The irony of the cybersecurity insurance market

By Advisen on April 18, 2014

The following was written by Robert S. Dowling, director of business development, supporting the Cyber Engineering Division at Dynetics Inc.

Without a doubt, cybersecurity incidents and associated costs are on the rise. In the past, being "hacked" was considered a nuisance that resulted in an annoying email that spread throughout the workplace, cyber-graffiti on a website, a virus that corrupted data, or at worst, a denial of service attack that temporarily halted operations.

Most organizations recovered quickly from these attacks with only minimal costs to recover data and limited impacts to employee productivity. So while cybersecurity insurance products made their entrance into the market place, few organizations saw the value in having cybersecurity insurance.

Today's business climate is much different. Hacking is no longer a weekend hobby, but a sophisticated profession sponsored by well-funded criminal organizations and nation states with a very clear target – personally identifiable information (PII) – the currency of an immense black market. (Rand's recent report *Markets for Cybercrime Tools and Stolen Data* provides an excellent characterization of this market.)

The value of PII and the presumption of its security are raising the stakes for those companies entrusted with its protection. When PII is stolen, a company is immediately liable for a number of direct and indirect costs: customer notification, customer credit monitoring, forensics, mitigation services, reputation management, fines, legal fees and settlements. With regard to settlements, recent court decisions are testing the liability limits for third-party damages for not providing "reasonable" cybersecurity even in the absence of a clear definition of "reasonable." (See *Patco Constr. Co. Inc. v. People's United Bank* and *Lone Star Bank, et. al v. Heartland Payment Systems.*)

Surely the massive breach of retail giant Target will spawn numerous court cases to further define cybersecurity liability.

A recent study by the Ponemon Institute found that in the U.S. in 2012 the average breach compromised 28,765 records at an average cost of $188 per record, with some industries experiencing costs as high as $233 per record; and the result of increasing costs for cybersecurity breaches is a growing interest in cybersecurity insurance.

Cybersecurity insurance premiums have grown from about $200 million in 2002 to over $1.3 billion in 2012 and over $1.6 billion in 2013. Insurance companies are reporting a strong surge in first time inquiries about cybersecurity insurance, and many clients are moving from looking at to buying policies as the near weekly revelations of cybersecurity breaches hit the newswires.

Insurance companies have little difficulty convincing clients that the risk of a cybersecurity breach is too high to be without insurance. But here is the irony: **Insurance companies are taking on significant risks by underwriting policies with little to no assessment of clients' cybersecurity risks.**

In today's cybersecurity insurance market, insurers assess most coverage risks by having clients complete self-assessment questionnaires or by interviewing clients about their IT policies, plans and procedures. As the coverage limits requested by clients increase, some insurers require more thorough risk assessments that can include third party assessments, but these more thorough assessments are less common. One of the main reasons that insurers are willing to underwrite coverage on limited information is that the cybersecurity insurance market is still very much a "buyers market." Between 80 and 90 insurance companies offer cybersecurity coverage and compete for market share with aggressive pricing techniques and a "client-friendly" application process. This coupled with the relatively low number of significant claims creates a comfortable environment to underwrite cyber liability on limited information. The irony, again, is that **insurers are largely unaware of their own risks from the very threat that is driving the growth in their market.**

At a recent cybersecurity insurance conference, insurance company reps and brokers described their processes for evaluating clients and setting premiums for cybersecurity insurance policies, which relied on questionnaires and interviews. At one point, a broker commented that upon learning a client had experienced a cybersecurity breach she would hesitate to underwrite a policy without sufficient evidence the cause of the breach had been mitigated. Interestingly, no "hesitation" was indicated if the client did not report a prior cybersecurity breach. But in 2013, Mandiant reported that "*nearly two-thirds of organizations learn they are breached from an external source*," and "*the typical advanced attack goes unnoticed for nearly eight months*"report may actually indicate a less mature, higher risk cybersecurity culture than one that is actively identifying breaches. **Therefore, the insurer's risk of paying claims is significantly increased by that lack of any real insight into the client's cybersecurity.**

Two scenarios will likely evolve over time:

- Overly aggressive insurers will be exposed and forced out of the market when a widespread cyber attack triggers numerous claims; and
- Insurers that do survive will be forced to limit coverage and raise premiums to account for the unknown risks.

Unfortunately both of these scenarios will develop at a time when more clients will be seeking cybersecurity insurance coverage as the cyber threat becomes more sophisticated and the business impacts become more severe.

To combat these two scenarios and promote a wider adoption of cybersecurity insurance, the insurance industry needs a cost-effective approach to Cybersecurity Risk Assessments (CRAs) – one that actually improves client cybersecurity while at the same time provides insurers a quantitative risk score.

In turn, insurers will be able to issue policies and set premiums based on those risk scores. CRAs then become the catalyst for a continuous cycle of benefits:

- A CRA identifies vulnerabilities and corresponding solutions that enhance cybersecurity;
- Enhanced cybersecurity results in fewer claims;
- Fewer claims allows insurers to offer higher coverage limits and lower premiums;
- Lower premiums increase demand for cybersecurity insurance;
- Cybersecurity insurance requires a CRA.

As mentioned, some insurance companies already recommend or require third-party CRAs as a condition of underwriting cybersecurity insurance policies. These CRAs require more initial investment but produce a win-win scenario for insurers and clients: Insurers pay fewer claims when clients are more secure; clients reduce costs with lower premiums and fewer breaches; and, most importantly, clients are more secure. Therefore, wider adoption of cost-effective CRA's can be the catalyst for a more robust Cybersecurity Insurance Market.