A Bigger Boat

Expand your knowledge to address emerging cyber risks

By John Spiehs

"You're gonna need a bigger boat" is probably the most famous line from the movie "Jaws." As Roy Scheider glimpses the great white shark for the first time, the look of fear on his face is priceless, realizing they're in over their heads and facing a catastrophic ending.

Some people may not consider a data breach a catastrophe, but then maybe those people aren't small business owners with their livelihood tied to their business. No one wants to be told too late that "you're gonna need a bigger policy."

If you're not familiar with cyber policies, you might think it's an add-on with low limits and not much coverage. However, cyber markets are booming, often offering primary limits up to $10 million. Today's market is also evolving to provide more unique coverages that meet the market demand while responding to burgeoning cybercrime risks. For example, ransomware, business email compromise and social engineering are three common cyber losses today.

Ransomware is far more common, destructive and expensive than just a few years ago. A typical ransom in the past may have demanded 1 Bitcoin, which is worth around $10,000 at the time of publication. The ransom could be cheaply paid while decryption was fairly painless, allowing insureds to resume business quickly.

But now, more sophisticated and more difficult to remove ransomware is being deployed after credential-stealing trickbots have gathered information for months. Ransoms are no longer measured in the thousands but the hundreds of thousands and even millions of dollars. Negotiations can drag on for days and decryption is often difficult and time-consuming. Even when decryption is complete, restoring data to systems that need extensive remediation can be an endeavor.

Meanwhile, business email compromises, normally arising from a phishing attack, result in stolen login credentials, which leaves email accounts and systems exposed. What's in your emails? Often more than you think. Our inboxes frequently include personal health information, personally identifiable information and credit card information.

For businesses, the most valuable information is connected to accounts receivables, banking information and invoices. When bad actors obtain this information, it leads to social engineering—a form of trickery where cybercriminals use a business's invoices, emails and bank account information to defraud the insured or its clients and vendors.

Traditionally, business interruption coverage is triggered due to property damage. However, decryption and data restoration arising from a cyberattack can last for weeks, just like a property loss. Cyber policies can now cover business interruption, extra expense and data restoration for losses between $1 million and $10 million. Cyber markets are now offering coverage for property damage and bodily injury arising directly from a cyberattack, as well.

The world of data security and cyber insurance may seem like shark-infested waters, but there is a multitude of resources available to brush up on cyber risks and coverage trends. Subscription services like Advisen, NetDiligence's e-Risk Hub and ePlace Solutions, as well as industry conferences and free articles and blogs, such as Krebs on Security, can all help.

The bigger boat you've been looking for is here. Invest time in some of these resources and soon you'll be able to dive in comfortably and swim without looking over your shoulder.

John Spiehs is vice president and claims expert at Swiss Re Corporate Solutions and works out of the office in Kansas City, Missouri. Insurance