STRADLEY RONON ATTORNEYS AT LAW

Adviser Alert

A Publication of the Stradley Ronon Investment Management Group

WWW.STRADLEY.COM

APRIL 2014, NO. 3

Stradley Ronon Stevens & Young, LLP
2005 Market Street, Suite 2600
Philadelphia, PA 19103-7018
215.564.8000 Telephone
215.564.8120 Facsimile
www.stradley.com

With other offices in:
Washington, D.C.
Malvern, Pa.
Harrisburg, Pa.
Wilmington, Del.
Cherry Hill, N.J.
New York, N.Y.

CYBERSECURITY UPDATE: What Should In-House Counsel Think About Following a Data Breach?

By Kenneth L. Greenberg

In our first Cybersecurity Update, we discussed the focus for 2014 on cybersecurity by the Securities and Exchange Commission's (SEC) National Exam Program and how investment advisers and investment companies can prepare for that regulatory focus. Our second Cybersecurity Update addressed the March 2014 SEC Roundtable on Cybersecurity. In this Cybersecurity Update, we discuss legal considerations for in-house counsel relating to a data security breach.

The phone rings and someone from IT is on the line. The person informs you that he or she suspects your company has just suffered a data security breach. In an ideal world, your firm has a data security breach response team in place, and has also adopted a data security breach response policy that provides the immediate steps the team should take to begin to investigate, contain and remediate the situation. While a checklist of actions that need to be taken to investigate, contain and remediate a data breach are beyond the scope of this Cybersecurity Update,[1] this article will focus on certain legal considerations in-house counsel should be aware of when faced with a data security breach.

- **Immediately involve experienced outside counsel before engaging any other outside service providers to assist with investigating and remediating the data security breach.**

  While you are probably not surprised to read this first bullet point in a newsletter written by an attorney at a law firm, there are sound reasons for involving outside counsel.

  Analysis of State Data Security Breach Notification Laws. First, as we mentioned in our prior Cybersecurity Update, 47 states, the District of Columbia, Puerto Rico, the Virgin Islands and Guam have enacted data security breach notification laws.[2] You will need experienced counsel to help analyze your data security breach to determine whether these state notification laws have been triggered because there has been a "breach of security" involving "personal information" as defined in such laws. Unfortunately, the state data breach notification statutes are not uniform and what constitutes a "breach of security" involving "personal information" in one state may differ from that in another state. For example, in California, a breach of security is defined as an "unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information."[3] Connecticut's data security breach notification law, on the other hand, not only includes the term "unauthorized acquisition" but also includes the term "unauthorized access,"[4] and Massachusetts includes "an unauthorized acquisition

or unauthorized use."[5] Similarly, while many states define "personal information" to include unencrypted information regarding an individual's first name or first initial and last name plus (1) a Social Security number; (2) a driver's license number or state-issued identification card number; or (3) a financial account number, credit card number or debit card number with password,[6] other states list other items that constitute personal information, such as date of birth and maiden name[7] or passport number.[8] Some states require notice of a data security breach to the state attorney general,[9] another government agency[10] or credit reporting agencies.[11] Some states require notification within a specific time frame.[12] Experienced counsel can help in-house counsel navigate the complexity of these requirements and assist in determining whether and to whom notification is required and whether, even if not required, notice is prudent for other reasons.

Attorney-Client Privilege/Work Product Immunity. By having outside counsel (as opposed to in-house counsel) directly engage cybersecurity and computer forensic experts and other service providers needed to investigate and remediate a data breach, communications and reports between lawyers and the various firms that may need to be engaged are more likely to be protected from discovery requests in litigation or investigations as either attorney-client privileged communications or attorney work product prepared in advance of litigation.

Attorney-Client Privilege. Generally, except in circumstances where the privilege is waived, when a client seeks legal advice from a lawyer, confidential communications between the lawyer and the client are permanently protected from disclosure. Neither the lawyer nor the client may be compelled to testify regarding the matters communicated to the lawyer by the client when seeking legal advice or the legal advice provided by the lawyer to the client.[13] Although the privilege may be considered waived if an attorney-client communication is disclosed to a third party, courts have recognized circumstances where communications and reports by a third party hired by a lawyer for aiding the attorney in rendering legal advice to the client are subject to attorney-client privilege.[14] It should be noted however that the attorney's hiring of a third party, in and of itself, does not subject the communication or report to attorney-client privilege.[15]

Work-Product Immunity. Work-product immunity is broader than attorney-client privilege, which is limited to confidential communications involving legal advice. Work-product immunity protects materials prepared by outside counsel "in anticipation of litigation," and its purpose is "to preserve a zone of privacy in which a lawyer can prepare and develop legal theories and strategy 'with an eye toward litigation' free from unnecessary intrusion by his adversaries."[16] Attorney work product is discoverable but "only upon a showing that the party seeking discovery has substantial need of the materials in the preparation of the party's case and that the party is unable without undue hardship to obtain the substantial equivalent of the materials by other means."[17]

- **Review your company's insurance policy to see if a data security breach is covered.**

  Traditional Insurance. For firms that have not purchased separate cybersecurity insurance, it may be possible to file claims under traditional insurance policies such as commercial general liability, fidelity insurance bond, directors' and officers' liability, or errors and omissions liability coverage for certain losses due to a data security breach. The terms, conditions and exclusions under the policy will need to be closely reviewed, as many policies do contain express "electronic data" or "data breach" exclusions. In addition, insurers have sought to deny policy coverage for data security breaches. For example, recently, in February 2014, in *Zurich American Insurance Co., et al. v. Sony Corp. of America, et al.,* No. 65198-2011 (N.Y. Sup. Ct. New York City), a New York trial court granted a summary judgment in favor of Zurich American Insurance Co. and ruled that Zurich American Insurance Co. had no duty to defend Sony Corp. of America and Sony Computer Entertainment America under a commercial general liability policy in connection with litigation stemming from the April 2011 hacking of Sony Corp.'s PlayStation online services.

  Cybersecurity Insurance. Many insurance companies offer separate cybersecurity insurance offering first-party (*i.e.,* losses related to the policyholder) and third-party (*i.e.,* losses related to clients) coverage. First-party coverage may include losses due to theft of confidential information due to hacking, breach notification expenses, forensic computer investigation/crisis management/reputational damage expenses, regulatory fines or regulatory action defense costs, business interruption expenses, and cyber-extortion costs. Third-party coverage may include payment of legal expenses arising from litigation with clients as well as credit-monitoring and fraud-resolution services for individuals or businesses impacted by the data breach.

  For both traditional and cybersecurity insurance, it will be important to determine what claims can be submitted to your insurance company and what the deadlines are for submitting any required notice. Cybersecurity insurance policies may

also have specific remediation steps that will need to be reviewed and followed to preserve coverage. For example, the policy should be reviewed to see if prior written consent from the insurance company is needed before engaging any data breach service providers. Such policies may also have pre-breach requirements that should be assessed and worked into your firm's compliance program ahead of a breach.

Cybersecurity is still relatively new, and the scope of coverage and embedded data protection requirements are not uniform across insurers offering these types of policies. Working with an experienced insurance broker to understand not only the scope of coverage, but also the nuanced requirements is essential. The insurance company may also be a valuable resource in assisting you in managing the response to a data security breach.

- **If the cause of the data security breach appears to involve a third-party service provider, review service contracts to determine whether the service provider will have indemnification or liability obligations to the firm.**

Service contracts often detail the standard of care that applies to a service provider and under what circumstances the failure to meet such standard would result in liability to your firm. Similarly, the service contract may detail the circumstances regarding when the service provider will indemnify your firm for losses it experiences and the procedures for seeking indemnification for such losses from the service provider, which may include timely notice. Certain service agreements may also have separate provisions that specifically address privacy and data protection. It is important for in-house counsel to determine whether the circumstances of the data breach involve a failure to meet a standard of care that may allow a liability claim or justify a request for indemnification. To the extent it is determined that a service provider may be liable for the data security breach or be subject to an indemnification obligation, the terms of a service provider agreement should also be reviewed regarding any notice or other procedural provisions for asserting liability or seeking indemnification from the service provider.

- **Prepare for possible criminal or civil litigation or regulatory investigation.**

A data security breach may result in civil or criminal litigation or regulatory investigation. The gathering and handling of evidence will be critical for not only investigating the incident and documenting how your firm's data was compromised, but evidence may also be needed for any legal

If you would like more information, contact Kenneth L. Greenberg at kgreenberg@stradley.com or 215.564.8149.

proceedings or investigations that result from the data security breach. In-house counsel not experienced with such investigations will want to consult with experienced outside counsel about how evidence should be collected and handled so as not to taint its admissibility in court, if needed.[18] Outside counsel can also assist with discovery issues such as the maintenance of privileged document logs and other processes that may limit the scope of materials that need to be provided to outside adverse parties. If litigation or an investigation is commenced against your firm, in-house counsel must also be sensitive to the duty to preserve evidence. A court finding of spoliation of evidence could result in a judge instructing the jury to allow an inference that any destroyed evidence was unfavorable to your firm.

- **If the cause of the data security breach is a result of an act of an employee, review compliance policies and procedures and other company policies to determine whether they may have been violated.**

To the extent that the data security breach appears to involve the action of one or more employees, legal and human resources will want to work in conjunction to determine whether any firm policies and procedures have been violated; what the consequence of that violation will be for such employee(s); and any procedures required to take action

IN-HOUSE LAWYER DATA SECURITY CHECKLIST

The following is a checklist of certain items in-house counsel may want to consider before and after a data security breach. It is by no means a comprehensive list of items, but merely a list of some of the more significant considerations.

Pre-Breach:

❑ Consider identifying one or more individuals within IT, corporate, legal/compliance and other relevant parts of the organization who will constitute your firm's data security team.

❑ Review existing data security breach, data privacy and computer security policies and procedures, and consider their effectiveness and any potential gaps. Also consider whether the policies and procedures meet any minimum standards required by the firm's insurance policies. Periodically (*e.g.,* annually or more frequently, if desired) reassess these policies and procedures.

❑ Review insurance policies to ensure coverage is consistent with business needs.

❑ Review third-party service contracts to ensure that computer security issues are properly addressed. Understand each party's obligations under the contract if a data security breach occurs. If needed, negotiate cyber-specific representations, warranties and indemnities in key service provider contracts.

Post-Breach:

❑ Review and determine actions required under firm data security breach, data privacy, computer security, crisis management and/or business continuity policies and procedures.

❑ Establish/activate data security breach response team and leader.

❑ Determine who within the organization needs immediate notification (*e.g.,* senior management, human resources and/or security).

❑ Determine what outside services may be needed to assist with the data security breach (*e.g.,* outside counsel, computer forensic investigators, data breach remediation firms and/or public relations firms), and hire such experts through outside counsel. Note that outside counsel can assist with identifying such experts and may already have relationships with them.

❑ Notify insurers within required policy time frames.

❑ Analyze whether international, federal and/or state data security breach notification laws or regulations apply to the data breach incident, and determine whether notifications are required. If needed, prepare a notification/communications plan.

❑ Determine whether it is necessary or appropriate to contact law enforcement agencies (*e.g.,* FBI, state or local police, and/or state attorney general's office) and applicable regulators (*e.g.,* SEC, Commodity Futures Trading Commission and/or Financial Industry Regulatory Authority).

❑ Review service provider contracts and determine whether any notification obligations exist and their required time frame.

❑ Establish, with assistance of experienced counsel, acceptable methods for gathering and handling evidence in order to preserve the admissibility of such evidence in court, if necessary.

❑ Consider whether and to whom to send "litigation hold" notices.

❑ Maintain a record of actions taken in response to the data security breach. ▪

---

[1] For the more technical computer-related aspects of steps to be taken in a data security breach, *see* Computer Security Incident Handling Guide, Recommendations of the National Institute of Standards and Technology, Special Publication 800-61, Revision 2 at http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf.

[2] *See* "State Security Breach Notification Laws," National Conference of State Legislatures, Apr. 11, 2014, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification.laws.aspx.

[3] Cal. Civ. Code § 1798.82.

[4] Conn. Gen. Stat. § 36a-701b(a). See also N.J. Stat. § 56:8-163.a (access by an unauthorized person).

[5] Mass. G.L.A. 93H § 1(a).

[6] *See,* e.g., 73 Pa. Stat. [Trade and Commerce] § 2302; or Colo. Rev. Stat. § 6-1-716.

[7] N.D. Cent. Code § 51-30-01.

[8] Or. Rev. Stat. § 646A.602.

[9] *See e.g.,* Cal. Civ. Code § 1798.82(f) (if more than 500 California residents are notified as a result of a single breach); Conn. Gen. Stat. § 36a-701b(b)(2); Indiana Code § 24-4.9-3-1(c); Md. Code Comm. Law § 14-3504(h); and Mo. Rev. Stat.§ 407.1500.2.d.(8) (if more than 1,000 persons are affected).

[10] *See, e.g.,* H.R.S. § 487N-2(f) (if breach involves more than 1,000 persons, notify Hawaii Office of Consumer Protection); S.C. Code 1976 § 39-1-90(K) (if 1,000 or more persons affected, notify the Consumer Protection Division of the Department of Consumer Affairs); New York Gen. Bus. Law § 899-aa.8 (notify Attorney General, Department of State and Division of State Police); and N.J. Stat. § 56:8-163.c(1) (notify the Division of State Police in the Department of Law and Public Safety).

[11] *See, e.g.,* Mo. Rev. Stat. § 407.1500.2.d.(8); S.C. Code 1976 § 39-1-90(K) (if more than 1,000 persons affected); H.R.S. § 487N-2(f) (if more than 1,000 persons affected); and New York Gen. Bus. Law § 899-998(b) (if more than 5,000 New York residents affected).

[12] *See, e.g.,* Fla. Stat. § 817.5681(b)(1) and (3) (no later than 45 days following the determination of the breach but may be delayed upon request by a law enforcement agency); Ohio R.C. § 1349.19(B)(2) and (D) (no later than 45 days following discovery subject to the legitimate needs of law enforcement activities); 9 Vt.S.A. § 2435(b)(1) (no later than 45 days following discovery of the breach, consistent with legitimate needs of law enforcement agency); and Wis. Stat. § 134.98(3) and (5) (not to exceed 45 days after the entity learns of the acquisition of personal information subject to request by law enforcement not to notify).

[13] For a general discussion of the privilege, *see United States v. United Shoe Machinery Corp.,* 89 F. Supp. 357 at 358-9 (D.C. Mass. 1950) and *SmithKline Beecham Corp. v. Apotex Corp.,* 232 F.R.D. 467, 472-473 (E.D. Pa., 2005).

[14] *See, e.g.,* United States v. Kovel, 296 F.2d 918, 921-923 (2nd Cir. 1961) (attorney-client privilege has been accorded to communications made by a client to an accountant in attorney's employ in connection with the client's obtaining legal advice from the attorney); *United States v. Cote,* 456 F.2d 142, 144 (8th Cir. 1972) (attorney-client privilege has been accorded to memoranda and working papers prepared by an accountant at the attorney's request to aid in advising his client whether to file an amended tax return); *United States v. Judson,* 322 F.2d 460, 462-63 (9th Cir. 1963) (attorney-client privilege has been accorded to a statement of the client's net worth and related memoranda prepared by an accountant at the attorney's request); and *United States v. Alvarez,* 519 F.2d 1036, 1045-1046 (3rd Cir. 1975) (attorney-client privilege has been accorded to a psychiatrist hired by the defense to aid in the preparation of an insanity defense). Other courts have generally acknowledged that there are circumstances where attorney-client privilege can attach to reports of third parties made at the request of the attorney, *see, e.g., In re Grand Jury Proceedings, 220 F.3d 568, 571 (7th Cir. 2000); United States v. Bornstein, 977 F.2d 112, 116-17 (4th Cir. 1992); and Fed. Trade Comm'n v. TRW, Inc., 628 F.2d 207, 212 (D.C. Cir. 1980).*

[15] *See Cavallaro v. United States,* 284 F.3d 236, 247 (1st Cir. 2002).

[16] *See, United States v. Adlman,* 134 F.3d 1194, 1196 (2nd Cir. 1998) quoting *Hickman v. Taylor,* 329 U.S. 495, 510-511 (1947). See also Rule 26(b)(3) of the Federal Rules of Civil Procedure and United States v. Nobles, 422 U.S. 225, 238-239 (1975) (noting that work-product doctrine protects materials prepared by agents for the attorney as well as the attorney himself).

[17] Rule 26(b)(3) of the Federal Rules of Civil Procedure.

[18] *See, e.g.,* "Evidence Gathering and Handling" on p. 36 in Computer Security Incident Handling Guide, supra, footnote 1.

Stradley Ronon's Investment Management Group

ATTORNEYS

Bruce G. Leto, Chair .....bleto@stradley.com.....215.564.8115
John M. Baker .....jbaker@stradley.com.....202.419.8413
Fabio Battaglia III .....fbattaglia@stradley.com 215.564.8077
Shanna B. Bayer .....sbayer@stradley.com 202.507.6406
E. Carolan Berkley .....ecberkley@stradley.com 215.564.8018
Joan E. Boros.....jboros@stradley.com 202.507.6413
Emily Taylor Brody .....ebrody@stradley.com 215.564.8071
Jessica Burt .....jburt@stradley.com.....202.419.8409
Anthony V. Coletta Jr. .....acoletta@stradley.com 215.564.8154
Joel D. Corriero .....jcorriero@stradley.com.....215.564.8528
Jana L. Cresswell.....jcresswell@stradley.com.....215.564.8048
Brian Crowell .....bcrowell@stradley.com.....215.564.8082
Matthew R. DiClemente .....mdiclemente@stradley.com 215.564.8173
Lisa A. Duda .....lduda@stradley.com 215.564.8143
Ruth S. Epstein .....repstein@stradley.com 202.292.4522
J. Stephen Feinour Jr. .....jfeinourjr@stradley.com 215.564.8521
Amy C. Fitzsimmons .....afitzsimmons@stradley.com....215.564.8711
Alison M. Fuller .....afuller@stradley.com 202.419.8412
Robert K. Fulton .....rfulton@stradley.com 215.564.8042
Alan R. Gedrich.....agedrich@stradley.com.....215.564.8050
Jamie M. Gershkow.....jgershkow@stradley.com 215.564.8543
Kenneth L. Greenberg .....kgreenberg@stradley.com....215.564.8149
Cory O. Hippler.....chippler@stradley.com 215.564.8089
Peter M. Hong .....phong@stradley.com.....202.419.8429
Nathan M. Iacovino .....niacovino@stradley.com.....215.564.8164
Kristin H. Ives .....kives@stradley.com 215.564.8037
John Y. Kim .....jkim@stradley.com.....215.564.8020
Lisa M. King .....lking@stradley.com 215.564.8733
Jonathan M. Kopcsik .....jkopcsik@stradley.com 215.564.8099
Mena Ryley Larmour.....mlarmour@stradley.com.....215.564.8014
Cillian M. Lynch .....clynch@stradley.com 202.419.8416
Michael D. Mabry .....mmabry@stradley.com 215.564.8011
Prufesh R. Modhera.....pmodhera@stradley.com.....202.419.8417
Michael W. Mundt.....mmundt@stradley.com 202.419.8403
Molly O'Brien .....mobrien@stradley.com 202.292.4527
Michael P. O'Hare .....mohare@stradley.com.....215.564.8198
David F. Roeber.....droeber@stradley.com 215.564.8179
Mark A. Sheehan .....msheehan@stradley.com.....215.564.8027
Nicole Simon .....nsimon@stradley.com.....215.564.8001
Amy G. Smith .....asmith@stradley.com 215.564.8104
Lawrence P. Stadulis .....lstadulis@stradley.com 202.419.8407
Merrill R. Steiner.....msteiner@stradley.com.....215.564.8039
John L. Sullivan .....jsullivan@stradley.com.....202.292.4524
Joan Ohlbaum Swirsky .....jswirsky@stradley.com 215.564.8015
Angela N. Velez.....avelez@stradley.com 215.564.8691
Christopher J. Zimmerman ....czimmerman@stradley.com 202.419.8402

IMG PRACTICE GROUP ADMINISTRATOR

Sinclair A. Ziesing .....sziesing@stradley.com 215.564.8055

LEGAL ASSISTANTS

Katherine Bennett .....kbennett@stradley.com.....202.507.6407
Robert Dillon .....rdillon@stradley.com.....215.564.8649
Dawn E. Mac Donald .....dmacdonald@stradley.com 408.241.1770
Kristopher R. Pietrzykowski ....kpietrzykowski@stradley.com..215.564.8114
Maximillian Schultz .....mschultz@stradley.com 202.419.8411

FUND TAXATION

ATTORNEYS

Zachary P. Alexander.....zalexander@stradley.com 215.564.8043
David J. Karasko .....dkarasko@stradley.com 215.564.8542
Kristin M. McKenna .....kmckenna@stradley.com 215.564.8176
William S. Pilling III .....wpilling@stradley.com 215.564.8079
Christopher C. Scarpa .....cscarpa@stradley.com.....215.564.8106

FUND ENFORCEMENT AND LITIGATION

ATTORNEYS

Steven B. Davis .....sdavis@stradley.com.....215.564.8714
Gregory D. DiMeglio .....gdimeglio@stradley.com 202.419.8401
Keith R. Dutill .....kdutill@stradley.com 610.640.5809
Zachary T. Knepper .....zknepper@stradley.com 202.419.8414
David C. Franceski Jr. .....dfranceski@stradley.com 215.564.8062
Paula D. Shaffner.....pshaffner@stradley.com 215.564.8761
Rachel Tausend .....rtausend@stradley.com 202.419.8405

EXCHANGE-TRADED FUNDS (ETFs)

ATTORNEYS

Fabio Battaglia III .....fbattaglia@stradley.com 215.564.8077
E. Carolan Berkley .....ecberkley@stradley.com 215.564.8018
Matthew R. DiClemente ....mdiclemente@stradley.com 215.564.8173
Lisa A. Duda .....lduda@stradley.com 215.564.8143
J. Stephen Feinour Jr. .....jfeinourjr@stradley.com 215.564.8521
Kenneth L. Greenberg .....kgreenberg@stradley.com....215.564.8149
Bruce G. Leto .....bleto@stradley.com.....215.564.8115
Michael D. Mabry .....mmabry@stradley.com 215.564.8011
Michael W. Mundt .....mmundt@stradley.com 202.419.8403

CFTC ISSUES

ATTORNEYS

Ruth S. Epstein .....repstein@stradley.com 202.292.4522
Kenneth L. Greenberg .....kgreenberg@stradley.com....215.564.8149
Peter M. Hong .....phong@stradley.com.....202.419.8429
Kevin P. Kundra.....kkundra@stradley.com 215.564.8183
Merrill R. Steiner.....msteiner@stradley.com.....215.564.8039

ERISA

ATTORNEY

James F. Podheiser.....jpodheiser@stradley.com 215.564.8111

FUND BANKING ISSUES

ATTORNEY

Christopher S. Connell .....cconnell@stradley.com.....215.564.8138

ISDA/STRUCTURED FINANCE MATTERS

ATTORNEYS

E. Carolan Berkley .....ecberkley@stradley.com 215.564.8018
Deborah Hong .....dhong@stradley.com.....610.640.5818
Kevin P. Kundra.....kkundra@stradley.com 215.564.8183