Analyzing Nonstandard Cyber and Privacy Insurance Policies

October 2014

"Plans are of little importance, but planning is essential."
-Winston Churchill

"How you climb a mountain is more important than reaching the top."
-Yvon Chouinard, founder of Patagonia

"It's not that I'm so smart, it's just that I stay with problems longer."
-Albert Einstein

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

It seems to be a daily occurrence—another large organization's computers are hacked, and private customer and employee information is released into the public domain. But cyber and privacy exposures are not for the large organization alone; these are exposures for organizations of any size, any industry, without any distinction between for-profit or nonprofit. But risk managers and insurance brokers alike ask me how to determine the proper coverage when cyber and privacy insurance policies are not standardized.

Risk management professionals—whether risk managers or insurance brokers—must determine how to create an insurance placement to address an organization's cyber and privacy exposures. But the use of insurance is not that easy when cyber and privacy insurance policies are not standardized and differ, sometimes significantly, in coverage terms and conditions by insurer. So how does the risk management professional decipher the various proposals from insurers to decide which policy may be best for the organization?

They decide first by understanding the exposures contemplated for coverage and second by creating an analysis platform so dissimilar insurance policies can be compared as objectively and equally as possible. Thus, planning is a must-do first step, and the ability for the risk management professional to roll up his or her sleeves and dig into analysis is a very close second step. See the wisdom in simple statements made by Churchill, Chouinard, and Einstein above?

Cyber and privacy insurance analysis requires risk management professionals to have a plan, a method, and an understanding of what coverage is needed for the organization. But how, as these are not typical filed policies like forms from Insurance Services Office, Inc., or American Association of Insurance Services? Cyber and privacy policies will differ by insurer. It is in the planning. It is in the analysis. It is not throwing one's hands up and getting lost in unnecessary details. It is a step-by-step plan to dissect policies to determine how the organization's exposures can be most effectively covered and at the most efficient cost of deductible/retention plus premium.

Step 1: What Are the Exposures?

All risk management processes must start at the same point of exposure identification: one can not effectively insure what one does not understand. We start with what is considered cyber and privacy insurance and pull the exposures out of its definition. Let's not let the word "cyber" cloud our concern for "privacy" exposures, as the loss of private data in paper form can be just as disastrous to an organization as a public release of its private e-data files. Let's use excerpts from International Risk Management Institute's definition of "Cyber and Privacy Insurance" to get an idea of exposures:

"... cyber and privacy policies cover a business's liability for a data breach in which the firm's customers' personal information, such as Social Security or credit card numbers, is exposed or stolen by a hacker or other criminal who has gained access to the firm's electronic network. The policies cover a variety of expenses associated with data breaches, including notification costs, credit monitoring, costs to defend claims by state regulators, fines and penalties, and loss resulting from identity theft. In addition, the policies cover liability arising from website media content ... property exposures from ... business interruption, data loss/destruction ... and cyber extortion."

From the definition above, we can categorize exposures in order to compare exposure to coverage offered by an insurer's terms/conditions on a policy-by-policy basis, even when policy language may not be the same. The categories can be such as these:

- notification costs;
- credit monitoring;
- costs to defend claims by state regulators;
- fines and penalties;
- loss resulting from identity theft;
- website media content;
- business interruption;
- data loss/destruction; and
- cyber extortion.

Step 2: Define the Exposures in Terms of Coverage Needs

The risk management professional can create definitions that he or she feels are necessary for a specific organization's cyber/privacy exposures from breach of e-data and paper. This approach, while discussed for cyber/privacy insurance, is a

starting point for anyone preparing any type of insurance policy analysis, not just cyber/privacy policy analysis. It is proper and expected that risk management professionals will ask for input from others within the organization, including but not limited to information technology (IT) staff. Risk management is most successful when it is conducted as a team sport.

Coverage Category	Claim/Exposure
Regulatory Proceeding	Costs incurred to defend organization for failure to disclose an event to governmental authorities when required by any security breach notice law
Security and Privacy Liability	Cost to defend organization from allegations of privacy violation including costs of settlement or judgment
Digital Asset Loss	Cost to replace lost/damaged e-files
Event Breach Costs	Cost incurred by organization arising out of (1) forensic investigation of breach; (2) use of public relations, crisis management firms, law firms; (3) notifications costs (i.e., printing, advertising, and mailing); (4) cost of identity theft call centers, credit file monitoring, and similar costs; (5) other costs as may be approved by the insurer
Network Interruption	Loss of income from material interruption of organization computer systems due to security/breach event and costs incurred as a result of the network interruption. Depending on the organization, this may not be a significant exposure and may not need to be insured.
Cyber extortion	Costs incurred when insurer approves extortion payment(s) made to hacker or other criminal party to stop a planned event from occurring. Coverage also can include costs to conduct an investigation after the fact into the act of extortion.
Internet Media Liability	Cost to defend organization from allegations of privacy violation from unauthorized website changes, including costs of settlement or judgment

An important exposure issue that is often overlooked when comparing cyber/privacy policies is if the named insured is allowed to release others from liability if done in writing prior to loss. This act by the named insured will limit or eliminate an insurer's right of subrogation at time of loss. Many cyber/privacy policies do not allow any restriction in the ability of the insurer to subrogate. This means that, if a release of liability is entered into, the policy may be void at time of loss. Many IT service vendors require a partial or full release of liability as part of their service contracts with organizations. These pre-loss releases may not be fully known, understood, or even shared with the risk management professional, thus putting a policy condition in effect that can void coverage. This exposure needs proper vetting and careful policy analysis.

Step 3: What Are the Expected and/or Catastrophic Costs of a Data Breach Event?

Matching coverage to exposure is only a portion of the analysis. Proper insurance limits are required as part of the policy analysis. Pursuit of insurance limits is not a perfect activity, as one must consider limit availability and cost of limits as part of the overall limit equation. There are many issues to consider when limits are to be quantified for cyber/privacy insurance.

- There is no formula to set a reasonable coverage and/or policy limit.
- Use of settlement and/or judgment information is suspect, as there is not sufficient credible public information. Caselaw is still developing on damages a person or organization can claim when personal information is used by unauthorized persons. There is not adequate quantification of damages by persons for costs, judgments, or settlements from mass breach of e-data or paper records.
- Direct costs (i.e., "event breach costs") for US data breaches (i.e., forensic experts, outsourced hotline support, free credit monitoring subscriptions, and discounts for future products and services) are estimated to be $188 per record by the Ponemon Institute in its "2013 Research Report" based on calendar 2012 data. These costs can become staggering as the number of breached records increases.

Breached E-Records	Estimated Direct Costs
1,000	$188,000
10,000	$1,880,000
100,000	$18,800,000
1,000,000	$188,000,000

The direct costs above are just "event breach costs" and do not include third-party-related defense or settlement/judgment costs for damages claimed by injured parties. Thus, the overall costs of a cyber/privacy breach can increase substantially from those direct costs shown above. This means that there may be millions of dollars of potential liability for an organization when all costs are known from a data breach. But the direct costs are a sound starting point for limit analysis by the risk management professional.

Step 4: Read and Understand a Complete Proposal

First, request not just a proposal of terms/conditions, limits, deductible, and premium but also a specimen of how the policy will be issued with coverage part and all expected endorsements. Second, read each proposal and sample policy completely to become familiar with how the policy and its coverage will address a cyber/privacy event. Third, now that you understand the nuances of a specific policy (i.e., the pros and cons), you can effectively compare it to other proposals and other sample policies.

Step 5: Create a Spreadsheet for Policy Analysis and Comparison

I find it easiest to create a line-by-line spreadsheet of policy attributes in order to compare each important policy term, condition, exclusion, or other point of coverage—whether enhancement or restriction.

The spreadsheet left-hand column is essentially an outline of the policy being reviewed, listing insuring agreements, general conditions, exclusions, and other important coverage provisions and/or restrictions. I start with one policy and use it to create the initial outline. As I review other policies, I may find new items to compare from that policy with the prior one and add to the left column as needed. Review of other policies may increase the outline further.

The use of a color scheme will help point out key differences by policy. Different colors are used to separate issues in each quotation. It is possible that a quotation with more "green" than other quotations may be more restrictive at time of loss, depending on the circumstances of the loss and resulting claim(s).

Color	Definition for Color
Green	Better than other policy/quotes
Yellow	Average/common to each policy/quotes
Orange	Needs further review
Red	Apparent severe coverage restriction

Sample Cyber and Privacy Worksheet

Name of Organization ***Must read policy for actual definition and coverage intent***

Computer system: *hard/software. . . owned, operated, control of organization or hosted by 3rd party.*
Cyber extortion: *expenses and monies for threat or extortion act.*
Defense w/in limit: *overall limit applies to all coverage including defense costs .*
Digital asset loss: *cost to replace loss of e-data.*
Event/breach mgmt. cost: *forensic investigation, credit reports, PR, notification, etc.*
Media liability: Organization *liability for website content.*
Network interruption: *loss of net income , increased operating costs from material interruption.*
Privacy event: *failure to protect confidential info (i.e. e/data or other-paper)*
Regulatory proceeding: request for info, civil investigation, etc.. brought by Gov't agency.
Security/privacy liability: Organization *liability for damages from breach of confidential info.*

Quote Number	1	2
General Conditions	**Insurer ABC**	**Insurer XYZ**
Quote date	**Valid until 9/3/14**	**Valid until 8/15/14**
Coverage Type	Cyber/privacy	Cyber/privacy
Named Insured	ACME OPTIMAL ORGANIZATION	ACME OPTIMAL ORGANIZATION
Retro date	Policy inception	Policy inception
Overall Limit	**$10,000,000 shared/aggregate**	**$10,000,000 shared/aggregate**
Defense inside/outside limit	Inside	Inside
Regulatory Proceeding	**$10,000,000**	**$10,000,000**
Security/Privacy liability	**$10,000,000**	**$10,000,000**
Digital asset loss	None-need to determine exposure	None-need to determine exposure
Event/breach mgmt costs	**$10,000,000**	**$10,000,000**
Network Interruption *	**$10,000,000**	**$10,000,000**
Cyber extortion	**$10,000,000**	**$10,000,000**
Internet media liability	**May not be needed**	**May not be needed**
Retention-unless stated	**$5,000**	**$500,000**
Regulatory Proceeding	**$5,000**	**$1,000,000**
Network Interruption	**24 hours**	**12 hours/$500,000**
Annual Premium	**$xx,xxx**	**$xx,xxx**
Surplus lines tax and fees	**$x,xxx**	None-admitted insurer
Total annual cost	**$xx,xxx**	**$xx,xxx**
Material Subjectivities	Complete specific insurer app	Complete specific insurer app
Material Subjectivities	**Confirm compliance/HIPPAA, other**	N/A
Policy Form Review	**Policy Form Review**	**Policy Form Review**
General Conditions	Claims-made and reported	Claims-made and reported
Advance notice of cancellation	**Only if premium not paid**	**Only if premium not paid**
ERP/Tail-auto	125% AP-1 yr; 200%-2 yr; *	**1-100%, 2-175%; 3-200%, 6yr-neg**
Territory	Worldwide	Worldwide
NI may waive right of recovery	**No release allowed**	**Prior to loss in writing**
Definition of Insured	NI, D&O, Ee, written-AI	NI, D&O, Ee, written-AI
Confidential info-paper/e-data	Personal info in "any form"	Personal info in "any form"
Security failure/Privacy Event	failure to protect confidential info	failure to protect confidential info
Defense	Duty and right to defend	Duty and right to defend
Hammer clause	50%	50%
Settlement authority	**Silent**	**Insurer with consent of Insured**
Attorney chosen by insurer	**NI subject to insurer consent**	**Yes. NI may have option**
Loss include punitive, exemplary	**Yes unless prohibited by law**	**Yes unless prohibited by law**
Regulatory Proceeding	gov't proceeding, etc.	gov't proceeding, etc.
Broad def of "personal" info	Yes	Yes
3rd party contractor negligence	**Yes**	**Yes: "Information Holder"**
Event management	Costs from security/privacy event	Costs from security/privacy event
Covered loss	PR, 3rd party notice, credit reports	PR, notice and credit reports, e-data restore
Event costs	**No time limitation to report costs**	Events costs needed 90 days
Network Interruption	loss of profits/inc expenses	loss of profits/inc expenses
Limited-if any exposure	**Remove for premium credit?**	**Remove for premium credit?**
Cyber Extortion	funds for security/privacy threat	funds for security/privacy threat
Security threat	Threat/attack own/used computers	Threat/attack own/used computers
Privacy threat	threat to release confidential info	threat to release confidential info
Terrorism-included or excluded	**Excluded**	**No exclusion**
Professional services excluded	**Professional services exclusion**	**No exclusion**
ERP/Tail-auto-London Excess	**Not FF-less broad than primary**	N/A

Step 6: Review Cyber/Privacy Coverage Proposals

The insurance proposals, specimen insurance policies, and spreadsheet analysis should be reviewed together with the appropriate personnel of the organization. An objective decision to purchase cyber/privacy coverage can be reached after all cyber/privacy insurance documents are reviewed and, most important, understood.

Conclusion

A thoughtful and careful approach to understanding cyber/privacy exposures and coverage will allow a risk management professional to have a better understanding of coverage needed for his or her organization. The process outlined in this article can be easily adapted to other types of exposures and coverage analysis.

To view this article at IRIM.com please follow this link:http://www.irmi.com/expert/articles/2014/austin10-commercial-property-insurance.aspx

---

William K. Austin, CRIS is co-founder and principal of Austin & Stanovich Risk Managers, LLC, a risk management and insurance advisory consulting firm specializing in all aspects of commercial insurance and risk management, providing risk management and insurance solutions, not insurance sales. Services include fee based "rent-a-risk manager" outsourcing, expert witness and litigation support and technical support to insurance companies, agents and brokers.

Contact William K. Austin
401-751-2644
wkaustin@austinstanovich.com.
www.austinstanovich.com.
