CLM Claims & Litigation Management Alliance™
ADVANCING ETHICS, COOPERATION AND EDUCATION

CLM 2016 Cyber Liability Summit
October 5, 2016 in New York City

Breaking News and Trends for Professional Liability Cyber Claims and Cases

I. Insurance Trends and Available Policies

Professionals are under attack by the hackers. The hackers' preferred mode of attack is the phishing scam, and their tactics are getting highly sophisticated such that the links often are too tempting to avoid. Another trend is the intensification of ransomware attacks in which professionals' systems are encrypted and held hostage, usually for bitcoins payments that pale in comparison to the value of unlocking the data.

Consider the statistics. In 2015, the ABA's annual Legal Technology Survey reported that 25% of law firms with at least 100 attorneys admitted that they experienced data breaches involving intentional intrusions or stolen or lost devices. Of those respondents, 47% further admitted that their firms had no response plan in place to address a data breach. For firms with at least 500 attorneys, 55% had a data breach response plan in place, a disappointing number given their size and risks.

The same statistical trends hold for other professionals. Accounting and financial-services firms, for example are low-hanging fruit. SIFMA's recent "Quantum Dawn 3" cybersecurity testing found substantial areas in which cybersecurity preparations were lacking. After testing the cyber readiness of 650 participants from more than 80 financial institutions and government agencies, SIFMA's after-action report noted multiple "opportunities to improve response protocols and strengthen coordination among the industry participants." Several of these opportunities were in the area of individual firm preparedness, including the needs to enhance executive leadership, develop incident-response plans and teams, and enhance firms' "internal playbooks" to prepare for "various types of attacks or threat vectors."

On January 5, 2016, FINRA published its annual Regulatory and Examination Priorities Letter, which identified central areas of focus for the coming year. Significantly, the Letter discussed cybersecurity as one of the critical "broad issues" in connection with supervision, risk management, and controls. As stated in the Letter, "FINRA remains focused on firms' cybersecurity preparedness given the persistence of threats and our observations on the continued need for firms to improve their cybersecurity defenses."

FINRA specifically noted the continued vulnerabilities and gaps in firms' cybersecurity preparedness. As stated in the Letter: "While many firms have improved their cybersecurity defenses, others have not – or their enhancements have been inadequate."

Also consider the headlines. In March 2016, it was widely reported that several prominent law firms, including Cravath Swaine & Moore LLP and Weil Gotshal & Manges LLP, had been hacked by cybercriminals seeking to obtain confidential and/or insider information for publicly traded companies. Also in March 2016, cybersecurity firm Flashpoint issued advisory alerts to 48 prominent law firms, including Sidley Austin LLP, Kirkland & Ellis LLP and Jenner & Block LLP, informing them that they had been targeted by a Russian cybercriminal looking to hire hackers to gain access to their computer systems so that he could profit from insider trading.

These statistics and headlines illustrate the reality that professional-service firms – whether law, accounting or consulting firms – are a gold mine for hackers who seek to use, sell or ransom highly sensitive client information. Recent data breaches highlight the potential and catastrophic consequences for professional-service firms that fail to take reasonable measures to protect their clients' highly sensitive information.

These data breaches also highlight the need for such professional-service firms to consider cyber insurance policies as an important purchase to address their firms' data-security risks. The cyber market is growing exponentially. The domestic industry has seen an increase to 60 carriers that offer stand-alone cyber policies. In 2015, these carriers generated approximately $2.75 billion in annual gross written premiums, and this number is expected to increase to $10 billion by 2020.

It is critical for professionals to explore and secure cyber coverage rather than rely on their standard PL or E&O policies. As always, however, the devil is in the details, and cyber policies vary widely in their coverage of first-party and third-party costs and damages. Accordingly, professionals must closely examine the policy terms, sub-limits, exceptions, and exclusions before determining which policies best fit their risk profiles.

II. Claims Trends and Coverage Issues

Several trends stand out in the nature and magnitude of cyber claims. First, insureds are facing enhanced exposure to the intensified regulatory activity in the cyber arena. This is particularly true in connection with regulatory investigations and fines in the healthcare industry through the Office of Civil Rights (OCR), which finds its authority in numerous statutes including HIPPA and its privacy, security, and breach-notification rules.

In September 2015, the DHS Inspector General critiqued OCR for not doing enough in the area of cyber enforcement, encouraging it to "strengthen its follow-up of breaches," and "strengthen its oversight of compliance." OCR is obliging, and the result has been increased pre-breach and post-breach costs and exposure. Moreover, consider the disconnect between actual harm and settlements, as evidenced by the recent $850,000 settlement by Lahey Hospital for 599 stolen records.

The FTC also has increased and intensified its cyber activity. Claiming authority under at least 33 different laws, rules, and guides (including of course the 100-year-old FTC Act barring "unfair" and "deceptive" practices), the FTC has been securing numerous consent decrees from companies that suffered a breach or presumably did not satisfy alleged representations regarding clients' or customers' data. Now that the FTC is further emboldened by its victory in the seminal *Wyndham* case, and its subsequent settlement with a 20-year consent decree, expect more actions, lawsuits, claims, and expensive settlements that include draconian audits and penalties.

Another trend, referenced above, is ransomware, which may be covered by extortion and/or business-interruption policies. Given the increasingly virulent variants of ransomware, the damages and harm have expanded exponentially. More data is at risk, and ransom has been increasing, sometimes to many thousands of dollars in bitcoins.

Also occurring now, and likely increasing in the foreseeable future, are insider threats, often by privileged users. Professionals are uniquely subject to these threats given the sad reality of weaker controls and the difficulty of detention. As a result, professionals must be cognizant of the need for strong preventive measures, including digital vaults for sensitive data, real-time monitoring and detection, strong passwords, restrictive use and access controls, expeditious disabling of credentials and access, and solid policies and training.

As for coverage, cyber risks may or may not be covered by PL, GL, and E&O policies that neither expressly include nor exclude coverage of data-security risks. Coverage issues turn on the language of these policies, which vary widely between carriers.

There has been a rise of cyber claims by professionals under non-cyber policies, and the resolution of these claims almost always occurs long before anyone approaches a courtroom. Nevertheless, one recent case suggests that these non-cyber policies are candidates for cyber claims, depending again on the policies' language. In *Travelers Indem. Co. of. Am. v. Portal Healthcare Solutions, L.L.C.*, 2016 U.S. App. LEXIS 6554 (4th Cir. Va. Apr. 11, 2016), a Virginia appellate court determined that an insurance carrier had a duty under the insureds' GL policy to defend against a class-action suit in connection with a data breach. Other courts have gone the other way. Accordingly, it would be wise for professionals to strongly consider a cyber-specific policy to protect their firm and their firm's clients' sensitive information against data breaches.

III. Lawsuit Trends and Practical Tips for Defending Them

A. Trends

Lawsuits against professionals are on the rise. There are no definitive or dependable statistics, but the headlines are telling. In May 2016, Edelson P.C. announced that, after a year-long investigation, it had identified 15 major law firms that had failed to take adequate preventive measures to protect clients' sensitive data, and that it had filed a class-action lawsuit under seal against a Chicago-based regional law firm. Edelson also announced that it planned to file class-action lawsuits against several additional law firms, and would seek injunctive relief and damages based on an "overpayment theory" that the firms' clients purportedly had overpaid for legal services because a portion of the legal fees were devoted to keeping the client's sensitive data secure. The overpayment theory has met with mixed results in several jurisdictions when tested in other lawsuits involving services and products.

In April 2016, a New York couple sued their real-estate attorney for legal malpractice and breaches of fiduciary duty when the attorney's AOL email account was hacked, which caused the couple to wire $1.9 million to hackers. The suit alleged that the hackers not only read all of the attorney's emails, but also impersonated the attorney to convince the couple to wire the funds.

These types of lawsuits likely will multiply given the trend of relaxed standing in various courts and jurisdictions. Many prior decisions dismissed cases on standing grounds, holding that plaintiffs did not suffer sufficiently tangible injuries, and often relying on the U.S. Supreme Court's opinion in the *Clapper* case (which dealt with surveillance, not data breaches).

However, courts increasingly are denying motions to dismiss, and permitting these cases to proceed to discovery, despite the absence of specific identifiable harm to individual or class plaintiffs. Many examples abound, including high-profile cases filed against Target, Sony, Adobe, and Neiman Marcus. These courts found that plaintiffs suffered sufficient harm through, for example, the increased risk of their personal information being sold on the black market.

The new frontier of standing is the area of statutory penalties. Plaintiffs have filed many cases in which they have suffered no cognizable harm, yet they seek penalties provided in data-security or privacy statutes. The U.S. Supreme Court, in the recent *Spokeo* decision, held that plaintiffs must allege "concrete" and "particularized" harm, yet the muddled decision also held that plaintiffs' harm need not be "tangible." Lower courts now are wrestling with how those standards apply in various cases based in whole or part on statutory penalties rather than actual harm.

B. Practical Tips

Promptly upon discovering a potential data breach or incident, a critical first step is to initiate an investigation. The central objectives are to determine the nature and scope of the intrusion or loss, and to take tangible measures to stop or at least mitigate the resulting harm. The incident-response plan is the roadmap for meeting these objectives. Once these objectives are satisfied, additional investigatory measures will be necessary in order to develop and implement strengthened data protections, communicate with regulators and other interested constituencies, and prepare for potential litigation in administrative tribunals and courts.

Firms need to protect their communications as much as possible during these investigations. It is in everyone's interests to communicate openly and often critically, and the incentives to do so are magnified exponentially if those communications are protected from disclosure to regulators and the outside world.

Outside counsel should be retained as "breach coaches" in order to protect associated communications, to the extent desirable and legally possible, under the attorney-client privilege and work-product doctrine. Courts generally recognize the privileged and protected nature of these communications when requested and/or directed by outside counsel for purposes of assessing legal risks and counseling on legal issues. By contrast, courts exhibit increased skepticism when adjudicating privilege assertions over communications that did not involve counsel, or that involved only in-house counsel (whose communications are more easily characterized as undertaken for business purposes rather than legal advice).

These principles also hold true for pre-breach risk-reduction programs. Outside counsel should be involved as "pre-breach coaches" to develop and implement measures aimed at reducing risks and damages from prospective breaches or incidents. Communications should occur at the direction or request of outside counsel, for purposes of assisting counsel to assess and address legal risks. Outside counsel should be central to the chain of written communications – hard-copy and electronic (including of course emails) – to ensure that those communications are appropriately labeled and managed to preempt prospective arguments that potentially applicable privileges or protections were waived.

IV. Conclusion

Firms cannot totally eliminate the risk of a data breach or incident, whether caused by a malicious hack or simply human error. However, firms can – and, given intensified regulatory oversight, must – identify and address their cybersecurity risks through the implementation of tangible measures that have become an invariable part of the industry landscape.