Crafting a Cybersecurity Policy

By Charles N. Insler

Defending Against Today's Digital Threats

■ Charles N. Insler is an attorney with Hepler Broom LLC in St. Louis, Missouri, where he concentrates his practice on complex commercial litigation, including antitrust and unfair competition litigation, business torts, class action litigation and alternative dispute resolution. Mr. Insler is a member of Hepler Broom's HBCyberGroup, which created an alliance with leading information security, data storage, reputation management, and insurance brokerage firms to integrate information security client services. He is a member of the DRI Appellate Advocacy, Commercial Litigation, Intellectual Property Litigation, and Young Lawyers Committees.

In October, *The Economist* warned that total computer security was impossible; that no amount of money, employee training, or consultant time could create an invulnerable network. One way to offset this uncertainty and vulnerability was insurance. But while the insurance industry was showing "increased interest in offering cover for computer-related risks," such "cyber-insurance is, however, still very much in its infancy." One additional problem for the industry was that the "complexity of computer networks makes it very difficult to quantify risk accurately." *And this was 2002. Putting It All Together*, The Economist, Oct. 24, 2002.

In 14 years, things have changed and they haven't. As our defenses have evolved so too have the threats, nearly in lockstep. Yesterday's spam and phishing have become today's ransomware, botnets, and spear phishing. Even the relatively crude distributed denial-of-service (DDoS) attack remains in vogue. An impenetrable network, immune to breaches and hacking remains a well-recognized impossibility.

For its part, the cyberinsurance market is still—more than a decade later—in relative infancy, though there are signs that it is poised for explosive growth. *See* Stephen Joyce, *Cybersecurity Insurance Explosion Poses Challenges,* Bloomberg BNA, Jan. 4, 2016. Cybersecurity insurance premiums could reach $7.5 billion by 2020, triple what they are today, according to one study. Jim Finkle, *Cyber Insurance Premiums Rocket After High-Profile Attacks,* Reuters, Oct. 12, 2015.

This potential for growth comes at a time when there are no real insurance standards for pricing, terms and conditions, and policy language in the cyberinsurance field, leaving one analyst to note that "the cybersecurity insurance market still resembles 'the Wild, Wild West.'" Finkle, *Cyber Insurance Premiums Rocket After High-Profile Attacks.* At the same time, quantifying the exact risks and potential exposure remains a daunting task—akin to underwriting air travel at the time of the Wright brothers. *See* Jimmy Koo, *More Incident Data Needed for Cybersecurity Insurance*, Bloomberg BNA, Mar. 28, 2016 (noting that one of the major obstacles for providing more coverage is the ongoing lack of actuarial data).

This potential for growth comes at a time when there are no real insurance standards for pricing, terms and conditions, and policy language in the cyberinsurance field, leaving one analyst to note that "the cybersecurity insurance market still resembles 'the Wild, Wild West.'"

Yes, You Really Need a Cybersecurity Policy

Data breaches are now commonplace, with companies both large and small falling victim to hackers. *See A Guide to Cyber Risk*, Allianz Global Corporate & Specialty (2015) (noting that almost two-thirds of all targeted attacks hit small- and medium-size businesses). According to one estimate, there were over 800 million records breached in 2013, with the cost of each breached record ranging from more than $100 (in the retail sector) to more than $300 (in the health care sector). *Defending the Digital Frontier*, The Economist, July 12, 2014. On average, the cost of a data breach has been estimated at $188 per compromised record, with the average data breach implicating 28,765 records (for a total average cost of $5.4 million). Nicole Perlroth and Elizabeth Harris, *Cyberattack Insurance a Challenge for Business*, N.Y. Times, June 8, 2014; *but see Ponemon Institute's 2015 Global Cost of Data Breach Study Reveals Average Cost of Data Breach Reaches Record Levels*, Ponemon Institute, May 27, 2015 (estimating that the average cost to respond and remediate a data breach is $3.8 million).

The CGL Policy is not that policy. *See NAIC & The Center for Insurance Policy and Research,* Cybersecurity, available at http://www.naic.org (last visited April 5, 2016). "[M]ost standard commercial lines policies do not cover many of the cyber risks mentioned above. To cover these unique cyber risks through insurance requires the purchase of a special cyber liability policy." *Id.* To be sure, some courts have found that an insured's digital claims were covered by its CGL Policy. *See, e.g., Eyeblaster, Inc. v. Federal Ins. Co.*, 613 F.3d 797, 802 (8th Cir. 2010) (holding that a computer user's allegations of damage to his computer after accessing the insured's website fell within the "plain meaning of tangible property" covered by the insured's General Liability policy—even though the policy excluded "software, data or other information that is in electronic form" from its definition of tangible property); *see also Travelers Indem. Co. of Am. v. Portal Healthcare Sols., LLC*, 35 F. Supp. 3d 765, 767 (E.D. Va. 2014) (holding that patients' class action, alleging the insured allowed confidential medical records to be accessed by online searches, was a covered "publication" and that the insurer had a duty to defend its insured), *aff'd*, 644 F. App'x 245 (4th Cir. Apr. 11, 2016) (per curiam).

Other courts, however, have rejected efforts to seek data breach coverage from CGL policies. *See Zurich Am. Ins. Co. v. Sony Corp. of Am.*, No. 651982/2011 (N.Y. Sup. Ct. Feb. 24, 2014) (holding that Zurich's CGL policy did not afford Sony coverage for the 2011 data breach of its Playstation network because the third-party hackers, and not Sony, published the stolen information), *appeal withdrawn*, 6 N.Y.S.3d 915 (N.Y. App. Div. 2015); *see also Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co.*, 83 A.3d 664, 672 (Conn. App. Ct. 2014) (holding that the plaintiffs' claims were not covered because

they could not show the information on physical tapes containing employee data were ever accessed, and could not, therefore, show there was a "publication" within the meaning of the policy), *aff'd,* 115 A.3d 458 (Conn. 2015) (per curiam).

Recent exclusions to CGL policies make future successes all the less likely. In May 2014, new Insurance Services Office (ISO) cyber exclusions for CGL policies went into effect, excluding coverage for damages arising out of

> (1) any access to or disclosure of any person's or organization's confidential or personal information, including… financial information, credit card information, health information or any other type of nonpublic information; or (2) The loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.

ISO Endorsement CG 21 07 05 14. This exclusion applies even if "damages claimed for notification costs, credit monitoring expenses, forensic expenses, public relations expenses or any other loss, cost or expense incurred by you or others arising out of that which is described in Paragraph (1) or (2) above." *Id.*

This new endorsement expressly aims to eliminate coverage for those costs most likely to be incurred following a data breach. *See id.* While insurers and insureds may continue to litigate data breaches and similar intrusions under CGL policies, *see Travelers Indemnity Co. of Conn. v. P.F. Chang's China Bistro, Inc.*, No. 3:14-CV-1458 VLB (D. Conn. Oct. 2, 2014) (seeking a declaratory judgment that Travelers has no obligation to defend or indemnify P.F. Chang's under CGL policies in litigation arising of out the theft of its customers' financial information), purchasing a specific cyberinsurance policy is the recommended practice following the new endorsement.

What Should the Cyberinsurance Policy Include?

Like any insurance policy, a cyberinsurance policy should be crafted and tailored to meet the specific needs of that insured's particular industry and business. That being said, an insured should determine whether its cyberinsurance policy will cover a few basic contingencies, among them:

(1) Liability for Security Breaches. This coverage should include a company's liability for failing to prevent unauthorized access to its computer systems, which would include the liability associated with charge backs, reissuing cards, account monitoring, and fines imposed by the credit card companies or credit card processors. These liabilities can be the "largest share of the losses" associated with a data breach. *See Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa.*, 691 F.3d 821, 824 (6th Cir. 2012); *see also Lone Star Nat. Bank, N.A. v. Heartland Payment Sys., Inc.*, 729 F.3d 421, 426 (5th Cir. 2013) (holding that even absent physical harm, Heartland, a payment processor, "may owe the Issuer Banks a duty of care and may be liable for their purely economic losses [resulting from replacing compromised cards and reimbursing fraudulent charges]"). This coverage should be the starting point of any policy.

This new endorsement expressly aims to eliminate coverage for those costs most likely to be incurred following a data breach.

(2) Costs Associated with Privacy Breaches. This coverage should include the costs of notifying consumers of a breach, establishing customer support numbers, and providing credit monitoring or identity protection services. *See, e.g., Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 696 (7th Cir. 2015) ("The injuries associated with resolving fraudulent charges [there were 9,200 reported fraudulent charges from 350,000 exposed cards] and protecting oneself against future identity theft… are sufficient to satisfy the first requirement of Article III standing."); *Corona v. Sony Pictures Entm't, Inc.*, No. 14-CV-09600 RGK EX, 2015 WL 3916744, at *5 (C.D. Cal. June 15, 2015) ("[T]he Court finds that Plaintiffs adequately allege a cognizable injury by way of costs relating to credit monitoring, identity theft protection, and penalties [from frozen credit]."). While class action litigation is almost certain to follow any data breach, if the class members have not actually had their personally identifiable information (PII) misused, a court may dismiss the class action on standing grounds. *See In re SuperValu, Inc.*, No. 14-MD-2586 ADM/TNL, 2016 WL 81792, at *1 (D. Minn. Jan. 7, 2016) ("In data security breach cases where plaintiffs' data has not been misused following the breach, the vast majority of courts have held that the risk of future identity theft or fraud is too speculative to constitute an injury in fact for purposes of Article III standing.") (citing cases), *appeal filed,* No. 16-2528 (8th Cir. June 2, 2016).

Forty-seven states, the District of Columbia, and Puerto Rico have security breach notification laws, *see, e.g.,* Mo. Rev. Stat. §407.1500, and the average cost of notification now stands at $170,000. Ponemon Institute's 2015 Global Cost of Data Breach Study Reveals Average Cost of Data Breach Reaches Record Levels. At least here in Missouri, the data breach notification law can only be enforced by the Missouri Attorney General; there is no private cause of action. *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1056 (E.D. Mo. 2009). Any cyberinsurance policy should cover litigation and notification costs related to a data breach.

(3) Costs Associated with Restoring, Updating, or Replacing Business Assets Stored Electronically. Following a security breach, system equipment—from servers to desktops—can be damaged or irreparably compromised. Determine whether the policy will cover the costs of replacing or restoring software, hardware, and company records, as well as the personnel time associated with these efforts.

(4) Business Interruption and Extra Expense. Do not underestimate the impact of a digital interruption. Benign computer glitches already have the ability to cause millions of dollars in damages, such as when thousands of United Airlines flights were delayed or cancelled because of net-

work connectivity issues. Christopher Drew, *United Airlines Grounds Flights, Citing Computer Problem,* N.Y. Times, July 8, 2015. If benign computer failures have such a high cost potential, imagine the impact of a targeted attack. Allianz Global Corporate & Security estimates that business interruption costs could equal or exceed direct losses from a data breach in the coming years. *A Guide to Cyber Risk*, Allianz Global Corporate & Specialty; *see generally Silverpop Sys., Inc. v. Leading Mkt. Techs., Inc.*, No. 1:12-CV-2513-SCJ, 2014 WL 11164763, at *1 (N.D. Ga. Feb. 18, 2014) (noting the ability of a data breach to disrupt a relationship between two companies), *aff'd,* 641 F. App'x 849 (11th Cir. 2016) (per curiam). Business interruption expense should be part of any cybersecurity policy.

(5) Liability Associated with Libel, Slander, Copyright Infringement, Product Disparagement, or Reputational Damage to Others When the Allegations Involve a Business Website, Social Media, or Print Media. *See Cybersecurity*, NAIC available at http://www.naic.org (last visited April 5, 2016); *see also A Guide to Cyber Risk*, Allianz Global Corporate & Specialty (noting that Allianz provides coverage for "[d]efense costs and damages for which the Insured is liable, arising from the publication or broadcasting of digital media content.").

(6) Expenses Related to Cyber Extortion or Cyber Terrorism. Ransomware, where digital criminals lock and encrypt system files, is becoming a persistent threat. The FBI received nearly 2,500 complaints of ransomware in 2015, with a cost to victims of more than $24 million. David Fitzpatrick and Drew Griffin, *'Ransomware' Crime Wave Growing*, CNN Money, Apr. 4, 2016. In February 2016, in one of the latest iterations of this cyber extortion game, Hollywood Presbyterian Medical Center agreed to pay $17,000 in bitcoin to release the ransomware holding its systems captive. Richard Winton, *Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating*, L.A. Times, Feb. 18, 2016.

Cyber extortion is relatively easy to pinpoint; cyber terrorism, less so. To amount to an "act of terrorism," at least as defined by the Terrorism Risk Insurance Act (TRIA), the Secretary of the Treasury, working with the Secretary of State and the Attorney General, must first certify that the act was an act of terrorism. To date, the Treasury has never certified any digital intrusion as a terrorist act. The TRIA also contemplates that a terrorist act must cause at least $5 million of damage and be intended to coerce the population or influence policy. Terrorism Risk Insurance Act, Pub. L. No. 107–297, §201, 116 Stat. 2322, 2337 (2002). This may prove a difficult, if not impossible, definition to meet. Coverage for ransomware and other cyber extortion methods is a must.

To date, the Treasury has never certified any digital intrusion as a terrorist act. The TRIA also contemplates that a terrorist act must cause at least $5 million of damage and be intended to coerce the population or influence policy.

(7) Coverage for Expenses Related to Regulatory Compliance for Billing Errors, Physician Self-Referral Proceedings, and Emergency Medical Treatment and Active Labor Act proceedings. *See* NAIC, *Cybersecurity*, available at http://www.naic.org (last visited April 5, 2016). Hospitals and healthcare providers hold a veritable treasure-trove of data, making them a favorite of hackers. For those in the health-care industry, an appropriate cybersecurity policy is a necessity.

(8) Coverage for Government Investigations or Fines. Any data breach may compel investigation by state and federal authorities. *See Retail Ventures*, 691 F.3d at 824 (noting expenses for attorney fees in connection with "investigations by seven state Attorney Generals and the Federal Trade Commission (FTC)."). The U.S. Court of Appeals for the Third Circuit has upheld the authority of the Federal Trade Commission to regulate cybersecurity under the unfairness prong of §45(a). *See F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240 (3d Cir. 2015); *see also id.* at 256 (faulting Wyndham for having been hacked three times and allegedly having no firewall at critical points, not restricting specific IP addresses, not using any encryption for certain customer files, and not requiring certain users to change their factory-set passwords). An insured should decide whether its cyberinsurance policy should cover litigation costs related to any government investigations and any resulting fines.

(9) Crisis Management and Public Relations Costs. Loss of reputation can be a significant expense following a cyberattack. Public relations firms may be needed to handle the crisis and restore faith in a company's brand. *See Retail Ventures*, 691 F.3d at 824 (noting that the plaintiff incurred expenses for "public relations" in the wake of its data breach). According to one study, nearly half of businesses viewed loss of reputation as the most significant threat following a security breach. *See A Guide to Cyber Risk*, Allianz Global Corporate & Specialty. Public relation costs should be a part of any cyberinsurance policy.

Special Considerations for Insureds

Beyond these coverage areas, insureds should consider several specific, potential exclusions. Among them:

(1) Beware Sublimits. Sublimits can turn a $10 million policy into a $1 million policy if an insurer argues that an entire set of damages and expenses falls within a single sublimit. Sublimits can cost an insured dearly, as the Hotel Monteleone in New Orleans recently discovered after its insurer's claims handler took the position that the Payment Card Industry Fines or Penalties Endorsement—with a $200,000 limit—applied not just "to amounts owed for violations of PCI DDS [Payment Card Industry's Data Security Standards] requirements, but also applie[d] to fraud recovery, operational reimbursement, and case management fee losses arising out of the 2014 cyberattack." *See New Hotel Monteleone LLC v. Certain Underwriters*

at Lloyd's of London, No. 2:16-CV-0061 (E.D. La. Jan. 5, 2016) (Doc. 1–2 at ¶¶16, 59) (seeking coverage under a $3 million CyberPro Insurance Policy). Beware the sublimits.

(2) Beware Coverage Limits. The demand for cybersecurity insurance is outpacing insurer's willingness to write these policies. Stephen Joyce, *Cybersecurity Insurance Explosion Poses Challenges.* Target's data breach cost the company nearly $250 million, but policies covering $100 million in damages are exceeding rare. *Id.; see also* Finkle, *Cyber Insurance Premiums Rocket After High-Profile Attacks* (noting the difficulty of obtaining coverage in excess of $100 million). Insurance giant AIG currently offers $75 million for a cyber-attack, but such coverage is reserved for global banking institutions—institutions believed to be among the most adept at securing their networks and mitigating cyber risk. Finkle, *Cyber Insurance Premiums Rocket After High-Profile Attacks*. For large companies and those with the greatest potential exposure, using a syndicate of insurers may be the only option for comprehensive coverage.

(3) Purchase Prior Acts Coverage. The pre-existing condition exception was once the bane of those seeking affordable health insurance. Pre-existing digital bugs and infections can be equally noxious and pose similar coverage issues. The "average time between an attacker breaching a network and its owner noticing the intrusion is 205 days." *The Cost of Immaturity*, The Economist, Nov. 7, 2015. Depending on the coverage date or the limit of a policy's retroactive date, an insured may be outside of its policy from day one. Insureds should be sure to purchase prior acts coverage that provides at least six months of retroactive coverage.

(4) Consider Physical Property Impacts. Cyberinsurance should not just be for digital risk. Digital intrusions and cyberattacks have the ability to impact physical property in a very analog way. In December 2015, hackers successfully targeted two power companies in Ukraine, knocking out the electricity for more than 80,000 customers. David Sax, *In the Age of Cybercrime, the Best Insurance May Be Analog*, Bloomberg Businessweek, Mar. 10, 2016. As pacemakers, thermostats, automobiles, and other household devices become networked (the so-called Internet of Things), the ability for cyberintrusions to produce real-world physical damage is increasing dramatically. Insureds should be aware of any limitation on property damage.

(5) Beware Minimum Required Practices Exclusions. There is a fine-line between a data breach and a failure to maintain adequate security measures. As several commentators have noted, the failure to maintain adequate security measures is the very essence—the *sine qua non*—of a data breach. *See* Danielle Gilmore and David Armillei, *The Future Is Now: The First Wave of Cyber Insurance Litigation Commences, and the Groundwork is Laid for the Coming Storm*, Aspatore, Feb. 2016. Few insurers would *not* be able to point to an insured's failure to maintain sufficient security measures in the aftermath of a data breach.

There is a fine-line between a data breach and a failure to maintain adequate security measures. As several commentators have noted, the failure to maintain adequate security measures is the very essence—the *sine qua non*—of a data breach.

The "Minimum Required Practices" exclusion requires a policyholder to maintain the cybersecurity procedures and controls identified in its application *as a condition for coverage. See Remarks by Deputy Sec'y Sarah Bloom Raskin at the Am. Bankers Ass'n Summer Leadership Meeting*, Treas. JL-0112, July 14, 2015. While these exclusions are typically negotiable, if the exclusion is found in a policy, then the insured must maintain those measures called for by the exclusion. *See id.* This exclusion has already been the subject of a declaratory judgment action. *See Columbia Casualty Co. v. Cottage Health Sys.*, No. 2:15-CV-03432 DDP-AGR (C.D. Cal. May 7, 2015) (Doc. 1 at ¶¶8, 42–44) (seeking a declaration that Columbia has no obligation to provide Cottage Health with a defense or indemnification in connection with a data breach because Cottage Health failed to implement the procedures and risk controls identified in its application). Beware of a Minimum Required Practices exclusion.

(6) Pay Attention to the Treatment of Company Employees. Hackers are not particular about whose data or PII they compromise. A data breach can implicate not just client records and data, but also the PII of company employees. *See Corona*, 2015 WL 3916744, at *1 (noting that the hackers of Sony Pictures obtained the PII of at least 15,000 current and former Sony employees). Any cybersecurity policy should include protection for claims brought by company employees. If the policy has an "insured versus insured" exclusion, be sure that company employees are exempted from this exclusion.

Company employees can be victims; they can also be the perpetrators or instigators of a data breach. A disgruntled employee may allow intruders into a network, actively post information on the Internet, or, as may be the case with the Panama Papers, forward 2.6 terabytes of sensitive company data to outside reporters. *See* Nicola Clark, *How a Cryptic Message, 'Interested in Data?,' Led to the Panama Papers*, N.Y. Times, Apr. 5, 2016. Be sure the cyberinsurance policy addresses such an eventuality and that it does not impute an employee's conduct to the entire company (with the exception, perhaps, of directors and officers). Otherwise, an event that would normally be covered may fall within an exclusion for dishonest, deceptive, or illegal conduct by the insured. *See* Matthew Foy and Jonathan Schwartz, *Sony's Interview Quagmire,* In-House Defense Quarterly, Spring 2015.

Company employees can, unwittingly, perpetrate data breaches. With spearphishing (or "whaling" for larger targets),

criminals use personally-addressed emails that purport to be from a company executive, co-worker, or client to access protected information or to perpetuate a fraud. Because the messages looking genuine, they are far more successful than previous, widely cast phishing efforts. *See* Erika Kinetz, *Mattel Fought Elusive Cyber-Thieves to Get $3M Out of China*, Associated Press, Mar. 29, 2016. A number of insureds have recently brought suit after their insurers denied coverage for spear-phishing incidents. *See Ameriforge Group, Inc. v. Fed. Ins. Co.*, No. 4:16-CV-377 (S.D. Tex. Feb. 12, 2016) (Doc. 1-1 at ¶¶10–12, 24) (claiming coverage for $480,000 payment from spear-phishing fraud under the Computer Fraud Coverage or Funds Transfer Fraud Coverage sections of insurance policy); *Medidata Solutions, Inc. v. Fed. Ins. Co.*, No. 1:15-CV-907 ALC (S.D.N.Y. Feb. 6, 2015) (Doc. 1 at ¶¶2–4) (claiming coverage for a $4.8 million wire transfer from spear-phishing fraud under Computer Fraud, Funds Transfer Fraud and Forgery sections of insurance policy). Any policy should address employee conduct and employee PII.

(7) Beware War and Nation-State Exclusions. The days of traditional, pitched-battle warfare are long gone. Today's battlefront is a digital one, with sophisticated hackers sitting behind computer screens rather than rifles. The sophistication of today's hackers points increasingly to state actors, some with military affiliations. *See, e.g.,* Adrian Chen, *The Agency*, N.Y. Times Magazine, June 2, 2015; *Hackers Inc.*, The Economist, July 12, 2014. The United States and its allies are also believed to have engaged in such digital espionage, with reports indicating that American and Israeli software experts were behind the Stuxnet virus that damaged Iran's centrifuges. *Defending the Digital Frontier*, The Economist, July 12, 2014.

Insureds should carefully examine the war and terrorism exclusions of any policy. For example, form CG 00 01 12 07 excludes coverage for any "[w]arlike action by a military force…."). It is unclear how this exclusion will be applied in the cybersecurity context and how to define precisely what constitutes an act of war or terror in the digital world. The advent of Tor and other avenues for concealing location and usage information makes the prospect of identifying the exact origin of an attack only that much more difficult. Carefully consider a war or nation-state exclusion.

Special Considerations for Law Firms

Law firms stand as especially attractive targets for hackers. Law firms hold sensitive and confidential information desired by hackers, but often without the full set of security features used by the underlying client. For hackers seeking trade secrets, financial records, or pending corporate transactions, law firms usually represent the path of least resistance. Nicole Hong, *When Do Law Firms Have to Disclose a Data Breach?*, Wall. St. Journal, Mar. 30, 2016. Few believe that a law firm's security features approach those of the corporations whose information they hold. *See id; see also* Michael Riley and Sophia Pearson, *China-Based Hackers Target Law Firms to Get Secret Deal Data*, Bloomberg, Jan. 31, 2012.

Law firms stand as especially attractive targets for hackers. Law firms hold sensitive and confidential information desired by hackers, but often without the full set of security features used by the underlying client. For hackers seeking trade secrets, financial records, or pending corporate transactions, law firms usually represent the path of least resistance.

None of this is news. In September 2010, China-based hackers infiltrated seven Canadian law firms in an effort to derail a $40 billion takeover of Potash Corp. of Saskatchewan Inc. by BHP Billiton Ltd. Riley, *China-Based Hackers Target Law Firms to Get Secret Deal Data*. Law firms seeking a backstop for such breaches should not necessarily trust their Errors & Omissions or professional liability coverage. A special cybersecurity policy would likely be necessary to cover any damages related to (1) loss of revenue from a network outage; (2) costs to restore compromised data or investigate a breach; (3) costs for notifying regulators; (4) engaging a public relations firm; or (5) covering a ransomware attack. *See Views on Cybersecurity Insurance for Law Firms From Lockton Cyber Risk Practice Leader Ben Beeson*, Bloomberg BNA, Mar. 23, 2016; Joe Patrice, *The One Insurance Policy Your Practice May Not Have But Definitely Needs,* Above the Law, Mar. 22, 2016, available at http://abovethelaw.com (last visited April 5, 2016).

Law firms—and other companies for that matter—should not hesitate to test their own systems. Indeed, it is becoming increasingly common place to hire "white-hat" hackers to identify system vulnerabilities before those with the "black hats" have the chance. *See White Hats to the Rescue,* The Economist, Feb. 22, 2014; *see also* Nicole Perlroth, *Hacking for Security, and Getting Paid for It,* N.Y. Times, Oct. 14, 2015 (noting that the large technology companies provide bounties to hackers who identify holes in their software).

Conclusion

Ransomware, spear-phishing, malware, and other digital intrusions are here to stay. Worse yet, the sophistication of hackers and digital criminals will only grow, keeping pace—or even outpacing—the concomitant efforts at digital security. A tailored cybersecurity policy is a necessary component of both a company's insurance portfolio and its digital defenses.