CLM CLAIMS & LITIGATION MANAGEMENT ALLIANCE™

ADVANCING ETHICS, COOPERATION AND EDUCATION

CLM 2015 Cyber Liability Summit
October 21, 2015 in New York City

Death by Twitter: Impact and Appropriate Governance of Social Media to Prevent Data Breach or Liability Claim Doomsday

I. Social Media as a Portal for Cyber Attack

The Number of Social Media Users and Social Media Attacks are Growing Exponentially

Industry Composition and Cyber Event Type

Recent data tracking cyber related loss patterns with special emphasis on social media exposure confirms that industry groups handling large volumes of data are the most likely to experience a breach related loss. Another key factor is the level of Personally Identifiable Information (PII) detail collected. The "service industries" include the following data rich business segments: restaurants, hospitality, healthcare and hospitals. These service industry groups comprise 47% of the "cyber events;" that is, those which are reported to a governmental entity. A "cyber event" such as that sustained by Home Depot would be considered a single "cyber event."

Second to the service industry is the 18% of losses arising in Finance, Insurance and Real Estate and related business segments. One of the significant developments resulting from the frequency and severity of the loss in this segment is the emergence of risk transfer by those companies with a large number of suppliers. This issue is now referred to as vendor required cyber coverage. This is the development of certificate driven insurance and this development brings a host of claim concerns e.g. additional insured and other insured coverages issues.

Cyber Event Type and Source of Data Loss

The general data which confirms an increase in losses arising through Social Media is reflected in the denial of service data and privacy violations. It is also significant that the frequency of "privacy violations" has increased significantly; causing markets to exclude TCA related claims. Where such exclusions are desired, it is crucial that the terms and conditions be clear on this point.

The Number of Social Media Users and Social Media Attacks are Growing Exponentially

Over the past few years, there has been a radical categorical increase in social media cyber events. The number of events has risen by more than twenty-five per year in the past 3 years. With the increased use of social media, those increases are likely to continue. The most frequent area of loss (53%) arises from business interruption e.g. denial of service caused by business failure. The second and even more expensive loss type arises from data breach (29%) in reported social media related cyber events. The industry groups with the highest loss experience are again those in the service industry, in particular healthcare. Many healthcare providers, and to a lesser degree, financial service providers, utilize social media as an important tool for interacting with clients.

Case studies where social media was the source of the breach

On January 1, 2014, The Syrian Electronic Army (SEA) appears to have compromised Skype's Twitter account. Skype was acquired by Microsoft in 2011. There was evidence to suggest the attackers were able to gain access to Skype's Facebook and WordPress blogs as well, likely indicating either shared passwords or perhaps compromise of Skype employees' email accounts. The nature of the attack seems to indicate either that the same password was shared between the three social media accounts or that a Skype employee's e-mail account was compromised. More importantly, it indicates that Microsoft isn't using two-factor authentication on its social media accounts.

Case Involving social media companies

On February 18, 2013, hackers breached the Twitter account of fast-food chain Burger King, posting the online equivalent of graffiti. Burger King Worldwide Inc. suspended its Twitter account about an hour after it learned of the attack. Several tweets carried the logo of Burger King's larger rival McDonald's, but spelled the latter company's name incorrectly. Others sought to tarnish Burger King, the third-largest U.S. hamburger chain, and its employees.

II. Liability Claim Exposure

While social media has become a prevalent means of renewing or maintaining personal contacts, as well as a 21st century tool for conducting business, one concern which should be of primary consideration is that, like it or not, social media is, for the most part, exchanged via public forum. Personal opinion, comment, bias and often private information are published for all to see. Consequently, recent years have seen an explosion of liability claims arising out of the use of social media.

Issues Surrounding Ownership and Responsibility for Use of Social Media

Employees who spend time creating and maintaining social media sites often develop a sense of "ownership" of such efforts and end up at odds with their employers over rights to the site and content upon termination of employment. While work performed within the course and scope of employment is generally found to belong to the employer, it often doesn't stop zealous employees from attempting to keep what is "theirs." Clear guidance and direction with specifically defined goals along with frequent oversight of employee efforts can help minimize these types of conflict.

On the flip side of that issue, just as ownership of these social media sites lies with the company whose employees create them, responsibility for their use and content also belongs to the owner. Maintaining control over administrative access, tracking employee use and postings and carefully monitoring content of sites such as company blogs and websites is critical. At the same time however, in monitoring employee use, companies must be conscious and respectful of labor laws which protect employees' right to organize.

There are a Variety of Claims Which May Arise Through the Use / Misuse of Social Media

Social media is the future of marketing. At a low cost, it provides electronic exposure to potentially millions of people and future clients. With that widespread presentation also comes exposure to many different causes of action where the social media is either intentionally misused or negligently ignored. Types of claims which frequently arise include defamation and breach of contract and also include claims for deceptive trade practice, fraud and violation of the right to privacy.

Defamation: While defamation may be a cause of action as old as time, with the advent of social media, it is brought into the 21st century. Generally defamation claims require that (1) a false statement be made to others about plaintiff; (2) which caused damage to plaintiff's reputation; and (3) which results in damages. Most critically, the calculation of those damages is typically based upon the extent of the false statement's "circulation."

Defamatory statements presented via social media can go "viral" in an instant. Even false statements or other defamatory comment or material, intended for a limited audience, can reach hundreds or thousands in a very short period of time. This not only expands the statement's "circulation" but complicates reparation / mitigation efforts.

Breach of Contract: New wrinkles on old contractual claims are becoming more frequent in the social media age. The facility to create (and breach) binding contracts with ease has triggered a rise in breach of contract claims. One recent example arose in the context of a post employment non-solicitation agreement. A former employee, who had signed an agreement that he would not solicit former clients, encouraged his LinkedIn contacts to "check out" the new website he had designed for his new employer. Because his contacts included customers of his former employer who had not been "unlinked" from his LinkedIn account, the former employer brought a breach of contract claim against the former employee.[1]

Another former employee was deemed to be in breach of contract by violating the terms of a confidential settlement agreement through the use of social media. The former employee was found to be in breach when his daughter posted on Facebook "Mama and Papa Snay won the case against Gulliver. Gulliver is now officially paying for my vacation to Europe this summer. SUCK IT."[2] The Third District Court of Appeal in Florida held that the father, through his

[1] *BTS, USA, Inc. v. Executive Perspectives, LLC and Marshall Bergmann*, Docket No. x10 CV 116010685, 2014 Conn. Super. LEXIS 2644 (October 16, 2014).

[2] *Gulliver Schools v. Snay*, 137 So.3d 1045 (Fla.App. 3 Dist. 2014).

daughter, had, in breach of the agreement, advertised to the "Gulliver community" that he had been successful in his discrimination lawsuit against the school.

Other Claims: While these are all causes of action which certainly pre-dated the internet, bringing them in the context of social media adds many more wrinkles. These new concerns may also include claims such as deceptive trade practice where representations or promises set forth on social media are not met or violation of privacy rights where protected information is revealed without consent. These claims have caught companies off guard and unprepared for the huge increase in litigation.

III. What Preventative Measures Can be Taken

With the rapid growth of social media, the number of users and exposure to attack and litigation claims, planning for the unforeseen is key. The future is uncertain. The attacks are more frequent and the means unanticipated. Courts around the United States are continually deciding social media cases, in many instances without governing precedent. Inoculation against the dangers is critical.

Companies Must Develop an Internal Social Media Use Policy

Setting the expectations early and clearly defining the rules for accessing and using social media provides a system of checks and balances which is critical in an ever changing environment. Without those clearly defined guidelines, companies are at risk.

In the *BTS* case noted above, the court ultimately rejected the former employer's claims. Among the critical findings, the court noted that the employer had no policies or procedures regarding the employee's use of social media, nor did it request or require ex-employees to delete the former employer's clients and customers from the employee's LinkedIn accounts. In fact, the court found, "to this day [the employer] allows employees to maintain LinkedIn accounts without monitoring or restriction from the employer." Consequently, the court found for the employee on the breach of contract claim.

Effective social media policies need to address several concerns. First, the policy should require administrative approval prior to postings to a company's blog or Facebook page. That approval should be specific and involve a person or persons who have been previously delineated as company representatives on social media. This furthers the goal of a central focus and consistency.

Second, the policy should provide specific guidelines for employees to be followed whether on a company social media site or their own private site. Additionally, while posing potential dangers, employees can also be among the very best of a company's advocates. Clear guidelines given to employees about their own personal use of social media can also protect a company's image and prevent the potential for a damaging remark.

And finally, companies must conduct training so that the employees may become familiar with the content of the policy, as well as more complex industry regulations they may have to abide by. It also reiterates for the employees the importance of the policy and compliance therewith.

Carefully Monitor and Maintain Administrative Control of Social Media

Social media is often the sole face known to clients and potential clients. In essence, a company's social media site is its image. It is thus critically important. Reality proves that social media is accessed at the workplace by employers and employees alike. Critical to this discussion is what risks exist through employee access to the company social media. Allowing unfettered access provide tremendous risk that individuals (including disgruntled employees) may damage a company's image, may divulge private information, or subject the company to exposure for one or more claims as a consequence of illegal or inappropriate acts. Even an employee's casual "best wishes to Mary Fisher as she undergoes open-heart surgery," via a company's social media site may expose the company to a claim arising out of the violation of HIPPA laws. Careful administration and monitoring social media can limit such risk.

Additionally, maintaining small administrative control over social media can facilitate prompt action in the event of a triumph or in the midst of a problem. It is the quickest medium for delivering your thoughts on the latest technology and news that affect your industry or quickly responding to a customer service issue that may arise. Regardless of the content, messages must always be consistent with the identity of the company. Even discounting the risk of harm by a disgruntled employee for example, multiple person access to a company's social media content can be misleading and create confusion among customers.