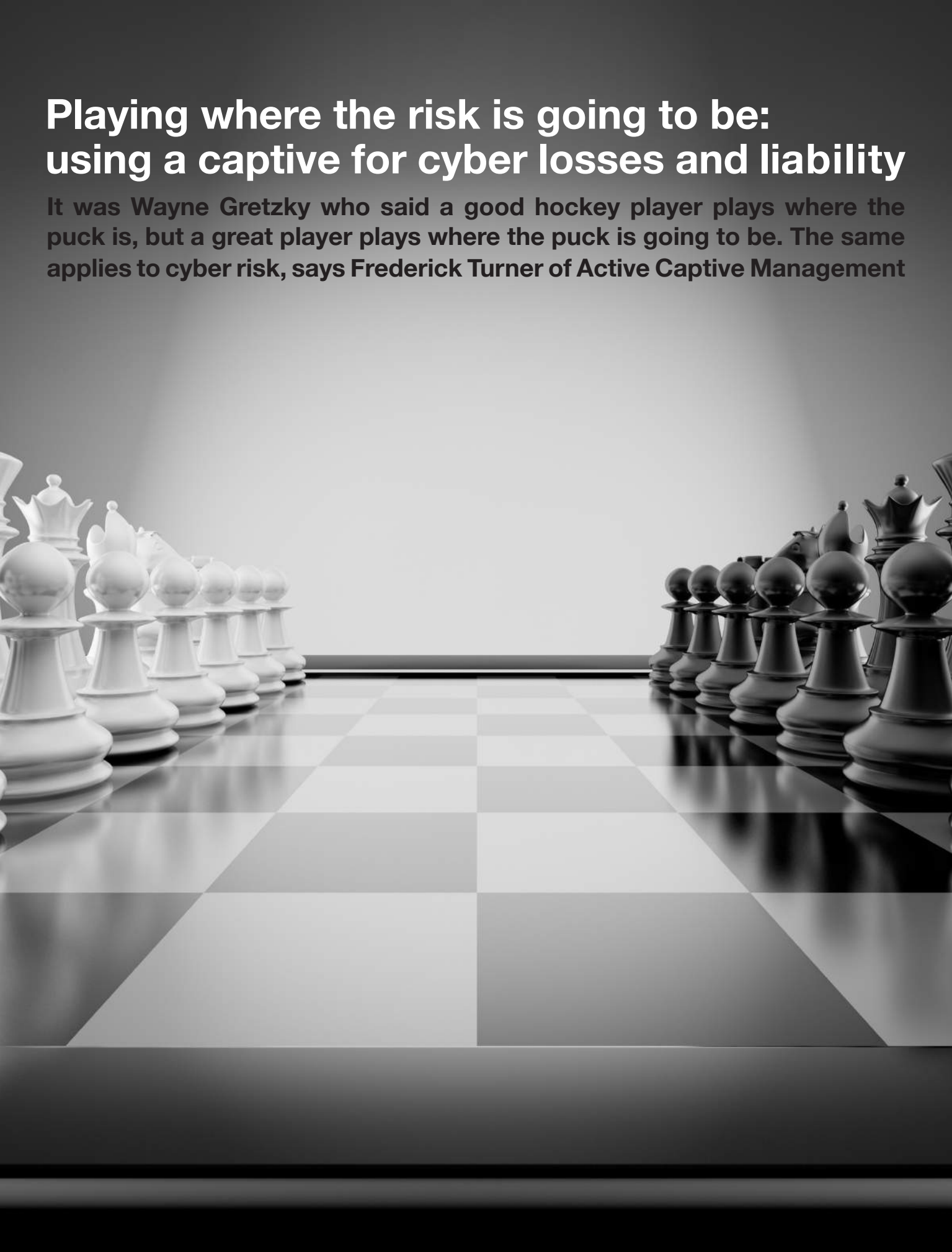
Playing where the risk is going to be: using a captive for cyber losses and liability

It was Wayne Gretzky who said a good hockey player plays where the puck is, but a great player plays where the puck is going to be. The same applies to cyber risk, says Frederick Turner of Active Captive Management



It seems like everywhere you look these days—on the news, in articles, on social media, in blogs and in insurance newsletters—there is something written or said about cyber risk and the serious danger that it poses to just about every business, to governmental or company infrastructure, and to both local and world economies. In today's internet savvy and cyber connected world, cyber risk and liability issues loom large and are increasingly prevalent. It's safe to say that of all the many contingencies a company should plan and prepare for, cyber concerns are currently one of the most important issues for any company's management to address.

But understanding cyber risk can be overwhelming as the variety and type of risk classified as 'cyber' in nature is in itself varied, and sometimes obscure. Threats or loss caused by hackers, cyber thieves, competitors or employees misusing, misappropriating, losing or improperly disclosing data or confidential information are just some of the risks companies face.

Expenses associated with cyber-related class actions or other lawsuits, business interruption or data restoration, or regulatory compliance costs in the form of notification and credit monitoring expense, can result in losses valued in the millions. In fact, the financial impact of a cyber breach can be significant. Per a 2013 study conducted by the Ponemon Institute, the average cost per record for a data breach is $188—this study does not include the cost of outside counsel or settlement payments if the breach event winds up being litigated.

Yet, no matter the monetary size of the cyber loss, a cyber claim can have many direct points of impact—on the company financials, intellectual property rights, the day-to-day operation of the company, insurance and risk management, and even customer or third-party confidence in the company and the services it provides. Proactively defining a company's cyber risk as part of a corporate risk management function, where the end result is a cyber loss prevention and safety/mitigation plan, which includes insurance, could markedly reduce the average cost to the company when a cyber breach or loss occurs.

There are many commercial insurance policies on the market nowadays covering cyber risk. But those policies can be less than perfect. So perfect risk management protection against cyber risk has to involve more than just commercial market insurance. In fact, it's often the case that companies should consider alternative risk management in the form of having a captive insure cyber risk.

The way to be a great risk manager when it comes to protection against cyber loss is to have a triangulated risk management programme where the three points of the triangle are: (i) cyber risk management in place at the corporate/company level; (ii) cyber insurance from the commercial market where it's cost effective to bind such coverage and where such coverage exists and fits the risk; and (iii) captive insurance rounding out the insurance programme or replacing the commercial insurance entirely if the commercial market doesn't have the appetite for the risk, isn't appropriately or fully covering it, or where commercial prices are cost prohibitive.

An internal cyber risk management plan

Company management needs to assume responsibility for monitoring the company's points of vulnerability or attack relative to cyber risk. For example, management needs to understand the financial risk to the business if there is a breach of security and data is lost or compromised. A business generally needs to understand the type of information and data it controls and maintains, how valuable it is to the performance and ability of the company to conduct its business, and whether and how the company can absorb costs to cure or correct any data or information breach or loss. This means that company management needs to be proactive in confirming that steps are being taken to identify, prevent, and mitigate against cyber related risk and losses.

Management needs to be committed to understanding all laws and regulation applicable to the company relative to cyber privacy and security and/or data exposures. It also needs to routinely and continually pose questions to senior executives and key decision makers to determine and address the company's preparedness for cyber loss and continue to monitor cyber risk management protocol on a going-forward basis. And management needs to generally understand how the company is insured (or not) for cyber exposures.

Prior to developing any actual cyber risk plan, company management should seek to foster a proactive corporate culture where cyber risk is studied, monitored and understood. This includes a heightened awareness of security risks from senior management through the to the lowliest employee levels and encouraging the timely and accurate reporting of security breaches. The only way for mitigation to work in the event of a cyber breach or loss is for crisis management to begin within hours, rather than days.

This cannot happen unless there is a mitigation plan in place before any such breach occurs. Some oversee cyber risks through the function of the IT committee, whereas others use the audit committee.

Every company today should think about cyber and should understand its risk and how to prevent against it. Just recognising that there is indeed a risk is the first step, then both internal and external resources can be used to develop a comprehensive risk management and response plan. So, what would external resources be? A key resource is insurance coverage.

A solid insurance programme includes captives

Company management also needs to know the extent of a company's insurance relative to cyber risk and loss. This can be easier said than done. Commercial market coverage for cyber risk has been around since the early 1990s, but even today—years in the making—commercial forms can be hit or miss in terms of what is intended to be and then actually covered. Standard ISO-form commercial general liability coverage is not really designed to cover cyber risk and all its iterations, and nowadays these policies typically exclude cyber claims and losses. Many commercial carriers are now writing cyber coverage on very specific and tailored forms, but even then, such forms are still evolving as the risk continues to evolve, with no standard language and generally, no one form that covers all angles of the risk.

One recent example out of an Illinois Appellate Court holds that the claim was excluded under a professional liability policy that offered coverage under a cyber endorsement. The claim involved coverage for costs and fees associated with a class action lawsuit alleging damages due to unsolicited text messages sent to various cell phone customers for discounted medical procedures (Doctors Direct Insurance v David Bochenek, No 1-14-2919, 3 August 2015). In this case, the court held that the policy's US Telephone Consumer Protection Act exclusion applied to the cyber portion of the coverage even though the class action claim clearly fell within the policy's definition of "privacy wrongful act". This can be typical, where exclusions really can be quite extensive and can dramatically narrow the coverage. With commercial cyber, policyholders can pay hefty premiums for what is really pretty thin coverage.

Moreover, commercial market underwriting can often be overwhelming and time consuming for cyber lines. The process can be extensive where insured companies have to 'prove' to the commercial underwriter that they have a risk management plan in place, and in the event that such plan is not in place and coverage is written, this could result in a coverage denial.

Recently, the US Court of Appeals for the Third Circuit ruled in favour of the Federal Trade Commission (FTC v Wyndham Worldwide Corp, No 14-3514, 24 August 2015). The court held that Wyndham's published privacy policy governing how the company safeguarded personal and confidential information must match its actual practices. When the written policy was proven to be a "paper tiger" in that it did not match what was actually happening at the company to protect data and confidential information, the court held Wyndham liable for losses and damages associated with the data breach,. The court found it unfair of Wyndam to have advertised privacy practices in order to attract customers only to fail to actually uphold these practices. Had Wyndham had commercial cyber coverage, its failure to uphold written policies on privacy protection could also have resulted in a denial of any claim made to the commercial carrier, if the privacy practices were disclosed to the carrier as part of underwriting and if they were a condition precedent to coverage.

> "Businesses should work with commercial brokers to define and negotiate commercial coverage as a starting point and then could look to a captive to write cyber coverage to fill in gaps in the commercial market policy"

What all this largely means is that even those companies that seek to purchase commercial market cyber coverage, and in the end do obtain some form of commercial cyber line, are likely still self-insuring much of this kind of risk. Of course, businesses should work with commercial brokers to define and negotiate commercial coverage as a starting point and then could look to a captive to write cyber coverage to fill in gaps in the commercial market policy, covering what cannot be obtained from that market or what is excluded under the commercial lines, or even covering an excess layer. In the world of cyber, being able to write high limits excess to a first dollar defending commercial primary could be a nice idea, enabling the insured to have higher limits for a cyber loss at a lower cost and transfer the risk to both a commercial carrier and a captive programme.

A captive could also write the cyber coverage on either a third- or a first-party basis and could create a highly tailored policy that perfectly fits the company's risk, which is different than what the commercial market would be able to do and is key to this line of cover because the risk itself can be so individualised.

Further, in the captive world, arms-length premium pricing models need only contemplate the risk of the entities inside the corporate 'family tree'—this can make the coverage generally far more cost effective, even for those members of the family that have the greater risk. Whereas in the commercial world, many forms of cyber coverage are just expensive, perhaps cost prohibitively so, especially when you consider how many lines an insured might be required to purchase out of the commercial market to satisfy outside parties that require rated, commercial carriers.

So, if the insured has to carry a heavy programme load of rated general liability or other lines, there might not be much room in the budget to pay for an expensive cyber line on top of that, even if such a line is needed. A captive could literally come to the rescue in that situation, enabling the insured to have it all, relative to insurance coverage, and build out a complete coverage programme utilising both commercial and captive insurance.

Where's the risk going to be?

Managing cyber risk means that a company implements cyber best practices that start with company management and an overall awareness of the risk itself, then the company can and should develop a contingency and response plan in the event of a cyber incident.

Risk management should also ensure that the company has a thorough insurance programme in place as protection against fortuitous or unplanned cyber loss. Even the best laid cyber risk mitigation or management plans can nevertheless result in loss, liability or damage.

Being a good cyber risk manager involves good contingency planning. Being a great cyber risk manager involves insurance as part of that contingency planning where the programme includes not just commercial insurance, but also captive insurance rounding out the programme and filling in coverage for those troublesome areas of risk where the commercial market cannot suffice to cover (or affordably cover) all angles of the risk.

Play your insurance where the risk is going to be—plan ahead. With cyber, planning ahead is everything. **CIT**

Frederick Turner
Founder
Active Captive Management