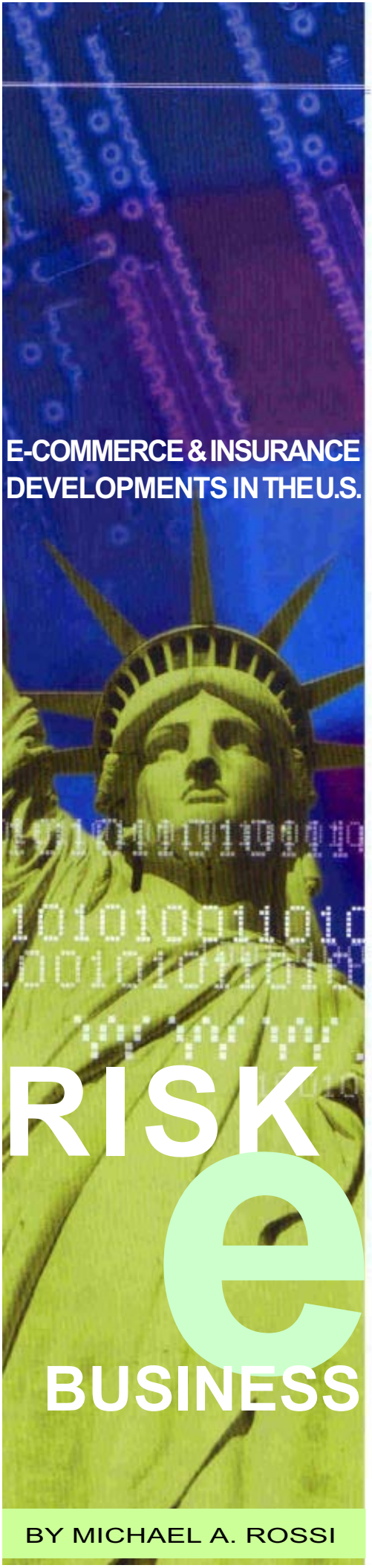


BY MICHAEL A. ROSSI

In many parts of the world, the last year has seen a growing awareness of the risks inherent in e-commerce activities, namely, the use of the Internet to conduct business, and the continued reliance on internal computer systems, networks etc to keep operations running. This increased awareness has resulted in several developments in the areas of risk management and insurance. This article briefly addresses the insurance-related developments in this area from a US perspective. Interestingly, these e-commerce insurance issues are playing out the same way in the UK as they are in the US. The author's hunch is that similar developments are happening in Australia. Therefore, it is hoped that this article proves useful for Australian risk managers.

Due to considerations of space and readability, the article has been divided into two parts, the second of which will appear in the September edition of *Corporate Risk.* This first instalment provides a general overview of the state of e-commerce insurance, and then discusses developments in the area of first-party risks. The second instalment will discuss the field of third-party risks, and provide some direction for risk managers who are considering how best to deal with their company's e-commerce exposures.

BRINGING ORDER TO CHAOS

Perhaps the best way to sum up the US experience to date is to say that chaos surrounds the issue of how best to insure e-commerce risks. Why chaos? Because there is absolutely no consensus among the insurance industry, brokerage industry or policyholder community in the US with respect to how best to address these issues. Everything is in a state of flux.

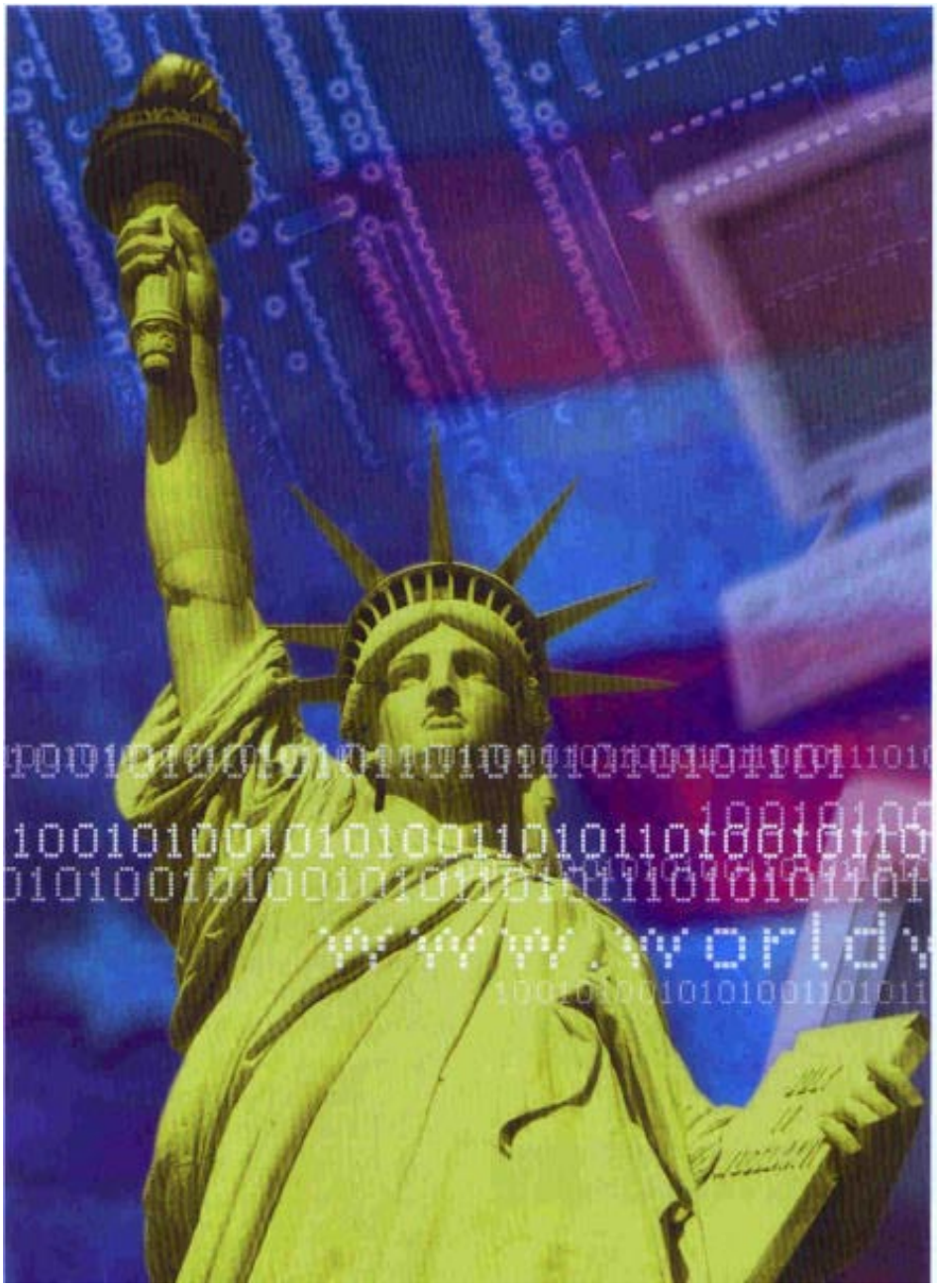
First, a handful of insurance companies have developed insurance products expressly designed to insure third-party liability and first-party risks related to e-commerce activities. The liability policies cover, among other things, claims for injury or damage because of a wrongful act, error or omission. They apply to both professional services and to media risks (such as the spread of a computer virus, the infringement of some form of intellectual property right, the invasion or infringement of right of privacy or publicity, and defamatory conduct).

The first-party policies cover, among other things, lost income and extra expenses because of the "crash" of the insured's computer system or website(s), the denial of access to the insured's computer system or website(s), or other type of loss of computer data, software and programs (whether caused by an employee or third person). Such policies also cover extortion risks relating to the insured's computer system and website(s).

Some insurers are selling policies that insure only such third-party liability risks. Some insurers are selling policies that insure only such first-party risks. And some insurers are selling policies that insure both the third-party liability and first-party risks. But other insurers are responding in a different way - by saying either that the new policies are not needed, or that it is impossible to underwrite the risks that are being underwritten by these new policies (especially in the first-party context).

Second, the policyholder community has responded to these issues in different ways. US Fortune 1000 companies, for the most part, are taking the position that they do not want more stand-alone policies that they have to buy, administer and negotiate, and for which they have to maintain a separate tower of insurance. In contrast, smaller companies, especially dot com start-up companies, are buying these policies (at least the ones for third-party liability risks). They lack the risk manager experience, premium size and other clout that a Fortune 1000 company can bring to bear when dealing with these issues. Thus, although there may not be a market for much of these new insurance products for the Fortune 1000 companies, there is a growing market for these products among smaller companies.

Third, insurance brokers are also responding in different ways. One broker has taken a lead in developing an insurance product designed to insure third-party liability and first-party risks for e-commerce activities. That broker is Marsh, with its Net Secure product. Some brokers, however, are agreeing with



Fortune 1000 companies that ecommerce risks can be addressed by amending traditional policies. Others have perceived the policyholder market differentiation described above, and are responding by selling the new insurance products to start-ups and the middle market, and creating alternative solutions for the Fortune 1000, by focusing on balance sheet protection with alternative risk transfer mechanisms.

Accordingly, any discussion of e-commerce insurance issues, to be comprehensive, must address each of these variant viewpoints and developments. Due to space limitations, not all of these issues can be discussed in this article.

The remainder of this article will therefore focus on the following discussion: what are the potential gaps in traditional insurance policies for e-commerce risks, and how can risk managers try to close those gaps by using insurance?

FIRST-PARTY E-COMMERCE RISKS

The author uses the term 'first-party risks' to refer to the risks generally associated with risks covered by commercial property policies, commercial crime policies and fidelity bonds, and kidnap and ransom policies. While it is true that these types of policies can also provide liability coverage in the context of such first-party losses (when a third party seeks to impose liability on the insured for a loss that is recognized as a first-party loss under the policy), the focus of the discussion here is on the first-party loss itself.

COMMERCIAL PROPERTY POLICY ISSUES

Many commercial property policies require 'physical loss or damage' to property in order to trigger both the property damage coverage and time element (eg business interruption and extra expense) coverage. Some e-commerce risks involve what may be called 'non-physical events', where it is not clear that physical loss or damage to property has occurred.

One example of a 'non-physical event' in e-commerce is a denial of service attack, where an insured's website (technically, it is the computer server hosting the website that it attacked, so by reference to "website" in this article, the author is referring to the computer server hosting the website) is bombarded with millions of e-mails from a bogus source, thereby blocking access to the site by legitimate users. A well-publicized spat of denial of access attacks occurred in February of this year, affecting web-based companies such as e-Bay and others. Does such an event constitute physical loss or damage to any property? Insurers say no. The author's hunch is that courts will agree with the insurance industry on this issue. If so, such a loss likely will not trigger either property damage coverage or time element coverage in a traditional commercial property policy.

Another gap may lie in the indemnity period provisions of a commercial property policy. These provisions are the key to the time element coverage provided by such a policy, because they determine the length of time for which the insured gets to claim coverage for lost income, extra expenses and other time element losses. However, the indemnity period provisions in standard commercial property policies are not well-suited for all e-commerce risks, even if the e-commerce event at issue triggers coverage in the first instance (ie, satisfies the 'physical loss or damage' requirement).

For example, some traditional policies

provide that the indemnity period for losses involving computer data, software, programs etc (which usually fall within the definition of 'electronic data processing media' or EDP media covered by the policy) is the time it takes to copy lost or destroyed media from backup tapes or the previous generation of such media. If that time period is minimal (eg a few hours or so), that coverage might not encompass the full-time period for which the insured sustains time element losses.

It is true that some traditional policies provide broader indemnity period provisions for EDP media, such as the time it takes to replace or restore lost or damaged media, including research and engineering costs. However, what if the loss at issue does not involve lost or destroyed computer data, programs, software etc, but rather simply involves the rendering of a website or computer system useless for a period of time to eradicate a computer virus or respond to other problems that do not involve the actual destruction or corruption of computer data, software or programs? In addition to denial of service attacks, this issue might also arise with certain types of computer viruses, such as the recent 'I Love You' virus. Early reports show that that virus did, indeed, cause damage to computer data, software and/or programs. However, it also appears that in most, if not all, cases, the virus did not destroy, corrupt or delete operating programs, thereby rendering a computer network useless. Rather, networks were brought down by their users to stop the spread of the virus in their computer systems.

In other words, viruses like the 'I Love You' virus appear to be conceptually different than viruses that cause a system or website to go down because they delete, destroy or otherwise corrupt data, software or programs that are essential to running that system or website, and that system or website is thereby rendered inoperable unless and until the lost, damaged or corrupted operating program is restored or replaced. In brief, with respect to the "I Love You" virus and similar viruses in the future, the author's hunch is that insurers whose policies are worded correctly will indeed recognize coverage for the cost to replace or restore any data, software or programs that were lost or damaged because of the virus. However, the author also believes that most, if not all, insurers will not recognize coverage for time element losses related to such viruses, by arguing that such losses did not flow directly from the lost or damaged data, software or programs rather, they flowed from the voluntary shut down of the insured's computer system. Insureds have arguments to rebut such a position, and should be entitled to full coverage based on several of such arguments. However, until such coverage issues are resolved by the courts, sound risk management should treat it as an issue that needs to be expressly addressed in an insurance program, if for nothing more than to confirm that the insurer's intent conforms with the insured's expectations of coverage.

Another risk with respect to commercial property policies deals with employee dishonesty. All commercial property policies the author has reviewed contain an exclusion for loss caused by employee theft. Some policies even exclude loss caused by employee malicious destruction. Even with this latter provision removed, the policy still will exclude loss caused by employee theft. The reader might think, that's not a problem, because employee theft losses are covered by commercial crime policies and fidelity bonds. The problem with this view is discussed below (in brief, such policies and bonds contain a time element loss exclusion, so while the property loss might be covered, the time element losses are not).

COMMERCIAL CRIME POLICY AND FIDELITY BOND ISSUES

The first gap to be discussed with respect to e-commerce risks and commercial crime policies and fidelity bonds is mentioned above, but it is so important that it deserves repeating. Standard commercial crime policies and fidelity bonds contain a time element exclusion. The exclusion bars coverage for business interruption, extra expense etc. The exclusion does not use such words, but that is how it has been interpreted by courts. The exclusion is typically labelled the "potential income" exclusion or "indirect loss" exclusion or goes by a similar name. So if your e-commerce loss is an employee theft loss, the big surprise is this. You cannot get it covered under your commercial property policy because of the employee theft exclusion. You are therefore forced to look to your commercial crime policy or fidelity bond. But that policy does not cover time element losses. That is a gap through which you could drive a truck.

Another gap for e-commerce risks has to deal with valuation issues for stolen computer data, software or programs. Whereas standard commercial property policies that have been slightly amended contain detailed valuation provisions for lost or damaged data, software or programs, standard commercial crime policies and fidelity bonds do not. Such policies typically provide coverage for the lesser of the actual cash value of the stolen property or replacement cost. It is not clear how much, if any, coverage will be provided for stolen EDP media under such valuation provisions.

KIDNAP AND RANSON

E-commerce activities bring with them extortion risks. For example, a computer hacker might demand money or something else of value from an insured under threat of unleashing a denial of service attack against the insured's computer system or website. Similarly, a computer hacker might threaten to attack an insured's computer system or website with a virus that will delete, destroy or otherwise corrupt the key operating data, software or programs necessary to operate such system or website. Also similarly, a computer hacker could threaten to hack into the insured's computer system and delete important information, perhaps not information necessary to run key operations, but important information nonetheless (eg, proprietary manufacturing, marketing, human resources, legal or other information). Some K&R policies limit coverage for extortion to threat of bodily injury. Obviously, such wording does not respond to the risk mentioned here. Some K&R policies do extend coverage to threat of damage to property. However, it is not clear whether such wording will respond to threats of denial of service attacks and other computer viruses that do not damage or destroy computer data, software or programs, but rather merely render such property useless.

NEW E-COMMERCE INSURANCE POLICIES

Several insurers have created and are selling stand-alone policies to cover one or all of the issues discussed above. The policy forms currently available include Marsh's Net Secure program, which is underwritten by a consortium of carriers, the E-Risk policy from Fidelity and Deposit Companies, a member of Zurich, the Secure System policy from ACE USA, the Networker policy from St. Paul, and several policy forms from different Lloyd's facilities. AIG and Chubb also have policies under development. Some of these programs provide both first-party coverage and liability coverage, where the insured can buy all or some of the coverages. And some of these programs can be purchased on either a difference in conditions/difference in limits (DIC/DIL) basis or a primary basis.

These policy forms are in a state of flux, with the carriers apparently reviewing each others' forms to try, as much as possible, to address the same issues. A more detailed comparison of these and other forms, and the issues to consider when buying them, will be the subject of future articles in this column. Suffice it to say, however, that with respect to first-party risks, most, if not all, of these policies provide some form of coverage for each of the issues raised above. So, one way for an insured to close up the gaps discussed above is simply to buy one of these new policies, at least on a DIC/DIL basis. In that way, if an e-commerce loss falls through the cracks of the insured's program as constituted by traditional

policies, the stand-alone e-commerce policy should respond to the loss.

AMENDING TRADITIONAL INSURANCE POLICIES

There is an alternative to buying one of the new e-commerce policies, at least theoretically. In brief, an insured could amend one or more of the policies discussed above to cover the gaps at issue.

For example, an insured could add express language to its commercial property policy describing all the different types of loss events that it could experience with respect to its computer systems, web site, data, software, programs, etc., and then stating that all of such events shall be deemed physical loss or damage for the purposes of coverage under this policy. The insured can also amend the "indemnity period" provisions to more closely tie into such special "physical loss or damage" language so that the time element coverage matches up with e-commerce risks. Also, the insured will want to make sure that the employee dishonesty exclusion is limited to employee theft, and excepts all other forms of "physical loss or damage" to property caused by an employee.

Also, an insured could delete the potential income or indirect loss exclusion (however worded) in its commercial crime policy or fidelity bond. The insured might also want to add express language for time element losses (both business interruption and extra expense at a minimum), rather than simply rely on the deletion of the exclusion. The insured also might want to amend the valuation provisions to more closely mirror the valuation provisions in its commercial property policy. In this way, whether the property is stolen by a third person (where the commercial property policy would respond) or by an employee of the insured (where the commercial crime policy or fidelity bond would respond), the coverage provided by the different policies in the insured's program should be the same.

Finally, the insured will want to either amend its extortion coverage in its kidnap and ransom policy to address e-commerce extortion risks, or perhaps add the coverage to its commercial crime policy or fidelity bond, or perhaps to its commercial property policy. There could be several options available, but the point is that it needs to be covered somewhere in the insured's program.

Indeed, there are any number of ways to add such coverages into a program. Much will depend upon how the insured's program is currently structured (ie, what is already in the insured's policies?), and the insured's insurers willingness to amend their policies. And that is the hitch. To date, most carriers selling the traditional policies discussed in this article (in the US as well as the UK) are not willing to amend their policies to cover the gaps relating to e-commerce risks. So while such amendments are theoretically possible, it remains to be seen whether such amendments will become practically possible. ■

The second part of this article, dealing with third-party risks, will appear in the September edition of **Corporate Risk**. *Michael Rossi is a lawyer in the LA firm Troop Steuber Pasich Reddick & Tobey, LLP. He provides legal advice to policyholders and insurance brokers throughout the world and can be contacted on* mrossi@inslawgroup