all departments within an organization is required.

By involving other areas of the organization, a more realistic evaluation of the potential threat scenarios and the potential bottom-line impact will provide more robust data on which to make risk management decisions.

Budgetary restraints

Since the overall potential impact from a cyber attack is underestimated, it is no surprise that 59% of barometer respondents reported feeling that budgetary restraints were a reason for businesses not being better prepared for a cyber event. Only 54% of the respondents responded that they felt they had not even analyzed the problem.

Global economy, company mergers, legacy IT systems and the technology development explosion can make potential expenses seem daunting.

An atmosphere where companies are underestimating the risk, budget constraints, and inadequate analysis, will lead to a potential issue.

But applying a think-tank approach can prioritize impact scenarios, bring the potential costs of solutions to the surface and help focus analysis on the most critical areas. This type of approach will provide better C-Suite data for budget development.

HOW CAN COMPANIES PROTECT THEMSELVES?

Improved hardware and software solutions, including monitoring tools, were voiced by 75% of respondents, and outlining better processes and access schemes were listed by 62%. Interestingly, only 56% of respondents said they felt that raising employee awareness was a critical prevention measure.

That said, IT security should be a concern of every employee. The human factor in this type of exposure should not be underestimated. Employees can cause large IT security or loss of privacy events, inadvertently or deliberately.

Even with improvements in the top three exposure areas listed above, this will not guarantee 100% IT security.

BETTER UNDERSTANDING OF CYBER RISK OPTIONS?Supporting full operational analysis

The aforementioned think-tank approach involving a full operational analysis - which includes IT, but is supported by all stakeholders - is required. The sharing of knowledge and information, where IT experts can identify the scenarios, but other business partners can quantify duration and cost, is necessary.

This method will assure proper C-Suite level decisions around aspects of avoidance, acceptance, control or transfer as it relates to cyber risk exposures. Avoidance, acceptance and control, for the most part, will involve internal avenues of solutions. The decision to transfer the risk seems to be an area on which both insurers and brokers could focus more attention.

Promoting enhanced awareness

The ability to make proper decisions involving the transfer of risk seems to be a grey area with risk managers. There is a significant amount of awareness surrounding cyber insurance in general, but many risk managers still do not have a good grasp on what exactly it is or does.

A company may develop a solution, which involves transfer of part or all of the cyber risk exposure to a carrier or other external option. If this is the case, there appears to be a lack of understanding about how the coverage responds if an event was to occur.

There is a need in the marketplace for education of both brokers and clients. Brokers have advised carriers that clients are constantly asking about cyber insurance, but many brokers admit they are not sufficiently well-versed to be able to effectively sell the product.

Almost all carriers in Canada have a cyber product at this point. But there is currently no standardization of wording so it can be difficult when comparing different product offerings.