CANADIAN UNDERWRITER.ca

Canada's Insurance and Risk Magazine

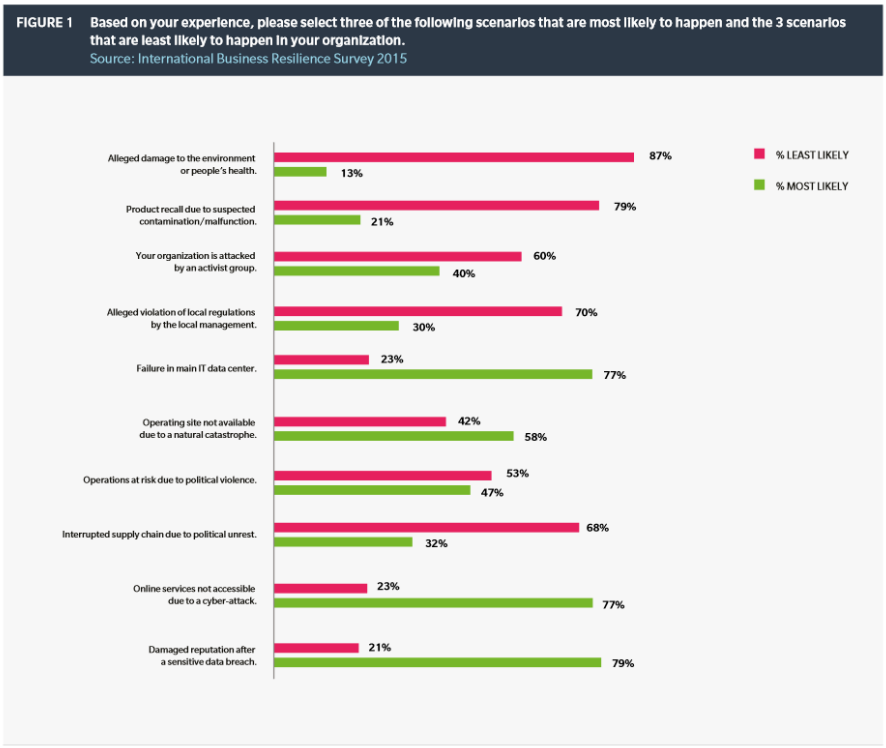
DAILY NEWS Oct 8, 2015 11:12 AM - 0 comments

Cyber, reputation risks remain top concerns: Marsh/DRII

2015-10-08

CEOs are overestimating their business' insurance coverage for both most likely and high-impact risks, which a survey released this week by Marsh and Disaster Recovery Institute International (DRII) indicates are cyber and reputational.

Of the almost 200 polled C-suite executives, risk professionals and business continuity managers from large and medium-sized corporations around the globe, respondents report they consider cyber and IT-related risks to be the most likely to occur and have the greatest potential impact on their operations, notes the ***2015 International Business Resiliency Survey***. *[click image below to enlarge]*



Among 10 suggested risk scenarios, **Marsh UK** reports in a statement, the results indicate the top risks in terms of impact and likelihood are as follows:

• reputational damage from a sensitive data breach – impact is 79%, while likelihood is 79%;

• failure in a main IT data centre – impact is 59%, while likelihood is 77%; and

• online services being unavailable as a result of a cyber attack – impact is 58%, while likelihood is 77%.

The apparent false sense of security around being adequately covered for the most likely and impactful risks faced by their organizations is worrisome.

“Some in the C-suite take it for granted that their organizations have specific insurance cover for cyber and IT-related risks. On the contrary, despite an increase in the take-up of new specific cyber policies globally, overall penetration remains low,” the report states.

“Organizations should perform periodic assessments of all operational risk scenarios that could affect their resilience in order to prioritize risk mitigation actions in accordance with their potential business impacts,” Marsh recommends.

Also of concern is the divide in views between CEOs and risk managers. Of the CEOs polled, 28% report they have dedicated insurance coverage against cyber attacks and 21% say they have dedicated insurance protection for reputation damage after a data breach, Marsh reports. That compares to just 6% of surveyed risk managers reporting they have dedicated coverage for these risks.

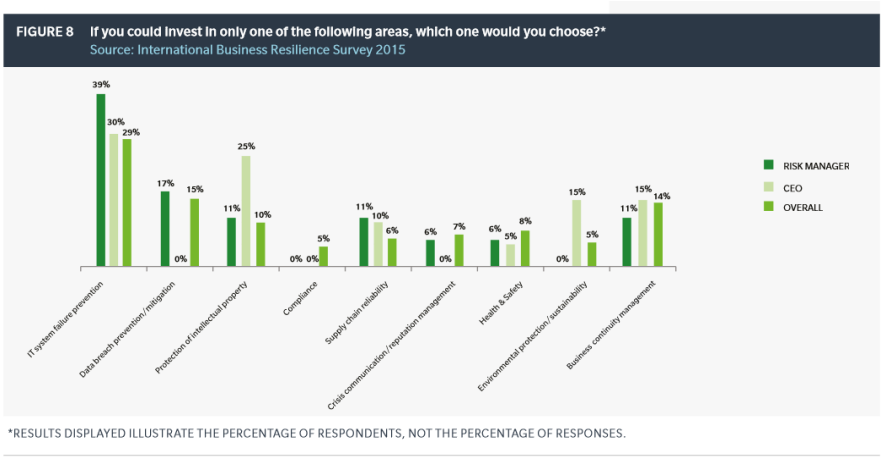
Notes the report, “For cyber risks in particular, the level of insurance take-up appears low when compared with the criticality with which the risk is viewed.”

With regard to what situations could have the greatest impact on their organizations’ reputation, about three-quarters of respondents point to the failure of the IT system and the lack of crisis management planning.

David Batchelor, president of Marsh’s International Division, suggests that with product innovations in speciality insurance, “this a good time for organizations to revisit their coverage to make sure that it is properly nuanced to meet the unique needs of their industry and the corporation’s business goals.”

In terms of investments, CEOs and risk managers were not divided.

In all, the report states that 66% of respondents believe they are currently investing enough in IT, or plan to increase investment in the next three years. Just 18% say they are not currently investing enough. [*click image below to enlarge]*



“Perhaps even more interesting is the finding that 29% of respondents would chose to invest in IT system failure prevention if they could only invest in one particular area – nearly twice as much as the second-highest choice, which is ‘data breach prevention/mitigation’,” the report adds.

Both CEOs and risk managers identified IT system failure prevention (29%) as the most important area in which to invest, while CEOs also highlight intellectual property protection (25%). Still, Marsh reports CEOs placed far less importance on the resiliency of IT systems (60%) in relation to reputation management.

Survey results also show a divide between traditional and non-traditional risks. With regard to preparedness, the majority of polled organizations believe they are better positioned to deal with traditional than non-traditional risks. More specifically, respondents rate their organizations’ level of resilience to be high for natural catastrophes and IT system failure (40% and 44%, respectively), but low for political violence and an activist group attack on social media (both at 32%).

The divide continues with respect to the views of CEOs and risk managers, with the two groups having “different perceptions about the severity and control measures in place for various risks facing their organizations.”

The report recommends that organizations “review existing business continuity and crisis management frameworks to ensure they are properly addressing emerging, as well as traditional, risks. Those companies that haven’t already should undertake a comprehensive review of their cyber exposures to ensure that resilience is built into those areas that need it most. In addition, firms should review the dependencies of critical services and processes from internal and third-party information systems and IT technologies.”

The risks with the lowest potential impact originate from a product recall event, Marsh points out, adding that respondents report impact is 15% while likelihood is 21%

The risks with the lowest potential impact originate from a product recall event, Marsh points out, adding that respondents report impact is 15% while likelihood is 21%.

Adds the report, “when asked about events they consider least likely to happen, there is a disconnect between risk managers, who mention violation of local regulations, and CEOs, who say it is the one of the risks that is most likely to happen.”

The report points to the importance of IT system resiliency in meeting business goals. “It is interesting to note that CEOs place less importance on the resiliency of IT systems in relation to reputation management, while giving greater attention to crisis management planning,” the report states. “Firms should consider including a comprehensive review of the dependencies of critical IT services and processes in their crisis management plans, and the results of this should be relayed to the C-suite,” it notes.

Related Topics

Legal
Risk Management/Commercial

Monitor These Topics

- Legal
- Risk Management/Commercial

Disclaimer

Note: By submitting your comments you acknowledge that Canadian Underwriter has the right to reproduce, broadcast and publicize those comments or any part thereof in any manner whatsoever. Please note that due to the volume of e-mails we receive, not all comments will be published and those that are published will not be edited. However, all will be carefully read, considered and appreciated.