THE TEXAS LAWBOOK

SERVING BUSINESS LAWYERS IN TEXAS

Cyber Risk – What's a Business to Do?

By Amy Dunn Taylor – (November 21, 2014) Blitz-Krieg and Bomber and Heartbleed – the names sound positively demonic and they are as Sony, JP Morgan, Target and others can attest. Virtually every business and organization is vulnerable, admittedly some more vulnerable than others. Each face the very real yet insidious threat of suffering a data breach.

What's a company or organization to do in the face of these invisible but very real threats? Is cyber risk insurable and if so, what products are available?

Traditional coverage available to businesses and organizations include comprehensive general liability policies and more specialized polices for business interruption, directors and officers acts, errors and omissions and corporate crime policies.

Each of these has its pros and cons in the cyber theft world but the one thing every risk manager, general counsel and chief information officer must know is this: Increasingly, traditional insurance products are being written to specifically exclude cyber risks and breaches.

There are both practical and business reasons and determining which insurance to purchase requires a thorough understanding of both sides of the equation.

The Practical Side

Under Comprehensive General Liability (GCL) policies, "damages" have been interpreted to mean money recovered by a party as compensation for loss or detriment suffered because of the wrongful acts of another. On top of traditional monetary damages, plaintiffs generally seek relief for cyber liability claims via statutory penalties, injunctive relief, restitution and attorneys' fees.

Whether these additional forms of relief amount to "damages" impacts an insurer's duty to defend and indemnify. Likewise, "property damage" has traditionally included "physical injury to tangible property" and "loss of use of tangible property that has not been physically injured." Is electronic data "tangible property"? Does it matter whether "physical injury" to the property exists? Does the impairment or breach of computer data and software amount to "property damage" such that coverage is triggered? These are issues that are being addressed in courts across the country.

Amy Dunn Taylor

Other traditional policies may offer businesses a place to turn in an effort to secure coverage for data breaches, cyber liability to customers and other related claims. These include business interruption, directors and officers, errors and omissions and crime polices. Each has its corresponding limitations though.

Business interruption polices typically provide coverage for "risks of direct physical loss or damage," but is the loss of computer data covered as a "physical loss?" At least one court has said no. In *Ward General Insurance v. Employers Fire Ins. Co.* (114 Cal. App. 4th 548, 2003), a California Court found that the loss of electronically stored data, without loss or damage to the storage media, was not a covered "physical loss," noting that the insured did not lose tangible material, but rather stored information. Other courts, including at least one appellate court in Texas have found to the contrary citing "physical damage" is not restricted to physical destruction to the computer's circuitry but ›

© 2014 *The Texas Lawbook*

also includes loss of access, loss of use and loss of functionality.

Directors and officers liability policies generally provide coverage for the wrongful acts, negligence or errors in business judgment by the officers and directors of organizations. Directors and officers may be able to seek coverage for their failure to implement any cyber security measures, or even adequate ones, but these issues have not yet been tested in the Courts. The anticipated claim against the insured is that it failed to implement industry standard protections which may be a bootstrap to claims against the insured's directors and officers. Time will tell.

Error and omissions polices generally provide coverage for the negligent acts, errors and omissions in the performance of the insured's professional services. Many policies limit coverage to acts that are no more than negligent and specifically exclude any intentional wrongful acts.

Crime policies afford coverage for theft of money, securities or property but often exclude theft of information, trade secrets and other confidential information. Even cybercrime riders are typically limited to theft of information and do not cover invasions of privacy as a consequence of the theft.

The Business Side

So what are the options available to businesses and consumers who desire to purchase a cyber-liability policy? Not surprisingly, the insurance industry has developed new insurance products designed to fill in the gaps left open by the more traditional policies. These products are becoming increasingly standardized to provide stable coverage. These new policies fall neatly into two categories: first party coverage and third party coverage.

First party coverage polices typically cover costs the insured incurs in responding to a data breach incident and any loss or damage to the insured's technology systems. Depending on the product, first party cyber liability policies may exclude or limit coverage for:

- losses caused by power outages or compromised telecommunications services
- fire loss;
- damage to computer hardware;
- design failure arising out of the architecture or configuration of the insured's computer system; and
- ordinary wear and tear of the computer system.

Third party coverage policies typically cover certain third party losses on a claims-made basis and may include damages arising from the distribution of content over the internet, damages arising from the unauthorized access or use of the insured's computer system and denial, impairment or interruption in service to a customer's account. Some polices may afford coverage to the insured for crises management expenses including:

- notifications to customers of an adverse event;
- credit monitoring and credit protection services for customers;
- management of negative publicity from adverse media reports; and
- preservation of evidence and forensic investigation if paid to outside consultants.

These optional coverages are often for only a limited or agreed-upon time period following the security breach and they may exclude claims or lawsuits against the insured, legal fees attendant to such claims, damages arising from the insured's violation of its own privacy policy or any fines or penalties imposed. New product suites include coverage for cloud computing, data privacy, network interruption and intellectual property issues. Areas where coverage has yet to be explored include a decline in stock price following a cybersecurity breach, impact on reputation and BYOD (buy your own device) ›

© 2014 *The Texas Lawbook*

risks created by adeptly designed malware which turns employees' devices (*i.e.* smartphones, tablets and PCs) into unwitting attackers at their own companies and of their own accounts.

In a nutshell, the savvy corporate consumer should shop for business appropriate policies and be well informed of the coverage ultimately purchased. An annual audit of policies may be a prudent move as well since these policies seem to change to meet ever-emerging needs.

Potential Typical Policyholders

At the risk of being superficial and glib, any business or organization with a computer system is at risk – certainly some more so than others. Policyholders could include:

- Financial institutions;
- Retailers;
- Investment managers;
- Brokerage houses;
- Credit card issuers;
- Energy sector organizations;
- Manufacturing enterprises;
- The military;
- Governmental agencies; and
- Anyone storing, collecting or holding sensitive information for their enterprise or for others.

Tips for Businesses in Choosing Cyber Risk Coverage

1. Buy the broadest coverage available; this includes 1st and 3rd party coverage.
2. Make sure your coverage protects information in the care, protection and control of third parties.
3. Assure that data recovery is covered.
4. Consider whether you need coverage for regulatory activity or requirements attendant to same.
5. Consider whether coverage should address data transmittals outside of the office and/or on unencrypted devices.
6. Assess the need for coverage if your business takes credit card payments.
7. Consider purchasing coverage for loss control evaluation services or identity theft resolution services. The former may help the smart corporation or organization minimize threats on the front end while the latter may assist in solving problems after-the-fact.
8. Examine need for coverage for injuries to corporate clients.

Considerations, Criteria and Requirements for Policyholders

In a perfect world, the partnership between a business and its insurance company would be based on full information and informed shared risks. This is even more true in the world of cyber liability policies and coverage. Not only is this good and prudent business and risk management; it is also wise.

In a world of increasing cyber threats or even simple computer lapses, any good business thrives on understanding where its weaknesses are and taking the necessary steps to compensate for those weaknesses. Likewise, carriers are interested in minimizing risk where possible.

There are a number of things businesses and carriers alike should explore together. Indeed, many of these are made prerequisites by some carriers who write these policies, including:

1. Participating in loss control evaluation services. These use third parties to examine a business's practices and technology and then come up with where vulnerabilities exist and how to best control those. Suggestions may include built-in alerts on computer systems, ways to protect information in the hands of third parties, encryption of data and data backup and restoration systems;
2. Reporting to the carrier on regulatory requirements and undertakings on a routine basis; ›

© 2014 *The Texas Lawbook*

3. Employing and implementing a policy to protect for breaches. An example is regular and sustained internal communications about potential risks;
4. Engagement of theft resolution services and;
5. Systematic and regular employee training as to cyber theft avoidance

With prudence, wisdom and constant vigilance, most businesses can tremendously diminish the risk of a cyber-invasion and with a strong business/insurance partnership, most other cyber risks can be managed wisely.

Amy Dunn Taylor is a Director in the Houston office of Kane Russell Coleman & Logan PC and author of Cybersaurus Lex, the Cyber Security law blog. She is a seasoned trial lawyer with more than 32 years of experience. She is also a trained mediator and arbitrator. She practices in the Litigation Practice Area. Her practice has included cyber security and risk consultation, product and premises liability cases, construction claims, mass tort and toxic tort personal injury claims such as silicone implants, asbestos, silica and mold exposure cases, business torts and contract disputes. She has tried virtually every type of civil case and worked on both sides of the docket.

Please visit www.texaslawbook.net for more articles on business law in Texas.

© 2014 *The Texas Lawbook*