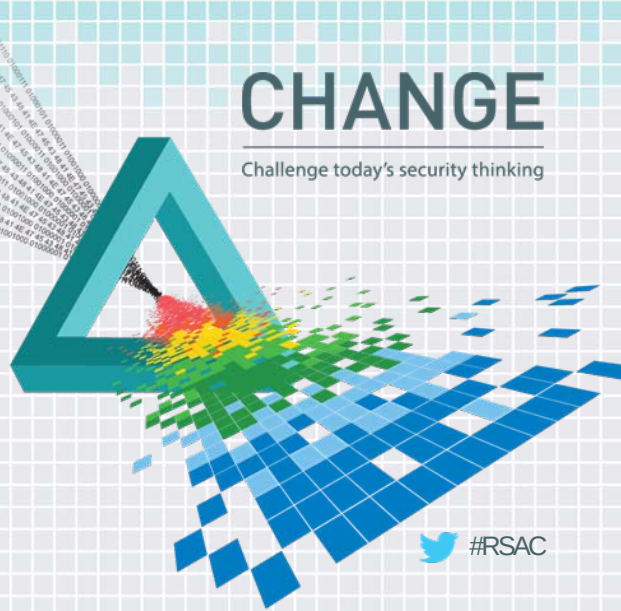
RSAConference2015
San Francisco | April 20-24 | Moscone Center



SESSION ID: LAW-T08

I Was Attacked by My Power Supply: A Mock Trial

Steven W. Teppler, *Esquire*
Abbott Law Group, P.A.

Lauren X. Topelsohn
Mandelbaum Salsburg

Hoyt L. Kesterson II
Terra Verde

Eric Hibbard
Hitachi Data Systems

Honorable John M. Facciola
U.S. Magistrate Judge *(ret.)*

Agenda for the mock hearing

We lay our scene

Summary of what has gone before

Call to order

Oral argument

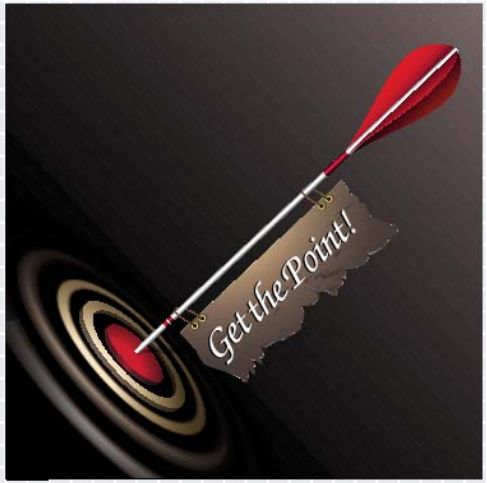
Decision and commentary by
Judge Facciola

We lay our scene

The Villain

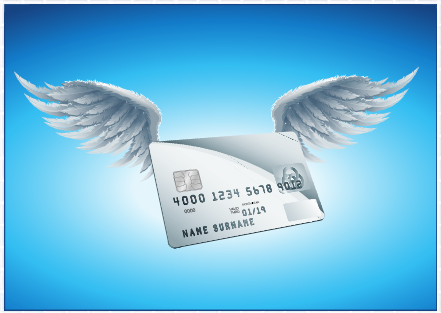
UPisUS

power to the people



Get The Point

purveyor of pointy objects



A Villain Enters *stage left*

- UPisUS, headquartered in the Netherlands with the operations center in Belgium, doesn't handle credit cards.
- It doesn't keep its software up to date either.
- A known, but unpatched, vulnerability is exploited by Snidely Whiplash, a known villain.
- Snidely installs a program into UPisUS systems that he manages from afar.
- He discovers the authentication credentials that UPisUS uses to remotely access the environments of its clients to enable updating the software of its product.
- He attempts to connects into each of the systems of those clients and succeeds with Get The Point, a company headquartered in Sherwood, Arkansas.
- He installs scraping software in each point-of-sale system in each store worldwide.
- Fly away little credit cards, fly away.

Lawyers Appear *center stage*

- Get The Point spends 148 million dollars for investigation, notification, and corrective actions.
- It suffers a drop of 18% in consumer revenue.
- It engages the law firm of Everdeen & Snow to seek damages.
- E&S filed a lawsuit against UpisUS in federal court in the Northern District of California claiming that UPisUS was negligent in that it allowed its systems to be used as a platform for an attack against Get The Point.
- It seeks to recover the cost of investigation, notification, and corrective actions and recover the loss of revenue, $300 million in total.

What is discovered

An intrepid assessor and US citizen had been hired as a consultant working under an NDA…

…to perform a risk analysis, including a security vulnerability assessment, for UPisUS at their request a year prior to the incident. At the Operations Center in Belgium he interviews staff about their backgrounds and duties; observes staff performing their duties; and conducts tests.

He delivers the only copy of the report to UPisUS headquarters in the Netherlands.

What has been illuminated

- The CIO of Get The Point has admitted during his deposition that the following controls mandated by the PCI Data Security Standard were not in place:
  - Get The Point should have only allowed UPisUS to connect to Get The Point's systems after UPisUS's request was approved by Get the Point.
  - Get The Point should have monitored all actions initiated by UPisUS while the connection is in place.

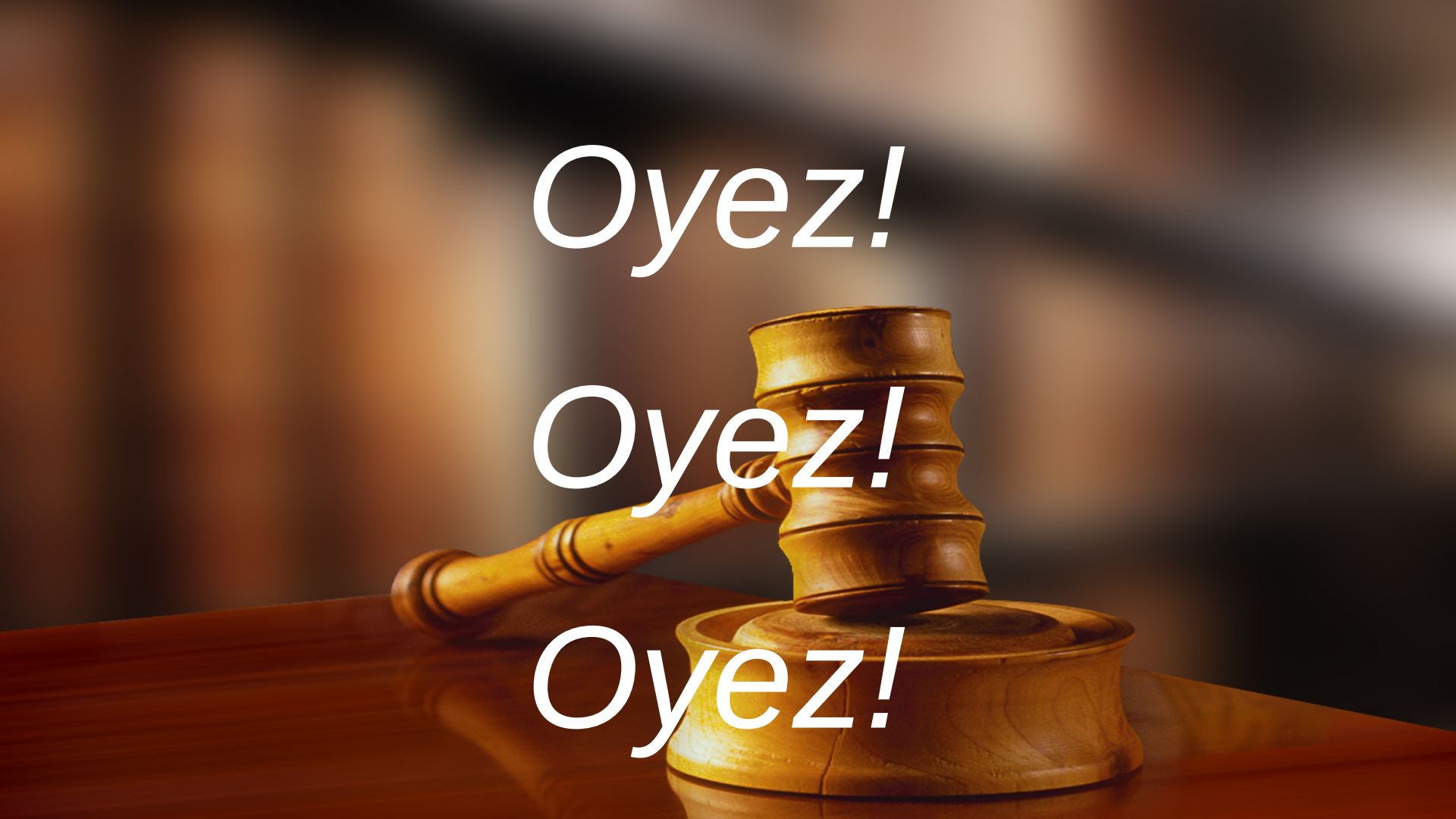
Mise en scène

- Plaintiff wants that report
- Defendant refuses to produce citing EU regulations forbidding it
- Plaintiff subpoenas the US resident consultant
- Defendant files a motion to quash the subpoena.
- Plaintiff files a cross motion to compel with the intent of making the consultant reveal the contents of the report.

The report

Dramatis Personæ

- United States Magistrate Judge John M. Facciola
  - Sitting by designation
- Steven W. Teppler, *Esquire*
  - Retained counsel for Get The Point
- Lauren X. Topelsohn, *Esquire*
  - Retained counsel for UPisUS
- Eric Hibbard
  - A security consultant who performed an assessment on UPisUS
- Hoyt L. Kesterson II
  - Greek Chorus


Oyez!
Oyez!
Oyez!

Post hearing discussion with Judge Facciola

- Discussion with the judge's law clerks—what should his ruling be?
- Judge Facciola's instructions

Hon. John M. Facciola
U.S. Magistrate Judge (ret.)
facciola@me.com

Steven W. Teppler, *Esquire*
Partner
Abbott Law Group, P.A.
steppler@abbottlawpa.com

Lauren X. Topelsohn, *Esquire*
Partner
Mandelbaum Salsburg
ltopelsohn@lawfirm.ms

Hoyt L. Kesterson II
Senior Security Architect
Terra Verde
hoyt.kesterson@tvrms.com

Eric Hibbard
CTO Privacy and Security
Hitachi Data Systems
eric.hibbard@hds.com