Tackling *e-commerce* insurance policies

by Michael A Rossi
president, Insurance Law Group, USA

In the August and September issues I provided an overview of the way that many corporate insureds in the USA and UK were responding to the increased levels of attention paid to e-commerce insurance issues.

One of the observations made in those articles was that many of the large corporate insureds in the US and UK that have been reviewing their e-commerce insurance have opted not to buy one or more of the new stand-alone e-commerce insurance policies. Rather, they are trying to amend the policies in their current programs where need be, because much of the e-commerce risks currently perceived to exist are, in their opinion, already covered by their programs.

This article gives a broad overview of the issues that a corporate insured should consider if it is going to use one or more of the new stand-alone e-commerce insurance policies to respond to e-commerce risks. It is written in the context of the author's experience working with multinational corporate insureds based in the USA .and UK that are trying to address their e-commerce insurance needs.

Why should risk managers care about the new stand-alone e-commerce policies?

I view this discussion as important for at least three reasons. First, the jury is still out, so to speak, on whether or not large corporate insureds will be able to amend their traditional policies and/or programs to respond to all of the risks addressed in the new stand-alone e-commerce insurance policies. It could be that the insurance industry in the USA and UK might force insureds to buy standalone e-commerce policies to address at least some of the risks at issue.

If so, it will be important to know what issues should be considered when buying such insurance.

Second, reviewing the stand-alone e-commerce insurance policies to see what issues are being addressed, and how they are being addressed, is really quite helpful when trying to amend traditional policies to better respond to e-commerce risks. Language from these policies in many instances can be plugged right into traditional policies as a means of clarification (if all agree that the intent to provide the cover is there, but the policy does not expressly explain how the cover is provided) or coverage enhancement (to add the coverage if all agree that the coverage was never in the traditional policy in the first place).

Third, many smaller companies in the USA (as well as the UK) that are exposed to e-commerce risks are buying the new stand-alone e-commerce policies, at least with respect to the liability coverages provided by such policies. This phenomenon is occurring for a number of reasons. The leading driver appears to be that such companies are just now building their insurance programs and, therefore, deem it viable to include such a policy in their program on a primary basis and build around it. Also, many such smaller companies do not have the clout, premium volume or risk management expertise necessary to make 'tweaking' traditional policies viable. (The carriers just are not willing to make many changes to traditional policies in regard to e-commerce risks for such companies.)

I presume that many of these same developments will occur in Australia over the course of the next several months to a year or more. Accordingly, this installment is really for those companies (large and small) that are looking to buy one of

the new stand-alone e-commerce insurance policies as they become more available in Australia, either because they want to or because they have to.

There are many issues to consider with respect to these policies. Space limitations allow for only a brief, broad-based overview of the subject, with some particular examples of issues to spot. Suffice it to say that in order to ensure that you are getting the best of what the market has to offer at any particular time, all quotes must be compared against other available forms in the market to identify coverage enhancements that should be negotiated. As with most other lines of coverage, all off-the-shelf e-commerce policies that the author has reviewed are lacking in some way when compared to the other forms in the market.

State of the market

Several insurance carriers are offering stand-alone e-commerce insurance policies in the USA and UK. The author has compiled a list of forms known to him at the following website: www.irmi.com. Readers are encouraged to visit that site, in the Expert Commentary - Insurance - Cyber Insurance column to review the table. It will be updated periodically with new policy forms being offered in the USA, UK and Australia.

One of the first issues to consider when buying one of these policies is understanding the state of the market. What are the different policy forms out there, what do they do, and what capacity (ie. limits of liability available) does the insurer selling the cover have? These are important issues to consider when reviewing quotes that the insured's broker brings back from the market.

There are several different ways to buy stand-alone e-commerce insurance. That is because the market is divided into endless variations.

Some of the new forms provide coverage only for professional services liability and media errors and omissions liability. Some of the new forms provide coverage only for employee dishonesty and third-party malicious conduct, such as crime and extortion (both for loss of property, money, securities, etc., as well as for business interruption and extra expense). But within that market there are several different variations, the difference being what amount, if any, of liability coverage is offered for indemnity and defence because of theft, for which the insured is liable.

Some policies provide coverage for not only employee dishonesty and third-party malicious conduct, but also for loss caused by natural perils, as well as by a computer programming negligent act, error or omission by the insured's employee or independent contractor. However, many of the forms exclude both of these perils.

Finally, some of the new forms combine one or more of the foregoing coverages into a program that provides both liability and first-party coverage.

As far as capacity goes, some of the insurers are offering only minimal capacity (eg. $2 or $3 million in limits). One can discern right away that such carriers are looking to insure only

smaller companies. Some of the insurers are offering greater capacity, but the limits seen to date really are not meaningful for many large Fortune 1000 companies. (Many companies are looking to maintain the same limits that are maintained in the other policies in their programs, eg. hundreds of millions of dollars for the very large companies, but capacity appears to be in the low tens of millions of dollars.)

A carrier to watch, however, is FM Global. That insurer had intended to launch e-commerce wordings for its Property and Crime coverages last December. It is rumored that such offerings will not be new 'stand-alone' products, but rather will be endorsements to FM Global's current policy forms. However, the launch date has continually been pushed back. If FM Global does come out with good wording and meaningful capacity, it really could open things up quite a bit for large multinationals looking to amend their traditional policies in their programs, rather than buy stand-alone e-commerce policies. Traditional carriers should have to start making amendments in order to compete. Also, the stand-alone carriers presumably would have to increase capacity to compete. This will particularly be an interesting course of events to follow as the property market in the USA and UK has hardened substantially for many policyholders in the last six months.

Readers can monitor the e-commerce policy chart on www.irmi.com to find out if FM Global does come out with the promised offerings.

Liability coverage

As with any insurance product line, there are many issues to consider and enhancements to seek with respect to any off the shelf stand-alone e-commerce insurance product. Space limitations prohibit a discussion of all such issues. Set forth below are some of the important ones to consider with respect to policies providing liability coverage. The reference to liability coverage here is to the policies providing coverage for professional services liability and 'media errors and omissions' liability. Liability risks also are associated with employee dishonesty and thirdparty malicious conduct, as well as with respect to natural perils and computer programming acts, errors and omissions. Those issues are discussed below under the 'first-party' coverage discussion.

E-commerce activities expose an insured to liability associated with the activities of others

A common issue for professional liability policies is how broad is the definition of the professional services covered by the policy. There are several different ways to address this issue. Some forms require the insured to list with specificity in the declarations or by endorsement the services that are intended to be covered. Some forms use defined terms to describe what services are covered. In both cases, if the insured gets hit with a claim arising from services not described, then coverage likely will be denied. However, some forms simply state that professional services are 'all services performed by or on behalf of the insured'. That appears to be a blanket professional services provision. Obviously, such a provision is preferable over the other two options.

Professional liability coverage, and to a lesser extend media errors and omissions coverage, can come in one of two forms. The first version covers claims for any 'negligent act, error or omission' whereas the other version covers claims for 'any act, error or omission' (other versions include coverage for 'any error or omission or negligent act'). The key difference is the absence of the word 'negligent' in front of the word 'act'. Many courts in the US interpret the insuring language of 'any act, error omission' to provide broader coverage than that afforded by the insuring language of any 'negligent act, error or omission'. Accordingly, Australian risk managers should confer with Australian insurance counsel to determine if the same

distinction holds true in Australia. If so, the word 'negligent' should be stricken from the insuring language.

E-commerce activities expose an insured to liability associated with the activities of others by way of banner ads, links and otherwise on the insured's website. Some e-commerce policies limit coverage to the insured's own advertising, broadcasting and publishing.

Patent infringement

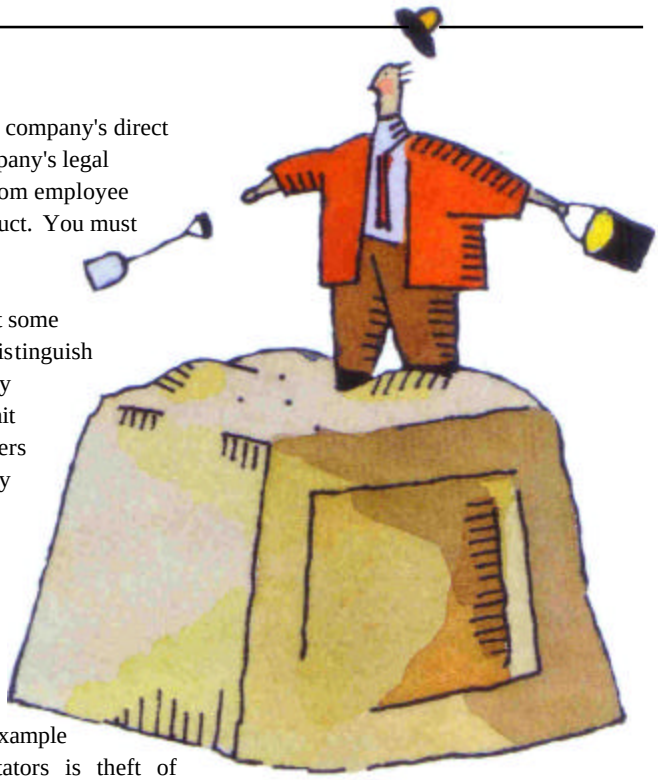
All of the policy forms reviewed by the author expressly exclude coverage for patent infringement. Companies involved in e-commerce, some argue, have a great likelihood of risk for contributing to patent infringement and/or inducing patent infringement with respect to products they do not manufacture. The typical stated concern here is that even if the insured did not manufacture the infringement product, the insured is nevertheless using, selling, marketing, or allowing to be sold, the infringing product. This issue not only goes to products being sold over the insured's website, but also to the software and computer code being used to run the insured's website. Some carriers will amend their policy forms to cover claims for such 'contributing to' and 'inducing' patent infringement.

As noted above, using the terms' liability' e-commerce insurance and 'first party' e-commerce insurance is a bit of a misnomer, because employee dishonesty and third-party malicious conduct exposures have liability risks associated with them. And coverage for the insured's liability arising from employee dishonesty and third-party malicious conduct can be provided by crime policies.

In any event, this section of the article discusses some of the issues to consider when reviewing e-commerce policies offering coverage for one or more of the following 'first party' risks: natural peril property damage, employee dishonesty, third-party crime/malicious conduct, extortion, computer programming error, and business interruption/extra expense

It is important to review the employee dishonesty and third-party malicious conduct sections of the policy. You must get coverage not only for your company's direct loss, but also for your company's legal liability to others arising from employee third-party malicious conduct. You must ensure defence costs are included.

Finally, please note that some of the e-commerce forms distinguish between the type of liability cover they offer. Some limit the cover to liability to others for the value of the property that was lost/stolen. Some, however, extend the cover to liability to others if the lost/stolen property was used by the perpetrator of the crime in a way that causes damages to others. The 'classic' e-commerce example given by most commentators is theft of credit card numbers or other information about an insured's customers and use of those numbers and other information to the financial injury of such customers. Another example given is theft of information about children who have come to a website, or whose parents have entered data about the children on a website, and a perpetrator getting a hold of the information and somehow harming a child (whether emotionally or physically).



Computer programming areas are a very hot issue in the USA as well as UK. Many e-commerce forms expressly exclude coverage for errors in computer programming. Some of the forms expressly cover the risk, but only for property loss.

Contingent risks

A common enhancement in traditional property policies offering business interruption/extra expense is to obtain coverage for 'contingent' business interruption and 'contingent' extra expense. Such coverage applies when an insured suffers a business interruption or extra expense loss because the insured's customer or supplier suffers a loss and cannot accept the insured's goods (in the case of the customer) or provide the insured with raw materials to created product (in the case of the supplier). A supplier or customer could 'go down' just as easily because of an e-commerce-related loss as it could 'go down' by fire, explosion, flood or earthquake. Thus, it is important to get contingent time element coverage into any first-party e-commerce policy.

The first-party coverage wordings all use different terminology to address the issue of whether, and to what extent, confidential information and trade secrets are covered. Some of the policies expressly cover all forms of confidential information, including trade secrets. Some of the policies expressly exclude trade secrets from being covered, and allow only coverage for customer and client information when it comes to confidential information.

In the final analysis, Australian risk managers should know and understand the coverage issues being addressed by the new stand-alone e-commerce insurance policies.

By understanding these coverages, risk managers will know what issues to look for if they choose to buy (or are forced to) one of the policies.

For further information, Michael Rossi can be contacted at mrossi@inslawgroup.com