Cybersecurity: New Trends And Emerging Standards In The Courts And Economic Marketplace

Judy Burnthorn
Deutsch Kerrigan & Stiles (New Orleans, LA)

jburnthorn@dkslaw.com | 504.593.0688
http://www.dkslaw.com/attorney/burnthorn

TINKERBELL

Paris Hilton & Tinkerbell

- August 2014 cyber attacks on JP Morgan and other banks*
- Checking and savings account information taken
- Possibly by Russian hackers in retaliation for sanctions

* Bloomberg.com iSight Partners

Other Cyber Breaches

* Coke
* The Love Bug
* Anonymous
* Comment
* U.S. Climate

Medical

- Health Insurance Portability and Accountability Act of 1996
- HIPAA

STATE LEGISLATION

- **47 States**
- **California**
- **New Jersey**
- **New York**

FEDERAL LEGISLATION

- Financial Institutions - Gramm-Leach-Bliley Act and 16 CFR § 314.1 et seq.
- Rules under Fair Credit Reporting Act detect and prevent identity theft
- The FTC Act 15 U.S.C. § 41, et seq.
- Computer Fraud And Abuse Act ("CFAA") 18 U.S.C. § 1030(g).

- **Federal National Institute of Standards and Technology**

SEC OCIE SAMPLE LIST OF INFORMATION REQUESTS, Pg 1

- "Identification of Risks/Cybersecurity Governance"
- "Protection of Firm Networks and Information"
- "Risks Associated with Remote Customer Access and Funds Transfer Requests"

SEC OCIE SAMPLE LIST OF INFORMATION REQUESTS, Pg 2

- "Risks Associated With Vendors and Other Third Parties"
- "Detection of Unauthorized Activity"

- SEC April 15, 2014 Sample List of Information Requests for Office of Compliance Inspections and Examinations (OCIE)

ENFORCEMENT ACTIONS, Pg 1

- Inadequate written policies and procedures.
- Failure to conduct cybersecurity assessments.
- Failure to respond to cybersecurity breaches.
- Protection of firm networks and customer information.

ENFORCEMENT ACTIONS, Pg 2

- Encryption
- Anti-Virus Software
- Firewalls
- User Access Restrictions
- Risks involving vendors and outsourcing relationships

See Southerland.com, News Commentary, Legal Alerts

FINRA Examination Priority Letter

- Cybersecurity
- "…Our primary focus is the integrity of firm's policies, procedures and controls to protect sensitive customer data. FINRA's evaluation of such controls may take the form of examinations and targeted investigations.
- FINRA January 2, 2014 Examination Priority Letter at p. 4

CAUSES OF ACTION

- Starbucks
- Zappos
- Linked In
- Eli Lilly
- Target
- Bell
- Daly v. MetLife

STANDING

- *Clapper v. Amnesty International*, 133 S.Ct. 1138 (2013)

COVERAGES AND EXCLUSIONS UNDER STANDARD POLICIES

- "Occurrence" and Triggers
- CGL Policy Concepts
- *Ingram Micro, Inc.*
- *Ward General Ins. Services*
- *Midwest Computers & More*

NEW CYBERSECURITY INSURANCE PRODUCTS

- First Part Or Third Party
- Intentional Or Negligent
- Sublimits
- Sample Policies
- IT Claims
- Regulatory Claims
- BI claims

Goodbye

CYBERSECURITY – New Trends And Emerging Standards In The Courts And the Economic Marketplace

INTRODUCTION

As technological dependency increases in our digital world, the ever-expanding realm of cyberspace provides a breeding ground for a new type of criminal, eager to exploit freely-flowing information. Cyberattacks routinely target and vandalize individuals and businesses, and can even threaten critical economic infrastructure and national security. Kirsten M. Koepsel, Chapter 1: Electronic Security Risks and the Need for Privacy, in Data Security and Privacy Law §§ 1:1–4 (2014). In fact, the global cost of cybercrime totaled approximately $114 billion in 2011 alone. *Id*. § 1:1. The huge price-tag of cybercrime makes it clear that our daily lives, economic vitality, and national security depend on a safe and secure cyberspace. Cybersecurity Overview, U.S. DEP'T OF HOMELAND SECURITY, http://www.dhs.gov/cybersecurity-overview (last visited July 10, 2014).

EXAMPLES OF CYBERBREACHES

Identity Theft

Identity theft is a form of cyberbreach, and in the United States, identity theft occurs once every seven seconds. 112 Am. Jur. Trials 1, § 1 (2009). By 2007, roughly one-in-thirty Americans had fallen victim to identity theft. Id (citing Cullen, The Wall Street Journal Complete Identity Theft Guidebook: How to Protect Yourself from the Most Pervasive Crime in America 59 (Three River Press, 2007)). A more recent study reveals that in 2012 alone approximately one-in-fourteen Americans age sixteen or older, or about 16.6 million persons, were victims of identity theft. Erika Harrell and Lynn Langton, Victims of Identity Theft, 2012, U.S. DEP'T OF JUSTICE, BUREAU OF JUSTICE STATISTICS 1 (Dec.12, 2013) http://www.bjs.gov/content/pub/pdf/vit12.pdf. Of those incidents, approximately eighty-five percent involved fraudulent use of existing account information such as credit card or banking information. *Id.*

Tinkerbell[1]

In 2005, Paris Hilton was one of the first to own a Smart Phone - a Sidekick II. Paris Hilton's carrier was T-Mobile. T-Mobile had a security site that permitted users to find out a customer's name and phone number. Once on this site, the user could reset their password. The password could only be reset after a security question was answered in order to confirm the user's identity. However, one of the security questions was "what is the name of your favorite pet." Paris Hilton's Chihuahua Tinker Bell was quite famous. Tinker Bell accompanied Paris almost everywhere. A hacker was able to go on to the T-Mobile website and change Paris Hilton's password by entering, in response to the security question, the name of Paris Hilton's dog – "Tinkerbell."

T-Mobile had additional security measures beyond the security question. Once the password was reset, an email would be forwarded to the user to make sure that the user was in possession of the phone. Information from the email was needed in order to access the account. However, the hacker who, in this instance, was only 17 years old, was aware that such a confirming email would be sent by T-Mobile. The hacker telephoned Paris Hilton to indicate that T-Mobile was having technical difficulties and suspected that some users may have received emails resetting their passwords. When Paris Hilton indicated that she had received such an email regarding a changed password, the hacker asked for the contents of the email. Once Paris Hilton had disclosed the contents of the email to the hacker, the hacker was able to access Paris Hilton's account.

Contacts of many including Christina Aquilera, Lindsey Lohan, and Vin Diesel were accessed. Additionally, inappropriate photos on Paris Hilton's phone were also accessed.

The Comment Breach

If, when you return from your vacation, you receive an email from your boss or your assistant asking "Welcome back, did you have a good vacation?" would you open it? If you do, you may be downloading harmful malware. This type of email is one type of ploy utilized by the hacker group Comment.

The Comment Group, received its name from its tendency to go on websites or blogs, make comments, and then implant a fake link into the comment that invades the web surfer's computer.

The Comment Group is reportedly based in China and supposedly does "hacking for hire."

In one episode, the Comment Group attacked representatives of the United States who were attending an international summit on climate change in Copenhagen. The Comment Group sent to the United States representatives an email which had a

1 See http://www.pedantictosts.com/intro-to-hacking-real-hacker-stories-are-even-better-than-the-movies.

subject line "China and climate change." The email had the appearance of being generated by a real international economic journalist. Once the United States representatives opened the email, the Comment Group was able to surveil their computer activity.[2]

In another incident, the Comment Group hacked Coca-Cola. It was reported that Coke was looking into a takeover of the largest soft drink company in China – Huiyuan Juice Group. An officer of Coca-Cola's Pacific Group opened an email that looked like it was from Coke's CEO. When the officer clicked this email, malware was downloaded onto his computer that permitted Comment to monitor Coke's emails and negotiations on the takeover. Eventually the Chinese government refused to approve the takeover.[3]

Waterholing – Comment is also known for waterholing. Comment researches and investigates its targets' likes, dislikes, activities, and routine. Comment will try to implant Malware on a website that the target is likely to visit. Once the target visits the website, the Malware is downloaded.[4]

The Love Bug Breach

The I Love You / Love Bug Virus – This virus spread quickly among users of Microsoft Outlook and corporate networks that use the Microsoft Exchange e-mail server because it sent a copy of itself to every e-mail address in a recipient's Outlook address book. Once launched, it downloaded an executable backdoor program from one of four Web sites. That program, Win-Bugsfix, stole passwords stored on computers and sent them to an e-mail address in the Philippines" some companies needed to shut off their e-mail systems to contain the virus, which caused disruption.

THE REGULATORY FRAMEWORK

State Legistation

Forty-six states have enacted legislation requiring notification in the event of a cybersecurity breach. See State Security Breach Notification Laws National Conference of State Legislatures (August 20, 2012).

California

California enacted legislation requiring notice to consumers whose information is compromised. Companies are required to disclose breaches of computer data if they reasonably believe personal information has been acquired by an unauthorized person.

2 See http://www.bbc.com/news/business-21371608.

3 See http://www.bbc.com/news/business-21371608.

4 See http://www.bbc.com/news/business-21371608.

New Jersey

Computer related theft N.J.S.A. 2 C: 20-25 (person who accesses information).

New York

McKinney's Penal Law § 156.10 (person who accesses a computer, computer service or computer network without authorization).

National Institute of Standards and Technology Framework

President Obama issued an executive order on February 12, 2014 calling on the National Institute of Standards and Technology to develop a framework of standards and best practices for cybersecurity controls. The framework may become a standard of care for industry at large. It should at minimum be a guide.

The framework will likely be cited in lawsuits. Plaintiff lawyers will likely assert that the federal framework establishes a standard of care.

Others believe that the federal cybersecurity framework will not be adopted as a standard of care in litigation. 2/25/14 Inside CyberSecurity 2014 WLNR 5287133

Some contend that the framework is so broad that it is unlikely to be very useful in litigation. It is possible that the NIST standard may be referred to by regulators as they adopt more specific security standards, which could in turn become standards of care. 2/25/14 Inside CyberSecurity 2014 WLNR 5287133

FEDERAL LEGISLATION

Medical

Health Insurance Portability and Accountability Act of 1996

Health Insurance Affordability and Accountability Act. 42 U.S.C. § 1320d-2.

Medical Breaches

In one hospital, "malware at one point slowed down fetal monitors used on women with high-risk pregnancies being treated in intensive-care wards." David Talbot, Computer Viruses are "Rampant" on Medical Devices in Hospitals, MIT Technology Review (Oct. 17, 2012), http:// www.technologyreview.com/news/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals.

In 2008, researchers gained remote access

to a defibrillator. The researchers conducted a "reprogramming attack," which "changes the operation of (and the information contained in) the defibrillator." The researchers then altered when the device administered electric shocks, gaining the ability to administer a shock on command. The researchers demonstrated that attacks against the device were possible: "[A]n attacker can keep a [defibrillator] in a state of elevated energy consumption" by making the battery-operated defibrillator communicate indefinitely with an outside device. Because attacks deplete battery life, this type of attack could prevent a defibrillator from functioning when a patient needs it. David Talbot, Computer Viruses are "Rampant" on Medical Devices in Hospitals, MIT Technology Review (Oct. 17, 2012), http:// www.technologyreview.com/news/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals.

In 2010, another set of researchers demonstrated that they could gain unauthorized remote access to an insulin pump from 100 feet away. The researchers "(1) chang[ed] already-issued wireless pump commands; (2) generat[[ed] unauthorized wireless pump commands; (3) remotely chang[ed] the software or setting on the device; and (4) den[ied] communication with the pump device." The researchers were able to instruct the insulin pump to flood the body with insulin, potentially killing a person. The researchers also found that a hacker could interrupt the communication between the insulin pump and the patient's insulin control unit, preventing the patient from adding insulin to the bloodstream when needed. The researchers noted similar security flaws with wireless blood glucose monitors. Many insulin pump systems also use a mobile phone to help patients monitor their glucose levels. A hacker who breached the security of the mobile phone may be able to use the phone to change the insulin pump's settings. See Nathanael Paul et al., A Review of the Security of Insulin Pump Infusion Systems, 5 J. of Diabetes Sci. & Tech. 1557 (2011), available at http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3262727.

Financial Institutions

Gramm-Leach-Biley Act and Regulation, 16 CFR § 314.1 et seq. (This Act regulates the ,handling of personal information by financial institutions. Financial institutions have "an affirmative and continuing obligation to respect the privacy of … customers and to protect the security and confidentiality of those customers' non-public personal information.")

16 C.F.R. § 314.1

§ 314.1 Purpose and scope.

(a) Purpose. This part, which implements sections 501 and 505(b)(2) of the Gramm–Leach–Bliley Act, sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

(b) Scope. This part applies to the handling of customer information by all financial institutions over which the Federal Trade Commission ("FTC" or "Commission") has jurisdiction. This part refers to such entities as "you." This part applies to all customer information in your possession, regardless of whether such information pertains to individuals with whom you have a customer relationship, or pertains to the customers of other financial institutions that have provided such information to you.

16 C.F.R. § 314.2

§ 314.2 Definitions.

(a) In general. Except as modified by this part or unless the context otherwise requires, the terms used in this part have the same meaning as set forth in the Commission's rule governing the Privacy of Consumer Financial Information, 16 CFR part 313.

(b) Customer information means any record containing nonpublic personal information as defined in 16 CFR 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.

(c) Information security program means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

(d) Service provider means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to this part.

16 C.F.R. § 314.3

§ 314.3 Standards for safeguarding customer information.

(a) Information security program. You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in § 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

(b) Objectives. The objectives of section 501(b) of the Act, and of this part, are to:

(1) Insure the security and confidentiality of customer information;

(2) Protect against any anticipated threats or hazards to the security or integrity of such information; and

(3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

16 C.F.R. § 314.4
§ 314.4 Elements.
In order to develop, implement, and maintain your information security program, you shall:

(a) Designate an employee or employees to coordinate your information security program.

(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

(1) Employee training and management;

(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

(d) Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Requiring your service providers by contract to implement and maintain such safeguards.

(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

16 C.F.R. § 314.5
§ 314.5 Effective date.

(a) Each financial institution subject to the Commission's jurisdiction must implement an information security program pursuant to this part no later than May 23, 2003.

(b) Two-year grandfathering of service contracts. Until May 24, 2004, a contract you have entered into with a nonaffiliated third party to perform services for you or functions on your behalf satisfies the provisions of § 314.4(d), even if the contract does not include a requirement that the service provider maintain appropriate safeguards, as long as you entered into the contract not later than June 24, 2002.

European Union Data Protection Directive – companies who possess personal information must protect it. Counsel Directive 95/46/EC, art 17(1) (1995).

The FTC Act 15 U.S.C. § 41, et seq.
Federal Trade Commission Cases
The Federal Trade Commission has acted against companies which do not properly secure information, contending that failure to properly secure information is an unfair trade practice. See eg *Sunbelt Lending Services, Inc.,* No. C-4129 (FDC 2995). *Federal Trade Commission v. Wyndham* was one of the first times that the FTC sued a major company in federal court for failure to secure customer information. (D.Ariz.2012)(No.2:12-cv-01365-SPL), The FTC's suit alleged that Wyndham and its subsidiaries had flawed security practices (including failure to erect firewalls, use appropriate passwords, or configure software to keep credit card information secure). Most of the Commission's information security cases have been based on the prohibition on "unfair or deceptive acts or practices" in § 5 of the FTC Act. The Commission's first cases were based on deception—a company had promised to keep sensitive information secure and failed to honor that promise. The FTC's complaints construe a promise to protect sensitive information as one to take steps that are "reasonable and appropriate under the circumstances." Reasonableness depends on the sensitivity of the information. Thus, the cases require balancing, with more sensitive information requiring more elaborate security precautions. The Commission has stated that not all breaches are actionable. The Commission looks to determine whether the company was employing reasonable and appropriate security measures.

Accidental breaches may constitute a violation. In one case, the defendant accidentally revealed the email addresses of all subscribers to its daily reminder service for Prozac users. The complaint alleged that the company had "not taken steps appropriate under the circumstances" to keep its promise to protect sensitive information.

The FTC has also pursued enforcement when the company has not guaranteed privacy, alleging that the failure to maintain reasonable security policies and practices is unfair. See BJ's Wholesale Club. BJ's Wholesale Club was an unfairness case. BJ's sent credit card information over its computer network without encryption. The network also included wireless access points that supported wireless devices. These access points did not include "readily available security measures to limit access." Unauthorized wireless users could access BJ's computer network, where credit card information was stored. The FTC alleged that there were inadequate measures to detect and investigate unauthorized access, and that BJ's unnecessarily increased the risk by retaining information for which it no longer had a business need.

Computer Fraud And Abuse Act
The Computer Fraud and Abuse Act ("CFAA") is a criminal statute relating to cyber attacks. It has a civil enforcement provision. 18 U.S.C. § 1030(g).

Federal Statutes That Limit Electronic Surveillance
Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C § 1809(a).

Electronic Communications Privacy Act
Scattered sections of 18 U.S.C.

CYBER BREACH CAUSES OF ACTION
Starbucks
On April 28, 2009, a Starbucks employee filed suit against the company on behalf of a class alleging "failure to adequately safeguard its employees' sensitive, personal information, including social security numbers." The lawsuit involved the theft of one laptop that contained information on approximately 97,000 employees. The complaint contended that it is now industry standard to encrypt such data and that the company's "failure to maintain reasonable and adequate security procedures to protect against the theft of . . . [personally identifiable information] has put Plaintiff and the proposed Class Members at an increased and imminent risk of becoming victims of identity theft crimes, fraud, and abuse." The complaint alleged that Starbucks had a common law duty to protect its employees' personal information and by not conforming to industry standards, it breached that duty *Krottner v. Starbucks Corp.,* 09-CV-0216RAJ, 2009 WL 7382290, *1 (W.D. Wash. 2009), aff'd, 628 F.3d 1139 (9th Cir. 2010), and, 406 Fed.Appx. 129 (9th Cir. 2010).

The employees sought damages for emotional distress and credit monitoring costs, alleging Starbucks breached an implied contract to protect their personal information and acted negligently in failing to better secure their information. *Id*. Although the plaintiffs' injuries were sufficient to confer standing, their claims were nevertheless dismissed before the class could be certified. *Id.* The Ninth Circuit upheld the lower court's decision and found the plaintiffs' damages (based on a risk of future identity theft) were not cognizable in

negligence. The court further noted plaintiffs failed to plead the existence of an implied contract obligating Starbucks to safeguard their personal information. *Krottner,* 406 Fed.Appx. at 131.

Zappos

In 2012, a customer filed a class-action suit against Zappos.com based on a breach that may have exposed credit card numbers of 24 million customers The suit alleged that Zappos owed a duty to keep customer information "in a safe and secure condition" away from the threat of unknown third persons. It survived a motion to compel arbitration, filed by Zappos, along with co-defendant Amazon based on an arbitration clause in the Zappos Terms of Use. The court stated that the Terms of Use was a "highly inconspicuous link buried in a sea of links," the court found that the Terms of Use failed to provide notice. As a result, the judge refused to compel arbitration. *In re Zappos.com, Inc. Customer Data Security Breach Litigation,* 3:12-CV-00325-RCJ-VCP (D. Nev. 2013) (MDL No. 2357), 2012 WL 10998240.

As a general matter, plaintiffs' anxiety, emotional distress, loss of privacy, credit monitoring costs, and time and effort spent mitigating the risk of future identity theft were injuries sufficient to confer standing. *Id*. However, the customers' breach of contract claims were dismissed, because Zappos' unilateral statements indicating that its servers were protected and that customer data was safe did not create any contractual obligation to provide data security. *Id*. at *3. Although the court found Zappos' misrepresentations provided the basis for plaintiffs' negligence claims, those claims were barred by the economic loss doctrine and were also dismissed. *Id.* at *3–4. Finally, because Alabama and Massachusetts' unfair trade practices statutes do not provide private causes of action, those claims were dismissed accordingly, and only some of the customers' state law claims survived. *Id.*

LinkedIn

In 2012, a user of LinkedIn filed a class-action complaint against that company following a data leak of approximately 6.5 million customers' information, including e-mail addresses, passwords, and log-in credentials. Like the Starbucks complaint, this complaint also alleged that a company possessing personal data failed to comply with industry protection standards. The complaint included several causes of action, one being negligence or gross negligence. It reads: "By agreeing to accept Plaintiff and the other Class and SubClass members' sensitive [personally identifiable information], Defendant assumed a duty, which required it to exercise reasonable care to secure and safeguard that information and to utilize industry standard protocols and technology to do so." The court found that plaintiff met standing requirements. Further, the court DENIED LinkedIn's motion to dismiss fraud claims under California's Unfair Competition Law. In Re LinkedIn User Privacy Litigation 12:03088 (N.D. Calif. March 28, 2014).

Eli Lilly

The Eli Lilli example shows that accidental breaches may potentially constitute a violation. Lilly accidentally revealed the email addresses of all subscribers to its daily reminder service for Prozac users. The complaint alleged that the company had "not taken steps appropriate under the circumstances" to keep its promise to protect sensitive information.

Target

Recent litigation regarding a December 2013 security breach of Target's consumer information database involves more than fifty class actions in over twenty-four courts across the country; these actions were filed less than three weeks after Target announced the breach. See Defendant Target Corporation's Motion to Stay Proceedings Pending Transfer Decision by Judicial Panel on Multidistrict Litigation, *Rothschild v. Target Corporation,* 1:13-CV-00178-EJF (D. Utah Jan. 10, 2014), 2014 WL 292128. In these actions, plaintiffs assert virtually identical claims, including breach of contract, negligent misrepresentation and concealment, invasion of privacy, violation of the Federal Stored Communications Act, state law consumer protection statutes, state law data breach statutes, and related equitable claims for relief. Id. Currently, these actions are awaiting transfer into multidistrict litigation. Id.

Bell v. Michigan Counsel 25 of American Federation of State County Municipal Employees AFLCIO Local 1023,

In *Bell v. Michigan Counsel 25 of American Federation of State County Municipal Employees AFLCIO Local 1023*, 2005 WL 356306 *5 (Mich. Ct. App. 2/15/05) a union had a duty to protect its members' personal information. The Court stated that the "defendant did owe plaintiffs a duty to protect them from identity theft providing some safeguards to ensure the security of their most essential confidential identifying information. . . .".

Catsours v. Department of California Highway Patrol, 104 Cal. Rptr. 3d 353, 376 (Cal. Ct. App. 2010).

In *Catsours v. Department of California Highway Patrol,* California State Police had a duty to an accident victim's family not to post pictures of victim online for "lurid titillation." Catsours v. Department of California Highway Patrol, 104 Cal. Rptr. 3d 353, 376 (Cal. Ct. App. 2010).

Daly v. Metropolitan Life Ins. Co.

In *Daly v. Metropolitan Life Ins. Co.,* the court found that there exists a fiduciary duty on the part of an insurer to protect confidential personal information of its customers which duty may be breached by unauthorized dissemination of the private information. 4 Misc.3d 887, 782 N.Y.S.2d 530, 2004 N.Y. Slip Op. 24280 (2004)

Oregon Hay Prod., Inc. v. Cmty. Bank

In a case that may be a preview of future litigation, an Oregon company sued its bank to recover approximately $250,000 that hackers stole from its accounts. The company alleged that the bank violated the requirements for commercially reasonable security procedures set forth in Uniform Commercial Code Section 4A. Brian Krebbs, Hay Maker Seeks Cyber Heist Bale Out, KREBS ON SECURITY, April 13, 2013, http://krebsonsecurity.com/2013/04/hay-maker-seeks-cyberheist-bale-out/;see Complaint at 1, Oregon Hay Prod., Inc. v. Cmty. Bank (Or. Cir. Ct.) (No. CVH120083).

STANDING

Standing may be a defense to a cybersecurity breach if the particular plaintiff's information was neither accessed nor appropriated. *Clapper v. Amnesty International,* 133 S.Ct. 1138 (2013) The plaintiffs in *Clapper* sought a ruling that the Foreign Intelligence Services Act, which includes certain surveillance provisions, are unconstitutional. The Supreme Court found that the plaintiffs had no standing to challenge the constitutionality of the Act.

CYBERSECURITY INSURANCE

Cyberinsurance has a number of important benefits. Cyber-insurance increases cybersecurity by encouraging the adoption of best practices. It is likely that a certain degree of security will be required to obtain cyber-insurance. Persons adopting better security practices may receive lower insurance rates. The security prerequisites used by cyber-insurers may become standards. Since insurers will be required to pay out cyber-losses, they have a strong interest in greater security, and their requirements will likely increase. See WHITE HOUSE, CYBER-INSURANCE METRICS AND IMPACT ON CYBER-SECURITY 1-2 Walter S. Baer & Andrew Parkinson, Cyberinsurance in IT Security Management, IEEE SECURITY & PRIVACY 50 (2007).

The Relationship Between Traditional Insurance Policies and Cyberdamage

Occurrence Policies

An occurrence policy is triggered depending on when the "event" which "causes" covered damage occurs. This may give rise to complicated coverage issues for cyberdamage. For instance, if a network failed, was the "occurrence" when the network was negligently constructed, when the network malfunctioned, or at a different time in the interim? Does an "occurrence" transpire when a programmer improperly prepares a program or later when the computer program fails?

A "claims made" policy may provide more certainty for cyber risks. The problem in determining when cyber damage takes place, with respect to an occurrence policy, may not exist with respect to a "claims made" policy.

Four theories have been utilized to determine when occurrence policies are triggered in latent injury matters:

- "Injury-in-fact" trigger: policies are triggered that were in effect at the time the injury took place

- the "exposure" trigger: policies are triggered that were in effect when a claimant was exposed to harmful conditions

- the "manifestation" trigger: policies are triggered that were in effect when the injury is discovered or becomes noticeable

- the "continuous" trigger: all policies are triggered that were in effect during all of the aforementioned periods.

Coverage Trigger Theories

A coverage trigger consists of "the event or condition which determines whether a policy responds to a specific claim." Cole v. Celotex Corp., 599 So. 2d 1058, 1075 n.50 (La. 1992). In general, four coverage trigger theories exist: (1) exposure; (2) manifestation; (3) continuous trigger; and (4) injury-in-fact. Trs. of

Tufts Univ. v. Commercial Union Ins. Co., 616 N.E.2d 68, 75 n.9 (Mass. 1993); 23 E.M. Holmes, Appleman on Insurance § 145.3[13][1] (2d ed. 2003). Under the exposure theory, mere exposure to the harmful conditions during the policy period triggers coverage. Cole, 599 So. 2d at 1076 n.51; see also Trs. of Tufts Univ., 616 N.E.2d at 75 n.9 (pursuant to the exposure theory, the insurance policies in effect during the years that the claimant's property was exposed to hazardous material are triggered). "Under the manifestation theory, coverage is triggered only when an injury manifests itself during the policy period." Cole, 599 So. 2d at 1076 n.52; Rubenstein v. Royal Ins. Co. of Am., 694 N.E.2d 381, 387 (Mass. App. Ct. 1998), affd, 429 Mass. 355 (1999). The continuous trigger theory combines the exposure and manifestation theories, and provides that "all policies in effect during the entire injurious process will be triggered and are required to respond." Cole, 599 So. 2d at 1076 n.53; see also Trs. of Tufts Univ., 616 N.E.2d at 75 n.9 (under the continuous trigger theory, "property damage occurs during each year from the time of first hazardous exposure through manifestation"). Finally, under the injury-in-fact theory, an insurance policy is triggered when evidence of actual injury exists during the policy period. 23 E.M. Holmes, Appleman on Insurance § 145.3[13][2] at 15 (2d ed. 2003); see also Trs. of Tufts Univ., 616 N.E.2d at 75 n.9 ("the injury-in-fact (or actual injury) trigger requires inquiry into when property damage actually occurred").

Insurers will almost certainly argue that an occurrence based liability policy is not triggered until "bodily injury" or "property damage" actually takes place. Courts hearing these cases could rule that the bulk of these claims do not occur until the date a network actually fails, the day data is actually corrupted, the date a virus actually strikes or the date a denial of service actually shuts down a network. Simply put (or so the argument will go) those are the moments when a failure takes place and quantifiable damages finally exist.

The CGL Policy – Physical Injury, Property Damage, Tangible Property, Etc.

"Property damage" is defined in many CGL policies as follows:

> a. Physical injury to tangible property including all resulting loss of use of that property. All such loss of use shall be deemed to occur at the time of the physical injury that caused it; or
>
> b. Loss of use of tangible property that is not physically injured. All such loss of use shall be deemed to occur at the time of the occurrence that caused it.

If a sprinkler system fails because of a computer failure and an office building burns-down, an insured will be able to argue that tangible property is physically damaged or if an occupant is burned that there is bodily injury.

The damage or injury is not so evident when an inferior computer product, bad data, or a computer virus are at issue. If an insured sells a malfunctioning computer product or transmits a virus, it is less clear whether there is physical injury to or loss of use of "tangible" property. Computer data may be unavailable, in some instances for a short time.

Is corrupted data property damage or physical loss under a First Party Commercial Property Policy policy?

The *Ingram* Decision

When a computer network failed to work in *American Guarantee & Liability Ins. Co. v. Ingram Micro, Inc., American Guarantee & Liability Ins. Co. v. Ingram Micro, Inc.,* 2000 WL 726789 (D. Ariz. 2000,[5] the damage constituted "physical" damage under a first party insurance policy.[1]

The *Ward General Ins. Services, Inc.* Decision

Another court came to a different conclusion than the *Ingram Micro* court. A California State Appellate Court found that a loss of computer information was not covered by a First Party Commercial Property Policy: (1) because the loss of data was not a "direct physical loss," as required by the policy language and (2) because the language of the insurance policy, not "public policy," controlled the relationship between the parties.

In *Ward*, the Insured suffered loss of data and consequential damage such as labor expenses to restore the data, loss of business income, loss of productivity, loss of commissions and loss of profits, because the data was unusable. The *Ward* court held the loss was not covered under a First Party Commercial Property Policy. *Ward General Ins. Services, Inc. v. Employers Fire Ins. Co.,* 114 Cal. App. 4th 548, 556-57, 7 Cal. Rptr. 3d 844, 851 (4th Dist. 2003).

The insured in *Ward* was an insurance services company. It was updating an Oracle database when

5 The 9th Circuit Court of Appeals declined to accept an interlocutory appeal on the insurance coverage issue. It was considering an appeal regarding a request to stay the trial. That appeal became moot, however, when the case was settled in late June 2001. The district court case was dismissed with prejudice on July 5, 2001.

a programmer's error or bad software caused the database to malfunction. The malfunction resulted in the loss of all the information that the company used to service its client's insurance policies. The company could not operate until the "crash" was rectified.

The insurance services company hired consultants who restored the database by manually inputting the lost data. The insured quantified the loss as $53,586.83 in extra expenses to restore the data and $209,442.80 in lost business income, lost productivity, lost commissions and lost profits while the company's database was down. It made a claim for coverage under its First Party Commercial Property Policy.

The Insurer denied coverage arguing there was no "physical" damage. The California court agreed, holding there was no coverage and the appellate court has now affirmed that decision.

The appeal court in *Ward* first looked at basic insurance policy interpretation standards. It indicated that the objective when interpreting an insurance policy is to give effect to the mutual intention of the parties. The court did this by examining the clear and explicit meaning of policy provisions considered in their "ordinary and popular sense." If an ordinary person would give certain meaning to policy language and that meaning was not ambiguous, that meaning should be adopted by the court. *Ward General Ins. Services, Inc. v. Employers Fire Ins. Co.,* 114 Cal. App. 4th 548, 556-57, 7 Cal. Rptr. 3d 844, 851 (4th Dist. 2003).

In determining whether coverage existed for the loss of data, the *Ward* court confined its analysis to the language of the insurance policy at issue. It did not use "public policy" as a ground to find coverage as had the *Ingram Micro* court.. The *Ward* court relied on cases which held that public policy could not be used to rewrite the coverage set out in the terms of an insurance policy. See *Ward General Ins. Services, Inc. v. Employers Fire Ins. Co.,* 114 Cal. App. 4th 548, 556-57, 7 Cal. Rptr. 3d 844, 851 (4th Dist. 2003) (citing AIU Ins. Co. v. Superior Court, 51 Cal. 3d 807, 818, 274 Cal. Rptr. 820, 799 P.2d 1253, 32 Env't. Rep. Cas. 1257, 21 Envtl. L. Rep. 20315 (1990) (the answer to a coverage determination is to be found "solely in the language of the policies, not in public policy considerations").

The policy in *Ward,* insured:

… direct physical loss of or damage to Covered Property at the premises—caused by or resulting from any "Covered Cause of Loss."

"Covered Cause of Loss" meant:

RISKS OF DIRECT PHYSICAL LOSS … . (Emphasis added.).

The *Ward* court addressed whether the phrase "direct physical loss of or damage to Covered Property," required direct "physical" loss as well as direct "physical" damage. The *Ward* court stated that if a writer wrote that an orphanage relied on donors to supply its children with "used shirts, pants, dresses, and shoes," that a reader would know the adjective used modified shirts, pants, dresses, and shoes. Accordingly, it said that the language "direct physical" modified "loss" as well as "damage to Covered Property. …" The court concluded that the policy covered only physical loss and physical damage to "Covered Property."

On this "physical" damage issue, the *Ward* court said:

The risk encountered in this case was a negligent computer operator, or, perhaps a defective computer program. Unless the harm suffered, i.e. the loss of electronically stored data without loss or damage of the storage media, is determined to be a "physical loss," we cannot say that the risk encountered in this case, a negligent operator, constitutes a risk of direct physical loss. (Emphasis added.)

According to the *Ward* Court, the pure loss of electronic data was not "physical" and thus not covered under a policy that insured only "physical loss" (and "physical damage").

The *Ward* court looked at other coverage forms on the policy such as the "Business Income Coverage Form," the "Electronic Equipment and Software Coverage Form," the "Valuable Paper and Records Form" and the "Electronic Data Processing Coverage Form." It concluded that each of these coverage parts required that a loss be caused by a "direct physical loss." Accordingly, even the Electronic Data Processing Coverage Form did not cover the loss of the data, because there was no evidence of any "physical" loss.

The *Ward* court looked at the meaning of physical as "having material existence" and "perceptible especially through the senses and subject to the laws of nature." Since material means "formed out of tangible matter" and tangible means "being perceived by the sense of touch" the *Ward* court concluded that there was no

"direct physical loss," only a loss of intangible, non-physical data.

The *Ward* court held that computer data and information did not have "material existence," was not "formed out of tangible matter," and was not "perceptible to the sense of touch." See Ward General Ins. Services, Inc. v. Employers Fire Ins. Co., 114 Cal. App. 4th 548, 554, 7 Cal. Rptr. 3d 844, 849 (4th Dist. 2003). Even though the data was stored in a physical medium, *Ward*, nonetheless, held that the information and data itself remained "intangible." It noted that the lost information was actually the loss of "the sequence of 1's and 0's stored by aligning small domains of magnetic material on the computer's hard-drive in a machine readable manner." *Ward General Ins. Services, Inc. v. Employers Fire Ins. Co.,* 114 Cal. App. 4th 548, 554, 7 Cal. Rptr. 3d 844, 849 (4th Dist. 2003). (Emphasis added.)

The *Ward* court stated that the Plaintiff did not lose anything tangible but rather only stored "information." It explained that the "sequence of ones and zeroes can be altered, re-arranged, or erased without losing or damaging the tangible material or the storage medium." *Ward General Ins. Services, Inc. v. Employers Fire Ins. Co.,* 114 Cal. App. 4th 548, 554, 7 Cal. Rptr. 3d 844, 849 (4th Dist. 2003).

The *Ward* court examined cases like *AOL v St. Paul,*[6] and *State Auto Property v. Midwest Computers*[7]. It agreed with these cases which had decided that traditional third party policies require some kind of loss to physical or tangible property for coverage to exist. *Ward General Ins. Services, Inc. v. Employers Fire Ins. Co.,* 114 Cal. App. 4th 548, 554, 7 Cal. Rptr. 3d 844, 849 (4th Dist. 2003).

The *Ward* court refused to consider the importance of the computer data in determining coverage. To the contrary,, it relied on the plain and ordinary language of the policy to hold that computer data is not "physical" and therefore not covered under a traditional policy which covers only "physical" loss.

The *Midwest Computers & More* Decision

The United States District Court for the Western District of Oklahoma ruled that the inability to use computer data was not property damage under a business liability policy. However, the court held that the loss of use of the computer(s) holding the information/data was property damage. *State Auto Property and Cas. Ins. Co. v. Midwest Computers & More,* 147 F. Supp. 2d 1113 (W.D. Okla. 2001).

In *Midwest Computers & More*, an appraisal company had purchased computers from Midwest Computers. The appraisal company sued Midwest Computers alleging that the computer system had caused damages.. The Complaint alleged that the appraisal company was "deprived of the use of [its] computers." It also alleged that it "lost extensive amounts of appraisal data and other business information which was [sic] stored on their computer systems."

The appraisal company had a policy of business liability insurance issued by State Auto Property and Casualty Insurance Company. The policy provided coverage for "property damage to tangible property." The definitions stated:

Property damage means:

> a. Physical injury to tangible property, including all resulting loss of use of that property …; or
>
> b. Loss of use of tangible property that is not physically injured …

The *Midwest Computer & More* court first examined whether "tangible" property damage had occurred, evaluating the ordinary meaning of tangible, which was:

Capable of being perceived esp. by the sense of touch: palpable [;] ... capable of being precisely identified or realized by the mind [;] … capable of being appraised at an actual or approximate value (assets). *State Auto Property and Cas. Ins. Co. v. Midwest Computers & More,* 147 F. Supp. 2d 1113 (W.D. Okla. 2001) (citing Webster's Ninth New Collegiate Dictionary, p. 1205, 1985.

The *Midwest Computers & More* court ruled that these definitions did not include data, which was stored on a computer disk or a computer tape. It stated that the computer itself could be perceived, identified or valued. However it held that:

… the information itself cannot be. Alone, computer data cannot be touched, held or sensed by the human mind; it has no physical substance. It is not tangible property.

6 *America Online, Inc. v. St. Paul Mercury Ins. Co.,* 207 F. Supp. 2d 459 (E.D.Va. 2002).

7 *State Auto Property and Cas. Ins. Co. v. Midwest Computers & More,* 147 F. Supp. 2d 1113 (W.D. Okla. 2001).

This language is different from *Ingram Micro, Inc,.* which found that when a network computer "physically lost the programming information and custom configurations necessary for them to function," that "physical" damage had occurred.

The *Midwest Computers & More* court continued its analysis of whether the loss of computer data was tangible property damage. It turned to the second part of the property damage definition, which defined property damage to mean:

"Loss of use of tangible property that is not physically injured.

The *Midwest Computer& More* court stated that the appraisal company had alleged that Midwest Computer's negligence had caused "a loss of use of their computers." In addition, the appraisal company contended that the company's owners "were left without the use of their computers." Based on these allegations, the *Midwest Computer & More* court held that:

"Because a computer clearly is tangible property, an alleged loss of use of computers was "property damage" within the meaning of plaintiff's policy."

The *Midwest Computer& More* court also held that the "property damage," the loss of use of the computers, was excluded from coverage.

The appraisal company's policy, excluded property damage to:

"that particular part of any property that must be restored, repaired or replaced because "your work" was incorrectly performed on it."

The court considered another part of this exclusion, which stated that the exclusion did not apply to "property damage,, included in the "Products Completed Operations Hazard," defined as:

"all …'property damage' arising out of … 'your work' except … work that has not yet been completed or abandoned." The court stated that the "your work" exclusion asserted by the carrier would apply if Midwest Computer had not completed or abandoned its work when the property damage occurred.

The appraisal company said that it had lost use of the computers because of work done by Midwest Computers on August 23, 1999, but that further work on October 12, 1999 caused the loss of computer data. Since the work was "ongoing" and not "compete" the Midwest Computers court held that the "your work" exclusion applied and there was no coverage for the loss of the computers.

The *Midwest Computers & More* case is authority for the proposition that loss of computer data or information was not "tangible" because it did not have "physical substance." Insurers may cite *Midwest Computers & More* in opposition to *Ingram Micro, Inc.,* on the issue of whether the loss of computer information and computer data constitutes tangible property damage.

It is far from settled whether the "loss" of computer information is "physical damage" or whether computer Information is "tangible property." In many instances, the exact wording of the insurance policy may be controlling. A policy which only covers: "Physical injury to tangible property" may produce no coverage. Policies like the one at issue in I*ngram Mic o Inc.* may cover:

"All risk of physical loss of, or damage to the insured property as well as the interruption of business, except as hereinafter excluded."

[8]see David R. Cohen and Roberta D. Anderson, Insurance Coverage for "Cyber-Losses," Tort and Insurance Law Journal, pages 898–907 (Volume 35, #4, Summer, 2000).

New Cybersecurity Insurance Products
Cyber Endorsements To Traditional Policies

Many carriers are now offering cyber-risk endorsements as add-ons to traditional policies such as general liability policies, crime policies, auto and other policies. Anderson, VIRUSES, TROJANS, AND SPYWARE, OH MY! THE YELLOW BRICK ROAD TO COVERAGE IN THE LAND OF …49 TTIPLJ 529, n. 334 (Winter 2014). Some such policies cover only the services which may be needed in the event of a cyber breach. Others also provide coverage for the response which is needed in the event of a breach. For example, these policies would cover the cost of notification in the event it is required by state statute. Other endorsements also cover third party liability.

8 David R. Cohen and Roberta D. Anderson, Insurance Coverage for "Cyber-Losses," Tort and Insurance Law Journal, pages 898–907 (Volume 35, #4, Summer, 2000).

Cyber Insurance Policies
First Party or Third Party
Cyber policies differ in who is insured. First party coverage applies to losses to the insured due to the failure of its computer equipment, the replacement or restoration of lost and corrupted information, computer viruses, intruder theft and business interruption.

Third party coverage, may apply with respect to the same types of risks, but the damage must be caused to a third party by the insured, before liability arises. Insureds may require both types of coverage and some policies offer both.[9]

First Party Cyber Policies
The first party policies often cover:

- the fraudulent entry of data
- the fraudulent alteration or destruction of data
- fraudulent attacks upon the Insured's computers or information technology

Data may include information, text, images, sounds or words, but exclude computer programs.

For many of these policies to be implicated, a person "intending" to cause harm to the insured or to obtain financial gain must perform the fraudulent acts. Intentional conduct is frequently required for coverage to exist

The language of policies such as this may not cover negligent entry, alteration or destruction of information.[10]

Another carrier's policy covers direct loss resulting from "injury" to "Information assets… ." and broadly defines "information assets." The policy states that "information asset" is:

your computer system, including the electronic data stored therein. Electronic data includes, without limitation, customer lists and information, financial, credit card, competitive, and confidential or private information stored electronically … . Information assets shall also include the capacity of your computer system or its components [to be available] to its users, including but not limited to memory, bandwidth, processor time, and use of com-munication facilities and any other computer-connected equipment.[11]

Even though the policy includes a broad definition of "information asset," it limits coverage by providing that coverage extends only to damages resulting from security failures within the insured's computer system. Such restrictions arguably would exclude coverage for losses resulting from accidental electrical outages and similar events.

Third Party Cyber Policies
Third party cyber policies may include coverage for invasion of privacy and for the cost of complying with state cyberbreach notification statutes. They may include coverage for damages caused to a third party by unauthorized transmission of information by computer. theft or loss of computer information may be covered.[12]

One carrier's policy covers "damages" the insured "shall become legally obligated to pay as a result of a Claim ... alleging a Data Privacy Wrongful Act or a Network Security Wrongful Act."[13] "Data Privacy Wrongful Act" is defined to include ""any negligent act, error or omission by the Insured that results in: the improper dissemination of Nonpublic Personal Information or "any breach or violation by the Insured of any Data Privacy Laws." [14]""Network Security Wrongful Act" includes "any negligent act, error or omission by the Insured resulting in Unauthorized Access or Unauthorized Use of the Organization's Computer System, the consequences of which include, but are not limited to:

(1) the failure to prevent Unauthorized Access to, use of, or tampering with a Third Party's computer systems;
(2) the inability of an authorized Third Party to gain access to the Insured's services;
(3) the failure to prevent denial or disruption of Internet service to an authorized Third Party;
(4) the failure to prevent Identity Theft or credit/ debit card fraud; or
(5) the transmission of Malicious Code."[15]

9 Norman, 1 Internet Law and Practice 2:34 et. Seq.; Anderson, VIRUSES, TROJANS, AND SPYWARE, OH MY! THE YELLOW BRICK ROAD TO COVERAGE IN THE LAND OF …49 TTIPLJ 529, n. 334 (Winter 2014).
10 Norman, 1 Internet Law and Practice 2:36
11 Norman, 1 Internet Law and Practice 2:36
12 See Norman, 1 Internet Law and Practice 2:37 et. Seq.; Anderson, VIRUSES, TROJANS, AND SPYWARE, OH MY! THE YELLOW BRICK ROAD TO COVERAGE IN THE LAND OF …49 TTIPLJ 594 et seq (Winter 2014).
13 Anderson, VIRUSES, TROJANS, AND SPYWARE, OH MY! THE YELLOW BRICK ROAD TO COVERAGE IN THE LAND OF …49 TTIPLJ n. 337-342 et seq (Winter 2014).
14 *Id.*
15 *Id.*

> The definition of "Malicious Code" includes "unauthorized and either corrupting or harmful software code, including but not limited to computer viruses, Trojan horses, worms, logic bombs, spy-ware, malware or spider ware."[16]

Another carrier includes similar coverages but as opposed to "the improper dissemination of Nonpublic Personal Information," the carrier refers in its Insuring Agreements to Loss" that the "Insured is legally obligated to pay resulting from a Claim alleging a Security Failure or a Privacy Event."[17] "Privacy Event" includes:

> (1) any failure to protect Confidential Information (whether by " "phishing," other social engineering technique or otherwise) including, without limitation, that which results in an identity theft or other wrongful emulation of the identity of an individual or corporation;
>
> (2) failure to disclose an event referenced in Sub-paragraph (1) above in violation of any Security Breach Notice Law; or
>
> (3) violation of any federal, state, foreign or local privacy statute alleged in connection with a Claim for compensatory damages, judgments, settlements, pre-judgment and post-judgment interest from Sub-paragraphs (1) or (2) above."[18]

"Security Failure" is defined to include:

> "(1) a failure or violation of the security of a Computer System including, without limitation, that which results in or fails to mitigate any unauthorized access, unauthorized use, denial of service attack or receipt or transmission of a malicious code;
> (2) physical theft of hardware controlled by a Company (or components thereof) on which electronic data is stored, by a person other than an Insured, from a premises occupied and controlled by a Company; or
> (3) failure to disclose an event referenced in Sub-paragraphs (1) or (2) above in violation of any Security Breach Notice Law."[19]
> "Security Failure" "includes any such failure or violation, resulting from the theft of a password or access code from an Insured's premises, the Computer System, or an officer, director or employee of a Company by non-electronic means in direct violation of a Company's specific written security policies or procedures."[20]

Intellectual Property Claims

Some cyberinsurance policies include coverage for intellectual property claims such as copyright, trademark or plagiarism. These policies may provide a duty to defend and/or a duty to indemnify.[21]

Regulatory Claims

Some third party liability policies provide defense and indemnity as to regulatory matters, including matters brought by the FTC.

Business Interruption Claims

Several cyber policies include business interruption coverage. However, certain policies provide business interruption coverage only in the first party context. Such policies are not designed to provide coverage for business interruption losses which the insured causes to third parties.[22]

CONCLUSION

There are a wide variety of cyber insurance products available, and at this stage of the development of the product, carriers are likely to be willing to negotiate in order to tailor the necessary coverage. Most states, by statute, do require that a person be notified in the event his or her private information is disclosed without authority. However, such State notification statutes vary widely in their specific terms. Moreover, there is no uniform judicial or statutory standard governing the degree of care required of those entrusted with confidential financial or identifying information. The one thing which is known is that breaches will continue, causing the body of jurisprudence regarding cyber liability and cyberinsurance coverage to continue to evolve.

BIBLIOGRAPHY

Scott M. Angelo, What Does It Take to Survive a Breach in Today's High-Risk World? When Your Prevention Fails (And It's Going To Fail), What Do You Do?, 14 U. Pitt. J. Tech. L. & Pol'y 280 (Spring 2014).

Kevin D. Ashley, Introduction: Cybersecurity in Pittsburgh, 14 U. Pitt. J. Tech. L. & Pol'y 273 (Spring 2014).

Derek E. Bambauer, Ghost in the Network, 162 U. Pa. L. Rev. 1011 (April 2014).

James Arden Barnett, Jr., Cyber Security: Fixing Policy with New Principles and Organizations, Recent Trends in Nat'l Sec. Law, 2014 WL 2315048 (April 2014).

16 *Id.*

17 Anderson, VIRUSES, TROJANS, AND SPYWARE, OH MY! THE YELLOW BRICK ROAD TO COVERAGE IN THE LAND OF …49 TTIPLJ n. 343-347 et seq (Winter 2014).

18 *Id.*

19 *Id.*

20 *Id.*

21 *Id.*

22 Norman, 1 Internet Law and Practice 2:38 et. Seq.

Craig Blackwell, Legislative and Regulatory Update, Am. L. Inst. Cont. Legal Educ., VCU0924 ALI-ABA 15 (Sep. 2012)

Christopher Bosch, Securing the Smart Grid: Protecting National Security and Privacy Through Mandatory, Enforceable Interoperability Standards, 41 Fordham Urb. L.J. 1349 (May 2014).

Jeremy J. Broggi, Building on Executive Order 13,636 to Encourage Information Sharing for Cybersecurity Purposes, 37 Harv. J.L. & Pub. Pol'y 653 (Spring 2014).

Michael Cochran, A Lawyer's Guide to Privacy and Information Security of Client Websites, 47 Md. B.J. 42 (Feb. 2014).

Amanda Craig, Federated Identity Management and the NSTIC: Co-Managing Information Privacy, 2014 U. Ill. J.L. Tech. & Pol'y 177 (Spring 2014).

Cybersecurity push fuels liability debate for infrastructure software developers, Inside CyberSecurity, 2014 WLNR 6003586, March 5, 2014.

Christine Daleiden, Information Security Basics for Lawyers, Haw. B.J. 4 (April 2014).

Sherri Davidoff, How Attorneys Get Hacked (And What You Can Do About It), 39 Mont. Law. 25 (May 2014).

DHS insurance report paints grim picture of health care cybersecurity, Inside CyberSecurity, 2014 WLNR 5287116, Feb. 25, 2014.

Brian E. Finch, Litigation Following a Cyber Attack: Possible Outcomes and Mitigation Strategies Utilizing the Safety Act, 30 Santa Clara High Tech L.J. 349 (April 2014).

Robert Gyenes, A Voluntary Cybersecurity Framework is Unworkable–Government Must Crack the Whip, 14 U. Pitt. J. Tech. L. & Pol'y 293 (Spring 2014).
Daniel E. Harmon, The Anti-Malware Market: Newer Security Programs Now Rival the Old Guard, 31 No. 18 Law. P.C. 1 (June 2014).

House panel sees existing liability protection for infrastructure software developers, Inside CyberSecurity, 2014 WLNR 6721157, March 12, 2014.

Insurance Industry eyes framework usage as prerequisite for cyber coverage, Inside CyberSecurity, 2014 WLNR 6721162, March 12, 2014.

Andre R. Jaglom, Internet Distribution, E-Commerce and Other Computer Related Issues: Current Developments in Liability On-Line, Business Methods Patents and Software Distribution, Licensing and Copyright Protection Questions, Am. L. Inst. Cont. Legal Educ., SU051 ALI-ABA 675 (June 2013).

Vincent R. Johnson, Cybersecurity, Identity Theft, and the Limits of Tort Liability, 57 S.C.L. Rev. 255 (Winter 2005).

Lawyers disagree on whether cybersecurity framework will reshape liability landscape, Inside CyberSecurity, 2014 WLNR 5287133, Feb. 26, 2014.

Ronald D. Lee, New Government Cybersecurity Standards Could Impact Many Companies, 18 No. 9 Cyberspace Law. 1 (Oct. 2013).

Matthew Moriarty, Thy Brother Came with Subtlety: How a Cause of Action Against Companies Who Leak Data Can Increase Security in the Digital Age, 62 U. Kan. L. Rev. 813 (March 2014).

Laurel A. Price, Advertising and Unfair Competition: Federal Enforcement, Am. L. Inst. Cont. Legal Educ., ST056 ALI-ABA 541 (June 2012).

David G. Ries, Cybersecurity for Attorneys: Understanding the Ethical Obligations, Am. L. Inst. Cont. Legal Educ., RSUM09 ALI-ABA 1 (Nov. 2012).

Rose L. Romero, Strategies for Preventing and Prosecuting Cyberstalking and Harassment Crimes, The Impact of Recent Cyberstalking and Cyberharassment Cases, 2014 WL 1600589 (June 2014).

Peter J. Schaumberg, Power to the People: Electric Transmission Sitting in the American West, 5 Rocky Mtn. Min. L. Found, Inst. Paper No. 6 (Nov. 2013).

Melanie J. Teplinksy, Fiddling on the Roof: Recent Developments in Cybersecurity, 2 Am. U. Bus. L. Rev. 225 (2013).

Ioana Vasiu, Break on Through: An Analysis of Computer Damage Cases, 14 U. Pitt. J. Tech. L. & Pol'y 158 (Spring 2014).
Peter S. Vogel, What Are You Doing To Protect Yourself and Your Clients from Cybercriminals?, 77 Tex. B.J. 390 (May 2014).

Katherine Booth Wellington, Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions, 30 Santa Clara High L.J. 139 (March 2014).

Faculty Biography: Judy Burnthorn

Partner | Deutsch Karrigan & Stiles | New Orleans, LA

504.593.0688 | jburnthorn@dkslaw.com
http://www.dkslaw.com/attorney/burnthorn

Ms. Burnthorn is a partner in the firm. For over 25 years she has focused on trying all types of commercial matters before juries, judges and arbitration panels.

Ms. Burnthorn handles litigation in the areas of professional liability, employment law, securities and commodities fraud, financial transactions, negotiable instruments, tax, business valuation, non-competition agreements, unfair trade practices, insurance (life, health, disability, directors & officers, and errors & omissions), and malpractice (CPA, attorney, surveyor, appraiser and insurance agent).

Ms. Burnthorn has extensive experience representing excess insurance carriers and insurance guaranty associations. She has also successfully handled multi-district litigation and class action matters. In multiple situations, she has had excess carriers she was representing included in settlements eliminating multi-million dollar exposures claimed by the plaintiffs to exceed the attachment point, without any settlement payment by the excess carrier. These accomplishments have come through familiarity with insurance and excess insurance concepts as well as with the duties owed by others in the transaction, including the insured and other layers within the market.

Ms. Burnthorn set precedent eliminating vicarious liability under provisions of the RICO statute, enforcing contractually shortened fidelity bond statutes of limitations against claims of waiver and invalidity, enjoining the prosecution of state litigation through injunctions issued in federal court, and enforcing coverage provisions of insurance guaranty association statutes. Prior to joining the firm, Ms. Burnthorn completed an externship with the Honorable Martin L.C. Feldman, USDC, E.D.La.

Practice Areas

- Commercial Litigation
- Labor & Employment
- Professional Liability
- Securities Litigation

Education

- J.D., magna cum laude, Tulane University School of Law, 1986 -- Tulane Law Review; Order of the Coif
- B.A., summa cum laude, Political Philosophy, Louisiana State University, 1982