RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: LAW-W02

The $100 Million Question: Were Reasonable Cybersecurity Measures Taken?

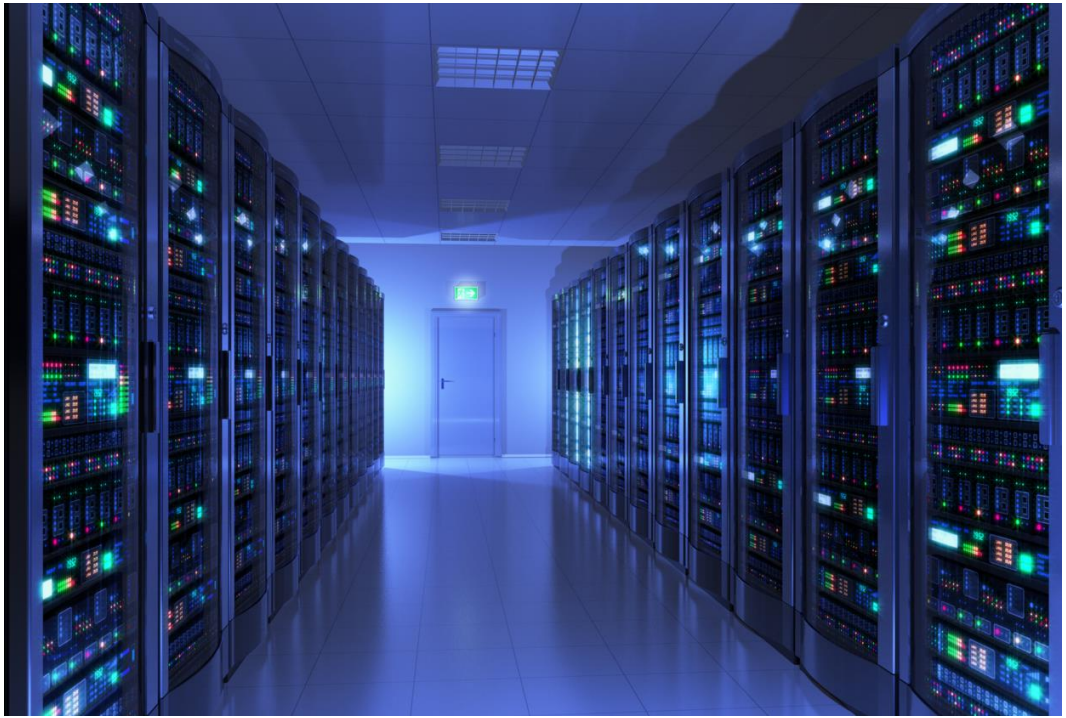
Joseph M. Burton, Esq.
Partner
Duane Morris LLP
@DuaneMorrisLLP

William S. Rogers, Jr., Esq.
Partner
Prince Lobel Tye LLP
@wsrogers26
@princelobel

Jon C. Stanley, Esq.
Counsel
Verrill Dana
@VerrillDana

#RSAC

The $100 Million Question: Reasonable?



Background

Security Incidents

- 4,778 data breaches since 2005[1]
- > 750,000 computers infected with Ransomware in 2015[2]
- $154 average cost per each lost or stolen record[3]

Subsequent Litigation

- ~200 cases filed[4]
- 24 different legal theories pursued[5]
- $574,984 average cost of defense[6]
- $258,099 average settlement[6]

[1] "Chronology of Data Breaches," Privacy Rights Clearinghouse (2016), http://privacyrights.org/data-breach/new
[2] "Overall Statistics for 2015," Kaspersky Security Bulletin 2015 (2015), https://securelist.com/files/2015/12/KSB_2015_Statistics_FINAL_EN.pdf
[3] "2015 Cost of a Data Breach Study: Global Analysis," IBM and Ponemon Institute (2015).
[4] Westlaw and LexisNexis search for "Data Breach" cases for all reported/unreported state and federal cases conducted on February 23, 2016.
[5] "2015 Data Breach Litigation Report," Bryan Cave (2015), http://bryancavedatamatters.com/wp-content/uploads/2015/04/2015-Data-Breach-Litigation-Report.pdf
[6] "The typical data breach lawsuit and how to protect your company," Moore&VanAllen (Oct. 2014), http://www.mvalaw.com/news-publications-347.html

Why the lack of cases?

- **Theories of Liability**
  - **Common law** (i.e. tort, contract)
  - **Statutes** (i.e. FTCA, breach notification laws)
  - **Regulation** (i.e. Safeguard, HIPAA Privacy Rule)
- **Basis for Dismissal**
  - **Standing** (*See Clapper v Amnesty International USA,* 133 S.Ct. 1138 (2013))
  - **Damages** (*See In re TJX Cos. Retail Sec. Breach Litig.,* 564 F.3d 489, 489 (1st Cir. 2009), *amended on reh'g in part* (D. Mass. 2009))
  - **Cause of Action** (i.e. economic loss doctrine; *See In re Anthem Data Breach Litig.*, 2016 U.S. Dist. LEXIS 18135 (N.D. Cal. 2016))
- **Settlement** (*See In re: Target Corp. Customer Data Security Breach Litigation*, Case No. 0:14-md-02522 (D. Minn. 2015))

Why the lack of cases?

***Patco Const. Co. v. People's United Bank*, 684 F.3d 197 (1st Cir. 2012)**

"The UCC explains that the '[c]ommercial reasonableness of a security procedure is a question of law' to be determined by the court. Id. § 4-1202(3)... 'it is whether the procedure is reasonable for the particular customer and the particular bank . . . .'" Id. § 4-1203 cmt. 4."

***F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015)**

"[A] comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of Cardholder Data…appropriate to Hotels and Resorts' size and complexity, the nature and scope of Hotels and Resorts' activities, and the sensitivity of the Cardholder Data at issue…"

***F.T.C. v. LifeLock, Inc.*, Matter No. X100023 (2015)**

"[T]he Commission alleged that LifeLock…fail[ed] to establish and maintain a comprehensive information security program to protect its users' sensitive personal data, including credit card, social security, and bank account numbers"

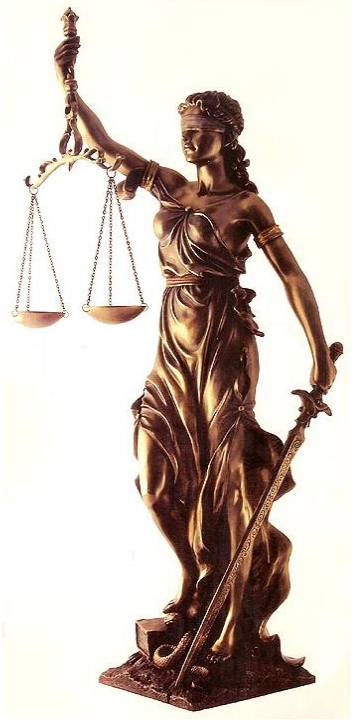
The Question is Answered Here

Proof of Standard of Care: Experts

- Why do we need expert witnesses in litigation?
- Experts assist a jury or the judge in understanding complex subject-matter outside the normal experience of most laymen
- Experts can testify not only to pertinent facts in a case, but they may offer their opinions about the significance of facts in evidence, and also suggest their opinions of proper conclusions concerning the ultimate issues in a case to the fact finder (judge or jury)

Proof of Standard of Care: Experts

- The Court determines who is an "expert" for the admissibility of proposed expert testimony into evidence at trial, which may be challenged by either party
- *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993) established that a Judge must act as a gatekeeper when determining whether expert testimony is admissible.



Proof of Standard of Care: Experts

- The plaintiff expert's role is to: establish his *bona fides*; an alleged standard of reasonable care or standard of performance; an alleged breach of the applicable standard; and to establish the causal relationship between the breach and the alleged damages sustained; and, the amount or extent of the damages.
- The defense expert's role is to: establish his *bona fides*; may be to dispute the qualifications or the testimony of the plaintiff's expert on any one or all of these issues

Proof of Standard of Care: *Daubert* Test

In the case of scientific or non-scientific technical experts, the testimony:

- Must be based upon sufficient facts or data;
- The product of reliable principles and methods (e.g. the scientific method); and
- The witness must have applied the principles and methods reliably to the facts of the case

Proof of Standard of Care: *Daubert* Test

- An inability to satisfy the *Daubert* standard means that such testimony is inadmissible.
- NOTE: Daubert and its progeny such as Kumho Tire Co. v. Carmichael, 526 U.S. 137 (1999) (applying the Daubert standard to non-scientists) have been incorporated into Federal Rule of Evidence 702
- State courts may have separate analogous standards governing the admissibility of expert testimony

Proof of Standard of Care: IT Experts *May* be Professionals under the Law

- They may be licensed lawyers or licensed computer or software engineers, P.E., by state law/state boards
- They may have industry accreditations or certifications which should be considered akin to professional licensure ((ISC)²CISSP; MSFT-MCSE/MCSA; Cisco CCNA/CCNP; CompTIA A+, etc.)
- Not all should qualify, but consider the finest hacker against which no system is safe. Is he/she and "expert" under *Daubert?*

IT Providers in Court

A Case In Point: *Eye Care & Eye Wear v. Enables IT, Inc. et. al.* (Maine Nov. 16, 2015)

- State Court Action in Maine Business and Consumer Court decided within the last three months
- Claim by Plaintiff Customer vs. IT Consulting Firm alleging breach of contract and negligence in the performance of contracted for services
- Defendant filed a motion for partial summary judgment alleging that no claim of negligence could lie for loss of purely economic damages, which were barred by the "economic loss rule"

The Economic Loss Rule

- The Rule: Economic losses are generally only recoverable in Contract, and losses due to physical harm to persons or damage to property are generally recoverable in Tort, i.e. Negligence
- But, an exception to the economic loss rule exists for recovery of economic losses allegedly sustained due to a professional's negligence or breach of a higher, specialized duty
- In Maine, the "professional services" exception applies to lawyers, doctors, architects, and accountants. IT too?

Is IT similarly a “Profession”?

- Factors Considered: 1) specialized knowledge and skill; 2) reliance by client on specialized knowledge and skill; 3) uniformly settled and applied standards of practice such as in licensing requirements, laws, regulations, accreditation standards, codes of conduct, etc.
- Not every service is subject to standards so widely and clearly established so as to justify imposing a specialized, extra-contractual duty of care, to avoid economic losses

Summary Judgment: GRANTED!

- The Court concluded "on this record" IT service providers, such as the defendant, are not "professional" service providers for purposes of the economic loss doctrine
- Do you agree with the Maine Court's ruling generally?
- The key here was a failure by counsel to provide a sufficient record substantiating the professional standing of the defendant IT providers, including expert opinion, which could have altered the analysis and outcome

Beyond the terms of a contract…

Are IT providers liable in tort?

Potentially yes, for economic loss.

What Are The Implications and Consequences?

- There Is No Universally Agreed Upon Standard of Care
- There Are Universally Agreed Upon Security Principals and Measures
- Security Measures Must Be Tailored To The Complexity and Sensitivity of Your Business and Its Information

ACTIONS: Applying Our Advice

- Consider the computer information systems you have in your organization, the data you store/handle/possess, and the employees, vendors, contractors, utilizing your systems and data
- Identify the professionals you would need in the event of a security incident, data breach, or regulatory action to assist you in prosecuting or defending your organization's legal rights concerning the actions of each of these types of players
- Maintain a file of qualified experts and audit it annually

ASK THE PANEL: ANY QUESTIONS?

Joseph M. Burton – JMBurton@duanemorris.com
William S. Rogers, Jr. – wrogers@princelobel.com
Jon C. Stanley – jstanley@verrilldana.com

PRINCE LOBEL

DuaneMorris®

Verrill Dana LLP
Attorneys at Law