Cyber: The View from the Ground Floor

By Lynn R. Crisci

There is a new risk in town and it's going by the name of 'Cyber.' Most news reports and trade journals provide information on a dizzying array of changes and developments related to this risk. The federal government is involved, and declared October 2015 as 'Cyber Month' on the Hill. The National Association of Insurance Commissioners (NAIC), a non-profit largely made up of state regulators, has also recently released the Cybersecurity Bill of Rights for consumers. Every state has passed regulations spelling out requirements for protecting personally identifiable information (PII) and consumer notification. There is a more general conversation about the Internet of Things (IofT); listing the vulnerability of everything from the national power grid to an individual's pacemaker. As a principal responsible for the management of a captive or risk retention group (RRG), you find yourself wondering what part of the hundreds of concepts and ideas you should consider. Which of these balls can you drop and which should you juggle to do the best by both those who make up your group and those who work in the operation of your business?

It is not an easy question; and the conversation is further complicated by the rapid state of change in the understanding of what is considered 'risk' and what is identified as being 'at risk.' Until the particulars of control and definition are sorted, there are four key phrases that I would either place on your news search or ask your professional advisor to monitor on your behalf.

There is a more general conversation about the Internet of Things (IofT); listing the vulnerability of everything from the national power grid to an individual's pacemaker.

Key Phrase One:

National Association of Insurance Commissioners (NAIC)
Cybersecurity (EX) Committee

This non-profit group has been the first out of the gate with what it has framed as an 'aspirational' framework of what consumers should be entitled to receive in terms of notifications and services following a cyber-attack that places their PII at risk. There is some controversy surrounding the release of their manifesto. Entitled the Cybersecurity Bill of Rights, this document describes six points that the NAIC feels should be an expectation of any consumer doing business with an insurance company, agent, or other business that collects, maintains, or uses their PII. While this document has drawn some fair fire from the insurance industry, the federal government, and others; you can assume that these guidelines will evolve to keep pace with any changes. One of the recommendations coming out of this group is that compliance for insurance companies including surplus companies, captives, and RRGs would be monitored by state insurance department examiners. Since the NAIC is made up largely of state regulators you can expect this recommendation will get some traction if the laws governing cybersecurity remain on the state level.

Key Phrase Two:

Cybersecurity Information Sharing Act (CISA)

This pending legislation, which passed the U.S. Senate in October 2015, now looks likely to pass in a form near its current language through the U.S. House of Representatives. The President

This article first appeared in the Winter 2015 issue of ***The Demotech Difference***, a publication of Demotech, Inc., www.demotech.com

had made statements that he feels the time is right for legislation on this issue. So unless something unexpected is slipped into the wording, it is likely this will be made law. The crux of the legislation is that there is a need for protecting PII, not only in its electronic form but in paper form. The wording currently being moved forward would require every business to adopt safeguards for both its internet traffic and its physical file handling. There are direct references to using guidelines set forth through the National Institute of Standards and Technology (NIST). Those of us who have been around awhile remember this organization as the Bureau of Standards. In this emerging age of technology, the Bureau has found new life and purpose. In what has been an interesting parallel action, local FBI and Secret Service offices have been reaching out to financial institutions — which by definition now include insurance — and are asking for cooperation in reporting any hacking incidents. At a minimum, you can anticipate some type of reporting requirement including a new procedure that you will need to understand and implement for your 'financial institution' to meet the guidelines that emerge.

Key Phrase Three:

Federal Trade Commission vs. Wyndham Resorts

While this case is likely to head to appeal, it is still a good indicator of things to come, and the risk of doing nothing. Keeping an eye on this particular case and related topics will be time well spent. In a nutshell, the Federal Trade Commission (FTC) has won an argument that it has standing to bring civil action on behalf of those whose information has been lost through a cyber-related hacking or other event. The argument is that if a business does not have appropriate security in place such that it was doing what was reasonable to protect its customers' identity, then its actions constitute Unfair Trade Practices. When you consider who the FTC considers as being worthy of protection, it is more

Moon Light PhotoStudio/shutterstock.com

than your customer, be they business or individual. They have expanded the blanket of their protection to include any third party vendors with whom you do business. It is a sweeping mandate, and one that we can expect will meet some challenges. What is troubling about this particular case and why you should pay attention is that the standard of what is considered 'reasonable' has not been established. Had we made a list of what is 'reasonable' two years ago, it would have differed from today's definition. For example, it now appears the 'reasonable' includes the right to one year of identity theft protection paid for by the company or agent involved in the data breach. For many of our smaller customers, and for the small group of employees we have that handle the day-to-day business of our captives and RRGs, the idea of paying these types of costs out of pocket gives a financial officer pause.

Key Phrase Four:

Federal Insurance Office (FIO)

While the NAIC and insurance carriers in general are not in favor of federal intervention, that doesn't mean it can't happen. The FIO became more active following the creation of the federal backstop for the Terrorism Risk Insurance Act (TRIA). While it is not a lively conversation, there has been a suggestion that the FIO might advocate a federal backstop for cyber events, similar to TRIA. If this were to happen, we may be facing a new surcharge or fee to help fund this backstop. Reporting requirements are also likely. There has been some suggestion that the laws that regulate the protection due a consumer be removed from the state level and instead be taken up by the FIO who would delegate monitoring and enforcement to state authorities. With the pending federal legislation around this topic, and the historic preference of the federal government to enforce their mandates through federal agencies and agents, it is probable that the FIO will have some role in the mandates that tumble down the Hill to land at your doorstep.

As a conscientious business person, understanding that every organization that does business with the public will be expected to meet some standard, and knowing that the 'standard' is still to be defined, what are the common sense steps you can and should take?

For you as a business handling PII of others:

You need a privacy policy. It needs to explain what personal information you collect, what choices customers have about their data, and how a customer can see and correct its data. This policy should be posted on your website and available in written format. It should also describe how you protect and store data, and what a customer can do if you fail to follow the policy. If you have not been reading the literature on what constitutes PII, be aware that it's about

more than social security numbers and birth dates. Combinations of otherwise harmless information, like e-mail addresses and names that are linked, are now considered PII.

You need to encrypt data that is considered PII within your systems. It is not enough to have a firewall. Encryption software and a regular maintenance schedule that includes upgrades is the new standard. You need to maintain records that demonstrate that you are aware, have a plan, and follow the plan. Purchasing a software package, installing it, and then not proactively monitoring for updates is no longer considered behaving in a responsible manner when it comes to your customers' information. Be aware that if you work with third party vendors and the data breach places them at risk, you can find yourself facing lawsuits from that quarter as well.

You need a protocol for your third party vendors. Do you use vendors for payroll or invoicing? Do you allow regulators or auditors to view your information that may include PII? All of these are examples of third party vendors. As a rule of thumb, third party vendors should never be allowed direct access to your systems. But what if you rely on the services they provide, and those services can only be provided using your data? Each situation needs to be carefully considered and should include documentation as to how you addressed the situation while maintaining the security of your customers, your employees, and others.

Passwords and people controls are a requirement. The number one way that data is compromised today is not through a direct hack to a computer system, but through an unintended invitation into the system. Employees should be required to update passwords on a regular basis. Employees should also receive training helping them to become more cyber savvy. Opening unknown email links, sharing passwords, or unwittingly providing system access by leaving terminals unlocked can lead to a breach. The better you arm your employees and yourself against being made someone's accomplice, the more you reduce the risk to your business and your customers.

The key is to realize that as a trusted advisor there may be an expectation that you recognized a risk and provided a recommendation.

For you as an advisor to captive or RRG members:

Consider transferring your customer's exposure in the event of a breach by securing a master cyber liability policy. All the risks outlined above apply to your customers as well as to your own business. Having coverage in place to handle some of the costs that may ensue following a breach is a reasonable strategy. Handling the entire captive through use of a master policy that provides a first layer can make the cost of cover more affordable. In assessing a policy, you should consider what services are available. In the current environment, it is access to information that may be the most important benefit you can provide. Most insurance offerings in this space include access to consultants whose function is to educate and coach a customer. This service may be offered as post-breach advice, pre-breach disaster recovery planning, or the product might offer both services.

The key is to realize that as a trusted advisor there may be an expectation that you recognized a risk and provided a recommendation.

The discussion about what constitutes a cyber risk and what measures are considered 'reasonable' will continue to evolve. Taking the offensive in seeking knowledge and taking action will be your best defense.

Author's Update: The challenge of writing ahead of a deadline about current issues is things change. Major developments since writing this:

1) CISA was signed into law on December 18, 2015. The final draft removed all definition of what constitutes personally identifiable information(PII) and the standards that could satisfy an organization's due diligence in protecting same. What emerged is a framework under which organizations are encouraged to voluntarily share information about cyber incursions with the federal government and the implementation of new standards within the Federal government aimed at ending their own hacking woes. There is one outward-facing piece that establishes a task force which will prepare a report on the health care industry's preparedness to respond to cyber risk.

2) Wyndham Resorts settled their case with the FCC. What does this mean? It means businesses still lack a gold standard against which they can measure whether their safeguards are adequate, and that the FCC has the authority to judge.

Visit www.cyberinsurance.news for more from Lynn.

Lynn R. Crisci, CPCU, ARM is Assistant Director, Product Development and Compliance, for HAI Group. She brings 30 years of industry experience of developing unique customer solutions to HAI Group. Prior to joining HAI Group she worked at The Hartford in their Specialty, Middle Market, and TPA Claims divisions for 14 years. At HAI Group, Lynn leads the Product Development and Compliance Division where her team develops new and revised insurance products and programs serving the needs of the public and affordable housing industries. Lynn can be reached at lcrisci@housingcenter.com.

HAI Group serves the public and affordable housing community with special, niche insurance programs as well as other value-added products and services. HAI Group is dedicated to providing reliable insurance, training, and software solutions in a manner which exceeds expectations.