First-Party Insurance for Cyber Risks

October 2009

"The only thing we have to fear on this planet is man."
-Carl Jung

"The pen is mightier than the sword."
-Edward Bulwer-Lytton

by William K. Austin
Austin & Stanovich Risk Managers, LLC

In July we reviewed electronic data ("e-data") exposures when analyzing an organization's risk to cyber[1] loss exposures (*see* Cyber Risk—Data Damage and Destruction beyond the Naked Eye). E-data risk controls have grown in sophistication and protection and can greatly limit the catastrophic potential of e-data loss from any peril—cyber or "brick and mortar."[2] But even the best controls can be breached, and e-data damaged, causing interruptions in an organization's need for ongoing operations.

Look closely at the above quote from Dr. Jung. What is chilling about cyber risk is that it is essentially man-made, when one considers that the majority of cyber risk is created by individuals with one goal in mind: to continually seek ways to compromise someone else's computer for personal gain or even worse just to prove that they can with the proof being damage, destruction, or control. Each day viruses are created and unleashed through the Internet. Each day we are faced with a need for new defenses and safeguards.

Think in terms of the peril of windstorm and the possibility of catastrophic damage to an organization: hurricanes happen every year, and with global warming, have seemingly increased in power and damage potential. But unlike cyber risk, a hurricane does not morph into a new type of windstorm in order to *intentionally* increase its potential to damage or destroy our physical environment. The risk management professional must face cyber risks of loss as being new and unique each day, if not each hour, that the organization is operational.

Insurance for theft of electronic property or damage of e-data damage and interruption of operations must be carefully considered to ensure adequate insurance coverage in terms of verbiage and policy limits for an organization to recreate damaged e-data, seek indemnity for stolen property (i.e., cash and securities), replace lost income from suspended operations, and offset any increased operating expenses. There is rarely a silver bullet for any insurable exposure. This is especially true when dealing with cyber first-party damage exposures as most property insurers exclude e-data from property covered or provide such a minimal sublimit that coverage is essentially nil.

In this article we discuss use of appropriate cyber property insurance after proper identification of cyber property damage exposures. Or, said differently, we need to take Mr. Bulwer-Lytton's quote to heart and find an insurance policy that provides coverage (verbiage and limit) necessary to protect our organization from cyber property risks of loss. For the purposes of this article, crime insurance for theft or damage of money and securities is considered a form of property insurance and included within the term "first-party insurance."[3]

How To Start the Process?

First, we need to define the exposures. We do this to identify all types of property subject to cyber risk whether owned, leased, or otherwise in the custody of the organization. This is to ensure we do not look at e-data only from a view of damage or destruction but also in terms of exposures such as extortion, embezzlement, fraudulent funds transfer, and other loss events that may be considered computer crimes.

Second, we need to create loss scenarios (i.e., exposures to loss) to determine what coverages are not provided by existing first-party insurance policies; it not efficient to obtain cyber property

insurance only to find out at time of loss that it duplicates coverage provided in other first-party insurance policies purchases by the organization. The scenarios can be created by talking to IT staff (in-house or outsourced), the preferred way, about what can happen to the organization if its e-data is damaged, destroyed, compromised, or results in its property being stolen such as money and securities or property of others in the custody of the organization (i.e., online theft of a bank's client's money, securities). The risk management professional can use cyber risk insurance applications and discussion with peer group risk management professionals as resources to create loss scenarios by viewing cyber exposures through different eyes and experiences.

Loss Scenarios

Almost any organization today is exposed to loss from damage or destruction of its computers and computer networks, including any resulting loss of income ("business interruption") and/or increased operating expenses ("extra expense"). An organization's use of computers and computer networks, its own as well as others, creates risks of loss not only to its self but to customers, clients, vendors/suppliers, and even unrelated/unknown individuals or entities ("third parties") that occur as a result from the organization's negligence. A first-party loss to the organization may also create a situation in which the organization is negligent and responsible to another party for cyber-caused damages and therefore result in a third-party claim against it.

Assume, for example the organization is negligent in its security systems and allows a computer virus into its network which results in loss (damage and/or destruction) of its own e-data (first party) and then such virus is spread to nonrelated parties, such as customers or vendors, who in turn lose data and sue the organization for the data loss and any resulting damages such as business interruption and/or extra expense. While this article is not focused on third-party liability exposures and need for insurance, the risk management professional should nevertheless consider the third-party exposures as part of his or her risk management due diligence when considering cyber exposures and appropriate use of insurance.

Cyber exposures are not static and evolve as society continues to use and rely on computers and individuals strive to find ways to invade computers for personal gain or other malicious purpose. To properly evaluate cyber risk insurance policies, one has to understand the extent of cyber risk coverage provided, if any, in existing first-party insurance policies purchased by the organization. Examples of cyber first-party insurance loss scenarios are shown in Column 1 of Schedule 1.

This schedule may not be complete or adequate for all organizations. Each organization needs to define its own loss scenarios, which may include some or all of those identified in Schedule 1. Certain scenarios may also create a third-party exposure; thus, this type of schedule can be used for both first-party and third-party (i.e., general liability, professional liability) loss scenarios. It should be noted that several loss scenarios in Column 1 may be covered in whole or in part by brick and mortar property insurance (including equipment breakdown coverage also known as boiler and machinery insurance) and crime insurance policies but for exclusions or limitations related to e-data.

Using loss scenarios will (1) allow the risk management professional to determine if there is adequate coverage for its existing brick and mortar exposures (i.e., power outage, electrical arching); (2) ensure that any duplication of brick and mortar and cyber risk coverage is kept to an absolute minimum; and (3) determine weaknesses in existing first-party insurance and where coverage from a specialized cyber policy may be needed. Columns 2 and 3 are completed by the risk management professional to confirm coverage, describe limited coverage, or point out lack of coverage. Column 4 will be discussed later.

This type of analysis must be done to determine what cyber exposures are not insured. The lack of coverage should not be a surprise, as many property and casualty insurance policies today have not been expanded to address cyber exposures. As a result of coverage gaps in brick and mortar property (and casualty) insurance policies, some insurers have created specific insurance policies to address cyber loss exposures. Column 4 in Schedule 1 is to be used by the risk

management professional to confirm the extent of coverage provided by any cyber first-party insurance proposed for the organization's cyber exposures.

Insurance Procurement

Cyber insurance policies differ by insurer as there is not a standard cyber first-party insurance policy. Insurers issue policies based on their understanding of cyber exposures, their willingness to insure the indentified exposures, and use policy terms and conditions that may be unique when compared to another insurer's cyber insurance policy.

The procurement process for cyber insurance policies is no different than that used to obtain any other type of insurance. Applications may need to be completed and specific information about cyber risk controls may need to be shared with prospective insurers in writing, by in-person onsite survey, or by conference call. It is important for the risk management professional to create a request for cyber risk coverage outline (i.e., coverage specifications) for inclusion with completed applications to ensure that the insurer responds with coverage appropriate for the organization and not a "generic/one size fits all" proposal. Limit and retention minimums and maximums beneficial for the organization need to be requested as well.

Terms and Conditions

The wording used by an insurer in any insurance policy is critical to the extent of coverage provided. Wording as in insuring agreements, definitions, and exclusions must be reviewed very carefully to ensure that when the policy is viewed in total, that coverage provided meets the actual exposures of the organization. In cyber first-party coverage, special attention must be given to the following concepts as actual definitions of each will differ by insurer: extortion, property or data damage, data protection, business interruption, and extra expense.

Limits

It is difficult to determine an appropriate limit for first-party coverage. There does not seem to be any public information that is credible to use as benchmarks. The organization may be able to obtain creditable and quantifiable exposure information from its brick and mortar insurers, from prospective cyber insurers, and through discussion with peers involved in the same or similar activities and industries. Coverage discussions with IT staff are highly recommended as well.

Retentions

A minimum deductible amount will be required by cyber insurers, not unlike other first-party insurance policies. The deductible chosen by the organization should be consistent with the risk-bearing capability of the organization and commensurate with the cost of the cyber insurance. It does not make sense to purchase cyber insurance (or any insurance policy) subject to a high deductible simply because the organization can afford that level of loss retention if the premium credit provided is not significant when compared to a lower deductible. Discussion with appropriate management of the organization may be prudent as well, depending on the retention amount being considered.

Conclusion

An organization's cyber risk controls (firewalls, encryption, passwords, etc.) may be appropriate as preventative and/or mitigation tools, but these controls should be used in conjunction with appropriate use of cyber first-party insurance. The decision to choose one insurance policy over another policy must be made by understanding the coverage differences of each policy and the significance of each difference. Coverage differences include not only limits and retentions, but actual policy terms and conditions. Once coverage is understood, then one must review premium cost for a policy in terms of coverage, limits, and retentions to determine if the premium is commensurate to coverage provided.

Schedule 1

	Loss Scenarios	Brick and Mortar Property Insurance	Brick and Mortar Crime Insurance	Cyber First Party Insurance
1	Damage to hardware/media by fire, windstorm, explosion, etc.			
2	Damage to hardware/media/data by electrical disturbance/arching			
3	Coverage for lost income and increased expense for "denial of service" from website attacks			
4	Employee (EE) hacking-damage to computer and related property			
5	Non-employee hacking damage to computer and related property			
6	Hacking caused damage and loss of income/Increased operating expense			
7	E-data damage from cyber vandalism (virus, harmful code), including time element and denial of service			
9	Employee theft by computer of money, securities and other property			
10	Employee theft by computer of customer/client money, securities and other property			
12	Non-employee theft by computer of customer/client money, securities and other property			
13	Theft of organization "identify"			
14	Theft of organization's customer/client "Identity"			

[1] **Cyber:** relating to, or involving computers or computer networks (as the Internet); the cyber marketplace." ~Definition from *Merriam-Webster Online Dictionary*.

[2] In the jargon of e-Commerce, **brick and mortar** businesses are companies which have a physical presence (for example, a building made of bricks and mortar)—which offer face-to-face consumer experiences. This term is usually used to contrast with a transitory business or an Internet-only presence." ~Definition of "brick and mortar" from *Wikipedia®, the free encyclopedia*.

[3] "**First party insurance**" is defined by *Black's Law Dictionary*, 7th edition, as "A policy that applies to oneself or one's own property such as … fire insurance." It should be noted that *Black's* defines "crime insurance" as "Insurance covering losses occasioned by a crime committed by someone other than the insured."

Contact information: William K. Austin, Principal
Austin & Stanovich Risk Managers LLC
wkaustin@austinstanovich.com
Telephone 888-540-7604 Fax: 888-650-7803
www.austinstanovich.com