CYBERCRIME: INSURANCE COVERAGE ISSUES AND OPTIONS

Thomas W. Brown

CYBERCRIME: INSURANCE COVERAGE ISSUES AND OPTIONS

Thomas W. Brown, Esq.
Cosgrave Vergeer Kester LLP
Portland, Oregon[1]

INTRODUCTION

Technology drives business and industry today. It permeates commercial life. And that leads to "only one thing: someone will look for ways to steal, damage, or interrupt that technology world for his or her own financial benefit or other purpose [and t]hat present reality is where cyber risk and the need for protection from loss and damage, either through insurance coverage or otherwise, intersect." Toni Scott Reed, CYBERCRIME: LOSSES, CLAIMS, AND POTENTIAL INSURANCE COVERAGE FOR THE TECHNOLOGY HAZARDS OF THE TWENTY-FIRST CENTURY, 20 Fidelity L J 55 (Nov 2014) (hereafter Reed). In other words:

> "The sheer scale of loss and damage resulting from cyberattacks is growing rapidly. The sophistication of the schemes used to inflict losses and damage is constantly expanding as well. Stories of cybercrime, hacking, system incursion, and other sophisticated schemes dominate the news cycle, affecting not only businesses as a whole, but also individual consumers. FBI Director Robert Mueller has accurately described our world today: "there are only two types of companies: those that have been hacked and those that will be." For that reason, cybercrime, and the potential insurance coverage that may be available to indemnify for loss sustained from cybercrime, are important subjects for analysis.
>
> "Hacking has long been an anticipated risk and a hazard for business. For that reason, there are many forms of insurance coverage that anticipated loss resulting directly from a computer hacking, and which were intended to provide coverage for those losses that directly follow a hacking. Hacking, in its many forms and iterations, is discussed in the analysis of this article, as are the types of insurance coverage that exist and that are developing to protect businesses from the hazard of hacking. One focus of the discussion is to analyze the full scope of insurance products that exist and that may be a source of coverage, depending upon their terms and scope."

Reed, 20 Fidelity L J at 55-56.

---

[1] Thomas W. Brown is with the Portland, Oregon ALFA firm. His practice for 35 years has focused on civil appeals in state and federal courts, insurance coverage opinions and litigation, professional liability defense, and serving as a neutral for arbitrations and mediations. Thom is the immediate past-chair of the ALFA Insurance Practice Group.

This paper briefly discusses (1) cybercrime and its costs; and (2) insurance coverage for cyber-attacks, borrowing heavily from Toni Reed's work as well as the work of several other commentators. While much remains unclear in terms of that subject, one thing is clear: businesses need to examine very carefully their existing insurance policies to determine the extent, if at all, that they cover the various cyber-activities risks and obtain additional, different coverage to ensure the best protection possible against cyber-activities losses.

DISCUSSION

1. What is Cybercrime?

> "The term 'cybercrime' is discussed in many contexts and settings, and while there are many variations on its definition, most appear to be consistent with the dictionary definition of 'crime conducted via the Internet or some other computer network.' Cybercrime can take many forms and can be accomplished through many different schemes. Cybercrime includes theft, fraud, misdirection of communication, identity theft, intellectual property theft, corporate espionage, system sabotage, data destruction, money laundering, and terrorism. Some of the main categories of threats from cybercrime include computer system intrusion for monetary or other benefit, manipulation of information or networks, data destruction, misuse of processing power, counterfeit items, or interception for espionage. Most often, these types of scheme are carried out by someone without authorized access to a computer system."

Reed, 20 Fidelity L J at 57 (footnotes omitted). *See also id*. at 57-61; Gregory D. Podolak, INSURANCE FOR CYBER RISKS: A COMPREHENSIVE ANALYSIS OF THE EVOLVING EXPOSURE, TODAY'S LITIGATION, AND TOMORROW'S CHALLENGES, 33 Quinnipiac L Rev 369, 374-76 (2015) (hereafter Podolak) (discussing specific subcategories of cybercrime).

2. Cybercrime's Costs

The general effects of cybercrime on businesses include direct and indirect financial losses, exposure to regulatory issues, liabilities to customers and financial institutions, damage to brand and reputation, and loss of public confidence. Reed, 20 Fidelity L J at 68. Cybercrime "also has a substantial overall impact on the economy, although it is more difficult to estimate.

Additionally, the executives of businesses that have experience hacking often face scrutiny and criticism in the fallout from cybercrime, often leading to public resignations. Consumers may lose confidence in providing their information to businesses and decline to do so as often. Society may suffer from those who seek to steal technology rather than innovate." *Id*. at 68-69.

3. Insurance Coverage for Cybercrime[2]

a. First-party losses

According to Reed:

> "First-party losses from cybercrime are those an owner sustains when cybercrime damages, destroys, or deprives the insured of the use of insured property. These losses are generally caused by security breaches from the recurring schemes and hazards discussed above, *e.g*. Trojan horses, malware, hacking, fraud--including computer fraud and funds transfer fraud; and e-commerce extortion.
>
> "First-party risks include the cost of replacing data that is lost through corruption of the system, loss of stolen property, the cost of replacing systems that become inoperable, and the labor expenses from re-entering data. Additionally, an insured faces first-party risks of defenses expenses, fines, or penalties from state and federal statutes and regulations that require companies to report breaches. Finally, there may be risks of lost income, consequential damages, and crisis management costs."

---

[2] The following articles provide excellent discussions of policy provisions in various policy forms that cover (or potentially cove) cyber-activities. Reed, 20 Fidelity L J at 83-104; Michael Sean Quinn, INSURANCE UNIVERSALS & THE ARRIVAL OF THE CYBER-POLICY--PART TWO: SOME SPECIFICS ON LIABILITY INSURANCE, 13 J Tex Ins L 19, 20-26 (Winter 2015) (hereafter Quinn) (providing specific examples of existing coverages); Micah E. Skidmore, NEGOTIATING COVERAGE & PURSUING CLAIMS UNDER CYBER-SECURITY & PRIVACY INSURANCE, 13 J Tex Ins L 27, 28-31 (Winter 2015) (hereafter Skidmore); Podolak, 33 Quinnipiac L Rev at 374-76; Daniel Garrie and Michael Mann, CYBER-SECURITY INSURANCE: NAVIGATING THE LANDSCAPE OF A GROWING FIELD, 31 J Marshall J Info. Tech. & Privacy L 379 (2014) (hereafter Garrie and Mann) (same). *See also* James L. Rhyner and H. Wesley Sunu, *Cyber Liability Insurance for Law Firms and Legal Organizations, in The ABA Cybersecurity Handbook* 193 (Jill D. Rhodes & Vincent Polley eds, ABA 2013); Lorelie S. Masters, *Insurance Protection for Security Breaches, in Data Breach and Encryption Handbook* 280 (Lucy Thompson ed, ABA 2011); Mary Thompson, *CNBC, Why Cyber-Insurance Will Be the Next Big Thing*, http://www.cnbc.com/id/101804150 (July 1, 2014) (also providing excellent discussions of topics).

Reed, 20 Fidelity L J at 72-73 (footnotes omitted). *See also id*. at 73-74 (providing various examples of first-party losses).

b. Third-party losses

According to Reed:

> "Third-party losses are losses that result when cybercrime damages or destroys data or steals information of a third party that is in the care, custody, or control of the victim of the breach, *i.e.* the insured. These losses are typically sustained from the following general cybercrimes: intrusion into computer systems to steal bank account numbers, transmission of a computer virus through the insured's computer system into the system of a third party, exclusion of an authorized third party from insured's computer system, and failure to give notice to a third party of the intrusion in violation of statute, regulation, or contract.
>
> "Third-party risks include loss of another's electronic data, software, and hardware and the resulting loss of use. Additional third[-]party risks include losses resulting from passing onto a third party malware that causes damages to the third party's computer or data, data security breach and privacy injury, liability under statutes like the Computer Fraud and Abuse Act, and litigation under tort actions, such as invasion of privacy, negligence, or contractual actions."

Reed, 20 Fidelity L J at 74-75 (footnotes omitted). *See also id*. at 75-76 (providing various examples of third-party losses).

c. Scope of available coverages

A. Traditional coverages

Most businesses purchase commercial general liability (CGL) insurance to cover potential liability to third parties, and that is the first place businesses often look for coverage in the event of a cybercrime. Although CGL policies may differ, most are based on standard policies promulgated by the Insurance Services Office, Inc. (ISO). CGL policies provide coverage for several areas of risk, but only Coverage A and Coverage B could possibly cover cybercrime losses. Coverage A addresses liability for "bodily injury" or "property damage" caused by an "occurrence" defined as an "accident." Coverage B in a standard CGL policy

provides coverage for "personal and advertising injury." Coverage under this provision often depends on whether there has been a "publication" that violates the claimant's "right of privacy," since those two terms are not defined in standard-form ISO policies. *See* Podolak, 33 Quinnipiac L Rev at 382-94 (discussing common issues under CGL policies).

Another traditional source of coverage is that of commercial property insurance. Commercial property insurance began with fire insurance, but has expanded to include many more risks, or "perils." A commercial property policy may either be a "named peril" policy and cover only damages from specific risks, or an "all risks" policy and cover damages from all risks except those excluded by the policy.

B. Errors and omissions policies

Errors and Omissions (E&O) policies provide coverage for liability arising out of an act, error, or omission of the insured in rendering or failing to render services. The policies are typically sold on a "claims-made" basis and cover only "damages." Insurance companies also provide E&O policies for software, information-technology services, and e-commerce businesses that provide for two basic risks (1) coverage for financial losses of third parties arising from failure of the insured's product to perform as intended or expected; and (2) coverage for financial losses of third parties arising from an act, error, or omission committed in the course of the insured's performance of services for another. These policies require that "wrongful acts" must be committed "in the course of the insured's performance of services for another."

C. Cyber-liability-specific policies

More insurers are beginning to offer specialized insurance policies specifically designed to protect against loss from cybercrime. These policies may include both first-party and third-party coverage. The first-party provisions or policies cover loss of data or network interruption,

while the third-party provisions or policies provide coverage for liability to third parties arising from the loss or theft of data. These newer insurance products focus on coverage for security of data, programs, and proprietary information, and for computer-based transgressions, including viruses, cyber-attacks, fraud, destruction, corruption, or extortion from threatened computer crime. These policies may cover crisis management expenses, such as expenses for hiring a public relations or law firm to repair the insured's reputation. Many policies provide "breach of notice" costs, including mailing, phone bank, and credit-monitoring costs. Additionally, third-party policies may include defense and indemnity coverage for regulatory liability, including claims for civil, administrative, or regulatory proceedings, fines, and penalties. *See* Garrie and Mann, 31 J Marshall J Info Tech & Privacy L at 387 (detailing various coverages in cyber-liability-specific policies); Podolak, 33 Quinnipiac L Rev at 394-409 (detailing various coverage issues involving cyber-liability policies).

D. Bonds and commercial crime policies

Financial institution bonds insure financial institutions against employee dishonesty and provide coverage for certain other specified risks. The standard form has been revised numerous times since its first issuance, but the most recent revision from 2004 includes the following insuring agreements: fidelity, on premises, in transit, forgery or alteration, securities, counterfeit money, and fraudulent mortgages.

Commercial crime insurance policies are a type of fidelity insurance offered to non-financial commercial and governmental entities, where fidelity insurance provides coverage for losses sustained as a direct result of an insured's employees' dishonesty. Generally, commercial crime policies provide coverage for losses the insured sustains as a direct result of the following: employee dishonesty or theft. forgery or alteration of written instruments, loss and damage

resulting directly from "theft," disappearance or destruction of "money" or "securities" from inside the premises of the insured; loss resulting from an actual or attempted robbery or safe burglary inside the premises; loss occurring outside the premises of the insured, loss of "money," "securities," and "other property" resulting directly from the use of any computer to transfer such items from that insured's premises to a person or place outside those premises, loss of "funds" resulting directly from a "fraudulent transaction" directing a financial institution to transfer such funds from the insured's "transfer account," and loss directly resulting from the insured having accepted counterfeit currency or money orders in good faith and in exchange for merchandise, money, or services.

E. Hybrid business packages

Insurers also offer hybrid policies that incorporate provisions from more than one of the insurance products described above. A hybrid policy may include provisions that cover traditional areas of coverage in a CGL policy as well as provisions that cover liability for errors and omissions. A financial institution bond may include extended coverages for indemnity for injury or death or directors or employees.

d. The existing legal world for cybercrime coverage issues

With the multitude of policy coverages and cyber-activities, comes the inevitable multitude of legal disputes. *See* Reed, 20 Fidelity L J at 77-78, 109-132 (providing detailed analysis of key issues and court decisions); Skidmore, 13 J Tex Ins L at 28-34 (same). Insureds are seeking – and likely will continue to seek – coverage under all possible forms and policies. And so insurers will continue to face a myriad of coverage issues over the upcoming years. And, while most likely, as time goes on, the fights between insured and insurers will focus on cyber-liability-specific policies as the market moves more and more toward such coverage forms, given

the variety of existing cyber-liability-specific policies (and their likely evolution in the future) along with the ever-changing nature of cyber-attacks, even that future narrowing of cyber-liability coverage disputes will almost certainly continue to result in frequent litigation over cyber-liability claims for years to come, challenging insureds and insurers and courts alike.