By Susan Greitz

Cyber Liability- Are You at Risk?

Online hackers and viruses number in the thousands and are a faceless threat 24 hours a day, seven days a week. That threat is also growing on a global scale. The challenge is that technology changes every single day and cyber threats are right behind, working overtime to keep up, or in some cases, staying ahead of those changes. These threats come in many different forms and can involve your e-business; the Internet; networks and informational assets. Look at the list below; if you answer yes to any of the following questions, you need to speak to your insurance agent about Cyber Liability protection.

1. Do you hold any client, vendor, employee or others private data?
2. Are you aware of the notice requirements in each state if you lose control of that data?
3. What steps would you take/who would you call if you lost those private records?
4. Do you have a corporate wide privacy policy?
5. Do you have a disaster plan specific to data breaches?
6. Are your records stored electronically? Are they on paper? Are the records secure? Do you shred old information?
7. Do any employees have access to private client records? Do you allow use of USB drives on computers with access to private data?
8. Are any records ever handled by a third party?
9. Are all of your laptops and wireless connections encrypted?
10. Are you confident your antivirus and firewall systems are 100% effective?
11. Have any of your systems been programmed by non-employees?
12. How would your clients respond if you lost their private records?
13. If your network was damaged or disabled by a virus or hacker attack, would it be material to your revenues/income? Do you have a backup system? How long would it take you to recover?

What kind of risks do you face? Consider direct loss because of 'injury' to electronic data or systems resulting from acts of others. There is also liability for financial losses or costs sustained by other resulting from internet or other electronic activities. These losses include theft of data, loss of future income, the cost of fixing the problem, expenses to protect customers, defense expenses and damages resulting from customer suits and suits from others. There are also expenses to comply with all federal and state notification requirements.

Examples of possible cyber claims:

- **Privacy** – An online retailer attempted to sell its customers' personal information to pay creditors as part of the retailer's bankruptcy. The retailer's privacy policy had stated that personally identifiable information would not be sold. Several parties threatened to sue.
- **Privacy & Security** – A hacker infiltrated an online shopping website and stole 300,000 customer credit card numbers. The website faced claims from the customers for unauthorized charges made on the credit cards.
- **Security** – Companies that unknowingly spread a worm, virus, or other corrupting file via email to third parties could face liability from those third parties for revenues lost as a result of the virus overloading the third parties' computer network.
- **Media/Content** – A pathologist posted a message on a bulletin board accusing another university affiliated doctor of receiving kickbacks from an outside company in exchange for his assistance with the company's efforts to obtain a contract to provide pathology services to the university. The university doctor sued, and a jury awarded him $675,000.
- **Intellectual Property** – A business that used a competitor's trademarked name as a metatag on the business website was sued by the competitor for trademark infringement and unfair competition.

When considering a cyber insurance policy, make sure it includes the following:

- Duty to defend
- Paper and electronic records
- Medical, personal, financial and corporate private information
- Notification costs, credit monitoring and other pre-claim expenses
- Check whether voluntary credit monitoring costs are included
- Fines and penalties, where insurable, including HIPAA
- Network security – hackers, virus, employee sabotage; damage to 3rd parties data/networks
- Check exclusions – safeguard exclusions; intentional acts of employees; Insured vs. Insured – are employee claims covered?

To control the risk of cyber threats, it's vital that your company have stringent policies in place regarding privacy, information security and employee computer usage. Employee training on a regular basis is also important. The technical security controls on your systems must be constantly monitored and updated – access controls, firewalls, passwords, encryption, and antivirus software. Finally, your company needs to have an Incident Response plan in place in the event that all precautions fail.