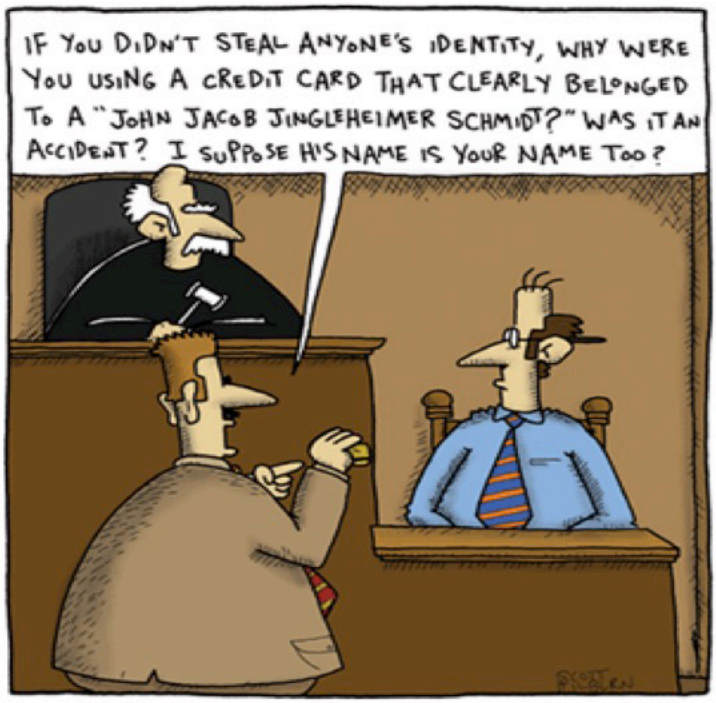
"We've Been Hacked!" - The Hackers, The Hacked, And Who's Responsible

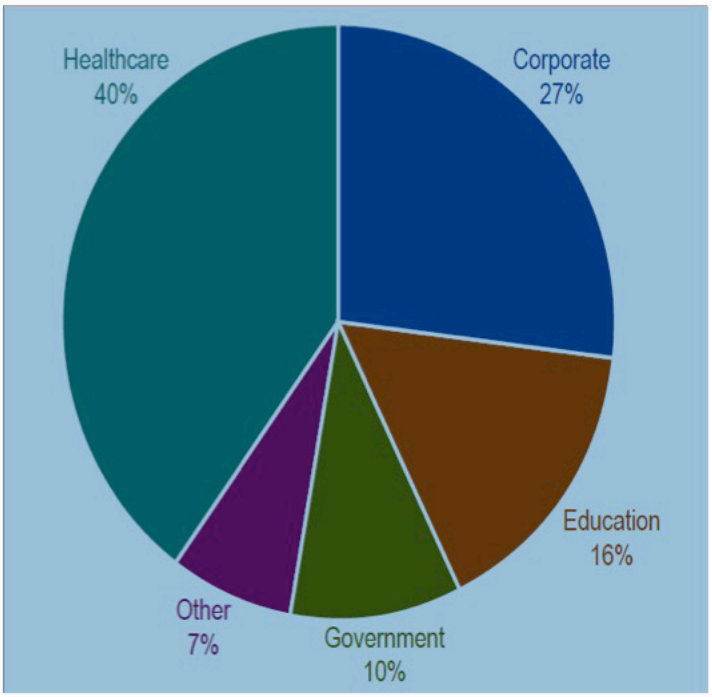
Anthony Todaro
Corr Cronin Michelson Baumgardner Fogg & Moore (Seattle, WA)
206.274.8666 | atodaro@corrcronin.com



"START WITH A JOKE"

THE PROBLEM

IT'S NOT JUST THE BIG GUYS



ATTACKS BY INDUSTRY

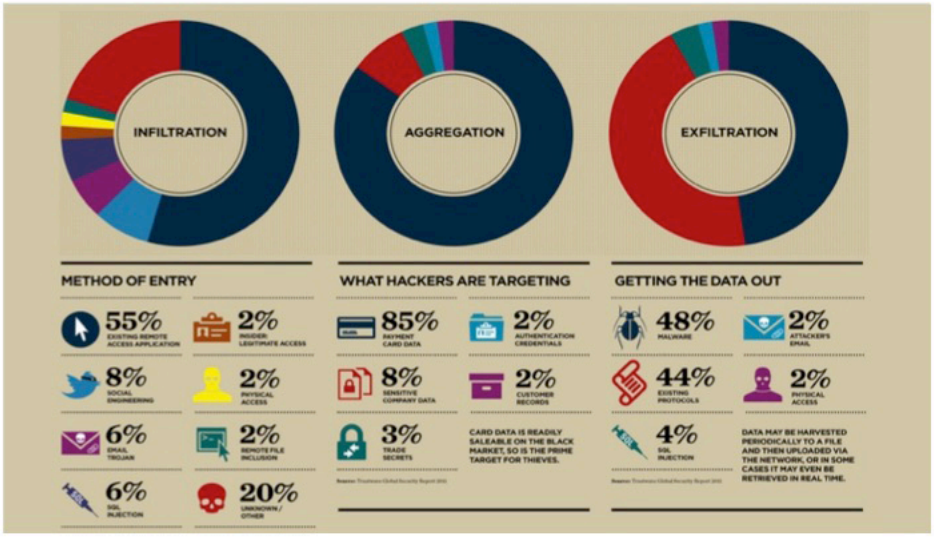
MALICIOUS DATA BREACHES: THE "WHO"

- Cyber Criminals
- Corporate Espionage and/or State Sponsored Hackers
- Hactivists

MALICIOUS DATA BREACHES: THE "WHY"

- **Cyber Criminals: MONEY!**
  - Organized criminal operations that access credit card information and resell bulk batches of card numbers through online forums.
- **Corporate Espionage and State Sponsored Hackers: INFORMATION!**
  - State funded operations aimed at gaining access to sensitive corporate and governmental information ranging from intellectual property to financial data.
- **Hactivists: DAMAGE!**
  - Politically motivated groups whose goal is usually to cause system failure or damage a company's operations.

MALICIOUS DATA BREACHES: THE "HOW"



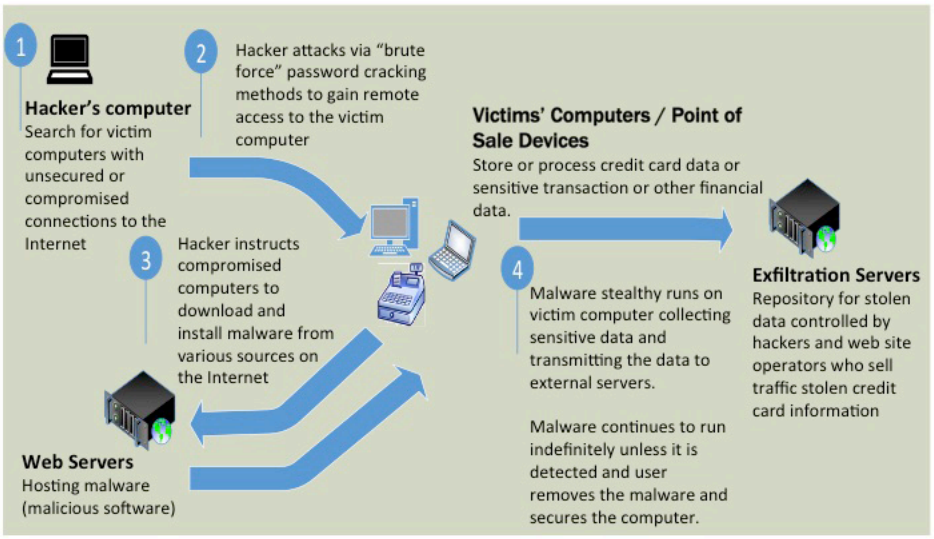
PFISHING

PFISHING VICTIM: TARGET

Brute force (also known as brute force cracking) is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through exhaustive effort (using brute force) rather than employing intellectual strategies.

BRUTE FORCE

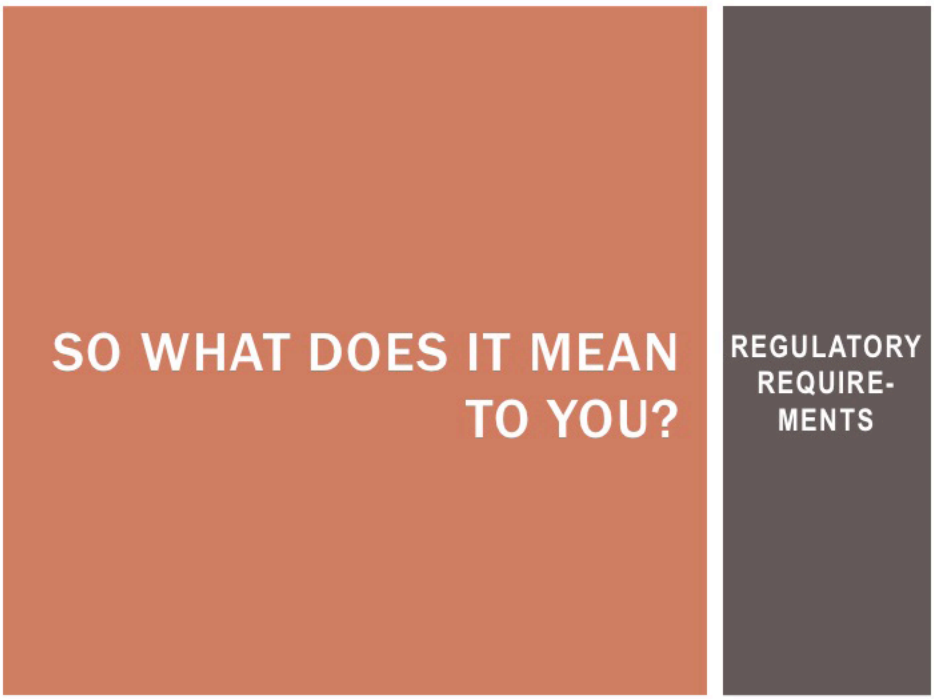
HACKING INFRASTRUCTURE




Company/Organization: Zappos
Industry: Retail
Record Type: Electronic
Method: Hacking
Type of Media: N.A.
Size of Breach: 24 Million Customers
Type of Data Breached: Names, Contact Information, Passwords, Financial Information
BRUTE FORCE VICTIM: ZAPPOS


FAILURE TO MAINTAIN PHYSICAL CONTROL OVER SOURCES OF INFORMATION: LAPTOPS, BACK-UP TAPES, AND PRINTED REPORTS
LOSS


Company/Organization: Nemours
Industry: Hospital System
Record Type: Electronic
Method: Loss
Type of Media: Backup Tapes
Size of Breach: 1.6 Million Records
Type of Data Breached: Names, Contact Information, DOBs, SSNs, Financial Information
LOSS VICTIM: NEMOURS


SO WHAT DOES IT MEAN TO YOU?
REGULATORY REQUIRE-MENTS

NON-LITIGATION COSTS

- **TREASURE:**
  - Average $5.5M per breach or $194 per record:
  - Target (December 2013):
    - $61M in 2013, $191M in 2014
  - Home Depot (September 2014):
    - $33M in Q4-14, $7M in Q1-15
  - Sony (November 2014):
    - $15M in '14-'15
- **TIME:** Hundreds of Hours: Required Disclosures/Regulatory Inquiries/Media Strategy
- **GOODWILL:**
  - It makes headlines: Requirement to alert media almost guarantees news reports.
  - It harms customer confidence: Studies report 55% of data breach victims express diminished confidence in the breach organization.
  - It increases scrutiny: Regulatory oversight likely to increase (costing more time/treasure).

SO WHAT DOES IT MEAN TO YOU?

LITIGATION!

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

In re: Target Corporation Customer Data Security Breach Litigation,

MDL No. 14-2522 (PAM/JJK)

This document relates to:
Financial Institution Cases.

MEMORANDUM AND ORDER

"And Plaintiffs' allegation that Target was solely able and solely responsible to safeguard its and Plaintiffs' customers' data is also plausible. Imposing a duty on Target in this case will aid Minnesota's policy of punishing companies that do not secure consumers' credit and debit card information" – Filed December 2, 2014

NEGLIGENCE:
THE DUTY TO SAFEGUARD (AN EMERGING "STANDARD OF CARE")

Payment Card Industry (PCI)

PCI Security Standards Council

- **Anyone who stores, process, or transmits credit card data must be PCI compliant**
- **Common PCI validation requirements**
  - Report on Compliance (ROC)
  - Self-Assessment Questionnaire (SAQ)
  - Letter of Attestation
  - Quarterly PCI scans
- **Sample PCI Data Security Standards Requirements**
  - Annual Penetration Testing (DSS 11.3)
  - Security Awareness Training (DSS 12.6)
  - Quarterly PCI scans (DSS 11.2)

PCI – The Myth of Outsourcing

- Outsourcing Credit Card Payment Processing Does *Not* Necessarily Make You PCI Complaint:
  - Credit Card Data must be protected at all points of usage – receipt, processing, retention, charge backs and refunds.
  - So, is it truly outsourced?
    - Outsourcing can create false sense of security and lack of vigilance – data usually still passes through company-hosted servers or is accessible.
  - If Primary Account Number (PAN) information is *not* stored, processed or transmitted through a system controlled by the merchant, then PCI DSS Requirement 12.8 requires that the merchant ensure that there is an agreement with that third party processor that includes acknowledgement that the processor is responsible for the security of the cardholder data.

WILL PAYMENT INFORMATION ISSUE JUST GO AWAY?

- **Banks are spending $8B on Smart Cards,**
  - "Smart Cards" use a computer chip technology (not a magnetic strip) that is difficult to replicate even if basic card information is compromised.
- **BUT, merchants are not spending the additional $25B needed to process them.**
  - Beginning in October, merchants are supposed to have chip readers in place or face liability for fraud (but many lack the means to pay for the readers or simply accept the risk of liability if there is a data breach).
- **So, the problem will continue….**

ARTICLE III (STANDING): DEFENDANTS' LAST/BEST STAND

- **Before *Clapper*:**
  - *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011) (unknown hacker gained access to employees' personal and financial information): Plaintiffs' injuries were "dependent on entirely speculative, future actions of an unknown third-party."
  - *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010) (stolen laptop with unencrypted employee data): Risk of identity theft is a sufficient injury for Article III standing and underlying claims.
- ***Clapper v. Amnesty International USA*, *133 S. Ct. 1138 (2013)*:**
  - Not a data breach case;
  - Holding: A "threatened injury must be *certainly impending* to constitute an injury in fact," and that "allegations of *possible* future injury" are not sufficient.
- **After *Clapper*:**
  - *Galaria v. Nationwide Mutual Ins. Co.*, 998 F.Supp.2d 646 (S.D. Ohio 2014): "[A]n increased risk of identity theft, identity fraud, medical fraud or phishing is not itself an injury-in-fact" without allegations or facts suggesting that harm is "certainly impending."

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE ADOBE SYSTEMS, INC. PRIVACY LITIGATION	Case No.: 13-CV-05226-LHK ORDER GRANTING IN PART AND DENYING IN PART DEFENDANT ADOBE SYSTEMS INC.'S MOTION TO DISMISS

Unlike in *Clapper*, where respondents' claim that they would suffer future harm rested on a chain of events that was both "highly attenuated" and "highly speculative," the risk that Plaintiffs' personal data will be misused by the hackers who breached Adobe's network is immediate and very real. Plaintiffs allege that the hackers deliberately targeted Adobe's servers and spent several weeks collecting names, usernames, passwords, email addresses, phone numbers, mailing addresses, and credit card numbers and expiration dates.

N.D. Cal. to Plaintiffs' Rescue:

"That's why they stole it!"

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE LINKEDIN USER PRIVACY LITIGATION

Case No.: 5:12-CV-03088-EJD

ORDER GRANTING IN PART AND DENYING IN PART DEFENDANT'S MOTION TO DISMISS

[Re: Docket No. 81]

When members register, they are required to confirm that they agree to LinkedIn's User Agreement ("User Agreement") and Privacy Policy ("Privacy Policy"). The Privacy Policy contains a statement that "[a]ll information that you provide will be protected with industry standard protocols and technology." … The statement in LinkedIn's Privacy Policy might be significant only to a small segment of consumers and many consumers may not even care to read it before making their purchase. Yet the California Supreme Court and the Ninth Circuit Court of Appeals have indicated that when those representations are false, a consumer who is induced by them to purchase a product that she otherwise would not have purchased has standing to bring an action under the UCL in federal court.

Don't Forget About Your Privacy Policy!

STANDING NOW: STILL AN OPEN QUESTION

- *In re Zappos.com, Inc., Customer Data Security Beach Litigation*, No. 12 CV 00325, 2015 WL 3466943 (D. Nev. Jun. 1, 2015) (Multi-District Litigation):
  - District Court *dismisses* Complaint on standing grounds in an MDL involving a purported class of 24 million victims;
  - District Court notes conflict between *Clapper* and recent opinions from within the Ninth Circuit but holds the standard used by both – essentially, (i) "credible threat of harm" and (ii) harm that is "both real and immediate" – to be virtually indistinguishable.
  - District Court distinguishes *Adobe* and *Sony* by noting that, in those cases, there was evidence that hackers used the hacked information to discover vulnerabilities in products (*Adobe*) or victims had experienced unauthorized charges on credit cards (*Sony*).
  - District Court holds that lack of similar evidence and passage of time undermine the conclusion that harm is "real and immediate":
    - "*The more time that passes without the alleged future harm actually occurring undermines any argument that the threat of harm is immediate, impending, or otherwise substantial.*"

WHAT DO YOU DO ABOUT IT?

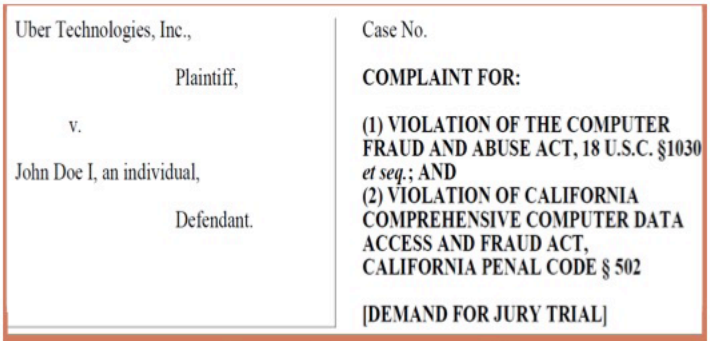
RESPONDING TO A DATA BREACH

- **Put it in writing:**
  - Have a written Data Breach Response Plan outlining (i) parties involved, (ii) responsibilities of each, and (iii) steps to be taken (e.g., preservation, notice, media response).
- **Have someone in charge:**
  - It may be time to have a Chief Security Officer.
  - Assign a corresponding individual from the Legal Department.
- **Call your insurer:**
  - Target recouped $90M of its losses from insurance.

2:20p - 2:40p
CYBER-LIABILITY – AN INSURABLE RISK THAT MUST BE PART OF YOUR RISK MANAGEMENT PLAN
Linda Woolf -- Goodell DeVries Leech & Dann (Baltimore, MD)
Every organization that uses technology faces cyber risk. Customer records, account numbers and passwords, credit card data, private health information, business financial information, trade secrets, authentication credentials and employee records are all at risk. Evaluating your cyber exposure and covering your assets with cyber liability insurance is a critical part of your risk management plan.

WHAT ABOUT AFFIRMATIVE LITIGATION?

- TRADITIONAL COMMON LAW CAUSES OF ACTION = TRESPASS TO CHATTELS / MISAPPROPRIATION / ETC.
- BEST WEAPON = COMPUTER FRAUD AND ABUSE ACT (CFAA)
  - Enacted in 1984 as a criminal statute aimed at hackers who gain access to government computer systems.
  - Amended in 1994 to create a private right of action.
  - Amended in 1996 to expand "protected computers" to those used in interstate commerce.



Uber Technologies, Inc.,

Plaintiff,

v.

John Doe I, an individual,

Defendant.

Case No.

COMPLAINT FOR:

(1) VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. §1030 *et seq.*; AND
(2) VIOLATION OF CALIFORNIA COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT, CALIFORNIA PENAL CODE § 502

[DEMAND FOR JURY TRIAL]

Building on from *SOLARBRIDGE TECHNOLOGIES, INC. V. JOHN DOE*, 2010 WL 3419189 (N.D. CA. AUG. 27, 2010) (authorizing third-party discovery in CFAA claim against John Doe), the Court orders non-party GitHub to turn over thousands of user logs in connection with Uber's efforts to identify the party that hacked its internal database of driver names and license plates.

N.D. Cal.:

Orders Third-Party GitHub to Produce Logs

"END WITH A JOKE"

Anthony Todaro

Partner

Corr Cronin Michelson Baumgardner Fogg & Moore (Seattle, WA)

206.274.8666 | atodaro@corrcronin.com

http://corrcronin.com/our-team/anthony-todaro/

Anthony is an experienced trial lawyer who has tried dozens of cases to verdict. Anthony's practice focuses on defending products liability, medical negligence and complex commercial and tort matters. Anthony has appeared in state and federal courts throughout Washington.

Anthony grew up in Seattle's Capitol Hill neighborhood. He attended Lakeside High School before heading to New York where he earned his undergraduate degree cum laude from Columbia University. After college, Anthony obtained his Series 7 and 63 certifications and worked as a securities broker on Wall Street. Anthony then traveled to Chicago, where he earned his J.D. from Northwestern University School of Law.

Anthony's previous legal experience includes trial work as a felony criminal prosecutor in the King County Prosecutor's Office, complex commercial work as an associate with the multi-national law firm DLA Piper, and tort and business litigation as a shareholder with the boutique trial firm Peterson Young Putra.

Anthony has been named a "Washington Super Lawyer" and has been dubbed a "Top Lawyer" in Washington by Seattle Met Magazine. Anthony is admitted in Washington and Oregon.

Representative Cases

- Wuth v. Laboratory Corporation of America – Representing LabCorp in wrongful life/wrongful birth claim relating to claim of negligence in the conduct of genetic testing.
- Brooklyn Court Litigation – Representing developer in dispute with joint venture partner concerning the development of a mixed use multi-family dwelling in the Roosevelt neighborhood.
- Spam Arrest v. Replacements/Sentient Jet/123greetings/Scotsman Guide – Representing various defendants in a series of related cases involving claim of violation of online agreements in connection with the sending of unwanted emails.
- Massey v. The Harvard Drug Group – Represented supplier of generic pharmaceuticals in multi-party products liability litigation related to claim of contaminated alcohol prep pads.
- Lindsey, et al. v. Intelius – Represented business owner in $60 million claim brought under the Washington State Securities Act arising out of purchaser's misstatements in connection with the acquisition of the business owner's company by Intelius. The case settled for a confidential sum following a mediation conducted by Tony Piazza.
- Jain v. InfoSpace, et al. – Defended InfoSpace in indemnification action arising from a $247 million judgment entered against former InfoSpace CEO Naveen Jain for violations of securities laws.
- Knoblauch, et al. v. Perky's, Inc., et al. – Represented purchasers of coffee stands in a weeklong arbitration trial of claims brought under the Franchise Investment Protection Act. The arbitrator awarded our clients damages, attorneys' fees, and a punitive multiplier.
- Eldrick "Tiger" Woods, et al. v. Christensen Shipyards, Ltd. – Defended luxury yacht manufacturer in an arbitration hearing against claims brought by golf champion Tiger Woods arising out of his assertion that Christensen had used photographs of the interior of his boat ("Privacy") without permission.

Education

- Northwestern University School of Law (J.D. 2000)
- Columbia University (B.A. cum laude 1996)