captive.com
The Business to Business Risk & Insurance Exchange

Captive Resource Center

Ask the Expert Forum
Ask the Expert FAQ
Captive Basics
Captive Daily Wire™
Learning Center
Templates and Tools
Pulse Surveys
Captive.com Store

Businesses and Associations

Links to Member Websites
Captive Yellow Pages
Captive Associations
Group & Rental Captives

Research & Information

News/Library
Domicile Showcases
Conference Calendar
Employment Opportunities
Website FAQ
Tips & Tricks

A.M. BEST RATINGS
find Insurance company ratings
Enter Company:
Advanced Search Options
GO

Membership Info
Credit Card Authorization
Captive.com, llc
Register for Site Updates
E-mail captive.com

Back to Document List

LexisNexis

Copyright 2014 Economist.com
All Rights Reserved

CFO.com

June 24, 2014 Tuesday 02:24 PM GMT

ACCOUNTING & TAX

767 words

How **Captives** Can Cut Supply-Chain, Cyber **Insurance** Costs

Jeffrey C. Joy

With premiums rising for cyber **insurance** and supply-chain coverage, CFOs and risk managers can curb the expense by self-insuring.

CFOs of corporations that have already set up **captive insurance** companies or are thinking about setting one up should ponder the benefits of self-insuring cyber perils and supply-chain business-interruption (BI) risks via a **captive** to supplement commercial **insurance** coverage.

Indeed, the financial risks to companies from cyber attacks are increasing at an alarming rate, according to recent research by McKinsey & Co. Similarly, many smaller companies may not have adequate contingent coverage.

Adding comprehensive or supplemental cyber risk and BI coverage through a **captive** should be considered an important contingent component to any company's strategic risk management plan. These risks are real for most companies, and the potential damages to a company's revenues and profits can be significant.

A cost-effective strategy can blend organizational risk management with an **insurance** program that includes **captive** coverages. Indeed, **captive**-**insurance** policies can be specifically crafted to cover a company's highly individualized risk. That's an advantage in the case of cyber and business-interruption losses, which manifest themselves differently in every company. For example, one company's costs relative to a data breach might include exorbitant notification expenses under state and federal law and high monitoring costs. Another company might absorb significant expense in recovering stolen or compromised data, but less on the notification and monitoring side.

At the same time, the commercial **insurance** market isn't entirely suited to writing risk in a highly specific, individually tailored fashion. Commercial insurers prefer to broadly standardize coverage, tending to underwrite in a way in which one size can fit all of a diverse insured population. That's been particularly true in the case of commercial general liability (CGL) coverage, a broad type of **insurance** written on a standardized form, and it's starting to be true of cyber coverage as well. Indeed, commercial cyber-**insurance** policies are also starting to look alike standardized.

Moreover, supply-chain and cyber **insurance** policies routinely exclude certain coverage. Commercial supply-chain **insurance**, for instance, may be limited to coverage of a company's loss of income and ongoing expenses as a result of physical damage to an insured's plant, building or other facility. Further, a rider may not be available to extend such coverage to losses stemming from damage to the premises of a supplier, or the rider may cost too much. In such cases, a supplemental policy written via a **captive** to cover these additional

http://www.captive.com/...ction=UserDisplayFullDocument&orgId=665&docId=l:2151405468&topicId=100021625&start=1&topics=single[6/25/2014 2:04:11 PM]

risks can be an effective risk management solution.

Similarly, if supply-chain **insurance** has geographic limits that exclude the part of the world in which a company's suppliers are based, a supplemental policy written by a **captive** can cover such risks.

Cost-Cutting Steps

To be sure, commercial carriers are offering cyber-**insurance** policies that cover first-party and third-party claims. First- party coverage typically includes losses to an insured's computer data or other harm to the company's business resulting from a cyber attack or data breach. Third-party coverage, which insures against claims brought by customers or clients that suffered losses as a result of the cyber attack on the insured company, typically pays for the costs of lawsuits.

But premiums for both supply-chain-interruption **insurance** and cyber-risk coverage are increasing annually. With that in mind, CFOs and risk managers at smaller companies could help their employers achieve significant premium savings by taking the following steps:

1. Increase the company's deductible on commercial coverage for those risks - boosting them, for example, from $50,000 to $250,000 on a policy with an overall coverage limit of $2 million.

2. Self-insure the $250,000 deductible, as well as the excess risk from $2 million to $5 million, through a **captive**.

3. Alternatively, all or a portion of the coverage over $2 million could be **reinsured** with a commercial carrier to reduce the potential loss to the **captive's** reserve account.

In the current environment, combining commercial cyber-risk and supply-chain-BI **insurance** with coverage written through a **captive** can provide businesses with more comprehensive and cost-effective coverage of these risks.

Jeffrey C. Joy is a tax attorney and Shareholder in the Orange County office of international law firm Greenberg Traurig LLP.

http://www3.cfo.com/Image

June 24, 2014

Back to Document List

Copyright © 2014 LexisNexis, a division of Reed Elsevier Inc. All Rights Reserved.
Terms and Conditions Privacy Policy

captive.com