2014 Willis Global Client Advisory Council Face-to-Face Meeting
August 13-15, Boston, MA

Breakout: You’ll Never Get Board Talking About Cyber!

*Cyber Risk Discussions in the Board Room*

Host(s): Tom Srail, Senior VP – Technology, Media and Telecommunications Industry Leader, Willis North America

Description: Regulators and boards are increasingly interested in discussing cyber risks. In this breakout, we will have an open dialogue around how GCAC members are having conversations with their leadership, what kinds of questions boards are asking and how they believe Willis could help enable their discussions. We will also solicit feedback on some tools Willis has developed to help facilitate board discussions.

Location: Oriental Ballroom, Arcade Level

Attendees: Avitabile, Anthony (Major League Baseball)
Carter, John (Time Warner)
Cooney, Brian (Barriere Construction Co. LLC)
Edelstein, Howard (Sealed Air Corporation)
Hangarter, Franc (American Airlines)
Jackson, Shaun (El Pollo Loco Inc.)
Loverich, Kim (Fidelity National Financial Inc.)
Natovitz, Shari (Silverstein Properties Inc.)
Sallade, John (County Commissioners Association of Pennsylvania)
Seiter, Aaron (PNC Financial Services)
Spezia, Tony (Covenant Health)
Vryhof, Bob (Republic Services)

Fidlow, Ben (Willis)
LaSala, Christine (Willis)
McCarthy, Colleen (Willis)
Whitehouse, Andy (Willis)

Pre-Read: *That’s the Board and They’re Asking About Cyber Risk* (WillisWire Blog Post) by Tom Srail
That’s the Board and They’re Asking About Cyber Risk

by Tom Srail

I recently penned (and filmed) a piece for the Willis monthly newsletter, Insights, and thought WillisWire followers might want to see it. Here you go.

The call, the email, the IM—it’s coming, if it hasn’t arrived already. It’s from someone on your board or your senior management team who has realized that they don’t know the answers to key questions about your organization’s cyber exposure.

The first questions are usually the obvious ones: What is the extent of our exposure and what is the extent of our protection in case of a cyber breach.

The next question, however, is often the most challenging one from a risk management perspective: Why did we make the choices we made about this risk and our insurance protection for it? Before we get to the why, let’s look a little more closely at the what.

What is the Extent of our Exposure?

The extent of cyber risk depends on several factors, primarily the type of cyber activity your company conducts and the type of data you collect. Simply put, the more sensitive the data you collect, the greater your risk.

What Business You’re in

It’s clear from recent headlines that retail companies are targets because of both the volume and sensitivity of the data they collect: when you conduct business chiefly through credit/debit card systems, your lifeline involves the use of your customers’ highly sensitive financial information. (For more on the risk retailers face at the hands of cyber criminals, see my recent post.)

Health companies are also especially at risk due to the sensitivity of the protected health information they gather and often store in the era of the electronic medical record.

Vendors

The extent of risk also depends on vendor relationships. Vendors are increasingly linking their systems to their clients’ systems in order to provide direct and seamless service. This has proven, quite publicly in a recent case, to present a potential access point to those clients’ sensitive data.

Supply Chain

Another cyber risk associated with vendors is through the supply chain. Should a cyber breach bring down one of your key suppliers, you could be severely impacted. We have seen recent indications that many companies may be underestimating their cyber risk in general, and in particular the risk posed by vendor...
relationships.

Other factors include, of course, the public relations damage that a breach can cause and the liability exposures that can ensue.

**What is the Extent of our Protection?**

Now to the second question. On the face of it, this is a simpler question to answer. You’re either covered by cyber insurance or a self-insurance arrangement such as a captive, or you’re not. As any organization hit with a cyber loss before the advent of cyber insurance knows, basic P&C policies do not cover cyber losses. But even if your answer is yes, you’ll need to be ready for the next question.

**Why Did we Make the Choices we Made About Cyber Risk?**

The best way to answer this question, which gets to the heart of the matter for risk management professionals, is with numbers. Whether you’re self-insured or covered under a cyber policy, a solid analysis of the financial risk posed by your cyber exposures is the only convincing way to justify your choices. Fortunately, tools are now available in the cyber insurance world that can produce these numbers for you.

The loss modeling tools for cyber risk take a close look at what type of data and how much data you store. They consider the loss data for your industry and your organization’s specific cyber and data profile. They also consider the nature of the exposure.

Large retailers may be obvious targets of cyber criminals, but the security systems in place and the sheer number of people involved mean that a breach is likely to be discovered quickly, allowing banks to cut the credit pipeline and cap the immediate damage. This is a limiting factor on the exposure.

The ensuing damage—the cost of notifying customers of a breach, the liability law suits, potential fines, loss of market share and good will, etc., must also be tallied in arriving at an accurate assessment of maximum probable loss (MPL). With your MPL, you and your risk management team can devise an appropriate risk transfer strategy, pick your limits and be as sure as you can be that you are not underbuying or overbuying insurance.

**What are our Peers Doing About Cyber Risk?**

The board and senior management are also asking an additional question: What are our peers doing? The answer to that question varies by industry.

- In the brick and mortar world of manufacturing, penetration of cyber insurance is in the range of 5%.
- For the health care, technology and retail sectors, the number is closer to 50%.
- For managed care companies, whose business is built primarily on the collection and analysis of personal health data, the figure is in the 80% range.

Many cyber experts believe that the day is approaching when cyber insurance will be as standard as property, casualty, and directors & officers cover. It’s hard to argue, as our dependence on computers and the cyber landscape appears to only grow.

Our need to answer to our top leadership regarding the steps we’re taking to manage the risks that come with that dependence appears to only grow as well.