

Insuring Technology Risks in a Professional Environment

A White Paper Prepared for the Professional Liability Committee of the National Society of Professional Engineers

Victor O. Schinnerer & Company, Inc.

Two Wisconsin Circle
Chevy Chase, Maryland 20815
301/961-9800

Email: vos.info@Schinnerer.com
Web: www.Schinnerer.com

Table of Contents

Executive Summary

Consulting professional engineers and other construction-related professional services firms have seen their internal management practices and project delivery procedures change significantly because of their escalating reliance on software and digital communication and production devices. Many firms have incorporated technological advances into their operations, ranging from email to parametric modeling software. Some, however, have not fully understood the business and professional exposures intrinsic in digital practice. Other firms have been hesitant to pursue the commercial and technical advantages emerging or now available because of their apprehensions—often unfounded—about increases in their professional liability exposure and business risk.

Construction-related professional services firms have unprecedented opportunities to increase their profitability, level of service, status in the marketplace, and support for their clients and the public good when they recognize how digital practice might change their risk profile and act to properly manage and insure their exposures. Victor O. Schinnerer & Company, Inc. has been working to identify risks, clarify existing coverage, and develop new insurance products to assist firms in their risk management efforts.

Professional and Technological Exposure Issues Intrinsic in Engineering Practice

Although the coverage provided by professional liability insurance is fairly well-defined through policy language and court decisions, many technology-based exposures faced by professional services firms are less well-defined and therefore often more challenging to cover. Professional liability exposures are only one small part of a spectrum of risk confronted by firms using electronic communication tools and systems.

While professional liability insurance does cover broadly defined design services, regardless of the means of communication or the form of the instruments of service, (and in the Schinnerer program includes coverage for harm caused by negligently devised project-specific software) it is not meant to cover general technology-

based risks. Such business risks might include lost data, virus corruption, or general software glitches. Professional liability insurance also does not cover personal injury exposures such as defamation or harassment not related to professional services, confidentiality and security violations in the sharing of personal information, the destruction caused by disasters, or the resultant cost of recovery efforts.

Major Types of Risk Related to Technology

There are exposures and risks created or exacerbated by the use of technology that are not inherent in the performance of professional services.

There are exposures and risks created or exacerbated by the use of technology that are not inherent in the performance of professional services. Managing these exposures—and, when possible, insuring against their effect—is prudent for all types of firms, but is especially important for professional services firms where their consequences can significantly impact both operations and reputation.

Technology opens firms to risks associated with the corruption of data, hacking, unauthorized access to information on an accessible network or website, and catastrophic data losses. Such exposures require specialty insurance in addition to standard insurance policies to properly address the risks involved.

Violation of Security or Confidentiality Interests

Any breach in the security of electronic communications can result in significant exposure to the entity that failed in a duty to prevent it. All parties are entitled to expect that others will take reasonable measures to secure private or confidential data in transmission and while stored. Safeguards on systems such as networks or websites exist to allow only authorized access. In addition to the expectation of security for shared information, there is an expectation that a party's private information will not be accessed, misused, or divulged to unintended recipients.

Unauthorized Access to Information

As information is shared over the Internet prevention of unauthorized access is vital. Protecting a server is essential, but even if a server is well-protected there can be other sources of vulnerability, including the desktop or notebook computers of

people inside or outside the company who might have legitimate access to the server. For engineering and other professional services firms, remote access through personal notebook computers from residences or alternative work sites can result in vulnerability if the access is not through a secured network such as a virtual private network (VPN). While the distinguishing characteristic of a VPN is not security, by channeling communications through a secure network, the likelihood of vulnerability is reduced. Obviously, these are exposures entirely separate from the provision of professional services.

Malevolent Software and Virus Distribution Exposures

Communications technology and the use of the Internet have dramatically increased the vulnerability of computer networks to hazards such as viruses, which are capable of spreading rapidly and causing widespread and substantial damage to data, software, and equipment. The proliferation of malevolent software creates an exposure to legal liability not only for the virus author and the intentional transmitter of a virus, but also for parties who inadvertently transmit a virus. An example of the latter would be someone who unwittingly forwards an infected attachment in a routine email transmission. A civil action against an inadvertent transmitter would most likely be pursued under a negligence theory, but it is clear that such negligence is related to furnishing professional services.

A civil action against an inadvertent transmitter would most likely be pursued under a negligence theory, but it is clear that such negligence is directly related to furnishing professional services.

Direct economic damages can be caused when a virus destroys or alters a file or information in the file. In these situations the consequences may be unforeseen and the economic damage considerable. The destruction of data always causes economic damage, even if the destroyed data can be replaced by secured copies.

Cyber Extortion

Cyber extortion involves a threat whereby one party threatens some type of "cyber" or electronic consequence unless the party is compensated in some fashion, usually with money. Cyber extortion can include a denial of service attack, theft of confidential data, or defacement of a website. A more recent variation is an attack that locks up or encrypts site data; the goal being access to the site's information in order to have users pay for its release.

Breaches in security are usually addressed by using a firewall

program as well as software that protects against malicious code such as viruses, worms, Trojan horses, spyware, etc. A website host facing a serious infection may have to endure a costly response effort and security audit. Defense of the system means isolating the compromised computer servers and restoring operations through a back-up system.

A malicious hacker altering code may not be attempting cyber extortion but rather simply trying to disrupt activity. In its simplest form, a denial of service attack is an attack against any system component that attempts to force that component to limit or even halt normal services. It may be as simple as flooding a website or network with phony inquiries or activities that overload the server, causing it to slow significantly or crash. Such an attack may be directed at a specific computer operating system, a specific port of service on a targeted system, a network or network component, a firewall, or any other system component. The key similarity in all of these examples is that, after a successful attack, the system does not respond to a request for service as before, and some expected service (or group of services) is denied or limited to authorized users.

Loss of Intellectual Property, Trade Secrets, or Confidentiality

The law on the ownership and use of intellectual property is in transition. As information is shared electronically, issues such as copyright, ownership, use, and the nature of trade secrets present challenges. While it is clear that a party has rights to its trade secrets and other confidential information, it is unclear what the U.S. legal system considers as necessary steps to protect such information and the liability of those who inadvertently release it.

Parties can be harmed by the release of confidential information, and in many cases, that harm cannot be rectified by ending access to the information or even by compensation for the harm. The party that has the care, custody, and control of confidential information owned by or shared in by others may have significant liability if that information is improperly disclosed or if unauthorized access to that information occurs.

A shared website such as a File Transfer Protocol (FTP) site or a building information model may contain confidential client information or trade secret information that rightfully belongs to the client or others in the collaborative process. In addition, the security interests of the project client may be compromised by the

intentional or inadvertent dissemination of design or construction information. Information broadly circulated in a collaborative team effort and emerging as the client-demanded project delivery method may jeopardize the current legal protections for confidential information and trade secrets, and may put the parties at risk for security breaches of both intellectual and physical property.

Website Hosting and Network Security

The safety of data and the confidentiality of client information is especially critical if a firm has added hosting of a project-related website to its services. Firms providing the hosting server need to be aware of and utilize reasonable security measures to enhance the safety of data stored on their network. Various software programs for scanning systems and networks for obtrusive invaders, spammers, malicious hackers, and other harmful problems are basic to the responsibility of website hosting and network security.

When a firm hosts a website such as a secure FTP site established for limited use by certain clients and other expressly authorized users, it must use proper procedures and communicate appropriate disclaimers to limit its risk. These actions include the authentication of user credentials—through appropriate levels of user identification and passwords—to ensure data integrity and to isolate appropriate access. This includes managing the system that provides parties with usernames and passwords to allow them to add, update, or delete electronic files. While the host does not guarantee and makes no warranties with respect to the authenticity of posted files, the additional exposure increases a firm's exposure well beyond professional liability. Having all authorized users agree to share data and to do so in a good-faith manner consistent with professional business practices does not preclude liability for improper access or use.

While website hosting may provide additional revenue, the obligations of network security create significant challenges to firms not normally operating as a commercial website entity.

While website hosting may provide additional revenue, the obligations of network security create significant challenges to firms not normally operating as a commercial website entity. Construction-related professional services firms may be capable of providing this undertaking and may wish to do so as a new business opportunity: a method of using excess server capacity or as a means of controlling the process and responding to the needs and concerns of a client. Firms performing such technology-related

services should develop a hosting agreement spelling out the contractual obligations of each party, including levels of security provided, and the responsibilities of each party with respect to not sharing user names or passwords with others. All users must agree to maintain some common level of network security measures. The hosting of a shared website, however, is not a service envisioned in the scope of coverage of construction-related professional liability insurance. Website hosting requires additional insurance coverages and management commitments.

Invasions of Personal Rights through Electronic Communications

The term defamation refers to a false statement made about someone or some organization that is damaging to their reputation. Defamation can take the form of libel when it is written or electronically transmitted. For a statement to be defamatory, it must be published to a third party through direct communication, such as email, or in a distributed communication source, such as a chat room or open communication system on a shared website. Furthermore, the person publishing the statement must have known or should have known that the statement was false. While email or a project website can provide a new context in which a defaming statement can be made and published, there is liability not only for the party creating the defamatory statement but also for the service provider. If a false, reputation-damaging statement is made by any user of a computer-based communication and documentation system, the statement may be found to constitute defamation.

The right to privacy can also be breached by the disclosure of information that is not necessarily untrue, but its publicity causes emotional distress or financial damages, and is confidential or private.

Courts usually determine whether an entity hosting a web-based communications system was a "distributor" of information or a "publisher" of information. As a distributor acting only as a conduit for information, a hosting entity may not be liable for the statement. However, a distributor who purports to monitor or control content has a higher level of responsibility—with the agreement to monitor or control comes the liability for the content, even if the distributor did not create the content. In contrast, if considered a publisher (with greater control over the content), the hosting entity might indeed be liable. A hosting entity may be able

to avoid liability if it did not know about a defaming statement or if it had no reason to know about the statement. If a distributor knows about a defaming statement and continues to distribute the information, liability is not as easily avoided.

The exposure of the publisher or distributor of recognized defamation may extend to liability for actions of an employee transmitting information from a personal computer that is not controlled or protected by the corporate network security.

Liability for Data Loss from Natural or Created Disasters

Basic to any digital information system is information redundancy. This may mitigate the harm that can be created by uncontrollable forces. But back-up systems that are not current with the constantly changing information common to interoperability may create an additional problem of having to establish or recreate current data sets.

Natural disasters such as hurricanes, earthquakes, or floods may affect not only the primary, shared database of project information, but also the redundant information. This could cause additional project costs or delays that could be characterized as foreseeable. A vector as basic as a power disruption—whether an undefended power surge or an unanticipated power failure—could create significant economic losses to others in the design and construction system, as well as to the project client.

To protect both archival files and projects in progress, firms need to have a comprehensive disaster plan and vital records program. Protecting the physical media on which electronic files are stored is one component of the preservation of electronic records. Many firms accomplish this by creating at least two copies of the storage media, one of which is stored off-site in a controlled storage area. Establishing off-site storage of vital digital files and other valuable records is one step in a disaster plan. Contingency plans should address various types of disasters and appropriate measures that should be taken.

If a party is hosting the information, it must take adequate steps to protect data through an appropriate frequency and extent of system back-ups, and to insure against data loss or face possible liability for the ensuing losses.

Risk Management for Major Types of Business Risk Related to Technology

Business entities can and should be proactive in protecting their electronic communication systems such as their computer networks. Risk controls include the following procedures:

- ✓ Using updated anti-virus protection and threat notification systems
- ✓ Securely configuring firewalls and installing available security patches
- ✓ Establishing physical security such as locked server rooms
- ✓ Routinely backing up network information and storing it in a secure location
- ✓ Having a security policy in force for employees and consultants
- ✓ Establishing authentication via user names and passwords and procedures to manage user names and passwords properly
- ✓ Incorporating locking systems for inactive computers
- ✓ Developing and testing a disaster recovery plan

Exposures Specifically Related to Engineering Technology and Functions

Almost all firms now have exposures related to their normal software use, their reliance on email, and their use of a website for advertising or information sharing purposes.

It is important that professional engineers and others providing services through professional practices are aware that there are specific exposures related to their normal use of software and digital systems. Almost all firms now have exposures related to their normal software use, their reliance on email, and their use of a website for advertising or information sharing purposes. And now firms are seeing their internal operations and their contact with clients and others in the design and construction process being significantly changed through the developing use of building information modeling.

Software Malfunctions

Software is never perfect; defects may exist despite extensive testing efforts and may become more prominent as different software packages are rushed to market. Because of End User Licensing Agreements through which a software user often waives all rights of recovery, if errors in software cause economic loss to

the user, the injured party has no realistic remedy. The user's liability to other parties is not similarly limited, causing a liability gap if the errors cause defects in designs or deficiencies in plans or other deliverables. While professional engineers and others in the design process are no longer in the age where an ethical firm has to be able to "calculate by hand" to achieve the same results as generated by software use, the increased reliance—or overreliance—on advanced software packages may transfer significant risk from a software vendor to a user. The duty of the professional engineer to certify the technical adequacy of the design or evaluation by signing and sealing deliverables establishes a level of liability that prevents the professional engineer from placing blame on the "tools" used to develop or communicate the design or evaluation. The resulting design error is a covered professional service even though the cause of the error might be defective software. Software makers typically attempt to limit liability for consequential damages and lost profits as a result of defects in their software, so the risk falls on the firm using the software.

Email Exposures and Record Retention Challenges

Electronic research and communication is becoming a basic part of every engineering firm's daily operations. Despite the benefits of such technology, however, the improper use of electronic research and the dangers presented by the ease and casual attributes of email may not only deprive firms of important time, but can also subject them to significant liability.

The integration of electronic practice into the business context—from CADD to email to project-specific websites—presents new challenges and raises new concerns.

There are two major risks in any rapid communication system. First, email is easy to generate and distribute. Composing and sending out email messages is usually undertaken without the careful thought or prudent editing that characterize most professional written correspondence. Thus, comments and attachments can be distributed—and redistributed—without the sensible review that should precede any professional communication.

Second, email is rarely preserved properly. Email is rarely archived as carefully-crafted correspondence in project files. Another risk is that information an email sender thinks has been

deleted simply lies hidden in electronic form, ready to be brought out after a problem is identified.

The liability tied to improper email use can also have a significant impact on the operations of a firm in other ways. Case law has held employers liable for employee misuse of email in situations ranging from sexual harassment to copyright infringement. Internet access adds to the problem of uncontrolled email use. Downloading and distributing information from the Internet may not only subject a company to intellectual property disputes, but may also generate employment practices liability claims. Additionally, because of employer responsibility for the acts of employees, even employee statements in Internet chat rooms could be deemed to be employer-authorized. These statements may subject the employer to claims involving contract obligations, defamation, invasion of privacy, and infliction of emotional distress.

Successful firms need to create policies and office procedures that help employees take advantage of electronic communication to enhance productivity and increase firm profitability without generating undesireable liabilities.

With the availability of project-specific websites, email based project documentation systems, and Internet research capabilities, the use of electronic media will continue to accelerate. Firms that do not address the management problems inherent in such systems may find increased risk from many sources. Successful firms need to create policies and office procedures that help employees take advantage of electronic communication to enhance productivity and increase firm profitability without generating undesirable liabilities.

The exposures related to security and confidentiality, the introduction of viruses, torts such as defamation and invasion of privacy, and concerns about information retention all are manifest in email:

- **Viruses**: Destructive viruses often enter the workplace through emails that include attached files. These viruses have varying degrees of destructiveness, ranging from jamming servers with volumes of messages to destroying or scrambling employee files.

- **Defamation and Harassment:** Emails containing libelous, offensive, racist, or obscene content could be the basis for a discrimination or defamation claim.

- **Copyright Infringement:** It is easy for employees to send and

receive copyrighted material and incorporate the work of others into an organization's database. However, information from the Internet or printed material from emails, without authorization from the author or publisher, could be a violation of the Federal Copyright Act for the employee and the employer.

- **Confidential Information:** Proprietary information stored on computer networks or shared sites can be easily transmitted. This makes it susceptible to both accidental and intentional misappropriation. Information meant to be confidential that is inadvertently disseminated to others can cause humiliation if personal information is disclosed, or financial devastation if corporate secrets are revealed.

- **Retention of Files**: Files can be left on an organization's network, stored in back-up files, or archived on an employee's hard drive. Deleting an email does not necessarily permanently delete the information. The email may have been forwarded or printed, or the content may have been downloaded into another format and stored. The law now requires the production of electronic communication during the discovery process in a lawsuit. This leads to significant costs in time and money to any firm. In addition, software can retrieve a message even after it has been deleted. If the organization's records are ever subpoenaed, email communications can be recovered and used as evidence.

To maximize the benefits and avoid the potential pitfalls of using email, many professional services firms have created email use policies. Many circulate such policies and include them in employee handbooks. Others have taken the extra step of programming reminders that appear on computer log-in screens. Firms without such policies should consider the following employee advisory suggestions:

- Transmissions are not private. Courts have ruled that email is an inherently public means of communication in which users lack any reasonable expectation of privacy.
- Email use may (or will) be subject to monitoring. Although the intentional interception of electronic communications is a

felony, the monitoring of employees' electronic messages has been held not to violate the federal statute.
- Only company-related use is authorized; any personal use, or any use for illegal or unethical purposes, is prohibited.
- Unauthorized email use can lead to discipline up to and including discharge.
- Corporate standards with respect to business communications apply to email; all communications must reflect professionalism and business letter writing standards.

Entity Websites and Publishing Exposures

File Transfer Protocol websites have their own exposure characteristics, and firms need to manage the risks associated with their business. Websites that provide information about a firm or solicit or retain clients that sound relatively innocuous can still generate claims related to copyright or trademark infringement, unfair competition, defamation, and similar claims. The types of losses that may be created by a website include:

- **Libel:** knowingly publishing false and defamatory information that harms a person's reputation.

- **Invasion of Privacy:** disclosing information that interferes with another party's peace of mind or right to confidentiality.

- **Infringement:** violating or interfering with another's intellectual property rights or the right to pursue business.

While finding and using online materials for personal purposes does not create liability, the use of materials for commercial purposes can render a party liable for copyright or trademark infringement, misappropriation of intellectual property, or false advertising. For example, if a firm creates a link on their website to another entity's website without permission, the linkage of the two websites may form a basis for liability because of the implication that the linking website has a relationship with the linked website.

In addition, while website owners are generally protected from liability for the incorporation of content provided by others (provided they do not monitor or filter the content), information provided by employees and, perhaps, some independent contractors may still create liability. Courts have determined that a

federal statute protects websites that unintentionally publish defamation created by another. It is unclear whether other claims, such as publicity or privacy rights violations, would be covered by the statute. The safe harbor applies only to "interactive computer services," a term which is not well-defined in the statute and which may not cover websites.

BIM Developments and Technology Risks

New technological tools like building information modeling (BIM) can produce significant benefits for all stakeholders in the construction process. Design firms, other construction-related professionals, and contractors can better collaborate on the details of designs, explore constructability, and determine the sequences of construction with better accuracy.

With BIM providing better coordination and detection of conflicts in structures and systems, design firms can avoid many of the construction document problems that lead to delays and change orders during construction. Even on a traditional design-bid-build project, increased communication and collaboration, more efficient fabrication and delivery time, and improved documentation can reduce the overall liability exposures of all project participants. The transformation to a more collaborative design and construction process with integrating tools like BIM seems to be approaching quickly.

Currently, BIM is used by a rapidly growing percentage of engineering firms but typically on a limited basis. Contractors also have much to gain from the scheduling and means and methods opportunities intrinsic in BIM, but there's a learning curve and cultural shift involved in adopting BIM, which has not yet gained momentum. Complete, integrated use of BIM across the entire design and construction team is rare. Often, a designer might use BIM to assist with design exploration, visualization, and design document coordination before delivering to the contractor completed two-dimensional plans created from the model. With input from subcontractors and suppliers, the contractor might then create another model for means and methods purposes. Because contractors can build the project virtually before they build it on site, constructability issues that might otherwise go unrecognized until the project is in the construction phase can be identified. Addressing these issues early is far more efficient and inexpensive.

Creating Confusion in Responsibilities

The movement toward a collaborative system enabled by BIM presents challenges to traditional legal concepts and might create exposures not neatly covered by one insurance policy. Design firms need to be aware of how their legal status affects their insurance coverage. Professionals provide services, and are recognized by the legal system as using judgment. Instruments of professional service are recognized as communication tools and not products sold on the open market. As the use of technology increases and data-rich models replace tangible instruments of service, courts might be confused as to the role of engineering firms. In addition to challenges of security and productivity problems that could be created by any failure in technology when an engineering firm assumes responsibility as the model manager or overall project coordinator, the exposure of the firm to devising construction means and methods, controlling scheduling or other requirements of construction, or even creating the final product for a client may expose the firm to risks that go beyond professional liability.

The U.S. legal system recognizes that design firms provide recommendations to their clients and that those recommendations must fall within a scope of reasonableness defined as the standard of care. When BIM is used as a project development system rather than as a design tool it alters the traditional allocation of responsibility and liability exposure by blurring the distinction between design and construction decisions regarding means and methods. Design firms currently only have to meet a standard of care; involvement in determining construction means and methods may change that obligation. This blurring affects contractors too. Any lack of a "bright line" between design and construction responsibilities might challenge the long-standing Spearin Doctrine, which establishes an implied warranty on the part of the client of the adequacy of plans and specifications that clients require contractors to follow. If the contractor designs rather than determines construction techniques, the protection of a client's implied warranty may be eroded.

Effective use of BIM only occurs when each user's role is defined. Typically in a BIM-based collaborative process, there is no unitary model containing all of the digital information provided by designers and other contributors, but instead many models generated for specific purposes by each design discipline, contractor, and fabricator. Each party can maintain complete

control over its own model, and with that control the lines of responsibility are easier to allocate. The data sharing process is structured to preserve this separate control, responsibility, and protection.

Assuming Risks as a Model Manager

The exchange of vast amounts of electronic data by multiple parties necessitates the identification of a person or entity to act as manager or gatekeeper of the primary database. Models are generally shared either on an FTP or hosted website. It is necessary for the client and all project stakeholders to establish clear expectations and obligations through contract terms or protocol documents as to specific duties such as maintaining the site, overseeing or providing access rights, preserving record versions of the models, and managing collaborative sessions. Ownership and use of the model and its elements must also be determined.

As collaboration increases, so does the role and risk of the information manager. The model manager's duties could range from the limited maintenance of the file transfer site, with oversight of user access rights, to the compilation of information provided by other project members and its dissemination in a useful form to the project team. Although past model managers have generally been design firms, this role might be held by different entities throughout the different project phases. Alternately, the model manager could be a third party with specialized expertise in managing large amounts of electronic data or adept at using the particular project software.

As collaboration increases, so does the role and risk of the information manager.

With reasonable process controls in place, the preparation and sharing of models are far more likely to create benefits for all parties. Processes must be built into the system for recording and displaying the various versions of the models residing in the sharing site at any particular time, and incorporating into the database change orders, responses to requests for information, and supplemental instructions. These processes create additional exposures for the model manager and should be spelled out accordingly in a contract.

Dealing with the Expanding Exposure of Technology

Although the party responsible for administering the model is charged with providing and controlling the technical resources

needed to enable connectivity, host the files, manage access, and ensure security, the increased use of information through electronic means creates exposures for all participants. For instance, although BIM will likely increase the quality of construction documents, the possibility of software errors exists, just as it does with use of predecessor technology, such as Computer Aided Design and Drafting (CADD). In addition, all firms can be harmed through security breaches that introduce viruses or worms into computer systems or divulge confidential or proprietary information not meant for release.

Project teams should assess the potential of electronic data loss or software error whether due to viruses, software corruption, hardware failure, or system destruction such as by power surges, fire, or water damage. The complete loss of the file sharing site or model data is easily addressed with appropriate precautions taken to minimize the risk through system backup, protection from unauthorized access, and protocols for project participants to reduce the likelihood that issues may arise from incompatible software, viruses, or other security breaches.

BIM offers the real prospect of greater efficiency and reduced liability exposure for all project participants. However, the concerns for preserving recognized legal status and control over both process and technology risks must be addressed.

Understanding the Scope of the Technology Exposure

There are business exposures and risks created by the use of technology that are not inherent in the performance of professional services. For instance, when a firm sells its expertise to train others in the use of software, it is acquiring an exposure distinct from the scope of professional liability insurance coverage. Hosting web-based systems, creating software that is not project specific, leasing employees or equipment, or creating products that are derivative of design services all usually require specific coverages.

Hosting data can create additional insurance issues. Running a commercial website may require special policies that go beyond the protection of a regular general liability policy to cover media liability and Internet liability exposures. Moreover, if the parties are developing custom software for the use of others, there are product risks involved that may not be covered by their customary policies.

Specialty insurance policies designed to cover these exposures vary greatly; assessment of policy language by an independent

insurance advisor is imperative to ensure firms purchase appropriate coverages for their exposures.

Risk Management Through Insurance Coverage

Design professionals need to examine both their internal practices and their insurance policies to ensure they address exposures from the use of technology in their practice. Most design firms carry professional liability, property, and general liability coverages, but these policies only address some of the new exposures encountered in the conduct of a professional practice in a cyber world.

Computer Equipment and Media

Computer hardware and software are costly, and firms need to protect their investment in these assets by purchasing specially designed property coverage, such as electronic data property (EDP) coverage. This type of insurance is often an endorsement to—or special section of—the insurance policy firms buy to cover their building, furniture, office supplies, and similar property. The policy responds if your property is stolen or damaged by a covered peril, such as fire, smoke, or water damage. Property or EDP coverage is called "first party" coverage, since the policy pays you for your own financial interest in property, as opposed to "third party" coverage, which responds by paying a third party on your behalf for damages for which you are held liable.

Some property or EDP policies include a sublimit that applies to damage from a cyber attack on the insured's data or media. Such coverage is often generically referred to as "virus" coverage. However, these sublimits are often quite low, so firms should rely on data backup procedures as their primary form of risk management.

In addition to the value of assets, property or EDP policies may also provide "business income" insurance, which covers the resulting loss of income from damage or theft to covered property, and "extra expense" insurance, which covers the additional expenses a firm incurs after a covered loss to minimize their "downtime" and lost income as a result of the damage to their property.

Commercial General Liability Insurance

The commercial general liability (CGL) policy is a "third party" liability policy, responding to an insured's liability to others for "bodily injury," "property damage," and "personal and advertising injury." Many insurance carriers base their policy language on the standard CGL policy drafted by the Insurance Services Office (ISO). Coverage is limited to the types of damages that meet the three defined terms above and that arise out of an insured's premises, operations, products or completed operations.

Most of the damages alleged from cyber attacks or technology problems have to do with computer systems, data, and personal or confidential information. These types of claims will not meet the typical definitions of bodily injury or property damage. Bodily injury is fairly straightforward, as it involves physical injury to a person. Property damage coverage is trickier, as it hinges on whether or not electronic data is considered "tangible" property. The most recent versions of ISO's CGL policy specify that property damage involves damage to "tangible" property, and further specify that "electronic data" is not "tangible" property. When allegations include damages to computer systems, it is usually the data, software, or programming that has been damaged, rather than the tangible computer equipment. Downtime from overloading a system with activity through a denial of service attack does not cause any damage to tangible property either; it just interferes with its ability to perform. Since electronic data (software and programming) is not considered "tangible" property, damage to it does not meet the definition of "property damage" and therefore it is not covered on the CGL policy.

The most recent versions of ISO's CGL policy specify that property damage involves damage to "tangible" property, and further specify that "electronic data" is not "tangible" property.

Technology may be used as part of a design solution, and bodily injury or property damage may occur as a result of an error or omission in the design, but most insurers attach exclusions to their CGL policies to preclude coverage for the professional services of architects and engineers. Many insurers routinely attach computer software errors and omissions exclusions for the same reason. Such exposures are more appropriately addressed by a professional liability policy.

Many firms use websites and the Internet as part of their marketing initiative to help advertise and promote their business. The "personal and advertising injury" coverage in CGL policies provides coverage for an insured's own advertising exposures, and recognizes websites as a means of advertising. "Personal and

advertising injury" is defined in ISO GL forms to include use of another's ideas in the insured's own advertisements, and infringement of copyright, trade dress, or slogan in the insured's own advertisements, in addition to libel, slander, disparagement, and violation of a person's right of privacy. But there are limitations to the coverage.

- **"In The Business Of" Exclusion:** ISO's CGL policy excludes all "personal and advertising injury" coverage for any firm deemed to be "in the business of" certain media-type operations, such as advertising, broadcasting, telecasting, publishing, designing websites or website content, or providing Internet search/access services.

- **Chatroom/Bulletin Board Exclusion:** ISO's more recent versions of the CGL policy exclude all coverage for "personal and advertising" injury arising out of chatrooms, bulletin boards, blogs and similar forums that are owned, hosted or controlled by an insured.

- **Unauthorized Use Exclusion:** CGL policies also exclude unauthorized use of another's name or product in an email, website address, metatag, or domain name.

With widespread use of websites it is not uncommon for firms to capitalize on income opportunities by placing frames, links, advertisements, etc., of other entities on their websites, advertisements, etc. The CGL policy specifies that the mere placement of frames, borders, links, or advertising (for the insured or others) on the Internet does not, in and of itself, mean that a firm is "in the business of" any specified media-type business. If a firm expands its operations beyond traditional design practice in to any of these media-type businesses, the CGL policy will no longer provide any "personal and advertising injury" coverage and a media liability policy may be appropriate to address these exposures.

Professional Liability Insurance

Professional liability policies are "third party" liability policies, which respond to an insured's liability for damages to others. A design professional liability policy covers the firm's liability arising

out of a wrongful act, error, or omission in the performance of professional services, generally defined as services performed for others in an architectural or engineering practice. Some policies expand the definition to include services performed by other types of construction specialty consultants. In general, professional liability policies are not intended to address problems with the technology a firm uses to communicate and deliver services. As a result, professional liability coverage generally does not extend to cyber liability exposures, such as a security breach, virus transmission, or computer system problem that may result in a firm being held liable for damages.

Professional liability policies are typically designed to cover services provided, as opposed to "products" sold or licensed by the insured to others. Product liability is traditionally an exposure covered by commercial general liability policies, but professional services exclusions on the CGL policy may preclude coverage for products that are part of professional services. It is not uncommon, particularly for engineering designs, to include software programs as part of the overall design services provided to a client. In recognition of this exposure and potential coverage gap, some professional liability policies include exceptions to their "product liability" exclusions, to extend coverage to software developed for a specific client in connection with the design services provided.

Some professional liability insurance policies have culled out specific coverage modules for technology exposure, but additional exclusions often apply, and the net result may limit, rather than broaden, the available coverage. Technology exposures other than client-specific software are best addressed by policies designed specifically for such exposures.

Specialty Coverages

When a firm expands their operations to include publications or electronic communication forums such as chat rooms, blogs, or bulletin boards, a specialized media liability policy may be appropriate to address a firm's liability for "personal and advertising injury" and intellectual property exposures associated with producing, disseminating, monitoring, or hosting content. These exposures are not covered by the CGL policy due to policy exclusions. Nor are they covered by a professional liability policy, as such services generally fall outside of the definition of covered professional services.

Firms developing software programs or applications that are not client-specific should consider a technology errors and omissions policy to address that exposure. Additionally, firms that are providing technology-based services to others, such as designing websites or hosting websites for others should also consider a technology errors and omissions policy. Coverage under professional liability policies is limited by the definition of covered professional services and by product liability exclusions. CGL policies respond only to certain types of defined damages, and insurers often attach exclusions for software errors and omissions for known exposures. Technology errors and omissions policies are "third party" liability policies that generally cover "wrongful acts" arising out of defined "technology services." The definition typically includes development of software or hardware, custom programming, website development, network integration, providing Internet access, and other types of technology services. Client-specific software designs may be covered by some professional liability policies, but to cover any other technology product that is sold or licensed, or to cover technology services that fall outside traditional design practice, a technology errors and omissions policy may be needed.

Technology errors and omissions policies are "third party" liability policies that generally cover "wrongful acts" arising out of defined "technology services."

Some of the exposures from using technology to conduct business can be insured by a cyber liability policy; such "third party" liability policies generally respond to liability arising out of security breaches or virus transmissions. Note that most of these policies contain stipulations that some level of network security and virus protection is maintained on the firm's computer systems, or coverage is voided. Cyber liability policies respond to an insured's liability to others in the event that a breach in security or virus causes damages to others' networks, data, or results in the release of confidential or proprietary information that harms others. These exposures arise out of business operations rather than professional services, and are therefore not generally covered by professional liability policies. Cyber liability policies address a firm's liability for damages that do not meet the defined types of damages covered by a CGL policy. Damage to "intangible" property, such as data, information, programming, etc., is generally covered by cyber liability policies, as are related damages from loss of use or additional expenses incurred to repair or restore data or network systems. Additionally, most cyber liability policies address a firm's liability for privacy violation if confidential or personal

information is stolen electronically.

Business Risks

Not all risks are covered by insurance. Some exposures are business risks, such as choosing hardware or an operating system adequate for business needs, choosing appropriate software packages, or the right amount of server capacity to support Internet and website operations. Firms are obligated to maintain their software, installing upgrades and patches and replacing obsolete software. To the extent that a firm relied upon the advice of a paid consultant, or to the extent that any of the products are faulty, a firm may pursue claims against the technology errors and omissions liability policies for the consultants, developers or manufacturers involved. When making a major technology investment, it is a good idea to require evidence of technology errors and omissions coverage from the product or service provider. However, absent a negligent party or product, such decisions are typically uninsurable business risks.

How Does Schinnerer Respond?

As the leading insurer of design professionals, Schinnerer is addressing the technology exposures discussed in this publication:

Computer Equipment and Media

Schinnerer offers proprietary property and electronic data property policies to cover the value of a firm's computer equipment, data and media. We offer business interruption insurance to cover income lost as a result of damage to covered property and extra expense insurance to cover unusual expenses incurred to keep operations running after a loss. Coverage is offered for targeted computer attacks against the insured's computer system; the limit of insurance provided for this coverage is usually $25,000. Schinnerer offers these coverages in partnership with an A rated carrier. Small to mid-size firms may be eligible for coverage under our business owners package policy (BOP). Larger or more complex firms will be offered coverage under a commercial package policy.

Personal and Advertising Injury

The commercial general liability policies Schinnerer offers are provided in partnership with an A rated carrier. The CGL policy forms are based on the language used by the Insurance Services Office. The coverage forms that compose our BOP are proprietary, but the CGL portion is based on ISO language, with some proprietary coverage enhancements. Our commercial package policy includes the most recently adopted ISO CGL form, along with proprietary coverage endorsements. With these products, Schinnerer provides our customers with coverage for their liability arising out of specified offenses, including libel, slander, disparagement, violation of a person's right of privacy, use of another's ideas in their own advertisements, and infringement of copyright, trade dress, or slogan in their own advertisements. Coverage is not contingent on whether or not the offense is committed electronically, except that there is no coverage for offenses committed in electronic chat rooms or bulletin boards. However, all personal and advertising injury coverage is excluded on the CGL policy for any firm that ventures beyond traditional practice into a media-type business.

Software Errors & Omissions

Schinnerer's Professional Liability and Pollution Incident Liability for design professionals is a "third party" liability policy offered in partnership with an A rated carrier. In addition to liability for coverage for professional services, coverage extends to software developed for client-specific solutions via an exception to the exclusion for sales and distribution of products. This means that, subject to policy terms and conditions, wrongful acts arising out of client-specific software are covered. Many of our competitors do not have product liability exceptions. Additionally, some competitors provide coverage for technology products, but employ additional exclusions, such as exclusions for bodily injury, property damage, intellectual property, or delay in performance. There are no additional exclusions that apply to the coverage extended for client-specific software in Schinnerer's policy.

Firms that expand services beyond traditional design practice to develop software independent of client-specific design solutions need more than their design professional liability policy to cover their exposures. Technology errors and omissions liability policies are third party liability policies designed to respond to a firm's liability for technology-based products or services, such as developing software, performing website hosting or website design services for others; providing computer consulting, programming or network integration services to others; providing Internet search/access services to others; and lending or leasing technology staff to others or providing technology-based training/support to others, and more.

Schinnerer's offers Techvantage®, a technology errors and omissions liability policy provided in partnership with an A rated carrier.

Cyber Liability

Any business that uses computers is exposed to losses from security breach and viruses and other cyber attacks. Schinnerer will soon offer a new cyber liability endorsement to cover many of the risks a firm encounters from conducting business electronically. The coverage endorsement will cover a firm's liability to others for a breach in the policyholder's computer network's security that results in:

- Identity theft.
- Network damage
- Theft of the information of others in the policyholder's care, including trade secrets,
- Infection of the networks or data of others, and
- Security breaches, including unauthorized employees who defeat security systems.

Additionally, the network protection for design professionals endorsement also covers the costs to comply with applicable laws requiring a firm to notify its customers or users if a security breach could potentially compromise private information, as well as costs to remedy privacy law compliance deficiencies if required by a governmental regulator.

This third party liability coverage will be offered as an endorsement to a firm's professional liability policy but with a separate limit of liability and deductible obligation. The coverage will be written on a claims-made basis with defense inside the limits just as with professional liability insurance. Limits up to $2 million will be available.

Media Liability

If a firm expands their operations to venture into broadcasting, publishing, telecasting, advertising, or providing Internet search/access services to others, personal and advertising injury coverage is normally excluded on the commercial general liability policy. Similarly, the CGL policy would not respond to claims arising out of a firm hosting, controlling, or monitoring an online discussion forum, such as a blog, chatroom, or bulletin board. These types of exposures are best addressed by a media liability policy.

Schinnerer does not currently offer this coverage, but we are looking to expand our product offerings.

Coverage Summary

The chart below summarizes much of what was discussed above with respect to the different coverages available to address technology exposures. A shaded box indicates the most appropriate place for design firms to cover the exposure. A "❖" indicates that the exposure may also be covered through this product, but purchase is not always needed. With the exception of media liability coverage, the recommendations are based on insurance policies offered by Schinnerer.

Exposure	PL	CGL	Prop/ EDP	Media Liability	Tech E&O	Cyber Liability
Software—developed specifically for a client in conjunction with your professional design services	■				❖	
Software—packaged for sale independent of client design services					■	
Libel/slander, violation of right of privacy, intellectual property right infringement in your advertisement for your services		■		❖		
Libel/slander, violation of right of privacy, intellectual property right infringement in a chatroom, blog, or bulletin board you own, host, or control				■		
Using your competitor's name or product in your email address, domain name, or metatag				■		
A security breach that results in blast emails to everyone in your address book, transmitting damage via virus to their data or network						■
Disclosure of private personal information via security breach of your system						■