AIG netAdvantage®

Security Liability Endorsement for Independent Agents and Brokers

Think you're protected from hackers and viruses? Think again.

A Growing Risk to Your Business

The advent of the Internet has created enormous business opportunities: exciting new ways to contact customers, efficient new ways to store information…and serious new threats to contend with.

Network security is a substantial and growing concern for every business – especially yours. Hackers or a computer virus could shut down your operations. Even more dangerous, sensitive customer information in your protection could be stolen, corrupted, or even deleted by a third party.

Who would pay the cost? (Not your first-party business interruption insurance. Not necessarily your professional liability insurance.) *And whose business would suffer the consequences of adverse publicity from a high profile claim?* The answer to both questions is likely you.

AIG Small Business Has a Solution

AIG Small Business's netAdvantage Security Liability Endorsement was crafted to meet the needs of insurance agents and brokers, providing third party coverage for claims resulting in liability arising out of an external computer attack that occurs because of failure of your network security.

Insurance agents and brokers face inherent risks to business operations which may not be covered under traditional professional liability or business interruption policies. If you can answer "yes" to any of these questions, you need to consider this coverage:

- Do you conduct business through online communication?
- Do you send or store sensitive customer data in your computer systems or network?
- Do you send or store or confidential information in your computer systems or network?
- Do you have a web site?

AIG® AIG Small Business®

AIG netAdvantage

Security Liability Endorsement Meets An Ever-Expanding Array of Risks

With increased reliance on electronic data stored on computer networks, the threat of litigation arising out of security breaches is too significant to ignore. Consider the potential liability resulting from computer attack that occurs because of a failure in of network security:

- **Invasion of privacy –** unauthorized disclosure of personal and confidential financial or medical information
- **Identity Theft –** misappropriation of personal data used for fraudulent purposes
- **Transmission of Malicious Code –** corruption of a third party's electronic data or system failure resulting from a computer virus sent by your employee
- **Denial of service –** failure of your system to thwart a denial of service attack, preventing your customers from accessing your network

Since your customers trust you with sensitive personal and financial information, they hold you responsible to protect their data. If you store credit card information, banking information, Social Security numbers, or other identifying information on your customers, in the event of failure of security that exposes this information, your customers will likely try to hold you accountable.

With the ***netAdvantage Security Liability Endorsement***, you position your business – and yourself – to address this liability risk head on.

The fact is, your customers are at risk, your business is at risk, your assets are at risk.

netAdvantage Security Liability Endorsement Provides Coverage your Business Needs and your Customers Demand

Now, you can protect your business from claims resulting from wrongful acts that result in a failure of security. Specific liability risks we cover that can arise out of failure of security include:

- Identity theft
- Malicious codes (viruses, Trojan horses, worms, and others)
- Denial of service attacks

…and other failures of security that corrupt, destroy, steal, or otherwise compromise your data.

The liability exposures created by your computer network and Web site are too serious to ignore. Let AIG Small Business help you address this risk.

For more information about our netAdvantage Security Liability Endorsement and how it can help protect your business, contact AIG Small Business today at 877-TO-SERVE (1-877-867-3783), or email us at ToServe@aig.com

Insurance underwritten by member companies of American International Group, Inc. The description herein is a summary only. It does not include all terms, conditions and exclusions of the policy described. Please refer to the actual policy for complete details of coverage and exclusions. Coverage may not be available in all states. Issuance of coverage is subject to underwriting. Non-insurance products may be provided through independent third-parties.

Developed in conjunction with AIG Product Development.

AIG® AIG Small Business®

AIG

AMERICAN INTERNATIONAL COMPANIES ®

Name of Insurance Company
To Which Application is Made:_____
(herein called the Insurer)

Network Security Supplemental Application

Name of Applicant: _____
(As used herein, Applicant includes the Applicant and its subsidiaries also seeking coverage).

If more space is needed to provide complete answers, please attach a separate document to this application .

1. Does Applicant have a virus protection program in place?	☐ Yes ☐ No If "Yes," please identify the software used:
2. Does Applicant have a firewall in place?	☐ Yes ☐ No If "Yes," please identify the firewall used:
3. Does Applicant enforce a software update process, including updating patches and anti-virus software?	☐ Yes ☐ No
4. Does Applicant have a process for managing computer accounts, including removing computer users in a timely fashion?	☐ Yes ☐ No
5. Do Applicant's access control procedures address access to critical and sensitive computer systems?	☐ Yes ☐ No
6. Does Applicant have physical security controls in place to control access to your computer systems?	☐ Yes ☐ No
7. Does Applicant have an information security incident response plan in place?	☐ Yes ☐ No
8. How long does it take to restore Applicant's operations after a computer attack or other loss/corruption of data?	☐ 12 hours or less ☐ 12-24 hours ☐ More than 24 hours
9. Does Applicant have person or group responsible for information security?	☐ Yes ☐ No
10. Does Applicant use standard configurations for firewalls, routers, and operating systems	☐ Yes ☐ No
11. Does Applicant have a program in place to periodically test security controls?	☐ Yes ☐ No If, "Yes," has your Company undergone any information security or privacy compliance evaluation? ☐ Yes ☐ No If, "Yes," please identify the type of evaluation, when it last took place, and whether your Company was found to be in compliance:
12. Does Applicant outsource any aspect of: (i) its computer system/network (i.e., hosting, back up site, etc); or (ii) its information security (i.e., intrusion detection, firewall, etc)	(i) ☐ Yes ☐ No (ii) ☐ Yes ☐ No If Yes to either (i) or (ii), please identify the principal vendor(s) (i) (ii)
13. During the past 3 years, has Applicant ever received a complaint concerning the security of its computer system or website?	☐ Yes ☐ No
14. During the past 3 years, has Applicant suffered any loss under a Commercial Crime or Dishonesty bond/policy?	☐ Yes ☐ No

15. During the past 3 years, has Applicant experienced any loss of service exceeding 8 hours (excluding any planned maintenance of its computer systems)?	☐ Yes ☐ No
16. During the past 3 years, has Applicant suffered any breaches of security causing damage to your computer systems?	☐ Yes ☐ No

BY SIGNING BELOW, THE UNDERSIGNED DULY AUTHORIZED REPRESENTATIVE OF THE COMPANY STATES AND REPRESENTS THAT THE INFORMATION FURNISHED IN THIS APPLICATION IS COMPLETE, TRUE AND CORRECT. ANY MISREPRESENTATION, OMISSION, CONCEALMENT OR INCORRECT STATEMENT IN THIS APPLICATION OR ATTACHMENT, SHALL BE GROUNDS FOR THE RESCISSION OF ANY POLICY ISSUED. SHOULD INSURER ISSUE A POLICY, COMPANY AGREES THAT SUCH POLICY IS ISSUED IN RELIANCE UPON THE TRUTH, COMPLETENESS, AND ACCURACY OF THE STATEMENTS AND REPRESENTATIONS IN THIS APPLICATION OR ATTACHMENT, AND SUCH APPLICATION IS THE BASIS OF SUCH POLICY, AND WILL BE ATTACHED TO AN BECOME PART OF SUCH POLICY.

THE UNDERSIGNED, HEREBY AGREES AND REPRESENTS THAT HE OR SHE IS A DULY AUTHORIZED REPRESENTATIVE OF THE APPLICANT, AND IS FULLY AUTHORIZED TO ANSWER AND MAKE STATEMENTS AND REPRESENTATIONS BY AND ON BEHALF OF THE APPLICANT.

Signed: _____ Date: _____

Print Name & Title: _____ Company: _____

Broker: _____

Address: _____

_____

Protecting Clients From Cyber Risk

By MEREDITH PEARL • Palmer & Cay / Atlanta, Georgia

Increasingly, we are being asked to talk to clients about the exposures created by their computer networks and Web sites.

THE RISE of the Internet has led to the creation of entire new types of businesses and has given tremendous new tools to others. But along with the new capabilities have come new loss exposures, which both insurers and insureds are still learning about.

At Palmer & Cay, a major regional broker, we believe that the risks the Internet poses to our clients are too great for them or us to ignore. We also believe that by helping our clients address them, we can become involved in an insurance market that, while still in its infancy, has significant potential for growth. In this article, I'll discuss how Palmer & Cay has structured its operations to help its clients deal with cyber exposures and how it works with the markets to arrange coverage.

I am an assistant vice president within a unit of Palmer & Cay called Executive Liability Advisors. ELA specializes in all executive liability products, including directors and officers liability, errors & omissions and crime insurance. ELA works with all Palmer & Cay producers and clients and provides various services such as consulting and claims advocacy.

Increasingly, Palmer & Cay producers are asking us to talk to their clients about the exposures created by their computer networks and Web sites, and about the cyber insurance policies that have been developed to respond to them. Among those that have been buying, or at least expressing interest, in such coverage are banks and other financial institutions, application service providers, Internet service providers, health-

care pro-viders and online retailers.

Network security is a major concern with many of these clients. A hacker or computer virus could shut down their systems or Web sites, creating a significant business income loss. Typically, standard BI policies do not respond to such losses because there is no damage to tangible property—just the intangible programs and data that reside in the networks. One can obtain cyber insurance policies that cover this BI exposure. Of perhaps even greater concern, especially for businesses that store sensitive customer information in their networks or on their Web sites, is the theft of such data by third parties. Litigation arising from such incidents can be covered by a properly written cyber insurance policy. Lawsuits arising from denial-of-service attacks, which can prevent clients of application service providers from accessing their programs and data, also can be covered by cyber insurance. Additional coverage enhancements can be added to a policy, providing insurance for such risks as information technology E&O or personal-injury exposures—libel and slander, copyright or trademark infringement, etc.—arising from the operation of a Web site.

Palmer & Cay producers typically arrange for ELA to interact with their clients via conference calls or face-to-face meetings. Generally, we talk with a financial officer or a risk manager. In some cases, our discussions might be with the CEO. To get a quick idea of whether clients are good prospects for cyber insurance, we ask whether they store Social Security numbers, credit-card numbers, benefit-plan information or other sensitive data in their networks or on their Web sites. A second qualifying question is, How much of your revenue is derived from Internet operations? If the answer is 50% or more, cyber insurance definitely should be considered.

During initial meetings, we also talk with clients about their security practices. What sort of "firewalls" do they have protecting their networks? How often are they updated? What sort of procedures (passwords, etc.) do they follow to limit system access to authorized employees? What sort of privacy policies do they have? What kind of antivirus products are they using? What provisions are there for system backup and recovery?

Meredith Pearl is an assistant vice president in the Executive Liability Advisors unit of Palmer & Cay, a major regional insurance broker. Ms. Pearl began her insurance career in 1994 as a professional liability underwriter at National Union Fire Insurance Co., part of American International Group. She also worked for Chubb and Royal & SunAlliance prior to joining Palmer & Cay at the beginning of 2003.

Another important function of this initial call is simply to educate clients. We discuss cyber insurance exposures in general and talk about the policies that have been developed to insure them. We point out large cyber-insurance gaps in standard property and general liability policies and explain that insurers do not intend to cover such exposures in those products.

When clients decide to pursue coverage, the next step is to have them complete an application. These forms are quite detailed and generally require the input of someone from the client's technology department. Depending on the coverage requested, other information may be required, such as copies of contracts that businesses like application service providers, Internet service providers or information technology consultants enter into with their clients or vendors. Naturally, underwriters will want the URLs of any Web sites used for e-commerce.

With a completed application, we can obtain indications from most markets; but before we can bind coverage, clients also will have to undergo a security assessment. For large clients or those with complicated risks, like financial institutions, an onsite security analysis usually is required. Some insurers will arrange for the analysis at no charge, depending on the account, but some clients may have to pay for these assessments themselves.

Clients with less complicated cyber risks typically can complete an online assessment rather than undergo a full-blown security audit. The client answers a series of questions about its security procedures, and a computer grades the answers. The insurer sends us the results, informing us whether the client is eligible for coverage.

For those clients who do not "pass" an online assessment, insurers send us recommendations for bringing their systems and procedures into compliance with their requirements. We review these recommendations with clients and may help them obtain outside assistance, if needed, to implement them.

Our markets for cyber insurance include American International Group's eBusiness Risk Solutions, Zurich, ACE and London. Our underwriters and we often make joint presentations to clients.

Once we have received indications from our markets, we present the various options to our clients. We also answer any questions the client may have. Among the more typical ones are "what-if" questions involving losses arising from ex-employees who hack into a client's system. Typically, we respond by going through various scenarios that explain when a loss involving a current or former employee might be covered by a cyber insurance policy and when coverage is more likely to be found under another product, like crime insurance.

Cyber insurance is still a relatively new product. Most policies have been developed only within the last four years, and few buyers really are aware of them. Buyers typically do not comprehend the cyber exposures they face, nor do they realize they probably have little coverage for them under their current policies. Hence, education is a key component of the sales process.

In some ways, today's cyber insurance market is like the employment practices liability market was during its early years. At first, few businesses bought EPLI, but sales increased as businesses learned more about the product and read about a number of high-profile claims.

We're finding that cyber insurance is definitely picking up momentum as our clients increasingly become aware of how much they rely on their networks and Web-based business and communication systems—and how much liability those assets also create for them. When they're ready to seek protection for those assets (and from those liabilities), we're ready to help.