IADC COMMITTEE NEWSLETTER

TECHNOLOGY

December 2015

IN THIS ISSUE

The technology explosion has undeniably added layers of complexity and created new and ever evolving economic risk for business. Understanding cyber threats and implementing cyber security controls that suit a company's overall objectives is critical to surviving a cyber attack. This article covers cutting edge trends in cyber threats and provides practical advice to minimize cyber risk through operational best practices.

Cyber Armageddon: Survival or Annihilation?

ABOUT THE AUTHORS

Theodore M. Schaer of Zarwin, Baum, Devito, Kaplan, Schaer, Toddy, P.C., is the Chairman of Zarwin, Baum, DeVito, Kaplan, Schaer & Toddy's Casualty Defense Department and is the Chairman of the firm's Cyber Liability, Privacy and Data Breach Response team. Ted has been certified by the International Association of Privacy Professionals. The CIPP/US certification is the preeminent privacy credential in the US private sector. Ted also serves as Chief Information Security Officer for his law firm. Ted counsels companies and their insureds on cyber liability and responding to a data breach. Ted is a columnist for the Huffington Post and regularly blogs on cyber liability issues. He has been interviewed by national media on cyber security issues. He can be reached at tmschaer@zarwin.com.

Elizabeth S. Fitch of Righi Fitch Law Group, is a founding and managing member of the Righi Fitch Law Group. She is a trial lawyer with 30 years of civil defense experience and has the AV Preeminent rating. Beth is the past President of Arizona Association of Defense Counsel and is the Co-chair of the Arizona State Bar Cyber Liability Committee. Her practice has concentrated on representing businesses and individuals in complex civil litigation matters. She has developed expertise in risk management and assists clients with risk transfer strategies. Beth is board certified in Privacy and US Data Protection (CIPP/US) and serves as the Dean of the CLM Cyber Claims College. She advises clients on privacy and cyber related issues and leads her firm's data breach response team. She can be reached at beth@righilaw.com.

ABOUT THE COMMITTEE

The Technology Committee keeps the IADC membership current on the use of technology in litigation, whether in the conduct of discovery or in the use of technology in the courtroom. It educates its members on the impact of technology in their practices – on the ways they communicate with each other, with courts and clients, on the systems they use to record and produce their work, and on technological developments in marketing for law firms. The committee provides information to its members on legal developments in the law governing the use and development of technology, in particular on Internet and computer law and related subjects. Through its members, it acts as a resource to the IADC staff and leadership on technology issues facing the organization. Learn more about the Committee at www.iadclaw.org. To contribute a newsletter article, contact:

John Christian Nemeth
Vice Chair of Publications
McDermott Will & Emery
jcnemeth@mwe.com

Fifteen million T-mobile customers are on pins and needles. Why? Because the fallout from Experien's announcement on October 4 that it experienced a data breach impacting T-mobile customers won't be known for months, even years. With the prospect of 15 million cell phone user's personal data compromised, this will surely be a wakeup call to individuals. But it is the untold stories that reveal the cyber threats for businesses. For every Target, Sony, and Anthem, companies everywhere are victims. Recent surveys have produced eye-popping data. [1]The 2015 McAfee Security Paradox Report reveals that 63% of midsize U.S. companies (51 to 1000 employees) have experienced a data breach this year. Why? The answer is simple: lack of proper security makes them easy targets for hackers. According to the 2015 NetDiligence Study the average payout was $1.2 million with the average legal costs of $434,000 and crisis services cost of $539,000.[2] What is the take away from these studies? ***All*** businesses are targets. When it comes to a cyber breach, it's not a question of "if"; rather, it's a question of "when".

What is the greatest cyber threat to my business?

When thinking of cyber exposures, what often comes to mind are system failures or hackers penetrating a company's electronic data. The human element of cyber risk is often overlooked. According to the Poneman Institute, the main causes of cyber breaches are: 37% malicious attacks, 29% system glitches and 35% human factor. Employee errors can lead to costly cyber incidents. Lack of employee awareness is one of the biggest risk factors. While the loss of portable devices such as laptops have resulted in breaches, social engineering is a powerful means to steal data: 85% of office workers have been duped by social engineering.

Hackers pray upon humans' trusting nature. Social engineering schemes are based on spoofed emails to lead users to visit infected websites designed to appear legitimate. Secretly installed spyware then trick users into divulging sensitive personal information such as credit card numbers, passwords, and social security numbers.

Interactions with customers and vendors expose businesses to cyber attacks. Many cyber breaches like the Target breach are due to third party vendor actions or vulnerabilities. Failure to properly vet vendors and to clarify in contracts which party is responsible for responding to and paying for cyber breaches can be a costly mistake.

[1] *NetDiligence Cyber Claims Study* (2014), available online at www.netdiligence.com/NetDiligence_2014CyberClaimsStudy.pdf.

Why is the cost of a breach so high?

Regulatory compliance is a significant cost factor. Federal and state governments have enacted privacy laws to protect personal information. Currently 47 states have enacted breach notification laws.[1] While all 47 states mandate notification to individuals whose personal information may be compromised, key differences do exist. Fifteen states require notification to governmental agencies[2] and 27 states require notification to national credit reporting agencies. [3] National breach notification legislation has been introduced in the United States Senate which will lessen post breach expenses by streamlining state regulatory requirements into a uniform national standard[4]. In addition to these expenses, damage to the business reputation can be crippling. A report by PWC indicated that 10% of businesses that suffered a breach were so damaged that they needed to change the nature of their businesses completely.

Is my business ready?

Protecting an organization's data is becoming ever more difficult. A company can best protect itself by conducting a cyber risk assessment and then adopting cyber security controls that suit the company's overall objectives and culture. The executive management team should work closely with cyber experts to identify the risk, threats, and vulnerabilities. The more economical approach may be to retain lawyers and/or an outside cyber consultant to perform an audit. Once the assessment is complete, the executive team should implement information security policies that meet long term goals and properly train employees to combat social engineering scams.

Despite these controls and employee training companies remain at risk for cyber breach and should have in place an Early Response Team ("ERT"). Swift action is required for timely compliance with regulatory breach notification requirements. This team should include the company's executive management, public relations, legal, and forensic cyber experts. While large companies may employ the necessary forensic and legal experts, smaller companies can be equally prepared with the selection of outside service providers.

Dedicating financial and human resources to protect sensitive and confidential information should be a priority for every

[1] *Security Breach Notification Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES, available online at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited Mar. 25, 2015).

[2] Idaho, Illinois, California, Louisiana, Puerto Rico, Hawaii, Missouri, South Carolina, Virginia, Maryland, New Jersey, New York, Maine, Massachusetts, New Hampshire, North Carolina. *Id.*

[3] Minnesota, Alaska, Colorado, the District of Columbia, Florida, Hawaii, Indiana, Kansas, Maine, Maryland, Michigan, Missouri, Nevada, New Jersey, Ohio, Oregon, Pennsylvania, South Carolina, Tennessee, Vermont, Virginia, West Virginia, Wisconsin, New York, Georgia, Texas, Montana. *Id.* at 121-22.

[4] S177 Data Security and Breach Notification Act of 2015

company. Preparation is the key to surviving a cyber breach that is certain to befall every company.

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:

JULY 2015
Fitbit Data Brings Another Dimension to Evidence
John G. Browning

DECEMBER 2014
The Ethics of Technology in E-Discovery – An Introduction
Peter J. Pizzi and Julia L. Brickell

SEPTEMBER 2013
Emerging Technology and Its Impact on Automotive Litigation
John G. Browning

JUNE 2012
iPad Apps: Brave New Frontier
Adam Bloomberg and J. Calhoun Watson

AUGUST 2011
TrialDirector: Electronic Trial Presentation – A Primer, Best Practice Tips
Thomas G. Oakes

MAY 2010
Know When to Hold 'Em: The Effective Use of Litigation Holds
Mike Taylor

JULY 2009
New Insights for Jury Profiling and Online Socialization
Merrie Jo Pitera and Stephanie S. Cox

APRIL 2008
Irish Supreme Court "Creates" E-Discovery: The Disappearing Line between Digital Data and Paper Documents
Robert C. Manlowe, Gregory D. Shelton, and Manish Borde

FEBRUARY 2008
Qualcomm v. Broadcom: Lessons for Counsel and a Road Map to e-Discovery Preparedness
Gregory D. Shelton

JANUARY 2008
Simonetta v. Viad Corp: A Disturbing Expansion of the Duty to Warn in Products Liability Cases
Gregory D. Shelton

MAY 2007
Are You Competent?: Providing Representation in the Digital Age
Gregory D. Shelton