A/E RISK REVIEW

A PUBLICATION OF THE PROFESSIONAL LIABILITY AGENTS NETWORK

Cyber Liability Prevention and Protection

This material is provided for informational purposes only. Before taking any action that could have legal or other important consequences, confer with a qualified professional who can provide guidance that considers your unique circumstances.

No one needs to convince you of the benefits of advanced technology to the design industry. Computers, design software, the Internet and now a plethora of mobile devices and applications enable design firms to provide their clients with more services and greater speed, accuracy and creativity in design.

With such benefits, however, come liabilities. The Internet provides gateways for outsiders and employees to gain access to company data. That data includes confidential and otherwise sensitive information regarding your company, your employees, your vendors and your clients.

Sophisticated hackers as well as disgruntled employees can gain access to that information with malicious intent. Laptops containing sensitive files can be stolen. Through the Internet, intruders can steal, alter or damage vital information, access financial accounts and credit card information, engage in identity theft and so on. As companies move to wireless networks and "cloud" technology, as they embrace social media and have more and more information stored outside of company servers and accessible through the Web, the threat only grows.

Should you be a victim of a cyber crime, losses can be substantial. According to a 2010 study by Ponemon Institute, the average organizational cost of a data breach is $7.2 million, or $214 per compromised record. And these numbers are on the rise.

If your data is damaged or destroyed, intentionally or unintentionally, valuable work may be lost and must be re-created. If intruders gain access to sensitive employee or client information, you may face lawsuits, a damaged reputation and lost business. Then there are the costs of contacting all potentially damaged parties to alert them that their information may have been compromised as well as possible fines and penalties if you were not following prescribed state and federal laws regarding protecting sensitive data of others.

Cyber liability goes beyond stolen or lost data. For instance, if an employee posts false and damaging information about a competitor on your Website, your company may face a charge of libel or slander. Likewise, an overzealous claim on your Website about the quality of your company's services may raise your standard of care and lead to an E&O claim from a dissatisfied client.

To limit cyber liability and data loss requires a two-pronged approach. First, implement policies and practices that reduce the chances of cyber losses and limit the damages should a breach of security or other liability occur. Second, have adequate insurance coverage in the event you are a victim of a cyber liability and your employees, your vendors or your clients claim losses due to company actions.

Company Policies and Procedures

Every company should establish and enforce cyber security policies. Identify the major types of critical information contained in your computer system and what safeguards are in place to protect them. Classify this data according to usage and sensitivity. Limit employee access to important files on a need-to-know basis. Set policies for the use of the Internet and email on company equipment and premises.

FOR MORE INFORMATION CONTACT:

Alexander & Sanders
YOUR PARTNER IN PRACTICE

4610 Bluebonnet Blvd. #A
Baton Rouge, LA 70809
Phone: 225-295-2995
Email: info@alexsand.com

Prohibit employees from downloading unauthorized software on company equipment. Limit who has authority to post information on the company Website or social media.
One often overlooked source of liability is the company photocopier. Copiers that are networked via the company's computer system are particularly vulnerable if sensitive documents are stored in their hard drives.

Make sure all company computers have up-to-date anti-virus software. Enforce a password protection policy and ensure all ID and password combinations are regularly updated. Make sure access to company computers and networks are denied as soon as an employee quits or is terminated from employment. Update vital passwords immediately.

Inventory and account for all company computers and software. Set policies limiting the types of files that can be stored on laptops, flash drives, discs and mobile devices that regularly leave the premises. Identity information is especially sensitive and should be safeguarded in the company network. Make sure software licensing agreements are enforced.

Use battery backup systems and surge protectors to protect against electrical problems. Regularly back up data, preferably to a secure offsite location.

Establish an emergency response plan in the event of lost or stolen data. Include employee procedures for computer operations after a data loss incident occurs. This will greatly improve the chances of recovery.

Have your IT staff regularly test your security measures and review log files looking for signs of attempts to breach your network. They should ensure all backup systems are operating according to plan.

Consider having an outside IT consultant perform a security audit on your offices. They can help you develop a sound security plan that can substantially lessen the chances of a security breach by outside hackers and inside workers.

Cyber Insurance

No cyber security plan can eliminate all liability risks. Fortunately, there are now insurance products that specifically cover cyber risks. Cyber liability policies cover both third parties (your clients and vendors, for example) and first parties (your company). Specific policy provisions will differ with each insurance company offering such coverage, but they typically include:

Network and Data Security. This covers damages to third parties due to compromised identity or financial information, privacy leaks, transmission of computer viruses, blocked access or "denial of service" for authorized users, and failure to notify third parties of a security breach (where required by law). Many policies also cover paper documents as part of data security.

Electronic Media Liability. This covers damages from personal injury, domain infringement, copyright violation, and similar claims due to information published on a company Website or via email or social media.

Security Breach Remediation and Notification Expense. Costs covered include forensic and legal fees incurred to determine whose information was affected, the cost of notifying those parties, establishing a call center for third party inquiries and credit monitoring.

Computer Program and Electronic Data Restoration Expenses. This coverage applies to expenses incurred to restore your data and equipment lost or damaged due to a computer virus, rogue employee theft, or hackers.

Computer and Fund Transfer Fraud. Policies cover your direct loss of funds, securities or other property due to someone gaining unauthorized access to your computer system.

Extortion. This covers costs incurred due to a credible threat from a third party to destroy your data or computer system, disclose third-party information, etc.

Regulatory Defense Expenses. This coverage applies to any fines imposed as a result of your company violating government rules regarding identity protection and security of third-party information.

Public Relations Expenses. Such coverage offsets costs you incur for PR services needed to mitigate negative publicity due to cyber liability.

Business Interruption and Extra Expense. This covers income lost and expenses incurred due to a disruption of your computer operations.

Let Us Be of Help

Again, each cyber liability policy will differ in terms of coverages and exclusions. We'll be happy to help you explore options and design a complete commercial, professional and cyber insurance package that meets your specific needs.

We may be able to help you by providing referrals to consultants, and by providing guidance relative to insurance issues, and even to certain preventives, from construction observation through the development and application of sound human resources management policies and procedures. Please call on us for assistance. We're a member of the Professional Liability Agents Network (PLAN). **We're here to help.**