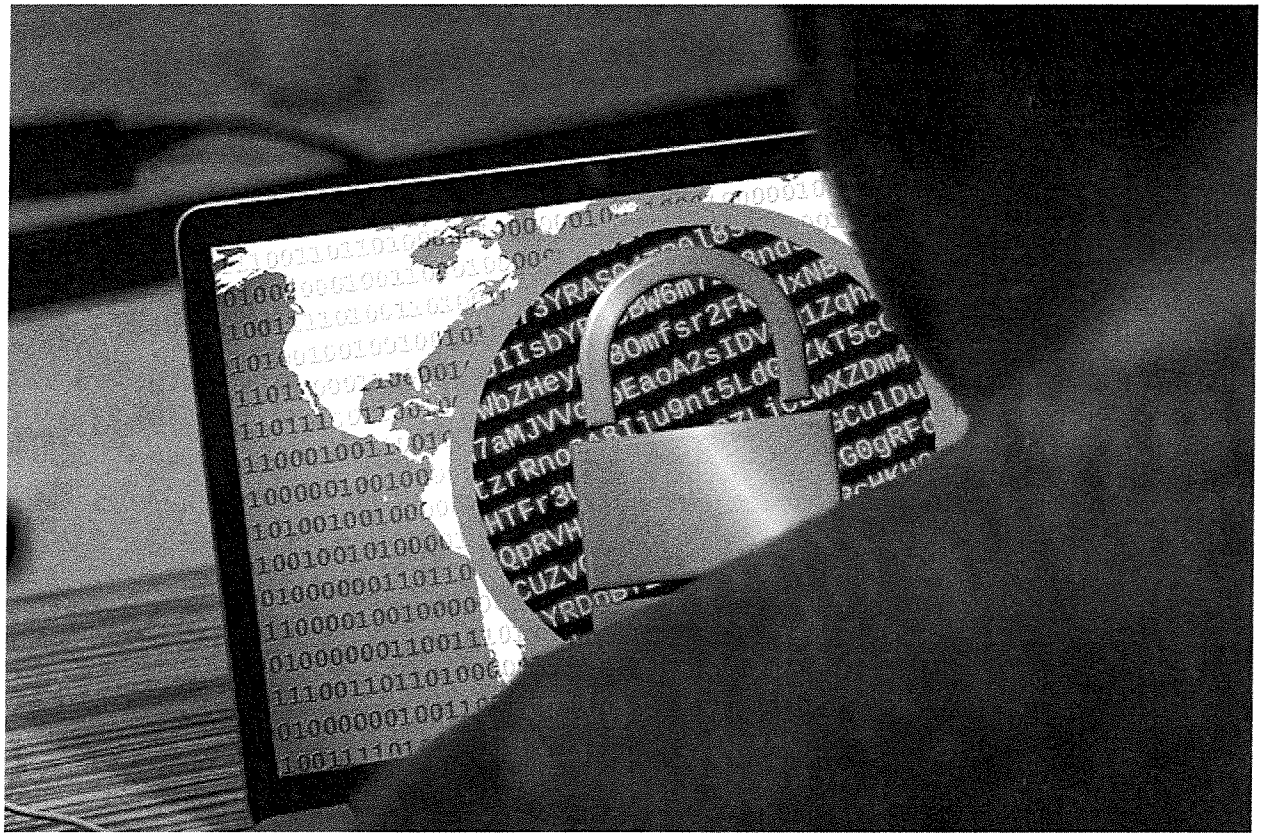
CAPTIVE INTERNATIONAL

Why captives can shine through on cyber

22-12-2017



As the threat from cyber crime becomes more complex and the general insurance industry struggles to keep pace, captive insurers can come into their own, writes Matthew Queen, general counsel and chief compliance officer, Venture Captive Management.

A 12-year-old with a $300 laptop can bankrupt your business. Cybersecurity is the most talked about risk management challenge because it is now a simple matter to shut down the majority of small to medium sized businesses in the US. Thanks to Shadow Brokers, a hacking group specialising in attacking the National Security Agency (NSA), hackers across the world now possess weapons-grade hacking tools.

Shadow Brokers has leaked a Windows hacking tool stolen from the NSA. Called Unitedrake, the implant is a tool designed to enable an attacker to fully take over control of a Windows computer. Shadow Brokers was even helpful enough to include an unencrypted NSA user manual for other hackers to use to assist with wielding the new exploit. This new malware can turn on webcams, microphones, log keystrokes, and access external drives.

Unitedrake was first disclosed in 2014 by Edward Snowden, and was subsequently obtained by hackers. Snowden did not leak the malware. Hackers managed to download the file from the NSA and circulated it on the internet without the US government's knowledge.

Now that the file is out in the open, all the government's tools are available to amateur and professional hackers.

It is not the first time this has occurred. The US government routinely fights 'blackhat' hackers who try to steal various types of software from the NSA, CIA, Department of Defense, and other agencies. Hackers are generally unsuccessful, but it only takes one victory to release a new weapon into the wild.

What is out there in the wild? For the most part, a bunch of amateurs. This is good and bad. On the one hand, it is good that professional hackers are not coordinating massive attacks on private enterprises and dragging the entire economy to a standstill. On the other hand, any idiot with a laptop and access to YouTube can now figure out how to use weapons-grade malware against any business.

Captives to the rescue

Unfortunately, data breaches are generally not covered by commercial general liability policies. And what about breachless cybersecurity claims? For example, hackers have been able to secure unauthorised access to insulin pumps through unencrypted radio frequency communication systems in hospitals. This unusual event may not be covered by a commercial general liability policy—or even some cybersecurity policies.

This is where captive insurance shines. Captive insurance is flexible and the stakeholders can draft their policies so that coverage issues are not a problem. Further, the vast majority of cybersecurity claims will not be for the limits of a policy. Ransomware attacks average around $300 per occurrence, which will definitely not pop a self-insured retention or jeopardise the solvency of the captive.

However, certain malware attacks threaten whether companies can operate as a going concern. This coverage can be custom-tailored to the organisation's unique needs so that insurance proceeds are available to keep a business operating while electronic systems are unavailable. These low-frequency, high-severity events are perfect for a captive insurance solution as these types of claim are relatively rare.

Perhaps the greatest value of the cybersecurity captive is that it guarantees a stream of income in case of a technological failure. As attacks on networks increase in frequency and severity, it is reasonable to assume that some attacks will take days to figure out. Further, the hackers may not simply want a ransom to return your data. Some people just want to watch the world burn.

With a captive in place management has the luxury of assessing the damage, informing key stakeholders of the event (service providers, clients, etc) and put together a plan of action toward recovery. Without a captive, the first question will hinge on whether the commercial insurance policy actually covers the occurrence. Captives allow management to spring into action.

Customised coverage

In addition, captives can write third party risks. Proper risk management should preclude the vast majority of attacks because the insured's system will be resilient. This creates an opportunity to offer customised insurance to third party companies. Key suppliers and clients may be too valuable to lose in the event of a cyber attack. Again, captives provide an opportunity to customise coverage and create a new stream of income for the captive owners.

Before 9/11, nobody seriously considered terrorism a legitimate concern on American soil. Since 9/11, terrorism has been the key focus of domestic security. It should not require a digital 9/11 for companies to invest in their cybersecurity. As noted above, any 12-year-old with a laptop has the resources to hack into almost any small to mid-size company and wreak havoc, so think of what a professional hacker could do.

Given these realities, cybersecurity captive insurance solutions will continue to become an integral part of captive insurance risk management. Captive insurance traditionally thrives where the commercial markets fail the consumers. In the healthcare sector, when professional liability rates rise, doctors frequently create captive insurance companies in response. Accordingly, as hackers innovate new ways of attacking networks, cybersecurity insurance rates will rise as coverage narrows.