FOA & SON
·1861·
INTERNATIONAL INSURANCE BROKERS

CORPORATE HEADQUARTERS • NEW YORK, NY • TEL 212 432 1234
EASTERN REGIONAL OFFICE • MELVILLE, NY • TEL 516 228 1234
PERSONAL LINES CENTER • VALHALLA, NY • TEL 914 773 4321

THE INSURANCE NEWSLETTER

Summer 2014

Another Look at Cyber Insurance

Security breaches and loss of personally identifiable information (PII) has been in the news more and more, with seemingly not a week going by without word of some new and significant breach somewhere. One of the most prominent was that suffered by Target stores, now estimated to amount to some 40 million credit and debit account numbers affecting 70 million people. Other retailers suffering similar breaches are names such as Neiman Marcus and Michaels Stores; many will remember the breach at TJ Maxx a few years ago, still considered the largest (so far).

Retailers aren't the only targets. Facebook, Google, Yahoo, Adobe, LinkedIn and Twitter were hacked; banks, credit card issuers, insurance companies and other financial services firms were also breached just in 2013. Healthcare providers, colleges and universities, governmental units, non-profits, and almost any other types of business or entity you can imagine...all are targets. The bad guys are motivated by the fact that they have figured out ways to profit even from less sensitive consumer information; social security numbers, payment card or other financial account data will always be prime targets for attack, but even data such as email names and login info, drivers license numbers, or just home addresses and telephone numbers has value to the black hats.

The fact is the bad guys are getting better faster than the good guys can stay ahead. Cybercrime is also an easy crime. Think about it; for an aspiring young neer-do-well, cybercrime has a lot to recommend it. Financial swindles, Ponzi schemes, burglary, robbing banks or just knocking off gas stations and other variations on traditional criminal themes are, with modern advances in law enforcement and increasingly pervasive use of surveillance cameras all generally high risk/low reward propositions. Drug dealing has always had low barriers to entry and prospects for rapid advancement, but the less severe side of that path is being eroded as states move to legalize or decriminalize marijuana. There is still a high potential reward in the upper levels of dealing harder drugs but there are a lot of unfavorable factors for an aspiring criminal to contend with, such as large capital investment in purchase, production and transportation of inventory, logistics and supply chain management challenges, and of course some very real workplace violence issues.

Cyber crime, by contrast, is easy, low risk and lucrative. The price of high powered electronics is relatively low, so it requires a fairly minimal capital investment. Working conditions are as good as they can get for a criminal, far from potential victims and even removed from potentially unstable coworkers. The range of potential targets is huge and you don't even have to be in the same country (or continent) as your victims. Another key plus for the bad guys, there are established underground markets in which you can dispose of your ill-gotten gains and convert purloined data to cash. Best of all, the chance of getting caught is quite low. Think about how many times you read about another breach; now think about how many times you read about a perpetrator being caught. Put it all together and for any ambitious young criminal type characterized by high intelligence and low morals, cyber crime is the way to go. No wonder hackers are growing more numerous, brazen and sophisticated every day.

Which all means that as a practical matter any organization possessing PII either 1) will be attacked, 2) has been attacked or 3) (the worst) has been attacked and

doesn't know it yet. The risk is real. That leaves some simple questions: what can you do to minimize your chances of being hacked, how do you respond if (when) that happens, and who pays for costs you'll incur after a breach?

To the first question, an ounce of prevention (translation: money spent for technology upgrades and IT staffing) can outweigh a pound of cure. There are big rich targets out there, often with very sophisticated data security and loss prevention measures in place. Hackers will go after them only if the potential payoff is worth the effort. For the average organization with smaller amounts of still valuable data, hackers will more than likely pass you by if your security is strong in favor of easier targets, which are everywhere.

Once breached, standard principals of crisis response apply: rapid response, communication, transparency, opening multiple lines of dialogue with regulatory authorities, the public, press, potentially affected business partners and other stakeholders. Since issues surrounding cyber crimes can be complex and confusing, there are some key differences. Laws and regulations that apply to breaches are many and varied and can be spread across multiple jurisdictions, standards for public responses are not well defined, and it can be hit or miss on whether or not your breach attracts (or keeps) the attention of news organizations. You also need to know who you need to be most concerned with responding to and reassuring: customers, clients, business partners, vendors, employees and regulators all present different and often thorny problems. All this makes responding to a breach tricky and complicated. Experts in the field say that most often breached companies, even those that made efforts to prepare beforehand, find themselves improvising as they go along, forced to respond as each new revelation unfolds.

Then there are the costs. You'll start writing checks pretty quickly after a breach, and costs can mount up rapidly. Fortunately there is reasonably priced insurance coverage available to cover those costs.

Cyber insurance (this is a generic term; insurers offering these policies have many different names for them) has evolved over the years. A decade or so ago underwriters seeking to develop these types of policies viewed the primary exposures they were trying to address as liability issues, and wrote liability policies to respond to third party suits arising from data breaches. For the most part such suits never really materialized, at least in the volume underwriters had expected.

Buyers for these types of liability policies never really materialized, either. What caused sales of cyber insurance to take off was the addition of substantial first party coverages to the forms being offered. This caught buyers' eyes; one lesson they learned early on is that there are substantial direct out of pocket costs they must bear almost immediately as a consequence of a breach. Direct costs include engaging forensic experts, legal advice, public relations expenses, outsourcing hotline support and providing credit monitoring services, and, eventually, regulatory fines and penalties. These add up fast.

These days when buyers consider cyber insurance the first thing they'll look for is coverage for direct out-of-pocket first party loss costs. Another crucial aspect to data breach preparedness is understanding legal and regulatory requirements for data breach notification and response. Facing a patchwork of 47 existing state laws plus numerous federal laws and regulations, understanding your post breach legal obligations and exposures is a daunting challenge. An important feature often found in cyber policies is breach response services, basically a phone number to call when you find out you've been breached where you can get immediate advice on how to respond. And underwriters still include third party liability coverage in most of these policies, too, but for most buyers the focus is on coverage for your own direct costs.

Insurance buyers have always been focused on obtaining insurance to cover losses to their tangible assets, buildings, contents and other property. These days they have realized that nontangible assets, in the form of information in their records and on their computers, is just as valuable and could be just as costly to the bottom line if lost. Cyber policies address this exposure; they are still relatively inexpensive, the coverage being offered now has real value, and the risk is real and growing.

If you have never looked at cyber coverage, now is the time to think about it. Give us a call and we'll be happy to talk with you about it.

TRIA Expires

When you renew most commercial insurance policies you are presented with a TRIA election form, giving you the right to reject or accept (at some additional cost) coverage for terrorism related claims. It's worth taking a moment to think about what that is all about.

Your insurance policies have always contained exclusions for claims arising from truly catastrophic events, like war or nuclear explosion. In and of themselves these types of claims could be insurable, but the concern has always been that the volume of claims arising from these types of occurrences could easily be so huge that the financial health or even the survival of the entire insurance industry could be compromised. Rather than trying to insure a risk that could be completely unpredictable and yet could bankrupt any insurance company, policies simply exclude them.

Until 2001 acts of terrorism were not considered acts of war, and no separate exclusion applied to them; claims that were presented after 9/11 were paid. But, the insurance industry took notice; here was an entirely new risk with the potential to drop billions of dollars of claims in their laps at any time, repeatedly. Terrorism risk is unpredictable, unquantifiable, impervious to actuarial analysis and potentially huge; that is the definition of an uninsurable risk. Exclusions for claims arising from acts or terrorism appeared almost instantly.

Insurance is a mechanism to protect and make whole those few who suffer unfortunate incidents by spreading the cost of those events over many others, and over time. Considered as a cost spreading device it's the perfect means to spread the risk even of events like terrorist attacks. For that reason Congress enacted the Terrorism Risk Insurance Act (TRIA) in 2002 in response to new policy exclusions for claims arising from acts of terrorism. The law provides a government reinsurance backstop for insurance companies offering coverage for terrorist acts, subject to certain definitions and retentions held by insurers. With TRIA as a backstop, the insurance industry can offer coverage for terrorism claims that it could not afford to offer otherwise. Extended first in 2005 and again in 2007, TRIA is set to expire at the end of 2014. Congress is again reconsidering the appropriate government role in terrorism insurance markets. There is no certainty that TRIA will be extended, or on what terms if it is.

For most insurance buyers this will have little impact, since buyers commonly reject TRIA unless they are an operation or location that might be considered a possible terrorist target. One policy you buy will be affected, though. Terrorism exclusions can be and have been added to almost all commercial insurance policies, but not workers compensation. The main insuring clause in your workers compensation policy says that it will pay for claims as required by the applicable state workers compensation law. No state WC law excludes terrorism claims. Consider 9/11; every one of those workers in the World trade Center buildings, every police, fire and other first responder, every other worker in surrounding areas forced to evacuate...all were, are, and will be in the future covered by workers compensation.

Like it or not you already pay a terrorism surcharge on your WC policy. Absent TRIA this would likely increase. Workers compensation is state specific, so states with a higher potential for terrorist attack like New York or California would likely see higher surcharges. Insurance companies could also try to soften that impact by increasing such charges across the country.

Another very real likely impact would be that employers with a work force concentrated in potential targets areas might not be able to buy WC in the standard market at all. There are already signs that large insurance companies are looking at aggregation, the concentration of policies they write in certain terrorism exposed areas. Absent TRIA, insurers may not wish to write any, or any more, WC policies in such areas. Buyers only resort would be to obtain coverage in residual markets or assigned risk pools, which of course charge higher premiums.

Expiration of TRIA and growth in the residual or assigned risk market would also mean that WC losses from a catastrophic terror attack would primarily be financed by taxpayers and employers in the state in which the attack occurs, adding to the challenge of rebuilding in that state. TRIA, in contrast, spreads such risk across the entire country.

We are keeping an eye on this issue for you.

Insurance to Value

This perennial topic is worth revisiting periodically; it comes to the forefront again driven by events following large natural catastrophes we have seen recently.

blizzards and ice storms and southern tropical storms all illustrate the problem.

Building (and rebuilding) costs have increased steadily over the past twenty years. The rise has been most dramatic in habitational type structures, but no class of buildings are immune to the many factors that are driving up building costs. Cost of building materials of all types are higher than ever, labor costs continue to creep upward, and, less visible but increasingly important, building codes continue to get more stringent, driving up the costs of any major renovation or construction.

Property owners who have not been diligent in keeping the amount of insurance they carry on their properties up to date can still survive an underinsured loss when the cause of loss is a single event, like a fire. Rebuilding may be delayed or prolonged while they shop for bargains and haggle with contractors, there may have to be some compromises on quality or standards, and additional financing may be needed, but usually the building can eventually be rebuilt or repaired.

Should the same loss take place as part of a larger natural catastrophe (wildfire, tornado, hurricane), all bets are off. Inevitably after such events, rebuilding

FOA & SON ·1861·
INTERNATIONAL INSURANCE BROKERS
68 South Service Road
Melville, NY 11747-2357

PRESORTED STANDARD
US POSTAGE
PAID
PERMIT NO 231
WINSTON SALEM, NC

costs rise as demand spikes. No deals are to be found on material costs, and busy contractors command top dollar.

Even now, property insurance rates are a relative bargain compared to other lines of insurance. It only makes sense to be sure that the limits you carry on your property coverages are adequate to cover the worst case scenarios.

Job Security and WC Claim Duration

File this one under the category “blindingly obvious”: The Workers Compensation Research Institute just released a carefully researched report that concluded that workers who are concerned that they may not have a job to return to after filing a workers compensation claim have longer disability durations than workers who feel secure in their employment. Lack of trust in an employee’s job security after a work accident led to an average increase of four weeks in the duration of a claim.

Given that the average duration of all temporary total disability claims is around 140 days, that means that an injured worker worried about his job costs about 20-25% more than one who feels secure in his ability to return to work.