'Heartbleed' Bug Underscores Need for Cyber Risk Insurance

American businesses took a one-two punch in the gut this spring: Investigators discovered a serious vulnerability in a popular cryptographic protocol in very common use by commercial Web developers all over the world. The so-called "Heartbleed Bug" was nestled in the very prominent OpenSSL cryptographic software library, and allowed cyber thieves to steal information that both the Web programmers and the end user/customers thought was protected. The popular website Mashable.com published an extensive list of websites and vendors whose systems may have been compromised by the Heartbleed Bug. If you do business with any company on this list that may have been affected, you may wish to change your password information.

Just a matter of days later, the largest arts and crafts story in America, Michael's, announced that thousands of credit card numbers had been compromised Aaron Brothers, a Michael's subsidiary, was also affected by an attack by highly sophisticated criminals using malware that had not been encountered before by their security consultant firms. Michael's has contained the threat, and the malware is no longer compromising credit card numbers and expiration dates. The attack occurred between May 8, 2013 and January 27, 2014, potentially affecting 2.6 million cards.

Furthermore, Florida officials are now investigating an attack on Hess customers who purchased gas using their credit cards. Criminals installed a number of card skimmers at a number of Hess stations in Florida.

These attacks come on the heels of a massive leak of credit card information at the prominent Target chain of retail stores.

The result isn't just a risk to customers and card-issuing banks. Businesses who take any form of electronic payment must consider themselves at risk of liability arising from the compromise of their electronic payment systems. As we saw from the Heartbleed Bug, even the most sophisticated businesses with large and highly skilled information technology staffs of their own were vulnerable to flaws in the coding far upstream.

Furthermore, as we see in the Hess case, smaller firms can no longer assume they will not be targeted by cyber-thieves. If they can install skimmers on gas pumps and go undetected for months, they can install them almost anywhere. And it may well be the business that winds up holding the bag for liability for damages caused by cyber attacks that they failed to prevent. A recent survey showed that some 72 percent of all cyber breaches occur at small-to-medium sized businesses.

Liability can also come from government sources: The Federal Trade Commission recently filed suit against the Wyndham hotel chain for failing to provide adequate security for customers' private information, after the FTC dealt with the fallout of three separate breaches in just a few years.

Cyber Risk Insurance

Fortunately, it is possible for businesses to purchase protection against this potentially devastating risk, through obtaining cyber risk insurance. This insurance protects the company against catastrophic liability arising from cyber attacks or other information security lapses. Policies are now available from a variety of firms, and are designed to be affordable and realistic even for the smallest businesses that may be affected.

What's covered?

Cyber liability insurance, or cyber risk insurance, is still evolving, but policies could cover one or more of the following risks, according to the National Association of Insurance Commissioners:

- Liability for security or privacy breaches. This would include loss of confidential information by allowing, or failing to prevent, unauthorized access to computer systems.
- The costs associated with a privacy breach, such as consumer notification, customer support and costs of providing credit monitoring services to affected consumers.
- The costs associated with restoring, updating or replacing business assets stored
- electronically.
- Business interruption and extra expense related to a security or privacy breach.
- Liability associated with libel, slander, copyright infringement, product disparagement or reputational damage to others when the allegations involve a business website, social media or print media.
- Expenses related to cyber extortion or cyber terrorism.
- Coverage for expenses related to regulatory compliance for billing errors,
- physician self-referral proceedings and Emergency Medical Treatment and Active Labor Act proceedings.

One size does not fit all. It's crucial to take a look at the specific language of the policy as well as the premium, and choose the policy that best fits your overall risk management strategy and liability exposure.

###