Beware of Potholes in the Information Superhighway

by Sue C. Quimby, CPCU, AU, CIC, CPIW, DAE

Rapid advances in technology have brought our world together, and in many ways, made our lives easier. But this progress is not without its drawbacks. As technology and internet usage evolve, and we become more dependent on them, companies may inadvertently leave themselves exposed and often extremely vulnerable to the gray zone of cyberspace. Standard insurance policies do not address all of these exposures. Cyberspace, or the information superhighway does not have a specific address - it is everywhere. This creates a unique challenge to insurers and their agents. It's essential for agents and insurers to understand and address these issues with their clients.

Most coverage forms define coverage territories as tangible places, such as the United States and its possessions or territories. However, cyberspace encompasses so much more than geographical places and airspace. Electromagnetic waves are transmitted from one side of the world to another within milliseconds, containing things that cannot be seen or touched: intangible things. Unlike loss exposures that can be seen, such as a hurricane or tsunami, cyber loss exposures are most often unfathomable, yet have the potential for similar financial impact. A local business selling products on their website opens their company to worldwide products liability, as well as attacks by hackers. The hackers seem to evolve with more aggression and ingenuity, determined to overcome any security measures that may be in place.

Common cyber loss exposures include:

Denial of Service Attacks: The insured's website is inundated with volumes of communications, which in turn, cripple the operating system until it comes to almost a complete standstill. Although there is no direct physical loss or damage to tangible property, the amount of income lost could be substantial, and this does not include the cost of marketing to restore lost good will and customer confidence.

Flaws in the Intelligence of a System: A malfunction interaction with another system component or components impairs the performance of the operating system. For example, if cryptographic hardware is used for passwords, malfunctioning hardware can potentially mismatch private information, thereby creating a security breach.

Security Breach or Privacy Loss: This involves an improper disclosure of personal information, whether intentional or unintentional. Examples include the disgruntled employee who steals social security lists to sell the information, or hackers who can "sniff" ATM passwords from across the street, or pick up keystrokes from the electromagnetic signals that are being emitted. Almost every state has a Security Breach Regulation. Companies must understand and be in compliance with the laws of each state where the breach occurred, as well as those states where the affected individuals reside. This can be very time consuming, however the penalties and fines for noncompliance can be substantial.

It is estimated that the cost to notify a person that a security breach has taken place is somewhere in the range of $200 per compromised customer. If 10,000 policyholders are

affected, that would equate to approximately two million dollars just in notification costs. This does not include the cost to repair the actual problem.

Copyright and Trademark Infringement: Just because the Internet is "free", it does not mean that everything found is 'free" for the taking. Copyright and trademark infringement claims may result from people downloading picture, or music, or printing information. This is true for personal lines customers as well as commercial.

In the beginning of his first term, President Obama said:

"It's long been said that the revolutions in communications and information technology have given birth to a virtual world. But make no mistake: This world -- cyberspace -- is a world that we depend on every single day. It's our hardware and our software, our desktops and laptops and cell phones… that have become woven into every aspect of our lives."

Recently, there have been a number of high profile cyber-attacks, including companies such as SONY, Target, and Staples. The SONY attack let to cancellation of the release of the movie The Interview, Target paid $10 million to settle a lawsuit ensuing from a breach of debit and credit card information of 40 million people and personal information of 70 million. Some of the attacks may not be as publicized. A USA TODAY report stated that U.S. Department of Energy computer systems were compromised more than 150 times between 2010 and 2014. Tax records of more than 300,000 individuals were accessed in May 2015.

The Federal Government continues to work to protect information on the worldwide web. Most recently, the Cyber Security Information and Protection Act was passed by the Senate. It would allow sharing of information between federal agencies and manufacturing and technology companies. Detractors fear that there are not enough privacy safeguards in the bill.

As more and more businesses and individuals turn to the Internet to conduct business, they are entrusting their personal and confidential data to cyberspace. Social media sites Facebook, Instagram, LinkedIn, Twitter and activities such as blogging create potential worldwide exposures. Information and photos that are published cannot be taken back. Even worse, these items can be edited and republished.

It is essential for insurance agents to address cyber exposures with their clients before claims happen. There are insurance programs available that address cyber property and liability exposures. The well-informed agent is an asset to his insureds.

Previously published in Today's Insurance Professionals®