June 2013

The text of this article first appeared in the June 2013 issue of *The Insurance Coverage Law Bulletin*, Vol. 12, No. 5

Insurance Coverage for Cyber Attacks

Part Two of a Two-Part Article

By Roberta D. Anderson

Last month, Part One of this article addressed the role of traditional insurance in covering cyber risks. This second installment first continues the discussion of traditional insurance coverages and then addresses specialty "cyber" policies.

3) Potential Coverage Under Property Policies

Injury to Covered Property: Most companies have insurance coverage that is intended to insure the company's assets. By way of example, the 2007 standard form ISO commercial property policy covers "direct physical loss of or damage to Covered Property at the premises described in the Declarations caused by or resulting from any Covered Cause of Loss." ISO Form CP 00 99 06 07 (2007), Section A. Such policies may be in the form of broadly worded "all risk," "difference in conditions," "multiperil" or "inland marine" policies.

As discussed previously in connection with CGL coverage, a company's ability to recover for cyber attacks under all risk property policies may turn upon whether data loss comprises "physical loss of or damage" to "covered property."

Business Interruption and Extra Expense: Many first-party policies also provide so-called "time element" coverages — including "business interruption" and "extra expense" coverages — that cover loss resulting from the company's inability to conduct normal business operations. These coverages may cover business interruption resulting from a cyber attack. "Business Interruption" coverage generally reimburses the insured for its loss of earnings or revenue resulting from covered property damage. For example, the ISO "Business Income (and Extra Expense) Coverage Form" covers the loss of net profit and operating expenses that the insured "sustain[s] due to the necessary 'suspension' of [the insured's] 'operations' during the 'period of restoration.'" ISO Form CP 00 30 06 07 (2007). "Extra Expense" coverage generally covers the insured for certain extra expenses incurred to minimize or avoid business interruption and in order to resume normal operations. For example, the ISO standard form covers, among other things, "Extra Expense" to "[a]void or minimize the 'suspension' of business and to continue operations at the described premises or at replacement premises or temporary locations. … " *Id.* The form defines "Extra Expense" as "necessary expenses" that the insured "would not have incurred if there had been no direct physical loss or damage to property caused by or resulting from a Covered Cause of Loss." *Id.*

A company may have coverage under these provisions for loss of business and extra expense associated with a cyber attack. For example, the Fourth Circuit in *NMS Services Inc. v. Hartford*, 62 Fed.Appx. 511 (4th Cir. 2003), upheld coverage for business interruption and extra expense coverage for the costs associated with an employee hacking incident that resulted in "the erasure of vital computer files and databases necessary for the operation of the company's manufacturing, sales, and administrative systems." *Id.* at 512. In that case, the insured's employee "had installed two hacking programs on [the insured's] network systems while he was still employed," which "allowed [the employee] to gain full access to [the insured's] systems by overriding security codes and unencrypting secured passwords, thus enabling [the employee] to cause the damage[.]" *Id.* The Business Income

Additional Coverage section in the policy at issue stated that the insurer would "pay for the actual loss of Business Income [the insured] sustain[s] due to the necessary suspension of your 'operations' during the 'period of restoration.' The suspension must be caused by direct physical loss of or damage to property at the described premises. … " *Id.* at 514. The Fourth Circuit easily determined that the business income and extra expense coverages applied because, in the court's words, there was "no question that [the insured] suffered damage to its property." *Id.*

A Texas appellate court likewise found coverage for business interruption in *Lambrecht & Associates, Inc. v. State Farm Lloyds*, 119 S.W.3d 16 (Tex. App. Ct. 2003). In that case, the insured sought coverage for the loss of computer data and the related loss of business income after a "virus caused the [insured's] computers to have difficulties while 'booting up,' perform a number of 'illegal functions' and eventually completely 'freeze up,' thereby rendering the computers useless." *Id.* at 23. The insured's computer system had to be taken offline, and its employees were unable to use their computers until the server was restored. *Id.* at 19. The insurance policy at issue committed the insurer to "pay for accidental direct physical loss to business personal property" and "the actual loss of 'business income' [the insured] sustained due to the necessary suspension of [its] 'operations' during this 'period of restoration.'" *Id.* The court disagreed with the insurer's argument that "the loss of information on [the insured's] computer systems was not a 'physical' loss because the data … did not exist in physical or tangible form," *Id.* at 23, and held that "the plain language of the policy dictates that the personal property losses alleged by Lambrecht were 'physical' as a matter of law." *Id.* at 25. The court further held that "the business income [the insured] lost as a result of the virus [wa]s covered under the policy." *Ibid*.

In addition to business interruption coverage, companies may have "contingent business interruption" coverage that covers the insured with respect to losses, including lost earnings or revenue, as a result of damage, not to the insured's own property, but to the property of an insured's supplier, customer or some other business partner or entity. ISO CP 15 08 04 02 (2001). This may be increasingly important coverage in the context of "cloud" outsourcing of maintenance and control over data to third parties. As one commentator has noted, "business interruption losses resulting from loss of access to the cloud should, in the majority of cases, be covered under so-called 'legacy' contingent business interruption forms." Lon Berk, *CBI for the Cloud*, Vol. 21, No. 6, Coverage, at p. 11 (ABA November/December 2011).

Newer First-Party Forms May Contain Sublimits: It is important to note that some standard forms seek to shift data loss from the principal coverage grant by excluding electronic data from the definition of "Covered Property" and instead providing coverage under "additional coverage" that may be subject to relatively low — presumptively inadequate — coverage sub-limits. For example, the 2007 ISO Commercial Property Form excepts "electronic data" from the definition of "Covered Property" and provides coverage under an "Additional Coverage" that is limited to "$2,500 for all loss or damage sustained in any one policy year, regardless of the number of occurrences of loss or damage or the number of premises, locations or computer systems." ISO Form CP 00 99 06 07 (2007), Sections A.2.n., A.4.e.(1), (2), (4).

Likewise, the 2007 ISO standard form Business Income (and Extra Expense) Coverage Form excludes coverage for electronic data under the main coverage part and provides coverage under an "Additional Coverage" subject to a $2,500 limit for "all loss sustained and expense incurred in any one policy year, regardless of the number of interruptions or the number of premises, locations or computer systems involved." ISO Form CP 00 30 06 07 (2007), Sections A.4, A.5.d.

These mechanisms underscore the importance of considering not only what cyber risks may be covered, but also whether the limits are sufficient.

Insurance Coverage for Cyber Attacks

4) Potential Coverage Under Other Traditional Policies

Many companies have various types of crime coverage, including fidelity insurance and financial institution bonds that may cover cyber risks and losses. Other types of conventional liability coverages, such as directors' and officers' ("D&O") liability, errors and omissions ("E&O") and professional liability coverages may also respond to cover cyber attacks and losses. In the *Eyeblaster* case discussed previously, for example, the Eighth Circuit also upheld coverage under an Information and Network Technology E&O policy.

Addressing the question of coverage under a crime policy, the Sixth Circuit recently confirmed that an insured was covered for more than $6.8 million in stipulated losses associated with a data breach that compromised customer credit card and checking account information in *Retail Ventures, Inc. v. National Union Fire Ins. Co. of Pittsburgh, Pa.*, 691 F.3d 821(6th Cir. 2012) (predicting Ohio law). In that case, the insured incurred substantial expenses for customer communications, public relations, customer claims and lawsuits, and attorney fees in connection with investigations by seven state Attorneys General and the Federal Trade Commission. *Id.* at 824. The Sixth Circuit confirmed that there was coverage under the computer fraud rider of the insured's blanket crime policy, which stated that the insurer would pay the insured for "Loss which the Insured shall sustain resulting directly from … [t]he theft of any Insured property by Computer Fraud." *Id.* at 826. "Computer Fraud" was defined as:

> the wrongful conversion of assets under the direct or indirect control of a Computer System by means of: (1) The fraudulent accessing of such Computer System; (2) The insertion of fraudulent data or instructions into such Computer System; or (3) The fraudulent alteration of data, programs, or routines in such Computer System. *Id*. at 826-27.

Specialty 'Cyber' Policies

The *Sony* coverage suit does not represent the first time that insurers have refused to voluntarily pay claims resulting from a network security breach or other cyber-related liability under CGL policies. Nor will it be the last. Even where there is a good claim for coverage, insurers can be expected to continue to argue that cyber risks are not covered under CGL or other "traditional" policies.

Insurers are marketing newer insurance products specifically tailored to cover cyber risks, and this has been called "the new frontier of the 21st century market." Harry Cylinder, *Evaluating Cyber Insurance*, CPCU eJournal (Dec. 2008).

The new cyber policies may come under names such as "Privacy and Security," "Network Security," and names that incorporate "Cyber," "Media" or some form of "Technology" or "Digital." "Cyber" risk coverage can be extremely valuable. But choosing the right cyber insurance product can present a real and significant challenge. The cyber coverages available in the marketplace for cyber risks are far from standard. There is a dizzying array of cyber products in the marketplace, each with its own different terms and conditions. The terms and conditions of these policies vary quite dramatically from insurer to insurer — even from policy to policy underwritten by the same insurer. Therefore, more than is the case with most types of insurance policies, successful negotiation and placement of cyber coverage requires identification and consideration of a company's potential risk scenarios, knowledge of the available coverages in the marketplace, and careful attention to the specific policy language under consideration. Consideration should also be given to the overall structure of the insurance program, which should be carefully reviewed, not only to eliminate potential gaps in coverage, but also to minimize coverage overlaps and attendant costs and inefficiencies. Coverage must be adequate

to address a company's risk profile, but should not include payment of premium for coverage a company does not need.

Of course, companies that have already purchased specialty "cyber" policies should be fully familiar with the coverage provided so that they can take full advantage of that coverage.

Cyber risk policies often offer both first-party and third-party cyber coverage as separate coverage parts, and companies can often select coverages on an individual or combined basis. The types of losses and liabilities that cyber risk policies may cover include the following:

- losses resulting from a data breach, including defense and indemnity costs associated with third-party actions against a company, as well as response costs associated with post-breach remediation, including notification requirements, credit monitoring, call centers, public relations efforts, forensics and crisis management;
- regulatory investigations, fines and/or penalties;
- losses resulting from a misappropriation of intellectual property or confidential business information;
- losses resulting from transmission of malicious code or denial of third-party access to the insured's network, and other security threats to networks;
- the cost to recover data that are damaged by malicious code or stolen;
- business interruption resulting from operations being disabled by a cyber attack; and
- extortion from cyber attackers who have stolen data.

In addition to providing indemnity coverage for judgments and settlements, the majority of cyber policies also cover the cost of defending claims resulting from data security breaches, regulatory investigations, infringement claims and other third-party liabilities.

The author is unaware of any cases addressing coverage under these newer policies. An overview of certain types of coverage available under these policies is provided below. Although specimens of these newer policies are available, the actual language contained in the policy issued to the company could substantially differ from the specimen policy. It is important to note that coverage in all cases will turn on the particular language of the policy as applied to the specific facts at issue.

1) Third-Party 'Cyber' Coverage

Data Breaches, DDoS and Malicious Code Transmission: "Third-party" cyber liability policies typically cover the insured against liability arising from, for example, data breaches, transmission of malicious code, denial of third-party access to the insured's network, and other security threats to networks. For example, the new Hartford CyberChoice 2.09SM specimen policy provides coverage for loss of customer data, denial of access, and other cyber risk events. The specimen policy states that the insurer will pay "damages" that the insured "shall become legally obligated to pay as a result of a Claim … alleging a Data Privacy Wrongful Act or a Network Security Wrongful Act." Network Security liability Insurance Policy Form #DP 00 H003 00 0312 (2012) at section I.

A covered "Data Privacy Wrongful Act" is defined to include "any negligent act, error or omission by the Insured that results in: the improper dissemination of Nonpublic Personal Information" which, in turn, is defined as:

Insurance Coverage for Cyber Attacks

1. a natural person's first name and last name combination with any one or more of the following:
   a. social security number;
   b. medical or healthcare information or data;
   c. financial account information that would permit access to that individual's financial account; or
2. a natural person's information that is designated as private by a Data Privacy Law.

Section III (DD), Section III (N(I)).

A covered "Network Security Wrongful Act" is defined to include:

> any negligent act, error or omission by the Insured resulting in Unauthorized Access or Unauthorized Use of the Organization's Computer System, the consequences of which include, but are not limited to:
>
> 1. the failure to prevent Unauthorized Access to, use of, or tampering with a Third Party's computer systems;
> 2. the inability of an authorized Third Party to gain access to the Insured's services;
> 3. the failure to prevent denial or disruption of Internet service to an authorized Third Party;
> 4. the failure to prevent Identity Theft or credit/debit card fraud; or
> 5. the transmission of Malicious Code.
>
> *Id.* (CC).

The AIG Specialty Risk Protector® specimen policy provides similar types of coverage. The specimen policy states that the insurer will "pay all Loss" that the Insured is "legally obligated to pay resulting from a Claim alleging a Security Failure or a Privacy Event." Specimen Policy Form 101014 (11/09), Security and Privacy Coverage Section, Section I. "Privacy Event" includes:

1. any failure to protect Confidential Information (whether by "phishing," other social engineering technique or otherwise) including, without limitation, that which results in an identity theft or other wrongful emulation of the identity of an individual or corporation;
2. failure to disclose an event referenced in Sub-paragraph (1) above in violation of any Security Breach Notice Law; or
3. violation of any federal, state, foreign or local privacy statute alleged in connection with a Claim for compensatory damages, judgments, settlements, pre-judgment and post-judgment interest from Sub-paragraphs (1) or (2) above.

"Confidential information" includes, among other things, "information from which an individual may be uniquely and reliably identified or contacted, including, without limitation, an individual's name, address, telephone number, social security number, account relationships, account numbers, account balances, account histories and password" and "any third party's trade secrets, data, designs, interpretations, forecasts, formulas, methods, practices, processes, records, reports or other item of information that is not available to the general public." Section 2(d)(1, 5).

"Security Failure" includes:

1. a failure or violation of the security of a Computer System including, without limitation, that which results in or fails to mitigate any unauthorized access, unauthorized use, denial of service attack or receipt or transmission of a malicious code;
2. physical theft of hardware controlled by a Company (or components thereof) on which electronic data is stored, by a person other than an Insured, from a premises occupied and controlled by a Company; or
3. failure to disclose an event referenced in Sub-paragraphs (1) or (2) above in violation of any Security Breach Notice Law.

Section 2(n).

In purchasing this type of coverage, consideration should be given to, among other things, the types of data included in the coverage. As the above policy language illustrates, specific types of covered data typically include an individual's personally identifiable information, known in shorthand as PII. Data can also include nonpublic data, such as corporate information, and even non-electronic data, such as paper records.

Media Liability: Many "third-party" cyber risk policies include defense and indemnity coverage for claims alleging infringement of copyright and other intellectual property rights and misappropriation of ideas or media content. Although it is important to recognize that some coverage may already exist in the "Personal And Advertising Injury Liability" coverage section of the insured's CGL policies, as discussed above, more specific — and potentially substantially broader — coverage may be obtainable through the purchase of specialty cyber coverage. For example, the Hartford CyberChoice 2.09SM specimen policy states that the insurer will pay "damages" that the insured shall become legally obligated to pay as a result of a claim "alleging an e-Media Wrongful Act." Section I (B). "e-Media Wrongful Act" includes any negligent act, error or omission by the Insured that results in:

1. infringement of copyright, service mark, trademark, or misappropriation of ideas or any other intellectual property right, other than infringement of patents or trade secrets; defamation, libel, product disparagement, trade libel, false arrest, detention or imprisonment, or malicious prosecution, infringement or interference with rights of privacy or publicity; wrongful entry or eviction; invasion of the right of private occupancy; and/or plagiarism, misappropriation of ideas under implied contract invasion or other tort related to disparagement or harm to the reputation or character of any person or organization in the Insured Entity's Electronic Advertising or in the Insured Entity's Advertising; or
2. misappropriation or misdirection of Internet based messages or media of third parties on the Internet by the Insured, including meta-tags, web site domains and names, and related cyber content.

Section III (Q).

The AIG netAdvantage® specimen policy covers "amounts" that the insured is "legally obligated to pay … as damages resulting from any claim" against the insured for the insured's "wrongful acts." Internet Media Module Form #90596 (2006), Section 3. "Wrongful acts" include certain acts and omissions that "result[ ] in a covered peril," which in turn is defined to include the following:

1. infringement of copyright, title, slogan, trademark, trade name, trade dress, mark, service mark or service name including without limitation, infringement of domain name, deep-linking or framing; plagiarism, piracy or misappropriation of ideas under implied contract or other

misappropriation of property rights, ideas or information; or any alleged violation of Section 43(a) of the Lanham Act or any similar state statutes; including without limitation unfair competition in connection with a claim for damages in connection with such conduct;

2. form of defamation or other tort related to disparagement or harm to character, reputation or the feelings of any person, including, but not limited to, libel, slander, product disparagement, trade libel; including without limitation, unfair competition, emotional distress or mental anguish in connection with a claim for damages in connection with such conduct; or

3. form of invasion, infringement or interference with rights of privacy or publicity, including without limitation, false light, public disclosure of private facts, intrusion and commercial appropriation of name, persona or likeness; including without limitation, emotional distress or mental anguish in connection with a claim for damages in connection with such conduct.

Section 5 MEDIA (c, h).

Regulatory Liability: Many third-party cyber risk policies include defense and indemnity coverage for civil, administrative and regulatory proceedings. For example, the Hartford CyberChoice 2.09SM specimen policy covers "reasonable and necessary Data Privacy Regulatory Expenses," which are defined to include "fines or penalties incurred by an Insured Entity and assessed in a Data Privacy Regulatory Proceeding." Section I (B), Section III (L). "Data Privacy Regulatory Proceeding" in turn includes "a civil, formal administrative or formal regulatory proceeding against an Insured by a federal, state or local governmental authority alleging violation of any law referenced under the definition of Data Privacy Laws. … " Section III (M).

2) First-Party Cyber Coverage

Damage to Computer Systems: "First-party" risks may include damage to the insured's own computer hardware or data, and cyber policies often cover this risk. For example, the AIG netAdvantage® specimen policy states that the insurer will pay for the insured's "actual information asset loss … resulting directly from injury to information assets" that results "from a failure of security of your computer system." Information Asset Module Form #90612 (2006), Section 3. "Information asset loss" is defined to include "software or electronic data, including without limitation, customer lists and information, financial, credit card or competitive information, and confidential or private information" "that are altered, corrupted, destroyed, disrupted, deleted or damaged … " Section 5 IA (b, c). CNA's NetProtect 360SM specimen policy states that the insurer will pay the insured "all sums" for "reasonable and necessary expenses resulting from an Exploit [defined as Unauthorized Access, Electronic Infection or a Denial of Service Attack that results in Network Impairment," each as separately defined] that are "required to restore the Insured Entity's Network or information residing on the Insured Entity's Network to substantially the form in which it existed immediately prior to such Exploit." Specimen Policy Form #G-147051-A (2007), Section II, Section X. Many other products offer similar types of coverage.

Business Interruption and Extra Expense: Cyber policies often include coverage for business interruption and extra expense caused by malicious code (viruses, worms, Trojans, malware, spyware and the like), DDoS attacks, unauthorized access to, or theft of, information, and other security threats to networks. For example, the AIG netAdvantage® specimen policy covers the insured's "actual business interruption loss … which [the insured] sustains during the period of recovery (or the extended interruption period if applicable), resulting directly from a material interruption [defined as "the actual and measurable interruption or suspension of [the insured's] computer system, which is

Insurance Coverage for Cyber Attacks

directly caused by a failure of security"]." Business Interruption Module Form #90593 (2006), Section 3, Section 5 BI (k). "Period of recovery" is defined as follows:

> "Period of recovery" means the time period that:
>
> 1. begins on the date and time that a material interruption first occurs; and
> 2. ends on the date and time that the material interruption ends, or would have ended if you had exercised due diligence and dispatch.
>
> Provided, however, the period of recovery shall end no later than thirty (30) consecutive days after the date and time that the material interruption first occurred.
>
> Section 5 BI (l).
>
> "Business interruption loss" includes "the sum of: (1) income loss; (2) extra expense; (3) dependent business interruption loss; and (4) extended business interruption loss" each as separately defined. *See* Section 5 BI (b, d, e, g, j).

CNA's NetProtect 360SM specimen policy states that the insurer will pay the insured:

> all sums …
>
> 1. for reduction of business income the Insured Entity sustains during a Period of Restoration due to the interruption of Commerce Operations [defined as "income producing activities"] by a Network Impairment that has been caused by an Exploit defined as Unauthorized Access, Electronic Infection or a Denial of Service Attack that results in Network Impairment [each as separately defined] during the Policy Period; and,
> 2. for Extra Expense that the Insured Entity sustains to minimize any such Network Impairment in order to resume Commerce Operations[.]
>
> Section II.C.

"Period of Restoration" is defined as follows:

> Period of Restoration means the period of time that:
>
> A. Begins with the date and time that Commerce Operations have first been interrupted by a Network Impairment and after application of the Business Interruption Waiting Period Deductible, as specified in the Declarations; and
>
> B. Ends with the earlier of:
>
> 1. the date and time Commerce Operations have been restored to substantially the level of operation that had existed prior to the Network Impairment; or
> 2. one hundred and twenty hours from the time that Commerce Operations were first interrupted by such Network Impairment.
>
> Section X.

Again, many other products offer similar types of coverage.

Remediation: Cyber policies that cover privacy and network security routinely pay remediation costs associated with a data breach. Such response costs include:

Notification and Credit Monitoring. Cyber risk policies frequently provide coverage for the costs associated with notification of a data breach and credit monitoring services. For example, Beazley's

Insurance Coverage for Cyber Attacks

AFB Media Tech® specimen policy provides coverage for "Privacy Notification Costs … resulting from the Insured Organization's legal obligation to comply with a Breach Notice Law because of an incident (or reasonably suspected incident) described in [the Information Security & Privacy Liability] Insuring Agreement …" Form #F00226 (2011), Section I.D (2011). "Privacy Notification Costs" is defined to include a number of "reasonable and necessary costs incurred by the Insured Organization," including among other things costs "to provide notification to individuals who are required to be notified by the applicable Breach Notice Law" and costs of "offering of one (1) year of credit monitoring services to those individuals whose Personally Identifiable Non-Public Information was compromised or reasonably believed to be compromised as a result of theft, loss or Unauthorized Disclosure of information giving rise to a notification requirement pursuant to a Breach Notice Law." Section I.D. 2.(a), 4.(a).

Forensic Investigation. Cyber risk policies often provide coverage for the costs associated with determining the cause and scope of an attack. For example, Hartford's CyberChoice 2.09SM specimen policy states that the insurer "will reimburse the Insured Entity for reasonable and necessary Cyber Investigation Expenses," which include "reasonable and necessary expenses the Insured Entity incurs to conduct an investigation of its Computer System by a Third Party to determine the source or cause of [a] Data Privacy Wrongful Act or Network Security Wrongful Act." Section III.(I).

Crisis Management. The costs associated with a cyber attack often include crisis management activities. Cyber insurance policies often provide coverage for such activities. For example, the AIG netAdvantage® specimen policy Crisis Management Module Form covers "crisis management expenses" as defined to include "amounts … an organization incurs for the reasonable and necessary fees and expenses incurred by a crisis management firm in the performance of crisis management services for an organization" arising from a "failure of security" or "privacy peril," each as defined. Crisis Management Module Form #90594 (2007), Section 3, Section 5, CM(a), (b)(1).

Public Relations. Cyber risk policies often provide coverage for the costs associated with public relations efforts in the wake of an attack (this may be included as part of the crisis management coverage). For example, CNA's Net protect 360SM specimen policy covers "Public Relations Event Expenses … to respond to adverse or unfavorable publicity or media attention arising out of a Public Relations Event," defined as "any situation which in the reasonable opinion of an Executive did cause or is reasonably likely to cause economic injury to the Insured Entity." Section I.B.1., Section X.

Extortion

Cyber policies often cover losses resulting from extortion (payments of an extortionist's demand to prevent network loss or implementation of a threat). For example, the AIG netAdvantage® specimen policy indemnifies the insured "for those amounts" the insured pays "as extortion monies resulting from an extortion claim … " Cyber Extortion Module Form #90595 (2006), Section 3. "Extortion claim" is defined to include "any threat or connected series of threats to commit an intentional computer attack … " Section 5 CE(b).

3) Beware of the Fine Print

Cyber insurance coverages may be extremely valuable, but deserve — indeed, require — a careful review. The specific policy terms and conditions must be analyzed carefully to ensure that the coverage provided meets the company's specific loss scenarios and potential exposures. In addition, the exclusions and other terms and conditions must be carefully read and understood. Some insurers, for example, may insert exclusions based on purported shortcomings in the insured's security measures if identified in the underwriting process or known to the insured prior to policy inception.

Insurance Coverage for Cyber Attacks

One specimen form policy excludes any claim "alleging, arising out of or resulting, directly or indirectly" from "(1) any shortcoming in security that [the insured] knew about prior to the inception of this policy," "(2) [the insured's] failure to take reasonable steps, to use, design, maintain and upgrade [the insured's] security, or "(3) the inability to use, or lack of performance of, software: (a) due to expiration, cancellation, or withdrawal of such software; (b) that has not yet been released from its development stage; or (c) that has not passed all test runs or proven successful in applicable daily operations." AIG net-Advantage® Specimen Policy, Base Form #91239 (2006), Section 4(t).

It remains to be seen whether broad exclusions of this kind will be upheld and enforced by the courts, however, particularly given that the new policies are specifically marketed to cover the risk of liability for negligence in connection with failure of network security.

Conclusion

Virtually every company is vulnerable to cyber attacks — a fact amply illustrated by the recent instances involving some of the world's most sophisticated organizations. When targeted by an attack or facing a claim, companies should carefully consider what coverage may be available. Insurance is a valuable asset. With the assistance of experienced coverage counsel, companies facing potential exposure will be in the best possible position to present a claim most effectively and, ideally, maximize their coverage. Before an attack, companies should take the opportunity to evaluate and address their potential vulnerabilities, the sufficiency of their existing insurance coverage and the potential role of specialized cyber risk coverage. Experienced counsel can assist in negotiating the most favorable terms available and ensuring that there are no gaps, or overlaps, in coverage.

Authors:

Roberta D. Anderson
roberta.anderson@klgates.com
+1.412.355.6222

K&L GATES

Anchorage Austin Beijing Berlin Boston Brisbane Brussels Charleston Charlotte Chicago Dallas Doha Dubai Fort Worth Frankfurt Harrisburg Hong Kong Houston London Los Angeles Melbourne Miami Milan Moscow Newark New York Orange County Palo Alto Paris Perth Pittsburgh Portland Raleigh Research Triangle Park San Diego San Francisco São Paulo Seattle Seoul Shanghai Singapore Spokane Sydney Taipei Tokyo Warsaw Washington, D.C. Wilmington

K&L Gates practices out of 48 fully integrated offices located in the United States, Asia, Australia, Europe, the Middle East and South America and represents leading global corporations, growth and middle-market companies, capital markets participants and entrepreneurs in every major industry group as well as public sector entities, educational institutions, philanthropic organizations and individuals. For more information about K&L Gates or its locations, practices and registrations, visit www.klgates.com.