Insurance for Cyber Risks:

Coverage Under CGL and "Cyber" Policies

ABA Section of Litigation 2012 Insurance
Coverage Litigation Committee CLE Seminar

March 1-3, 2012

Insurance coverage for data breaches, denial of service attacks, and cyber security events

SCOTT GODES, ESQ.
Dickstein Shapiro LLP
Washington, D.C.

JENNIFER G. SMITH, ESQ., CIPP
Global Technology & Private Practice
Lockton Companies
Washington, D.C.

THE RISE IN CYBER RISKS

A few years ago it might have seemed like every firm had a Y2K practice, and was prepared to provide advice and counseling about how to handle the anticipated end of the world. Luckily for society at large, the worst case scenario was not realized. Just a few years later, the focus on liability and risks as related to computers and network security has changed to another, but far more real, issue: the risk of data breaches, hacks, network interruptions, and other cyber risks. The number of data breaches and cyber attacks that companies and other entities have faced has been so widespread and expensive that 2011 was dubbed "the year of the cyber attack."[1] A recent PricewaterhouseCoopers report characterized "Cybercrime . . . as one of the top four economic crimes."[2]

Two of the most well-known cyber risks are cyber attacks and data breaches. One form of cyber attack is a denial of service incident. Denial of service attacks may be designed to bring a Web site or service down, preventing customers from accessing the site or the company's products or services. One research and development center has explained that denial of service attacks come in a variety of forms. The three basic types of denial of service attacks are:

- Consumption of scarce, limited, or nonrenewable resources.

[1]Garry Byers, *Rapid Cyber Attack Response: Three Days Make All the Difference*, Digital Forensic Investigator News (Sept. 28, 2011), available at http://www.dfinews.com/article/rapid-cyber-attack-response-three-days-make-all-difference.
[2]PricewaterhouseCoopers, *Cybercrime: Protecting Against the Growing Threat*, at 5 (Nov. 2011), available at http://www.pwc.com/gx/en/economic-crime-survey/download-economic-crime-people-culture-controls.jhtml.

LOCKTON®

- Destruction or alteration of configuration information.
- Physical destruction or alteration of network components.[3]

Some attacks are comparable to "tak[ing] an ax to a piece of hardware" and may be called "permanent denial-of-service (PDOS) attack[s]."[4] If a system suffers such an attack, which also has been called "pure hardware sabotage," it "requires replacement or reinstallation of hardware."[5]

Another cyber risk, perhaps more widely discussed in the news, is a data breach. The term data breach is used broadly, usually to describe incidents in which hackers, rogue current or former employees, or others steal or otherwise gain access to personally identifiable information or personal health information. For example, in *Anderson v. Hannaford Brothers Co.*, the court described a data breach against "a national grocery chain whose electronic payment processing system was breached by hackers . . . [with] hackers [having] stole[n] up to 4.2 million credit and debit card numbers, expiration dates, and security codes . . ."[6]

In the context of personal health information, "[U.S. Department of Health and Human Services] HHS issued regulations requiring healthcare providers, health plans, and other entities covered by the Health Insurance Portability and Accountability Act (HIPAA) to notify individuals when their health information is breached."[7] HIPAA imposes liability immediately for breaches of certain information by certain parties; the requirements state that the entity "shall" provide notice, and do not make reference to a letter from the government or a lawsuit to enforce the law.[8] When a "violation is not corrected . . . a penalty" may be imposed that is $50,000 for each violation, up to $1,500,000 in a calendar year, rather than $10,000 and a cap of $250,000.[9]

Setting the legal and enforcement issues aside, consider certain business issues that may motivate an organization to choose insurance as a risk transfer solution:

- Loss of assets, brand, and reputation.
- Investor fallout from uncovered losses with large claim and class action potential.
- Many functions are conducted by outside vendors and contractors who may lack insurance and assets to respond. What if the vendor makes a systemic mistake? What if they fail to purchase insurance or keep it? What if they are located in a country where this insurance cannot be obtained? What if the policy they purchased denies coverage or has inadequate limits?
- PCI (credit card industry security standards) compliant companies have had their security compromised from processes lapse, human error, or criminal insider.
- No system can be designed to eliminate the potential for loss, as people and processes failures cannot be eliminated. Insiders may be perpetrators.
- Responsibility rests with the data owner from a legal, regulatory perspective, and credit card association operating regulations.
- Insurance companies have become more aggressive in asserting (even if wrongfully so) that "traditional" insurance may not cover security liability or adequately cover privacy risks.

[3]CERT, *Denial of Service Attacks*, http://www.cert.org/tech_tips/denial_of_service.html (last visited December 8, 2011); CERT, *About CERT*, http://www.cert.org/meet_cert/ (last visited Dec. 8, 2011).
[4]Kelly Jackson Higgins, *Permanent Denial-of-Service Attack Sabotages Hardware*, Security Dark Reading, http://www.darkreading.com/security/management/showArticle.jhtml?articleID=211201088 (May 19, 2008).
[5]*Id.*
[6]659 F.3d 151, 154 (1st Cir. 2011).
[7]United States Department of Health and Human Services, *HITECH Breach Notification Interim Final Rule*, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html (last visited December 8, 2011).
[8]*See* 45 C.F.R. §§ 164.404, 164.410 (2011).
[9]74 Fed. Reg. 209 at 56125.

Coverage Under CGL Policies

Policyholders and insureds facing cyber risks and liabilities would be well served to analyze their entire slate of insurance policies to determine what coverages might apply to such risks. Indeed, the Division of Corporation Finance of the U.S. Securities and Exchange Commission recently released "CF Disclosure Guidance: Topic No. 2—Cybersecurity."[10] That guidance, in the context of cyber risks, notes insurance coverage for such risks, stating: "Depending on the registrant's particular facts and circumstances, and to the extent material, appropriate disclosures may include . . . [a] description of relevant insurance coverage."[11]

Is there coverage for cyber risks under a "standard form" commercial general liability ("CGL") insurance policy, one with insuring agreements drafted by the Insurance Services Office ("ISO")? That question is at issue at the time of this writing between Zurich (among other insurance companies) and various Sony entities in litigation. In 2011, Sony allegedly suffered various cyber attacks and data breaches, with the events allegedly costing Sony nine figures, and leading to multiple putative class action lawsuits against various Sony entities.[12] Seeking to avoid defending or indemnifying Sony, Zurich filed an action against Sony, seeking declarations that there is no coverage under various CGL policies, among other requests for rulings.[13]

Zurich itself had recognized, in at least one article, that "[t]hird-party liability policies such as Commercial General Liability (CGL) policies provide coverage to a company . . . for data security breaches."[14]

Standard form CGL policies often provide coverage for personal and advertising injury, bodily injury, and property damage."Personal and advertising injury" has several definitions; but for purposes of data breaches and cyber risks, one relevant definition is "[o]ral or written publication, in any manner, of material that violates a person's right of privacy."[15] The term "bodily injury" often is defined as including "bodily injury, sickness or disease . . . including death resulting . . . at any time."[16] When analyzing the scope of bodily injury coverage in the context of cyber risks, however, consider whether the definition of "bodily injury" has been expanded to include mental anguish, mental injury, shock, fright, or similar terms. "Property damage" in standard form CGL policies often includes "[p]hysical injury to tangible property, including all resulting loss of use of that property" and "[l]oss of use of tangible property that is not physically injured," but often states that "electronic data is not tangible property."[17]

The leading case addressing these issues held that personal and advertising injury coverage was available for computer- and Internet-based class action claims. In *Netscape Communications Corp. v. Federal Insurance Co.*,[18] the U.S. Court of Appeals for the Ninth Circuit's brief (and unpublished) opinion, along with the earlier trial court opinion that the Ninth Circuit reversed, illustrates that Netscape Communications Corporation (Netscape) was sued in putative class action lawsuits regarding a software program that provided Netscape with information about

[10] U.S. Securities and Exchange Commission Division of Corporation Finance, *CF Disclosure Guidance: Topic No. 2 - Cybersecurity*, (Oct. 13, 2011), available at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[11] *Id.*

[12] *See, e.g.*, Alastair Stevenson, *Sony Networks Hacked Post-PSN and PlayStation Store Restart*, International Business Times (June 3, 2011) http://uk.ibtimes.com/articles/156879/20110603/sony-hack-lulzsec-security-psn-playstation-network-hackers-security-breach-3-4.htm (Sony "suffered an estimated $177 million loss as a result of the first hack"); *see also, e.g., Zurich Am. Ins. Co. v. Sony Corp. of Am.*, No. 651982/2011, Complaint at 6 (N.Y. Sup. Ct. July 20, 2011) (alleging that various Sony entities had been named in 55 class action complaints).

[13] *See, e.g., Zurich Am. Ins. Co. v. Sony Corp. of Am.*, No. 651982/2011, complaint (N.Y. Sup. Ct. July 20, 2011).

[14] Zurich, *Data Security: A Growing Liability Threat*, http://www.zurichna.com/internet/zna/SiteCollectionDocuments/en/media/whitepapers/DOCold2DataSecurity082609.pdf.

[15] *See, e.g.*, ISO standard form CG 00 01 12 07.

[16] *See, e.g.*, ISO standard form CG 00 01 12 07.

[17] *See, e.g.*, ISO standard form CG 00 01 12 07.

[18] 343 F. App'x 271 (9th Cir. 2009).

users' internet activities and which Netscape used for targeted advertising.[19] The claimants alleged that Netscape's program violated the Electronic Communications Privacy Act ("ECPA") and the Computer Fraud and Abuse Act ("CFAA"). The court held that "[a]lthough the underlying claims against AOL were not traditional breach of privacy claims, given that coverage provisions are broadly construed, the underlying complaints sufficiently alleged that AOL had intercepted and internally disseminated private online communications."[20]

With a dearth of cases interpreting publication in the cybersecurity context, it is helpful to consider analogous cases. In *Zurich American Insurance Co. v. Fieldstone Mortgage Co.*, a leading case on the issue, the insurance company argued "that in order to constitute a publication, *the information that violates the right to privacy must be divulged to a third party*." The court correctly rejected that argument, explaining that "the majority [of circuits] have found that the publication need not be to a third party."[21] Other courts have followed the well-reasoned Fieldstone decision, finding that unauthorized access of credit reports meets the publication requirement under the relevant personal and advertising injury provisions.[22]

Those holdings are critical in the context of data breaches. Data breaches, as noted above, consist of situations in which private information has been publicized to third parties. Therefore, the basic insuring agreement relating to personal and advertising injury should be considered broad enough to encompass a data breach.

To the extent that CGL policies have broadened definitions of bodily injury, there may be an argument that bodily injury coverage applies to, or (at a minimum) provides a defense for, data breach claims. For example, one of the class action complaints filed against Sony alleges that "plaintiff and the Class have suffered damages, including, but not limited to, . . . fear and apprehension of fraud . . ."[23] Such an allegation could be read as falling within an expanded definition of "bodily injury," depending on how broadly the definition is written and whether it is construed as being tied to a physical bodily injury from the rest of the definition of the term.

The potential application of property damage coverage may be a more fact-specific inquiry in the context of cyber risks. For those policies excluding "electronic data" from the definition of "property damage," convincing an insurer that a data breach alone caused covered property damage, or gives rise to a duty to defend under property damage coverage, will be challenging for policyholders and insureds. Nonetheless, certain cyber attacks may result in property damage in the form of physical damage to tangible property. For example, certain denial-of-service attacks cause physical destruction or alteration of network components.[24] If an insured can demonstrate that there were allegations of such damage, or actual evidence of such damage, property damage coverage should apply, as the claim does not implicate software and data alone.[25]

The definition of property damage, in a standard form CGL policy, typically includes "[l]oss of use of tangible

[19] *Netscape Commc'ns Corp. v. Fed. Ins. Co.*, No. C 06-00198 JW, 2007 U.S. Dist. LEXIS 78400, at *3-4 (N.D. Cal. Oct. 10, 2007), rev'd, 343 F. App'x 271 (9th Cir. 2009).

[20] *Id.*, 343 F. App'x at 272 (citation omitted).

[21] No. CCB-06-2055, 2007 U.S. Dist. LEXIS 81570, at *14 (D. Md. Oct. 26, 2007) (emphasis added); *see, e.g., Pietras v. Sentry Ins. Co.*, No. 06 C 3576, 2007 U.S. Dist. LEXIS 16015 (N.D. Ill. Mar. 6, 2007); *Nautilus Ins. Co. v. Easy Drop Off, LLC*, No. 06 C 4286, 2007 U.S. Dist. LEXIS 42380 (N.D. Ill. June 4, 2007) (applying Florida law).

[22] *See Am. Family Mut. Ins. Co. v. C.M.A. Mortg., Inc.*, No. 1:06-cv-1044, 2010 U.S. Dist. LEXIS 2379 (S.D. Ind. Jan. 12, 2010).

[23] *Johns v. Sony Corp.*, No. 3:11-cv-02063-RS, Complaint ¶ 101 (N.D. Cal. Apr. 27, 2011). (The *Johns* case has been transferred to and consolidated with other actions in *In re Sony Gaming Networks and Customer Data Security Breach Information*, No. 3:11-md-02258-AJD-MDD (S.D. Cal.).

[24] CERT, *Denial of Service Attacks*, CERT, http://www.cert.org/tech_tips/denial_of_service.html (last visited Jan. 5, 2012); CERT, *About* CERT, http://www.cert.org/meet_cert/ (last visited Jan. 5, 2012).

[25] *See, e.g., Eyeblaster, Inc. v. Federal Insurance Co.*, 613 F.3d 797, 801 (8th Cir. 2010) (noting that coverage for software-, computer-, and technology-based claims would not be excluded from property damage if "[t]he complaint . . . ma[d]e a claim for physical injury to the hardware")

property that is not physically injured."[26] This phrase presents an opportunity to seek coverage for loss of use of tangible property, such as the loss of use of computers or networks rendered inaccessible or inoperable as a result of a cyber attack.

A real world example is found in the *Johns v. Sony* complaint. The putative class alleges that "Plaintiffs seek damages to compensate themselves and the Class for their loss (both temporary and permanent) of use of their PlayStation consoles . . . ."[27] Those loss of hardware use allegations should be considered loss of use of tangible property for purposes of pursuing and maximizing any insurance recovery.

In *Eyeblaster, Inc. v. Federal Insurance Co.*, the U.S. Court of Appeals for the Eighth Circuit considered a similar set of allegations. That dispute involved a complaint in which the claimant "alleg[ed] that Eyeblaster injured his computer, software, and data after he visited an Eyeblaster Web site."[28] The court analyzed the scope of property damage coverage. After determining that one prong of the property damage definition was not met, because the claimant alleged software and operating system damage, without allegations of damage to hardware, the court then considered whether the loss of use of tangible property prong of property damage was met. The court held that alleged computer freezes, pop-up ads, hijacked browsers, random error messages, slowed performance and crashes, and ads based on past Internet surfing habits constituted property damage in the form of loss of use of tangible property sufficient for coverage under a CGL policy.[29] Likewise, in *State Auto Property & Casualty Insurance Co. v. Midwest Computers & More*, an Oklahoma federal district court held that loss of use of a computer system allegations fell within the loss of use of tangible property terms of the policy.[30]

A final note specific to data breaches is the question of coverage for credit monitoring under CGL policies. Policyholders and insureds should anticipate that insurance companies will assert that credit monitoring costs are not covered under CGL policies. One such anticipated argument is that credit monitoring does not consist of "damages" "because of" personal and advertising injury, bodily injury, or property damage. Policyholders and insureds should note that courts have rejected similar insurance company arguments in analogous contexts. For example, class action plaintiffs have alleged that certain products (such as asbestos or lead paint) cause bodily injury at the cellular level, and, as such, they are entitled to the cost of medical monitoring that would allow said plaintiffs to know whether they will develop a cognizable injury or disease. For those decisions recognizing the underlying claim alleges a covered claim, those decisions have recognized that medical monitoring costs are "damages" "because of" bodily injury.[31] That authority should be considered a persuasive basis in response to anticipated insurance company arguments that credit monitoring costs are excluded from coverage.

Coverage Under "Cyber" Policies

No doubt countless side-by-side coverage comparisons have been lost in the land of good intentions trying to delineate the distinctions between CGL, property, and cyber insurance solutions. There are solid arguments that there is coverage for cyber risks under the insuring

[26] *See, e.g.*, ISO standard form CG 00 01 12 07.
[27] *Johns v. Sony Corp.*, No. 3:11 cv 02063, Complaint ¶ 8 (N.D. Cal. Apr. 27, 2011)
[28] 613 F.3d at 799.
[29] 613 F.3d at 800, 802.
[30] 147 F. Supp. 2d 1113, 1116 (W.D. Okla. 2001) (interpreting liability coverage under a business owner's policy). Ultimately, the court granted summary judgment to the insurer, holding that a policy exclusion for "Your Work" applied because the loss of use of the customer's computer system occurred prior to the completion of the policyholder's work on the system. *Id.* at 1116-18.
[31] *See, e.g., Baughman v. U.S. Liab. Ins. Co.*, 662 F. Supp. 2d 386, 394-95 (D.N.J. 2009) (medical monitoring costs are damages because of bodily injury).

agreements within a standard ISO form CGL policy. Likewise, policyholders have had some success in arguing that coverage may be afforded under the Computer Funds Transfer, Theft or Employee Theft/Dishonesty insuring agreements within a Fidelity and/or Commercial Crime program.[32] There also are solid arguments that coverage for private companies may provide coverage (specifically entity coverage) for cyber-related losses under a private company Directors & Officers Liability insurance program.[33] Notwithstanding those solid arguments and favorable case decisions, policyholders found themselves facing denials or in insurance coverage litigation to determine whether a CGL or other insurance policy will cover a data breach or other cyber event.

What is the solution then, for those organizations that are concerned with insurance companies taking aggressive positions as to coverage under CGL or other policies for cyber risks in the wake of a data breach or other cyber event? Insurance companies now are marketing stand-alone, dedicated insurance policies as being designed to address information risk. Those insurance policies should provide the solution.

Many refer to this solution as "cyber insurance." Cyber insurance is a coat of many colors, with as many product names as there are colors of the rainbow. Other variations include Information Security Insurance, Network Security Insurance, Privacy Insurance, Data Breach Insurance, Network Breach Insurance, Technology Solutions, Cyber-this, Cyber-that (e.g., "plus," "enhancement," "solution"), Information Insurance, or, when all else fails, some iteration of Professional Liability or E&O—seemingly irrespective of the buyer's actual services.[34] For the purposes of this article and to avoid calling attention to any one particular insurer, we will continue to refer to this solution as "cyber insurance."

Although the expression "no two forms are alike" may be a stretch under other circumstances, it is painfully, tediously true in the cyber insurance context. These forms vary vastly from the fundamental structure and scope of the policy to the retention and use of outside experts. Certain policies are duty to defend policies; others are indemnity policies. Certain policies have specifically delineated intentional torts drafted into the definition of "personal injury" or "wrongful act"; other policies—perhaps in an effort to avoid changing forms amid rapidly evolving regulations—leave such definitions or insuring agreements rather broadly defined. Some might even argue "vague and ambiguous." Each of these issues, and the many others not listed herein, serves as a reminder to potential buyers to rely on their experts in the search for the best cyber insurance solution for that particular organization.

The core elements of cyber insurance that are unique to this particular insurance solution may include coverage in varying degrees for the following:

- Network Security Liability
  - Claim Expenses and Damages emanating from Network and non-Network security breaches.
  - Media Liability

[32] *See Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, PA*, No. 2:06cv443, slip op. (S.D. Ohio Mar. 30, 2009). A careful analysis may be warranted regarding recent forms changes, in which the definition of "Other property" may have been changed to not include computer programs, electronic data or any property specifically excluded under the policy. *See, e.g.*, ISO standard form CR 00 23 05 06 – Commercial Crime Policy Loss Sustained (eff. NY 5/1/06).

[33] Note the potential general distinction here between private and public company directors' and officers' liability insurance programs. The former typically offers entity coverage for a fairly broad array of "Wrongful Acts"; unless "Side C" or "entity coverage" was purchased, the latter may not necessarily provide entity coverage in the absence of claims against an individual defendant.

[34] Insurance product managers may be well served to visit Rick Betterley's blog post from January 4, 2012 for a complete regurgitation of various product names and descriptions proposed by market participants at large. *See*, The Betterley Report Blog on Specialty Insurance Products at http://thebetterleyreport.wordpress.com/.

- Claim Expenses and Damages emanating from Personal Injury Torts and Intellectual Property Infringement (except Patent Infringement).
- Claim Expenses and Damages emanating from Electronic Publishing (Web site) and some will provide coverage for all ways in which a company can utter and disseminate matter.

- Privacy Liability
  - Claim Expenses and Damages emanating from violation of a Privacy Tort, Law or Regulation.
  - Claim Expenses and Damages emanating from a violation of a law or regulation arising out of a Security Breach.
- Privacy Regulatory Proceeding and Fines
  - Claim Expenses in connection with a Privacy Regulatory inquiry, investigation or proceeding.
  - Damages/Fines related to a Consumer Redress Fund.
  - Privacy Regulations Fines.
  - PCI Fines.
- Privacy Event Expense Reimbursement
  - Expense reimbursement for third-party forensics costs.
  - Public Relations costs.
  - Legal.
  - Mandatory Notification Costs (Compliance with Security Breach Notification Laws) and Voluntary Notification Costs.
  - Credit Monitoring.
  - Call Center.
  - Second Security Audits required by Financial Institutions (varies by market).
- Data/Electronic Information Loss
  - Covers the cost of recollecting or retrieving data destroyed, damaged or corrupted due to a computer attack.
- Business Interruption or Network Failure Expenses
  - Covers cost of lost net revenue and extra expense arising from a computer attack and other human-related perils. Especially valuable for computer networks with high availability needs.
- Cyber-Extortion
  - Covers both the cost of investigation and the extortion demand amount related a threat to commit a computer attack, implant a virus, etc.

Also significant, and perhaps unique to the cyber insurance market, is the rapid rate at which the underwriters have modified and/or enhanced their forms. Issues like contractual liability/indemnification, mandatory versus voluntary notification, and even the defining triggers under the policy(ies) appear to change every 18 months—with new product introductions every six months. Again, buyers are encouraged to carefully review the different program terms and conditions, so that they can prioritize and weigh their coverage needs against the solutions offered by the underwriters.

Although sorting through various cyber insurance solutions may be a daunting task to first-time buyers, it is worth repeating that insurance companies market this solution as being designed expressly to contemplate information risk, including data privacy and network security. A properly designed insurance solution may very well preempt a difficult explanation to senior management after a cyber loss, a much more favorable position to be in than explaining why the policyholder's insurance companies have sued the policyholder, simply because the policyholder put the insurance company on notice.

About the Authors

Jennifer G. Smith, Esq., CIPP, Lockton Companies
JSmith@Lockton.com
202.414.2604

Jennifer G. Smith is a Senior Client Advisor within Lockton's Global Technology & Privacy Practice. A former insurance coverage litigator, Jennifer designs risk management program integration strategies and insurance solutions with particular industry emphasis in e-commerce, online advertising, satellite communications, EPS providers, software service or application providers, and social media. Jennifer is a frequent ABA and ACC speaker and author in the subject matter areas of D&O Liability, Cyber, Technology E&O, Network Security/ Data Privacy, IP Infringement and Claims Advocacy/ Litigation Management. As a practice leader for the Global Technology & Privacy Practice, Jennifer has presented cyber-liability and cyber solutions to the FTC, SEC, ICANN and deputy federal CIO. In June 2011, Jennifer was called upon by the Department of Commerce's Internet Policy Task Force to draft a formal comment white paper on proposed voluntary codes of conduct to strengthen the cybersecurity of companies that rely on the internet to do business. In August 2011, Ms. Smith was called as an expert to testify in favor of (HR 611) and data security (HR 1707) legislation in the 112th Congress.

Scott N. Godes
Dickstein Shapiro LLP
GodesS@DicksteinShapiro.com
202.420.3669

Scott Godes is an insurance coverage litigator who has helped corporate insureds recover over $1.2 billion from insurance companies. He helps clients with cybersecurity, data breach, and privacy claims and related coverage questions.

Scott is a co-chair of the ABA's Computer Technology Subcommittee of the Insurance Coverage Litigation Committee and the co-lead of Dickstein Shapiro's Cyber Security insurance coverage initiative. He is the author of the cybersecurity and intellectual property risks chapter in the leading insurance coverage liability treatise (Appleman Law of Liability Insurance) and also wrote the Cyber Security section of the Insurance chapter in the Corporate Compliance Practice Guide. The net of his experience and writing background is that he is comfortable discussing these issues with insurance coverage lawyers and courts, as well as technologists and corporate officers.

LOCKTON®

www.lockton.com

© 2012 Lockton, Inc. All rights reserved.
Images © 2012 Thinkstock. All rights reserved.
g\washington, d.c.\2012\cyber risks.indd