Cyber 101: Protecting Your Business From Cyber Threats with Captive Insurance

By Christopher Gallo, Managing Director, and Dick Boccaccio, Insurance Consultant, CIC Services

When hackers breached the computer networks of Flagstar Bank, one of the largest financial providers in the United States, the attack compromised the data of 1.5 million customers in June of 2022. Financial companies are often the target of massive data breaches. In two of the largest attacks involving financial institutions, JP Morgan had more than 90 of its servers infiltrated to steal financial information and Capital One had a server accessed with 100 million credit card applications stolen. Financial organizations continue to make the list of "most hacked" and are disproportionally targeted. Hackers love stealing data—and the sensitive data from financial organizations is especially profitable. It can be sold to other criminals on the dark web, or it can be used to target phishing attacks or extortion.

A data breach is harmful for businesses: Not only is there reputation damage and negative P.R. associated with data breaches such as these, that involve personal and sensitive information, but it's costly. According to the *Ponemon Institute's* Cost of a Data Breach Report, the average cost in 2020 was $3.86 million.

The risk of cyber-crime has escalated across industries and the globe. In 2022, industries including retail, finance, technology, legal services, property and real estate, higher education, manufacturing, and more, have all seen increases. The FBI reported that there was a 300% increase in cybercrime reports since the COVID-19 pandemic and this is only expected to rise. In fact, **cybercrime is the biggest threat facing most businesses today**, according to PwC's Global Economic Crime and Fraud Survey 2022.

Why Protecting Against Cyber Crime is Challenging

Many businesses are not fully prepared for cyber risks. The Hiscox Cyber-readiness Report found that 73% of companies are unprepared—despite the same report finding that 53% of companies experienced a cyberattack in the last year and 27% experienced four or more attacks. If this threat is so prevalent, why are so many businesses unprepared? The nature of this threat is ever-evolving and complex, and risks of this nature are difficult to mitigate and protect against: As technology advances, cloud computing grows, social media continues its advance and cyber criminals become more sophisticated, the complexity is only more enhanced. While businesses can (and should) instill proper processes and training to safeguard against cyberattacks, the alternative risk transfer marketing offers a solution with captive insurance.

Why Captive Insurance Companies are Ideal Vehicles to Address Cyber Liability

1. Captive insurance provides necessary flexibility for an evolving threat

Data breaches are generally not covered by commercial general liability policies. A general liability policy covers bodily injuries and property damage resulting from a business's products, services, or operations. Also, sometimes the nature of a cybercrime is so new or unusual that even if it's not a data breach, it's not covered. Because cyber threats are relatively new and ever-changing, it can be difficult for a third-party commercial insurance company to keep up. Since captive insurance companies can issue customized, more flexible coverage to their parent companies, they can serve as an ideal insurance solution for cyber risk. Furthermore, a captive's flexibility also enables the parent company to maintain third party commercial cyber insurance and supplement third party coverage with a broad insurance policy from the captive to address gaps and secondary losses caused by a cyber incident. For example, a captive can protect against these secondary losses, according to a report by Aeon:

- Future lost revenue
- Dependent system failure business interruption
- Physical damage or bodily injury resulting from cyber peril (excess/DIC above other applicable insurance)
- First-party loss of inventory due to technology failure
- Loss of value of intangible assets

2. Captive insurance can fill gaps in a commercial policy

Due to recent cyber rate increases, securing cyber insurance can be costly with high premium rates and it typically has more stringent underwriting criteria. Also, the commercial cyber insurance market has an inconsistent approach to capturing and analyzing data which creates gaps in the coverage. Common gaps could include a lack of proper asset inventory, weak identity and access management and a lack of segmentation. One common gap is that cyber risk may not cover a data breach resulting from human error.

3. Captive insurance enables a business to maintain solid footing following an attack

Between lost work, lost revenue and potential ransoms, cyberattacks create an impact. But cyber threats also have a spill-over effect, setting off a chain of secondary losses. For example, a data breach can incur liability costs and it negatively impacts customer trust. With a captive insurance company, the premiums paid (minus claims) are profit. It's difficult to get excited about purchasing additional insurance. For many businesses, insurance is a necessary evil…it is definitely a necessity but can also be viewed as a sunk cost. Owning a captive insurance company gives a business an additional tool to address "non-traditional" but very real risks like a cyber attack. Thus, a business can purchase cyber insurance from its captive insurance company and simultaneously grow profit in its captive insurance company when claims are low.

In summary, the threat of cyberattacks is only going to escalate, as data has shown, and become increasingly more costly to businesses. Although a cybersecurity plan and processes are critical, cyber criminals are incredibly advanced and even the best laid plans won't prevent an attack. When it happens, insurance is the key to recovery. Businesses that have third party cyber insurance in place should consider supplementing their cyber insurance with a blanket cyber policy in a captive insurance company.