Cyber risk-data damage and destruction beyond the naked eye

July 2009

"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 and Blackberries that have become woven into every aspect of our lives.

It's the broadband networks beneath us and the wireless signals around us, the local networks in our schools and hospitals and businesses, and the massive grids that power our nation. It's the classified military and intelligence networks that keep us safe, and the World Wide Web that has made us more interconnected than at any time in human history.

So cyberspace is real. And so are the risks that come with it. It's the great irony of our Information Age -- the very technologies that empower us to create and to build also empower those who would disrupt and destroy. And this paradox -- seen and unseen -- is something that we experience every day."

-Excerpt from May 29, 2009 speech by President Obama on "Securing Our Nation's Cyber Infrastructure"

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

We can visualize damage to "brick and mortar"[1] exposures from perils such as fire, windstorm and theft so appropriate insurance treatment can be easily considered. "Cyber"[2] exposures are much more difficult to comprehend since we must deal with the unseen operations of electrical impulses that can span the globe from computer to computer in less than a second. An electrical impulse created with malignant code or destructive virus can spread havoc within an organization with the same disruptive impact as if the "brick and mortar" organization had undergone the effects of a natural disaster. The potential for an organization to suffer cyber loss from significant damage and disruption may occur almost instantly from anywhere in the world once the organization has an active internet connection. Any organization has the potential for a cyber exposure even if it is not involved in e-commerce[3]. The use of the internet has become the backbone of nearly all organizations whether it used solely for critical internal data management or in conjunction with e-commerce revenue generation.

Mention "cyber risk" to a gathering of risk management professionals and the focus for many will be on an organization's potential liability from negligent acts that cause others to suffer identify theft, invasion of privacy and credit card fraud. What about direct damage to the organization itself? While damages sought by injured third parties and the resulting reputational risk may be crippling to an organization, the cost associated with first party damage to an organization may be equally significant and just as detrimental in terms of its reputational risk. How prepared is your organization for electronic data damaged or destroyed from a cyber peril?

Cyber risk management and appropriate use of insurance is not a job that can be completed by just one person. The person charged with risk management and insurance procurement responsibility must solicit the organization's cyber exposure and cyber risk control information from those individuals in-house (or out-sourced) with information technology ("IT") responsibility. Cyber risk controls such as firewalls, virus protection, encryption, regular data back-up, off-site data storage and password protection must be implemented, tested frequently and continually improved. Insurance is not a substitute for cyber risk controls. As in any operational risk management model insurance and risk controls need to co-exist to the overall benefit of the organization.

Property Insurance

The need for property insurance arises from "brick and mortar" exposures and from those considered "cyber" exposures. To determine appropriate insurance coverage we must first understand what is defined as insured property, what events that cause damage to insured property are considered insured perils and if the resulting disruption in the organization's operations from covered damage will trigger time element coverages of business income and extra expense. Property insurance policies often differ by insurer since many insurers use independently filed forms and do not adhere strictly to Insurance Services Office ("ISO") filed policies. For this article we examine ISO property insurance forms, identified below, to establish coverage benchmarks.

Coverage Form	ISO Form No.
Building and Personal Property Coverage	CP 00 10 0607
Cause of Loss-Special	CP 10 30 06 07
Business Income (and Extra Expense)	CP 00 30 04 02
Electronic Commerce (E-Commerce)	CP 04 30 06 07

Readers must review their specific property insurance polices to ensure their organization has adequate coverage for "brick and mortar" and "cyber" exposures. This article will not provide all the answers on how to insure first party cyber exposures. Rather it is to create an awareness of cyber exposure to loss and potential deficiencies in property insurance including coverage for time element. Appropriate use of property insurance for cyber risk exposures will differ by organization; there is no "one size fits all" solution.

What should be the primary 1st party cyber property damage concern for any organization? Data in electronic format. What is "data"? Merriam-Webster's Online Dictionary ("MW") provides a common usage for "data". Cyber exposures may arise from all 3 aspects of the MW definition of data.

> *1: factual information (as measurements or statistics) used as a basis for reasoning, discussion, or calculation <the data is plentiful and easily available; 2: information output by a sensing device or organ that includes both useful and irrelevant or redundant information and must be processed to be meaningful; 3: information in numerical form that can be digitally transmitted or processed.*

ISO relies on common usage of the word "data" in its policy forms but specifically defines the term "electronic data" as:

> *"Information, facts or computer programs stored as or on, created or used on, or transmitted to or from computer software (including systems and applications software), on hard or floppy disks, CD-ROMs, tapes, drives, cells, data processing devices or any other repositories of computer software which are used with electronically controlled equipment. The term computer programs, referred to in the foregoing description of electronic data, means a set of related electronic instructions which direct the operations and functions of a computer or device connected to I, which enable the computer or device to receive, process, store, retrieve or send data. This paragraph (n) does not apply to your "stock" of prepackaged software".*

(Note: There is no legal definition for either "data" or "electronic data" in Black's Law Dictionary, 7th Edition).

How is electronic data insured by an ISO property insurance policy? It depends on the extent that ISO policy forms are followed by your organization's property insurer.

Starting with the Basics: Covered Property

Is electronic data considered covered property by ISO? We begin our analysis by review of the building and personal property coverage in the ISO CP 0010 0607 and the definitions summarized below.

- Building: "building or structure described in the Declarations (i.e. location) including completed additions, fixtures and permanently installed machinery and equipment". It is clear that data in any form is not contemplated nor covered within the definition of "building".
- Personal Property: "consisting of the following unless otherwise specified in the Declarations as furniture and fixtures; machinery and equipment; stock, all other personal property owned by you and used in your business, your use interest as tenant in improvements and betterments; leased property for which you are responsible to insure and personal property of others in your care, custody or control". Data is not addressed specifically in this definition so at first thought it may be considered personal property. We need to continue reading the policy form to learn more.

While the Covered Personal Property definition is broad we must look to "property not covered" to understand what property is actually subject to direct damage coverage. It is not until one nearly completes the list of "not covered" items that we find two exclusions related to electronic data: n and o. "N" excludes "electronic data" from "covered property" and "O" excludes the "cost to replace or restore the information on valuable papers and

records including that which exist as electronic data''. Thus there is no coverage for damaged or destroyed electronic data no matter what is the proximate cause of loss, i.e. brick and mortar perils such as fire or explosion or cyber peril such as electronic virus.

A $2,500 extension of coverage is provided in this ISO form for the cost *to replace* electronic data destroyed or corrupted by a *covered cause of loss*. No coverage is provided for *research* expense if data destroyed is first generation without any back-up. Covered cause of loss is expanded in this extension to include the following perils insured if the organization has either Special or Broad Form perils:

> *"a virus, harmful code or similar instruction introduced into or enacted on a computer system (including electronic data) or a network to which it is connected, designed to damage or destroy any part of the system or disrupt its normal operations. But there is no coverage for loss or damage caused by or resulting from manipulation of a computer system (including electronic data) by any employee, including a temporary or leased employee, or by any entity retained by you or for you to inspect, design, install, modify, maintain, repair or replace that system".*

While data corruption coverage is included as covered perils within this extension the limit of $2,500 is likely to be insufficient for most organizations following a major cyber loss occurrence. How far will $2,500 go within your organization to replace electronic data damaged or destroyed by these cyber perils? Most likely not far if the risk controls failed to protect as had been thought. Depending on the insurer's specific policy form filing it may be able to offer higher limits upon request. Additional limits should be considered based on exposure information obtained from IT personnel and the estimated recreation expense between data back-up cycles.

Some organizations will be told to purchase an e-commerce property policy to insure their electronic data cyber exposure. This approach may be the correct direction to go if the organization is in ". . . the business of e-commerce activity (which) means commerce conducted via the Internet or other computer-based interactive communications network". This quote is from the ISO e-commerce policy form CP 04 30 06 07. This policy does not address electronic data cyber exposures for organizations that rely on the internet as the backbone of their information infrastructure but use "brick and mortar" activities and operations for revenue generation. These other organizations will likely need to look to inland marine and/or specialty policies to cover data destruction from cyber peril. A policy title such as "e-commerce" may suggest cyber coverage but it will take a complete reading of the policy to ascertain if it will provide your organization with coverage for its electronic data loss exposures.

Time element

Will any resulting suspension of the organization's business or increased operating expense be covered as a result of the organization's destroyed electronic data? Generally "no" and it does not matter if the e-electronic data is destroyed by "brick and mortar" or cyber perils. We look to ISO business income (and extra expense) coverage form CP 00 30 06 07 for details. While time element coverage is provided when property at the premises is damaged (note-damaged property need not be "covered property) there is a specific limitation for computer operations. No time element coverage is provided for any "suspension" of "operations" caused by destruction or corruption of electronic data. How long can your organization operate without access to its electronic data. The ISO form discussed in this paragraph does provide limited time element coverage from an interruption of computer operations. The limit is $2,500. How long can your organization exist on a limit of $2,500? Time element coverage is provided by the ISO e-commerce policy but again the coverage proviso is if the organization is in . . . the business of e-commerce activity (which) means commerce conducted via the Internet or other computer-based interactive communications network. The "non" e-commerce organization may be able to secure coverage greater than $2,500 by request to its insurer or other types of property insurance policies as previously suggested.

<u>Conclusion</u>

Risk management professional must focus on first party electronic data exposures when analyzing all of an organization's cyber loss exposures. Electronic data risk controls have grown in sophistication and protection. It is

possible that physical risk controls including frequent data back-up and off-site storage can greatly limit the catastrophic potential of electronic data loss from any peril-brick and mortar or cyber. Insurance coverage will need to be carefully considered and analyzed for its ability to indemnify the organization for all costs of recreation, resulting suspension of operations and increased operating expense. Any property insurance policy that is presented as a cure-all for damage or destruction of electronic data will need to be carefully scrutinized. Coverage issues need to be understood and addressed prior to binding coverage. Learning of a coverage issue at time of loss is not an efficient use of any kind of insurance.

---

[1] 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*.

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

[3] "**e–commerce:** commerce conducted via the Internet." *~Definition from Merriam-Webster Online Dictionary*.

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