IADC COMMITTEE NEWSLETTER

CORPORATE COUNSEL

January 2018 – Second Edition

IN THIS ISSUE

This is the second newsletter article for the IADC Corporate Counsel Committee on the subject of cyber security and the internet. This article explores the increasing threat that corporate counsel, their clients, and key outside counsel are facing from internet based crime and social media, relating to business activities which originate from internet services or sources. Key data as well as Corporate Counsel responsibilities are highlighted in this article.

Cyber Security: The Dark Side of the Internet

ABOUT THE AUTHOR

Joseph F. Speelman is currently serving as General Counsel for a private, Swiss based energy information group. He has directed successful defense efforts against Public Nuisance lead paint litigation in 15 states, gaining defense verdicts in those states including achieving a defense verdict before the state of Rhode Island Supreme Court that reversed a lower court trial verdict and rendered a defense verdict by the high court. He can be reached at jfspeelman49@gmail.com.

ABOUT THE COMMITTEE

The Corporate Counsel Committee is composed of in-house counsel and others who, although in private practice, serve as general counsel for corporate clients. The Committee provides its members with educational programs and networking opportunities to address common concerns of corporate counsel. It also works to ensure that the IADC and its committees, through their work and offerings, meet the needs of corporate counsel. Learn more about the Committee at www.iadclaw.org. To contribute a newsletter article contact:

Joseph F. Speelman
Vice Chair of Publications
Petro-Logistics S.A.
jfspeelman49@gmail.com

The internet is a vast, unlit wasteland where predators, terrorists, uber criminals, thieves, con-artists, pedophiles, sexual predators, character assassins-for-hire, and foreign government agents lurk undetected, unchecked, and ungoverned. A recent report by a government crime data publication cited internet crime as "by far" the largest type of theft and it is growing faster than any other type of criminal activity. [1] A former high ranking FBI official opined that internet based theft is the "perfect crime" because the risk of being caught is approaching "zero" and the ability to become involved and commit a criminal act, such as theft, is easier than any other type of crime.[2]

In April, 2012 Bradley Cohen, a wealthy Los Angeles real-estate investor received a "Google alert" on his mobile phone. It contained a headline to an internet based article entitled "Is Bradley Cohen the Next Bernie Madoff?". The article contained a series of false statements suggesting Cohen had criminal convictions for fraud and money laundering and that his industrial real estate firm, Cohen Asset Management, Inc. was a ponzi scheme. That Google alert started a four year saga for Mr. Cohen, his family, and his company that led through the dark, back alleys of the internet. Cohen and his investigators encountered websites offering fetish sex and all sorts of angry, horrifying, and unbelievable rants, assertions, and personal attacks of many types and against many things, people, companies, and countries. This "adventure" led from England to Seychelles to Seattle, and to Los Vegas. It involved FBI agents, and more than two dozen attorneys and investigators costing millions of dollars. In the end, Mr. Cohen and his family were guarded day and night by armed guards to protect them as he fought to clear his reputation and that of his company. Fortunately, Mr. Cohen's story had an ending and a good one, thus far. However, he was only able to achieve those results because of his wealth. A full account of Mr. Cohen's four plus year nightmare is setout in excellent and compelling detail in the weekend edition of the Wall Street Journal, dated February 25-26, 2017. [3]

What the Cohen saga, and other similar stories, bring to light is something that law enforcement officials, government security agencies, and a few, select investigators, writers, and attorneys have known for some time. The internet is littered with demeaning, defamatory, and "just plain nasty statements" , articles, position papers, character assassinations, direct attacks on companies, countries, leaders, and individuals, the content of which is unsupported at best but most likely completely, blatantly false. Virtually none of these predatory concepts or things have their authors or creators identified or listed.[4]

---

[1] Steve Morgan, Forbes Magazine, January, 2016, "Cybercrime Costs Reach $2 Trillion by 2019".

[2] Cyber Risks – E-Privacy , IADC International Corporate Counsel College, 14-15 November, 2013, Paris, France. Remarks of retired FBI senior official Edward Gibson, Alvarez & Marsal.

[3] "One Man's Bid To Clear His Name Online", John R. Emshwiller, The Wall Street Journal, Weekend edition, Saturday/Sunday, February 25-26, 2017, Section A.

[4] Wall Street Journal, February 25-26, Supra, at note 3 above.

One of the most disturbing aspects of the above "horror story" is that this "dark side" of the internet has become deeply and increasingly involved in all aspects of business operations and experience throughout the world. One need only consult the headlines of major news media worldwide to find references, endorsements, and use as sources many pieces of information or mis-information by main stream information groups, government investigations, and, functions from these dark side "non-sources". A complete and completely falsely created espionage "dossier" on a political figure and leader surfaced recently. After much "ado" from various groups, the source of the dossier was finally identified as to who created it, where it was created, and that the information asserted in it as "verified and true" was, in fact, false and unverified. The source of funds that sponsored the document, as yet, has not been disclosed. [5]

Stories about companies or businesses surface constantly throughout the world. Where those stories or "news items" come from quite often is rather difficult to trace or identify. Counsel for such companies, both corporate counsel and outside counsel, must be in a position to manage an inquiry or search to identify sources of such articles and verify or establish the correctness of such pieces. It is becoming a required skill set for such counsel. In addition, very well prepared counsel, both corporate and outside, will be skilled in anticipating such occurrences and helping their clients avoid or perhaps eliminate them. It is a fact that the internet, because of its very nature, has, as described above, become a place where influence is "brought to bear" upon an issue, a company, a country, a point of view. A number of entities advertise their ability to utilize or create internet influence programs or strategies for businesses or individuals. [6] Setting aside for the moment whether such influence is proper, or legal, it is also a known fact that, while some types of such activity may be legal, even ethical; in the dark side of the internet, where there appears to be no principles, this influence becomes, or can become, something terribly wrong, unprincipled, defamatory, destructive, or worse. Understanding this and being capable of dealing with this very point, is an essential element of being effective, forward thinking corporate and outside counsel. [7] Recently, the Huffpost (Huffington Post) shut down a contributor blogging network because it was facing "a tsunami of false information" coming from the internet and, also, a $23.5 million lawsuit for libel and negligent injury relating to a since-deleted article published by the Huffpost. [8]

Internet based Crime Costs

The costs associated with cyber crime are increasing. In 2014, CNN reported that 47%

[5] "Steele Dossier Farce Shows Why Trump Relies On Twitter", The Hill, Paul R. Gregory, 10/27/17.
[6] "the balance"; https www.thebalance.com/understanding the role of social media in marketing; "Working Knowledge – Business Research for Business Leaders", Harvard Business School; https hbswk.hbs.edu/item/strategy-and-the-internet. 16 April 2001.
[7] Supra, Note 3, Wall Street Journal, February 25-26, 2017.
[8] "Huffpost Shut Down a Contributor Blogging Network As It Faces a 'Tsunami of False Information' ", FoxNews, Brian Flood, 18 January 2017.

of all American adults had already been hacked. Yahoo acknowledged at the end of 2016 that over 1.5 billion user accounts were compromised in a series of attacks spanning from 2013 to 2016. Yahoo dropped its sale price to Verizon by $250 million and delayed the acquisition until the 2nd quarter of 2017 as a result of these events. Internet service group PrivateTunnel reported that $81.6 billion was spent on information security (infosec) products and services in 2016 alone. The investments that corporations, businesses, governments, and other organizations will spend between 2017 and 2021 for information security will be over $1 trillion globally according to PrivateTunnel. [9] Bank of America has responded to the above issue by implementing the extraordinary policy of an "unlimited cyber security budget". [10]

Swiss megabank, Credit Suisse, in a recent advice to investors entitled "The Dark Side of Digitalization", provided the following, stark assessment : "There is a latent threat that the internet could collapse due to the weight of cyberattacks. If we do not do something soon, we are at risk of lasting economic damage." In advising that prevention is better than cure, Credit Suisse anticipates further development of managed detection and response (MDR) security technologies such as security information and event management (SIEM) as well as secure web gateways (SWGs). These integrated systems will, ultimately, become integral components of service packages from all responsible service companies to all of their business, government, and individual clients.[11]

Well run companies, at the behest of owners, governments, and key employees will be reaching decisions to look aggressively into these developing defensive technological improvements. The role of corporate counsel, and key, in house advisors on all matters cyber, must be at the forefront of those evaluations and must understand those technologies. Cyber security is the ultimate "risk" in risk management processes for companies, large or small, governments, and organizations. As has been said previously in IADC programs and literature, corporate counsel must be key leaders in any organization's risk evaluation process. This subject can only be defined as an "existential risk" to any company, government, or organization.

Key Facts and Statistics Regarding Cyber Security

There are more than plenty of "facts" and "statistics" being put out by internet security companies looking for business. I have sorted through those for you and there are some very important true facts that need to be kept in mind by all business, government, organizations, and individuals regarding this developing area. In no particular order, please take careful note of the following:

[9] "Costs of Cyber Crime : How Much Does It Really Impact You?" PrivateTunnel; https://www.privatetunnel.com/cost-of-cybercrime/

[10] Supra, Note 9, page 2 of 9.

[11] "The Dark Side of Digitalization", Credit Suisse, Investor Advisory; https://www.credit-suisse.com/corporate/en/articles/news-and-expertise/the-dark-side-of-digitalization-201702.html

- There is a hacker attack every 39 seconds affecting one in three Americans each year.
- 95 percent of breached records came from three sectors in 2016: Government, Retail businesses, and Technology firms.
- 43 percent of cyber attacks target small business. 64% of companies have experienced web-based attacks. 62% experienced phishing & social engineering attacks. 59% of companies experienced malicious code and botnets and 51% experienced denial of service attacks.
- The average cost of a data breach will exceed $150 million by 2020 as more business infrastructure is connected.
- Since 2013 there are 3,809,448 records stolen from data breaches every day, 158,727 per hour, 2,645 per minute, and 44 every second of every day.
- Over 75% of the health care industry has been infected by malware over last year.
- Large-scale denial of service attacks are up 140% as of 2016's fourth quarter.
- Cybersecurity Ventures reportedly estimate that the global cybersecurity sector will grow at a combined average rate of 9.8% to around $170.2 Billion by 2020. Approximately $1 Trillion is expected to be spent globally on cybersecurity from 2017 to 2021.
- More than 209,000 cybersecurity jobs in the US are unfilled, and postings are up 74% over the past five years. Unfilled cybersecurity jobs will reach 1.5 million by 2019.
- The risk is serious regarding IoT (Internet of Things) and it is growing according to recent data from a Symantec Internet Security Threat Report. There are 25 connected devices per 100 inhabitants in the US and it will rise to 50 to 200 million connected devices by 2020.
- Only 38% of global organizations, private and governmental, claim they are prepared to handle a sophisticated cyber attack.
- In 2017, Ginni Rometty, IBM's Chairman, President, and CEO stated: "Cyber crime is the greatest threat to every company in the world."[12]

I have included a few very key and well written items in the Further Resources section at the end of the article. It is critical that corporate counsel and their outside colleagues immerse themselves in the technical and operational vernacular of the cyber era. My experience is, the younger one is, the easier this becomes or, often, is already a skill set the counsel possess.

The Role of Counsel in Cyber Issues

It can be rather confusing for corporate counsel and outside counsel but it is not necessary to become a technical expert, but merely understand what is being discussed

[12] "The Scary Truth About Cyber Security", Cybersecurity . Cybint News ; https://www.cybintsolutions.com/cyber-security-facts-stats/

and its significance to the business operations of their client. For counsel to small companies the challenge can be greater as the other key members of risk assessments and decisions will most likely be either owners or senior officers of the company. In one sense that is good, it makes things move quicker and decisions come faster, but it is also important that key people are fully aware of relating decisions to legal risks. For all counsel, it is important to ensure that, despite being closely involved in risk assessments, they must ensure they remain in the role of providing proper legal advice. This can be a bit "tricky" depending upon the issue, the personalities involved, and the level of risk and cost involved.

Proper and forward looking advise from senior corporate counsel and their colleagues in key outside firms should focus on efforts regarding this essential business strategy area in finding the comprehensive, systemic avoidance technologies imbedded in new and existing electronic systems. They are being created as you read this article. The cyber era is a very critical time for all commercial entities and processes. It will be that way for a number of years, perhaps life times. Here are some things to keep in mind as you advise your clients in these matters:

- Most companies, governments, or institutions do not have up to date data processes relating to their electronic systems.
- Small companies may not have IT or in house personnel that deal with the company's electronic setup and, thus do not have much input for improvements or upgrades.
- The risk evaluation for all organizations will be critical and you must be involved in that process.
- Most companies have experienced a cyber event of some type.
- Costs of options will be important in all situations, and with small businesses it is very critical.
- Appropriate and effective business insurance should be integrated into any upgrade plan for businesses, especially small business.
- Corporate Counsel should manage the process of risk evaluation and work closely with the senior management group that considers the evaluation and begins to make decisions about needs and addressing those needs.
- Corporate counsel must understand and perhaps participate in the business planning, particularly for small businesses. Understanding the direction and future plans of your client is essential to looking past those plans to the inevitable risks that may develop. The longer range the knowledge of a business plan, the better in evaluating cyber risks. The more time there is to plan for cyber risks, the better and less expensive the costs will be to your client.
- Corporate counsel need to be proactive with their clients regarding potential issues, even though not legal issues (yet) that the company may be experiencing. As shown by the events discussed in this article, maintaining a very long view of public or civic events, incidents, or simply day to day relations with communities, neighbors, customers,

or even competitors can create an awareness of a potential internet event. The best problem is one that does not occur. Businesses used to wait until they were sued to begin thinking about or working on a problem. That is not good enough today. Avoid the problems, be mindful of the internet activity regarding your client. Work with public relations, IT, human relations, and business managers. They will like the help and appreciate the advice.

- Most publicly traded companies have a web based site, in their name, that is maintained by the SEC. Look at that site daily. I can assure you, someone will hit the site with something at some point. Get ahead of that issue.

I usually end these articles with a simple request to "be careful". After reading and re-reading this article several times, I am going to change my admonition……Be Very Careful Out There!

Additional Reading Material

1. ATTBusiness.com /products & services/cyber security report
2. The Evolving Role of Leadership in Cyber Security, Paul Gillin, ATTBusiness.com
3. Cyber Security Insurance – Its Complicated, Paul Gillin, ATTBusiness.com
4. Wired.com, 7/01/2017, The Biggest Cyber Security disasters of 2017 So Far – Lily Hay Newman
5. Threatpost.com, 01/19/2018, Oneplus Confirms Credit Card Breach Impacted Up To 40,000 Customers.
6. Technewsworld.com
7. CNBC.com/cyber security.
8. Darkreading.com/attacks – breaches – cyber security
9. Cybersecurity.cybint news, www.cybintsolutions.com
10. What Is The Deep Dark Web?, Cyber Intelligence.Cybersecurity/www.cybintsolutions.com. (good, basic description of the three parts of the web.)

Litigation Related Strategies

1. etszone, john@etszone.com, John Stautner; Litigation Influence Strategies.

Want To Scare Yourself

1. Digital Dark Side: Cyber Warefare, Ozgur Ozturk, U02113904, Boston University, Metropolitan College. Thesis Paper.

Cyber Law

1. Cybersecurity Law by Jeff Kosseff ; John Wiley & Sons [2017] ISBN 9781119232025 - 2017
2. Cybersecurity and Cyberwar : What Everyone Needs To Know / Peter W. Singer , Allan Friedman ISBN 978-0-19-991811-9 , Oxford University Press 2014

Past Committee Newsletters

Visit the Committee's newsletter archive online at www.iadclaw.org to read other articles published by the Committee. Prior articles include:

JANUARY 2018
Corporate Counsel Perspectives on Cybersecurity Insurance Procurement
Joseph F. Speelman

OCTOBER 2017
A Tidal Wave of Public Nuisance Law Suits across the US Involving Opioid Litigation
James K. Holder and Joseph F. Speelman

SEPTEMBER2017
What Next Rough Beast….The Second Coming of Nuisance Law Litigation
Joseph F. Speelman

DECEMBER 2016
Please Call Again: The Supreme Court Declines to Rein in TCPA Litigation
W. Jason Rankin and Charles N. Insler

NOVEMBER 2016
No Harm, but Still a Foul? Application of the Supreme Court's Punitive Damages Jurisprudence to Actions Seeking Statutory Damages
Jeffrey A. Holmstrand

OCTOBER 2016
Drone Law and Drone Regulation: A Primer
Lem Montgomery

APRIL 2016
Proportionality and Reasonableness: Using the 2015 FRCP Amendments to Rein in Discovery
Martin J. Healy and Joseph D. Fanning