Damage Models in Data Breach Class Actions

Evaluating damages in a data breach class action can prove a tricky affair. There are several different possible approaches; some reasonably well-established and some fairly novel. Appropriately understanding and deploying them (or defending against them) in a given case involves evaluating not only the strength of the model, but also the nature of the damage being alleged.

One of the main difficulties is most damage models have not been court-tested. Perhaps because of the fear of unknowns, data breach litigation often seems to resolve before decisions on class certification or dispositive motions (and, to my knowledge, no data breach class action has ever gone through trial). So, damage calculations remain somewhat theoretical, and precedent either supporting or rejecting them is sparse.

In this article, I will discuss a few possible approaches and when they might be most appropriate. I explain these models from the plaintiffs’ perspective, since that is my background, but hopefully the discussion is helpful for any practitioner.

Read more on page 9
Chair Message

As the incoming chair of the TIPS Cybersecurity & Privacy Committee, I welcome you!

Not a week goes by that we don’t learn of numerous and sometimes massive e-thefts striking at the heart of various tech-savvy businesses. No wonder we are all becoming “cyber-phobic” (shout out to insurance guru Chris Kende for coining this apt phrase). Our committee strives to help its members stay current so we can keep ourselves, our firms and our clients cyber-secure and confident of what to do to prevent e-theft and what to do if and when it occurs. Please keep reading to see what programs we have in the works to help us stay cyber-secure:

**Network Interruption vs. Business Interruption Coverage - Overlaps and Gaps** will be discussed on February 22-23, 2019 at the 27th Annual Insurance Coverage Litigation Midyear Conference (ICLC) being held at the Arizona Biltmore Resort.

What must we do to do to keep our law firms’ data cyber-secure and protect the data our clients entrust to us from being hacked? Join us at the TIPS Section Conference program in New York, May 1-2, 2019, to find out. Because of the importance of this topic, we will have not one, but two panels: Co-sponsored with the TIPS Excess, Surplus Lines and Reinsurance Committee, the first panel will discuss **Law Firm Exposure for Cyber Security Risks** and the second panel, co-sponsored with the TIPS Fidelity & Surety Committee, will discuss **The Next Cyber Loss Could Be Yours: The Fidelity/Crime Insurance Your Law Firm Needs to Carry**.

Our committee is also active in publishing useful cyber information. In addition to newsletters like this one, check out the upcoming TIPS Tort Source survey issue where recent federal and state cyber cases and statutes are addressed. Also be on the lookout for the Spring 2019 edition of TIPS for articles on **Basic Encryption for Lawyers, General Data Protection Regulation (GDPR) and Insurability and Internet of Things Liability**.

Perhaps the most exciting event in our committee’s pipeline is the first **TIPS National Cybersecurity Conference** on March 5-6 2020 in Atlanta, Georgia. **Mark your calendars now** to join national cyber leaders discussing cutting edge issues. It is an event not to be missed.

It takes a lot of passionate and hard working members to accomplish the work of our Committee. Special thanks to chair-emeritus Kathy Strickland, chair-elect Michelle Tilton, chair-nominee Larry Schiffer, programs chair Randolph Scott and newsletter chair Brian Findley. The list of additional committed committee members goes on and on. You know who you are and we are grateful for your help. We need more hands on deck. **If you aren’t already working on a project with us, please contact me and get started today.**

Jan Mulligan
Mulligan, Banham & Findley

©2018 American Bar Association, Tort Trial & Insurance Practice Section, 321 North Clark Street, Chicago, Illinois 60654; (312) 988-5607. All rights reserved.

The opinions herein are the authors’ and do not necessarily represent the views or policies of the ABA, TIPS or the Cybersecurity and Data Privacy Committee. Articles should not be reproduced without written permission from the Copyrights & Contracts office copyright@americanbar.org.

Editorial Policy: This Newsletter publishes information of interest to members of the Cybersecurity and Data Privacy Committee of the Tort Trial & Insurance Practice Section of the American Bar Association — including reports, personal opinions, practice news, developing law and practice tips by the membership, as well as contributions of interest by nonmembers. Neither the ABA, the Section, the Committee, nor the Editors endorse the content or accuracy of any specific legal, personal, or other opinion, proposal or authority.

Copies may be requested by contacting the ABA at the address and telephone number listed above.
**Editor Letter**

Welcome to the Fall 2018 Edition of our newsletter! I am your incoming Editor for the Fall 2018 through Fall 2019 year. We will continue to bring you cutting edge, thought-provoking articles on all things cyber this year, with issues every quarter.

This issue is a particularly fascinating one, with articles on data breach class action damage models, cybersecurity enforcement by the SEC, litigation against cyber-insurance professionals, and a piece on what to expect from our committee’s new mentor-mentee program.

Looking forward to a great year of exploring this rapidly-developing area of the law with you all. Please contact me at findley@janmulligan.com with any article proposals, suggestions or comments.

---

**Connect with Cybersecurity and Data Privacy website**

**Stay Connected with TIPS**

We encourage you to stay up-to-date on important Section news, TIPS meetings and events and important topics in your area of practice by following TIPS on Twitter @ABATIPS, joining our groups on LinkedIn, following us on Instagram, and visiting our YouTube page! In addition, you can easily connect with TIPS substantive committees on these various social media outlets by clicking on any of the links.

americanbar.org/tips
<table>
<thead>
<tr>
<th>Name</th>
<th>Firm Name</th>
<th>Address</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amber Locklear</td>
<td>Ropers Majeski Kohn Bentley</td>
<td>750 3rd Ave, 25th Fl, New York, NY 10017</td>
<td>(212) 688-5927</td>
<td><a href="mailto:alocklear@rmkb.com">alocklear@rmkb.com</a></td>
</tr>
<tr>
<td>Jennifer Parrott</td>
<td>Drew Ecki &amp; Farnham LLP</td>
<td>303 Peachtree St NE, Ste 3500, Atlanta, GA 30308-3263</td>
<td>(404) 885-8217</td>
<td><a href="mailto:jparrott@deflaw.com">jparrott@deflaw.com</a></td>
</tr>
<tr>
<td>Michael Menapace</td>
<td></td>
<td>6 Pheasant Run, North Granby, CT 06060</td>
<td>(860) 297-3733</td>
<td><a href="mailto:mmenapace@wiggin.com">mmenapace@wiggin.com</a></td>
</tr>
<tr>
<td>Joshua Mooney</td>
<td>White and Williams LLP</td>
<td>1650 Market Street, One Liberty Place, Ste 1800, Philadelphia, PA 19103-7395</td>
<td>(610) 649-3886</td>
<td><a href="mailto:mooneyj@whiteandwilliams.com">mooneyj@whiteandwilliams.com</a></td>
</tr>
<tr>
<td>Ndidi Moses</td>
<td>US Attorney Office</td>
<td>1000 Lafayette Blvd, Fl 10, Bridgeport, CT 06040-4759</td>
<td>(203) 275-8299</td>
<td><a href="mailto:ndidi.moses@usdoj.gov">ndidi.moses@usdoj.gov</a></td>
</tr>
<tr>
<td>Michael Nitardy</td>
<td>Frost Brown Todd LLC</td>
<td>7310 Turfway Rd, Ste 210, Florence, KY 41042-1374</td>
<td>(859) 817-5914</td>
<td><a href="mailto:mntardy@tbtlaw.com">mntardy@tbtlaw.com</a></td>
</tr>
<tr>
<td>Mitchell Orpett</td>
<td>Tibbler Orpett &amp; Meyer PC</td>
<td>225 W Washington St, Ste 2550, Chicago, IL 60606-3418</td>
<td>(312) 201-6413</td>
<td><a href="mailto:marpett@moberg.com">marpett@moberg.com</a></td>
</tr>
<tr>
<td>Pamela Palmer</td>
<td>Clark Hill PLL</td>
<td>1055 W 7th St, Ste 2400, Los Angeles, CA 90017-2550</td>
<td>(213) 417-5168</td>
<td><a href="mailto:ppalmer@clarkhill.com">ppalmer@clarkhill.com</a></td>
</tr>
<tr>
<td>Larry Schiffer</td>
<td>Squire Patton Boggs</td>
<td>30 Rockefeller Plaza, 23rd Fl, New York, NY 10112</td>
<td>(646) 557-5194</td>
<td><a href="mailto:Larry.Schiffer@squirepb.com">Larry.Schiffer@squirepb.com</a></td>
</tr>
<tr>
<td>Randolph Scott</td>
<td></td>
<td>57 Hayden Dr, Cincinnati, OH 45218</td>
<td>(513) 428-0699</td>
<td><a href="mailto:rascott67@gmail.com">rascott67@gmail.com</a></td>
</tr>
<tr>
<td>Scott Spearing</td>
<td>Hermes Neburn O’Connor &amp; Spearing PC</td>
<td>265 Franklin St, Fl 7, Boston, MA 02110-3113</td>
<td>(617) 728-0050</td>
<td><a href="mailto:sspearing@hermesneburn.com">sspearing@hermesneburn.com</a></td>
</tr>
<tr>
<td>Robert Stines</td>
<td>Freeborn &amp; Peters LLP</td>
<td>201 North Franklin St, Ste 3550, Tampa, FL 33602</td>
<td>(813) 472-7550</td>
<td><a href="mailto:rstines@freeborn.com">rstines@freeborn.com</a></td>
</tr>
<tr>
<td>Tamara Tomomitsu</td>
<td>Borden Ladner Gervais LLP</td>
<td>30 Rockefeller Plaza, Fl 23, New York, NY 10112</td>
<td>(212) 895-4221</td>
<td><a href="mailto:daniel.vinish@squirepb.com">daniel.vinish@squirepb.com</a></td>
</tr>
<tr>
<td>Ryan Weeks</td>
<td>Mills Paskert Divers</td>
<td>100 N Tampa St, Ste 3700, Tampa, FL 33602-5835</td>
<td>(813) 229-3500</td>
<td><a href="mailto:rweeks@msdelegal.com">rweeks@msdelegal.com</a></td>
</tr>
<tr>
<td>Nicholas Wittenberg</td>
<td>US EPA</td>
<td>1200 Pennsylvania Ave NW, Washington, DC 20460</td>
<td>(215) 367-0974</td>
<td><a href="mailto:nwitten@hotmail.com">nwitten@hotmail.com</a></td>
</tr>
<tr>
<td>Young Lawyer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bethany Corbin</td>
<td>Wiley Rein LLP</td>
<td>1776 K St NW, Washington, DC 20006</td>
<td>(704) 338-6116</td>
<td><a href="mailto:bcorbin@wileyrein.com">bcorbin@wileyrein.com</a></td>
</tr>
</tbody>
</table>
Trick or Treat: Does the SEC’s October Report Signal a New Shift in Cybersecurity Enforcement?

On October 16, 2018, the Securities and Exchange Commission’s (SEC) Division of Enforcement issued a report on Cyber-Related Frauds Against Public Companies and Related Internal Accounting Controls Requirements (the Report)\(^1\) warning that a public company’s failure to implement adequate cybersecurity controls to address the risk of “business email compromises” (BECs) may violate Sections 13(b)(2)(B) of the Securities Exchange Act of 1934 (the 1934 Act).\(^2\) This Report foretells a potentially seismic shift in securities regulation for cybersecurity, and the agency’s interpretation of the 1934 Act should be a stark warning to companies that have not taken affirmative steps to address risks posed by phishing attacks.

The Report arguably builds upon the SEC’s February 21, 2018 guidance on cyber disclosure by publicly traded companies, which advised companies to disclose cyber risks that are material, including amending prior filings to the extent such material risks were not adequately disclosed. Given the Report’s focus on “internal controls,” public companies and legal practitioners should anticipate that the existence and sufficiency of such controls will be a critical component of SEC regulation, investigations, and enforcement actions with respect to public companies’ disclosure and handling of cybersecurity risk and events. Further, if the SEC views cybersecurity controls as crucial for financial disclosures, as required by existing statutory regimes, i.e., the Sarbanes-Oxley Act and the 1934 Act, then the SEC should be expected to view cybersecurity controls as critical for compliance with federal securities laws. With this new shift, the SEC soon may require individual directors and officers to certify their companies’ compliance with cybersecurity controls, just as executive management for certain companies must do under New York’s cybersecurity regulations.\(^3\) This requirement, in turn, may create a new breeding ground for shareholder class actions and derivative actions. As discussed below, the SEC’s Report may be a vanguard of new and significant changes.

I. What are BECs?

BECs are a category of phishing attacks whereby a third-party fraudster impersonates a trusted source to trick the email’s recipient into wiring money to them. A company employee (typically, a lower-level employee) will receive a false email ostensibly coming from a trusted source (a company executive or established vendor) instructing that a payment be wired to a specified bank account that the fraudster

---

Joshua Mooney
White and Williams LLP

Andrew Lipton
White and Williams LLP

Richard Borden
White and Williams LLP

All views expressed herein are those of the authors, and are not the views of White and Williams or its clients.

Read more on page 12
Cybersecurity and Data Privacy

Cyberclaims and Litigation Against Insurance Professionals*

Technology such as cloud computing, machine learning, “internet of things” and autonomous vehicles are changing society. Along with these rapid societal changes, cyberthreats are evolving more quickly than chief information security officers can deploy systems to anticipate and prevent breaches. While these breaches were once considered threats only for larger corporations, they since have become problems for smaller companies and individuals as well.

This increased risk of cybervents presents a fertile market for the insurance industry to create new products. Insurance professionals who aim to serve the needs of their corporate clients (whether large or small) must market and provide advice about these new products.

The numerous vectors for cyberattacks — and the uncertainty surrounding how these new insurance products will respond to cyberclaims — has increased the risk of litigation against insurance professionals.

This analysis will briefly discuss uncertainty related to cyberinsurance policies, litigation against insurance agents and brokers, the evolving duty to advise clients about cyberinsurance, and risk management considerations to avoid litigation.

Cyberinsurance Policies

Although there are exceptions, courts have generally decided that commercial general liability insurance does not cover cybervents. To avoid confusion, many insurance carriers now affirmatively exclude cyberclaims from CGL policies.

Carriers are clearly communicating to insureds that they must obtain separate coverage addressing today’s cyberrisks in the form of cyberinsurance policies.

Unfortunately, the language in these policies is not standardized and is customizable depending on the carrier. Claims filed under them are frequently challenged in court, and each new court decision provides some answers — but also more confusion.

Confusion regarding coverage can easily arise when a social engineering vector causes an insured to wire funds to unintended recipients. A vector is the term used in the cybersecurity industry to describe the method of a cyberattack. Is the attack a cybervent, criminal fraud, employee error or all of the above?

Read more on page 16

Robert A. Steines, Esq.
Freeborn & Peters, LLP

Robert A. Steines is a Partner in the Tampa, Fla., office of Freeborn & Peters, LLP. A member of the firm’s Litigation Practice Group and Emerging Technologies Industry Team, he is a trial lawyer whose practice is focused on business disputes, professional liability defense, and cyber law. An IAPP US-law certified privacy professional, he also advises businesses on cybersecurity and data privacy issues. He can be reached at rstines@freeborn.com.
Join us for the premier CLE conference for insurance, defense, corporate, and plaintiffs attorneys.

**TIPS SECTION CONFERENCE**
May 1-4, 2019 | The Westin New York at Times Square | New York, NY

**LEARN:**
CLE programs from distinguished panelists including prominent judges and leading in-house and corporate counsel.

**NETWORK:**
Expand your circle at our complimentary nightly networking receptions.

**CELEBRATE:**
Entertaining social events in the Big Apple.

**JOIN:**
Become involved with our over 30 practice-specific committees for professional development and leadership opportunities

**ENJOY:**
Explore New York City with colleagues, new and old.

americanbar.org/tips
Damage... continued from page 1

**Damages stemming from identity theft-related losses**

This is one of the most traditional models. Basically, it involves providing some type of compensation for anyone who has suffered provable identity theft-related losses reasonably traceable to the data breach being litigated.

Quantification is usually straightforward, so instead the dispute often involves “traceability.” Given the ever-expanding number of large-scale data breaches—and the inherent difficulty in pinpointing a source of identity theft—a defendant can forcibly argue no plaintiff, much less a class of plaintiffs, can prove one breach in particular was the cause of the harm. Which, as a practical matter, is often true.

Thus far, it appears the traceability issue has only been tested at the pleading stage. On that point, some courts have suggested a defendant wishing to invoke the argument bears the burden of proving the harm was caused by some other breach. But, even if that is so, it doesn’t resolve the question of how that would impact class certification, as the defendant will still argue it is an issue requiring individual proof.

**“Benefit of the Bargain” Damages**

In some instances, the class members are paying for services that are breached. If so, an argument can be made the class members didn’t get what they paid for, i.e., they paid for secure services and didn’t receive them. The damages, then, are the difference in value between what the class members thought they were getting—a secure service—and what they actually got.

The question then becomes how much less was the service worth than what the class member paid for it? This one is difficult because there will almost certainly not be an itemized bill that includes data security as one of the entries. Assuming class members can’t otherwise get the defendant to segregate charges or costs for data security, an alternative approach is to use a conjoint survey.

A conjoint survey is a specialized market research tool designed to figure out the value consumers place on a particular attribute of a product or service, e.g., how much more might a buyer be willing to pay for a car with leather seats. It is frequently used by market research companies to help manufacturers and designers evaluate various options and trim packages and how to price them. Market research has determined consumers are notoriously poor self-reporters of this type of information, and so the conjoint is used in place of the more direct survey approach.

Conjoint surveys are not without controversy in the class action realm, but they have been accepted by some courts as a way to calculate consumer value on a class-wide basis. If, however, a conjoint survey is potentially in your future, one piece of advice:
make sure the survey is designed, vetted, and administered by someone with expertise in that area. Conjoint surveys require a lot of precision to do correctly, and errors in the methodology open the survey up to Daubert challenges. Correctly interpreting the results also requires sophistication, so have an expert who is able to do that as well.

In the case of data breach litigation, the conjoint survey could be used to parse out the value class members place on data security vis-à-vis the total service price. From this, it should be possible to determine a “benefit of the bargain” loss, e.g., if a class member paid $20/month for services and the conjoint survey revealed class members believed data security was 50% of the total product value, the damage would be $10/month.

“Lost Value of Personal Identifying Information (PII)” Damages

Finally, we come to the situation where the class member didn't pay anything for the service. This would be, for example, the average Facebook user, Gmail user, and so on.

There’s a saying from somewhere that goes “if you aren’t paying anything for a product, then you are the product.” That holds true for this model. Facebook, YouTube, and others make money by marketing you or marketing to you, or both. So you are “paying” for those services in a way, just not in the money directly leaving your account way. Instead, Google scrapes your email for content to sell to direct advertisers, Facebook scans your profile for the same purpose, etc.

Which leads us to the final model I will discuss: Loss of value of PII. This model is premised on the idea that a class member’s PII (personal information that can be used to identify the individual) has some market value. Big tech companies are willing to pay for access to it, and thieves want to steal it. And, indeed, some courts have agreed that loss of value of PII is at least a plausible theory, although that determination was again made at the motion to dismiss stage.

But, assuming PII does have some market value, and the data breach being litigated reduced that value, how can that be calculated? The main answer is “not easily.” Still, that hasn’t stopped creative people from trying. One measure is to look at what similar accounts sell for on the black market (known as the “dark web”). Another is to see what big data aggregators are willing to pay for similar data. And, finally, there are reports and surveys out there that attempt to calculate the value of a particular user account to, say, Facebook or other social media sites. These measures would at least provide some benchmarks, albeit inexact ones, for the total value of the PII.

Then calculating the diminution in value of that PII from the breach is exceedingly hard. There are generally few reliable benchmarks for that. One possible approach

Verizon dropped its purchase price for Yahoo! by $350 million after the breaches were revealed.
might be to compare the black market value, which is by definition breached data, with what the data might sell for in the legitimate market. Presumably, the black market value will be less—perhaps substantially less—thus showing a reduction in value. In the unusual case, it might also be possible to see what some later company was willing to pay for the breached data. So, for example, in the Yahoo! data breaches, Verizon dropped its purchase price for Yahoo! by $350 million after the breaches were revealed. How much of that related to the diminished value of the breached data is debatable, but it is likely more than zero.

These are but a few ideas. Data breach litigation is a new frontier, and a lot remains unclear. This allows for creativity, but not certainty.

Endnotes
1  This is an oversimplification to illustrate the point, but the basic tenets remain valid.
2  Ironically, some of these were created in other data breach class actions.
controls. Many times, these phishing emails have a time pressure component (i.e., “I will need the payment wired ASAP”), an impatient tone (“This is the third time we’ve made this request”), or involve a matter of “critical nature” (“This is vital to the company’s new strategic initiative”) in order to intimidate the recipient and inhibit him or her from questioning the request. In every successful BEC attack, the wiring instructions are followed, and payment(s) is/are sent. Once the money is wired, the funds are withdrawn by the fraudster, and the money is irretrievable.

BECs represent a significant risk to U.S. companies and to the economy as a whole. In a recent report, the Federal Bureau of Investigation estimated that BECs have caused over $5 billion in losses since 2013.4 The same report concludes that the loss totals for 2017 alone, approximately $675 million, represented the highest estimated out-of-pocket loss from any class of cyber-facilitated crime that year.5 What makes BECs so dangerous is their simplicity. Although false emails ostensibly coming from vendors can be a sophisticated endeavor because they may involve a successful intrusion into the vendors’ network and system, generally, BECs do not involve sophisticated fraud schemes or technology.6 Instead, they prey upon distraction, intimidation, and imitation – all weaknesses in human nature. Compounding the damage caused by BECs is the uncertainty of insurance coverage. Courts have struggled to understand the technology at issue and in turn have issued conflicting decisions.7

II. Implementing Internal Controls

The SEC long has recognized the significance of cyberattacks. It now has zeroed in on BECs. According to the SEC, the threat posed by BECs “underscore[s] the importance of devising and maintaining a system of internal accounting controls,” including training, to “protect assets in compliance with the federal securities laws.”8 Recognizing that BECs and other phishing attacks represent “an ever-increasing part of the cybersecurity threats faced by a wide variety of businesses,” the SEC now states that “public companies should pay particular attention to the obligations imposed by Section 13(b)(2)(B) to devise and maintain internal accounting controls that reasonably safeguard company and, ultimately, investor assets from cyber-related frauds.”9 Sections 13(b)(2)(B) (i) and (iii) state:

(2) Every issuer which has a class of securities registered pursuant to section 12 of this title [15 U.S.C. § 78l] and every issuer which is required to file reports pursuant to section 15(d) of this title [15 U.S.C. § 78o(d)] shall –
* * *

(B) devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that--

(i) transactions are executed in accordance with management’s general or specific authorization;

* * *

(iii) access to assets is permitted only in accordance with management’s general or specific authorization[.]

The Report concludes that these provisions now require public companies (governed by Sections 12 and 15(d)) to undertake affirmative steps through the implementation of cybersecurity controls to mitigate the risks posed by BECs and similar phishing attacks. Critically, this interpretation of Sections 13(b)(2)(B) (i) and (iii) easily may be applied to any significant cyber risk or known variant of cyberattack. Because companies with appropriate technical and administrative data security procedures are in a far better position to detect and prevent a successful cyberattack, the SEC is using existing securities laws to ensure that companies take affirmative steps to implement such safeguards. In essence, the SEC is charting new waters.

Moreover, the SEC’s focus on the human factor in cybersecurity risks should not be underestimated. For example, the SEC notes that “there were numerous examples where the recipients of the fraudulent communications asked no questions about the nature of the supposed transactions, even where such transactions were clearly outside of the recipient employee’s domain.” The Report further notes that “[h]aving internal accounting control systems that factor in such cyber-related threats, and related human vulnerabilities, may be vital to maintaining a sufficient accounting control environment and safeguarding assets,” and observes that “[s]ystems of internal accounting controls, by their nature, depend also on the personnel that implement, maintain, and follow them.” This focus suggests that while an SEC investigation may center upon technical and administrative aspects of any public company’s cybersecurity program, the agency also would investigate steps undertaken by the company to ensure effective implementation, including training. Simply, it is not enough to have a written security program in place. The program’s implementation must be effective.

To be clear, the Report does not endorse a one-size-fits-all approach. In the Report, the SEC states that companies “subject to the requirements of Section 13(b)(2)(B) must calibrate their internal accounting controls to the current risk environment and assess and adjust policies and procedures accordingly.” The Report also

“BECs do not involve sophisticated fraud schemes.... [T]hey prey upon... weaknesses in human nature.”
emphasizes that every public company that is a victim of a BEC is not necessarily in violation of federal securities laws. Instead, companies should ensure that they have reasonable measures in place and confirm that those measures have been implemented effectively. Companies “should evaluate to what extent they should consider cyber-related threats when devising and maintaining their internal accounting control systems,” and be mindful whether internal controls already in place “are sufficient to provide reasonable assurances in safeguarding their assets from these risks.” Those companies that do nothing, or fail to ensure that existing security controls address current risks and are implemented, may face an SEC enforcement action in addition to any loss suffered from a phishing attack. The Report is a clear example of how regulators are looking to existing laws to address ever-evolving cyber risks.

III. Forecasting Changes in Cybersecurity Enforcement

The SEC’s February 21, 2018 cybersecurity guidance for public companies emphasizes, among other things, that companies are required to establish and maintain appropriate and effective disclosure controls and procedures that enable them to accurately and timely disclose cybersecurity risks and incidents. Companies are also required to assess whether they have sufficient disclosure controls and procedures to ensure that relevant information about cybersecurity risks and incidents is processed and reported. Thus, the SEC’s most recent Report should not come as a great surprise. Yet, the Report may forecast significant changes.

The purpose of having strong disclosure controls is to assist companies in satisfying stringent disclosure obligations under the federal securities laws, including personal certification of disclosure executed by senior management under Sarbanes-Oxley. Further, the Report clearly signals that the SEC will place the responsibility of having adequate cybersecurity controls on management, an approach that already exists for internal controls over financial reporting under Section 404 of Sarbanes-Oxley. Thus, a pattern is emerging that suggests the SEC will replicate Sarbanes-Oxley requirements for cybersecurity controls. In other words, cybersecurity controls are not a component of risk management, they are an integral part of internal accounting controls themselves. If this is the case, the SEC may soon require executed certifications by individual directors and officers regarding cybersecurity controls, an approach that would place new obligations and pressure on senior management. The approach also would open new avenues for shareholder class action and derivative lawsuits. Such new liability, in turn, likely would lead to an increase in claims and costs, ultimately to be borne by D&O insurers, cybersecurity insurers, and their insureds.
The SEC’s October 16, 2018 Report should be viewed as a guidepost along a path that the SEC is charting for cybersecurity enforcement. The February 21, 2018 guidance required disclosure of risks; by requiring implementation of cybersecurity controls, the Report has now taken the next critical step. The Report may be a preview of the type of cybersecurity control enforcement actions that the SEC may pursue in the future. Public companies, and D&O and cybersecurity insurers should take notice.

Endnotes
3 23 NYCRR Part 500.17.b.
5 Id.
6 Report at 4. The Report on nine BECs involving a collective loss of approximately $100 million. Two of the nine companies lost in excess of $30 million. Id. at 3.
8 Report at 5.
9 Id.
10 15 U.S.C. § 78m(b)(2)(B)(i) and (iii).
11 Report at 6.
12 Id.
13 Id.
14 Report at 7.
In 2016, the Fifth Circuit Court of Appeals agreed with Great American Insurance Company that Apache Corporation’s loss of $1.5 million was not covered under a Computer Fraud Provision.¹

In 2013, an Apache employee in Scotland received a telephone call from a person identifying herself as a representative of Petrofac, a vendor for Apache. The caller instructed Apache to change the bank account information for its payments to Petrofac. The Apache employee replied that the change request could not be processed without a formal request on Petrofac letterhead.

A week later, Apache’s accounts-payable department received an email from a “petrofacltd.com” address. But Petrofac’s authentic email domain name is “petrofac.com.” The fraudsters created “petrofacltd.com” to send the fraudulent email. The email advised Apache that Petrofac’s account details were recently changed and directed Apache to make payment to the new account. A signed letter on Petrofac letterhead was attached to the email.

In response to the email, an Apache employee called the telephone number provided on the letterhead to verify the request and confirm the authenticity of the change request. Next, a different Apache employee approved and implemented the change. A week later, Apache transferred funds for payment of Petrofac’s invoices to the new bank account.

Within one month, Apache received notification from the genuine Petrofac that it had not received payment.

Apache submitted a claim to Great American asserting coverage under the Computer Fraud Provision, which states:

> We will pay for loss of, and loss from damage to, money, securities and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the premises or banking premises:
>
> a. to a person (other than a messenger) outside those premises; or b. to a place outside those premises. . .

In its denial letter, Great American advised Apache that its “loss did not result directly from the use of a computer nor did the use of a computer cause the transfer of funds.”

The Fifth Circuit acknowledged that the email was part of the scheme, but it concluded that the email was merely incidental to the occurrence of the authorized
transfer of money. The court opined that reducing the multi-step process to its simplest form, Apache made the transfers in order to pay legitimate invoices—not because of fraudulent information.

In Medidata Solutions v. Federal Insurance Co., through a sophisticated scheme of spoofed emails, a Medidata employee was tricked into wiring $4.8 million to an overseas account. Medidata held a $5 million insurance policy with Federal. The policy contained a “Crime Coverage Section” addressing loss caused by various criminal acts, including computer fraud coverage and funds transfer fraud coverage.

Relying on the policy, Federal argued that Medidata’s loss was not covered by the computer fraud clause, because the emails did not require access to Medidata’s computer system, a manipulation of those computers, or input of fraudulent information.

In challenging causation, Federal argued that “there is no direct nexus” between the spoofed emails and the fraudulent wire transfer. Federal also challenged coverage under the funds transfer fraud clause because the bank wire transfer was voluntary and with Medidata’s knowledge and consent.

The court explained that “a thief sent spoofed emails armed with a computer code into the email system that Medidata used.” To achieve the spoof, the thief’s computer code changed data in e-mail addresses. The fraud tricked several high level employees to consent to the wire transfers out of Medidata’s own bank account.

Ultimately, the court found coverage under the computer fraud clause and funds transfer fraud clause.

The Apache and Medidata cases illustrate the lack of agreement regarding what is and what is not covered under cyberrelated policies. Underwriters and courts are still grappling with what is considered a “cyberclaim.” This creates a significant problem for insurance professionals who offer cyberinsurance policies to clients.

**Litigation against insurance professionals**

Though it did not involve a sophisticated cyberevent, the fallout from a data breach experienced by Perpetual Storage, a Colorado Casualty Insurance Company insured, illustrates the exposure insurance professionals may face.

Perpetual Storage stored certain records, including hard copies, microfilm, microfiche and magnetic computer tape on behalf of the University of Utah. Backup tapes containing personal information of 1.7 million patients were stolen from a Perpetual Storage employee’s car.
The university said the theft caused it to incur more than $3 million in costs, consisting of one year of credit monitoring expenses for each impacted patient, printing and mailing costs, phone bank costs and other miscellaneous expenses.

Colorado Casualty filed a declaratory judgment action, contending that Perpetual Storage’s policy did not cover the university’s credit monitoring expenses or notice costs. Perpetual Storage file a third-party claim against its insurance broker alleging, among other things, negligent procurement of insurance, breach of fiduciary duty and failure to advise.³

After three years of litigation, the parties stipulated to a dismissal of all claims, counterclaims, cross-claims and third-party claims.

In 2011, an Illinois corporation engaged in electronic commerce sued its insurance broker alleging reduced revenues for a period of seven months due to a cyberattack that destroyed the corporation’s electronic commerce capability. The agent procured a policy that included “Business Income Extension for Web Sites” coverage for only the first seven days of lost revenue.

The corporation filed claims against the insurance broker for negligence and breach of contract.⁴ After several years of litigation, this case also ended with a dismissal by stipulation.

In a 2016 case, a Louisiana hotel alleged breach of contract, disputing the coverage limit of a cybersecurity policy issued through underwriters at Lloyd’s of London. The hotel also named the insurance agent in the suit.

The hotel alleged that when it sought cyberinsurance coverage, it required a policy that would cover operational fraud and operational reimbursement amounts for fraudulent charges and the cost of replacing payment cards as a result of a cyberattack.

The agent procured a policy with total policy limits of $3 million; however, unbeknownst to the hotel, the policy contained a sub-limit of $200,000 for operational fraud and operational reimbursement amounts.

The retail agent filed a third-party claim against the wholesale broker who claimed to have specialized in cyberpolicies.⁵ The parties quickly resolved the dispute and filed a joint motion to dismiss, which the court granted.

These cases are examples of situations in which a policy to cover cyberexposure was warranted based on the client’s business operations. But what if the insured does not specifically request a cyberinsurance policy?
If every company, large or small, is theoretically at risk of a cyberbreach, then insurance professionals may have an affirmative duty to advise corporate clients about cyberrisks and available coverage.

**Duty to advise**

Generally, an insurance agent or broker who undertakes to procure insurance for another and fails to do so may be held liable for damages resulting from the failure. As a general proposition, insurance agents and brokers do not have a duty to advise insureds as to the coverage needs.⁶

However, a well-developed body of case law has established an exception to this general rule. The exception applies if a “special relationship” exists between the broker and client, thereby triggering an enhanced duty of care to advise the client about the amount of coverage needed to completely meet its insurance needs.⁷

Case examples supporting a finding of a special relationship include situations in which:

The agent misrepresented the nature of the coverage being offered or provided, and the insured justifiably relied on that representation in selecting the policy.⁸

- The agent voluntarily assumed the responsibility of selecting the appropriate insurance policy for the insured (by express agreement or promise to the insured).⁹
- The agent professed expertise in a field of insurance being sought by the insured, and the insured relied on that expertise.¹⁰
- The agent or broker exercised broad discretion to service the insured’s needs and received compensation above the customary premium paid for the expert advice provided.¹¹
- The agent was intimately involved in the insured’s business affairs or regularly gave the insured advice or assistance in maintaining proper coverage.¹²

If an insurance professional has a corporate client and a special relationship exists, then there is arguably a duty to advise the client about the availability of cyberinsurance policies.
What is at stake?

Cyberevents in which thousands of people have their personally identifiable information stolen (including events involving Equifax, Home Depot, Target, Yahoo) garner extensive media coverage. Less attention is paid to attacks carried out using other vectors, like ransomware, which prevents a company from accessing information unless a ransom is paid.

In 2017, the WannaCry and Petya ransomware attacks impacted thousands of computers and blocked user access to data systems unless and until users made ransom payments. And ransomware attacks have already been reported in 2018.

In January, Hancock Regional Hospital was hit with a ransom demand for bitcoin from hackers who encrypted data files associated with the hospital’s most critical information systems.13

After notifying the FBI, its attorneys, cybersecurity specialists and the cybersecurity insurance company, the hospital made the decision to pay the hackers for decryption keys to access the data files and restore its information technology network.

Another troublesome vector is a denial of service attack that disrupts customers’ access to an organization’s system, such as an attack that affected Twitter, Netflix and Sony’s PlayStation Network.14 There is also the social engineering vector in which an employee is tricked into transferring funds or confidential information.

These types of cyberattacks cause business interruptions that could lead to losses amounting to hundreds of thousands of dollars. While larger corporations may survive such an attack, smaller uninsured companies may be forced to shutter.

And companies may pursue litigation against the insurance professional who failed to procure adequate insurance. If found liable, an insurance professional may have to pay the difference between the coverage that should have been in force, but for the error, and the actual net insurance recovery, if any.

Issues to consider

With all of this in mind, insurance professionals should appreciate the demand and need for cyberinsurance policies for every company that relies on computers and the internet — essentially every company. Although cyberinsurance is still relatively new, there are many insurance professionals who have in-depth experience and knowledge in this area.
But beware: The risk of litigation is extremely high if an insurance professional claims expertise in cybersecurity and the client suffers a breach that results in a denied claim.

Likewise, when an insurance professional is intimately involved in the insured's business affairs (for example, handles all the insurance needs for the client or regularly provides advice in maintaining proper coverage), then the agent should advise about cyberrisks, in writing, and engage a broker with far more knowledge.

In addition, when offering a cyberpolicy, insurance professionals should take great pains to review the language of the policy with the client. The client should understand what is, and what is not, covered. Because courts are still grappling with the language in some policies, there are no guarantees. At the very least, the insurance professional and the client should review the policy’s exclusions and definitions.

The definitions of “confidential information” and “personally identifiable information” are the most fundamental in a cyberinsurance policy.

Some policies define confidential information broadly as any information from which an individual may be uniquely and reliably identified or contacted. This may include an individual's name, address, telephone number, social security number, account relationships, account numbers, account balances, account histories or passwords. Under such a definition, an individual’s name, on its own, could be considered PII.

In contrast, other policies may identify very specific items that are considered confidential information that may mirror state-specific definitions of PII. For example, Florida defines personal information as an “individual’s first name or first initial and last name in combination with any one or more of the following data elements for that individual: a Social Security number; a driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity; a financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual’s financial account,” etc.

Beware of the exclusions for contractual liability; criminal conduct; terrorism, hostilities and claims arising from “acts of foreign enemies”; and exclusions for unauthorized collection of customer data. These exclusions could have unintended consequences.

A criminal conduct exclusion would bar any claims that resulted from a social engineering scheme. An exclusion for terrorism could bar cyberbreaches that resulted from foreign actors or governments.
Similarly, an exclusion for unauthorized collection of consumer data could affect any company engaged in online activities, especially activities in which consumer financial data is collected.

Although not a bulletproof defense in litigation, an insurance professional could attempt to limit the scope of services, in writing, to exclude any advice regarding cyberinsurance. From a business perspective, an agent or broker may not want to refer clients to competitors to evaluate cyberrisks.

**Embrace the Future**

Like many industries, insurance will change and evolve as society embraces new internet-reliant technologies. Insurance professionals will have to understand how new technology and the advent of cyberspace will affect their clients. Failing to embrace, evolve and implement strategies to offer insurance products for the cyberage will expose insurance professionals to litigation.

**Endnotes**

* A version of this article originally appeared in Westlaw Journal Insurance Coverage Vol. 28, Issue 20. It has since been revised to reflect appellate decisions.


8. See, e.g., Fitzpatrick at 452.


13. Cyber-attack shuts down US Regional Hospital’s online system, 2018 WLNR 1733059.

14. Widespread Assault Internet attack disrupts service Web-traffic manager Dyn Inc. struck twice, 2016 WLNR 32536680.

15. This commentary is not intended to provide an exhaustive risk analysis for insurance professionals; it is only the tip of the iceberg. The opinions expressed are those of the author and do not necessarily reflect the views of the firm, its clients or any of its or their respective affiliates. This commentary is for general information purposes and is not intended to be and should not be taken as legal advice.
New Insurance Law Books from TIPS

The Handbook on Additional Insureds
Second Edition
Michael Menapace, Timothy A. Diemand, Joseph G. Grasso, and Charles Pietto, Editors
Now completely updated, this handbook addresses all aspects involved when dealing with this complex coverage.

Resolving Insurance Claim Disputes before Trial
Timothy H. Penn and Judith F. Goodman, Editors
Understand how to effectively use ADR mechanisms such as arbitration, mediation, settlement conferences, and appraisal to resolve insurance claim disputes without the cost and delay of trial.

Order online
www.ShopABA.org

Order by email
orders@americanbar.org

americanbar.org/tips
Calendar

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 16-18, 2019</td>
<td>Fidelity &amp; Surety Law Midwinter Conference</td>
<td>Hilton San Diego Bayfront</td>
</tr>
<tr>
<td></td>
<td>Contact: Juel Jones – 312-988-5597</td>
<td>San Diego, CA</td>
</tr>
<tr>
<td>January 17-19, 2019</td>
<td>Midwinter Symposium on Insurance and Employee Benefits</td>
<td>Hyatt Regency</td>
</tr>
<tr>
<td></td>
<td>Contact: Danielle Daly – 312-988-5708</td>
<td>Coral Gables, FL</td>
</tr>
<tr>
<td>January 23-27, 2019</td>
<td>ABA Midyear Meeting</td>
<td>Las Vegas, NV</td>
</tr>
<tr>
<td></td>
<td>Contact: Arthena Little – 312-988-5672</td>
<td></td>
</tr>
<tr>
<td>February 21-23, 2019</td>
<td>Insurance Coverage Litigation Midyear Conference</td>
<td>Arizona Biltmore Resort &amp; Spa</td>
</tr>
<tr>
<td></td>
<td>Contact: Janet Hummons – 312-988-5656</td>
<td>Phoenix, AZ</td>
</tr>
<tr>
<td></td>
<td>Contact: Danielle Daly – 312-988-5708</td>
<td></td>
</tr>
<tr>
<td>March 20-22, 2019</td>
<td>Transportation MegaConference XIV</td>
<td>Sheraton New Orleans</td>
</tr>
<tr>
<td></td>
<td>Contact: Janet Hummons – 312-988-5656</td>
<td>New Orleans, LA</td>
</tr>
<tr>
<td></td>
<td>Contact: Danielle Daly – 312-988-5708</td>
<td></td>
</tr>
<tr>
<td>March 22-23, 2019</td>
<td>Admiralty and Maritime Law National Program</td>
<td>Sheraton New Orleans</td>
</tr>
<tr>
<td></td>
<td>Contact: Juel Jones – 312-988-5597</td>
<td>New Orleans, LA</td>
</tr>
<tr>
<td>April 4-5, 2019</td>
<td>Motor Vehicle Products Liability Conference</td>
<td>Hotel Del Coronado</td>
</tr>
<tr>
<td></td>
<td>Contact: Janet Hummons – 312-988-5656</td>
<td>Coronado, CA</td>
</tr>
<tr>
<td></td>
<td>Contact: Danielle Daly – 312-988-5708</td>
<td></td>
</tr>
<tr>
<td>April 5-6, 2019</td>
<td>Toxic Torts &amp; Environmental Law Conference</td>
<td>Hotel Del Coronado</td>
</tr>
<tr>
<td></td>
<td>Contact: Janet Hummons – 312-988-5656</td>
<td>Coronado, CA</td>
</tr>
<tr>
<td></td>
<td>Contact: Danielle Daly – 312-988-5708</td>
<td></td>
</tr>
<tr>
<td>May 1-5, 2019</td>
<td>TIPS Section Conference</td>
<td>Westin New York Times Square</td>
</tr>
<tr>
<td></td>
<td>Contact: Janet Hummons – 312-988-5656</td>
<td>New York, NY</td>
</tr>
<tr>
<td></td>
<td>Contact: Juel Jones – 312-988-5597</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Speaker Contact: Arthena Little – 312-988-5672</td>
<td></td>
</tr>
<tr>
<td>May 8-10, 2019</td>
<td>Fidelity &amp; Surety Law Spring Conference</td>
<td>JW Marriott Hotel Austin, TX</td>
</tr>
<tr>
<td></td>
<td>Contact: Janet Hummons – 312-988-5656</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contact: Danielle Daly – 312-988-5708</td>
<td></td>
</tr>
</tbody>
</table>

Hypertext citation linking was created with Drafting Assistant from Thomson Reuters, a product that provides all the tools needed to draft and review – right within your word processor. Thomson Reuters Legal is a Premier Section Sponsor of the ABA Tort Trial & Insurance Practice Section, and this software usage is implemented in connection with the Section’s sponsorship and marketing agreements with Thomson Reuters. Neither the ABA nor ABA Sections endorse non-ABA products or services. Check if you have access to Drafting Assistant by contacting your Thomson Reuters representative.