RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: LAW-F03

The Aftermath of a Breach: Best Practices for Working with Law Enforcement

MODERATOR: **Steve Ragan**

Senior Staff Writer
CSO
@SteveD3

PANELISTS:

Mitch Dembin
Federal Magistrate Judge
US District Court

Brian Coleman
Senior Manager of Computer Forensics
Pfizer

Edward McAndrew

Cybercrime Specialist
Ballard Spahr

#RSAC

The ever-present breach

- 43 percent of organizations surveyed in 2014 suffered a data breach.
- The average total cost of a data breach is $6.5 million.

USA TODAY

VTech data breach impacts 5 million accounts

KrebsonSecurity
In-depth security news and investigation

Data Breach at Health Insurer Anthem Could Impact Millions

CNN

Target settles for $39 million over data breach

Discovering the breach

- Your organization is notified by law enforcement that is has been breached *or*
- Your organization discovers its been breached.
  - What's the difference?
  - How does it influence your response?
  - What should you do next?
  - What type of information should you prepare to share with law enforcement?
- Inside versus external threats

You've been contacted by law enforcement

- What next?
  - Do you have incident response plan?
  - Review your post-attack plan of action
- Keep detailed records for law enforcement
- What types of information does law enforcement need/ want?

You discover you've been breached

- Capture the extent of the damage
- Take steps to minimize additional damage
- Notify law enforcement
- Work with law enforcement to contact other potential victims

Lessons from the OPM breach

- Post-breach response
- Private versus public organizations

THE WALL STREET JOURNAL.

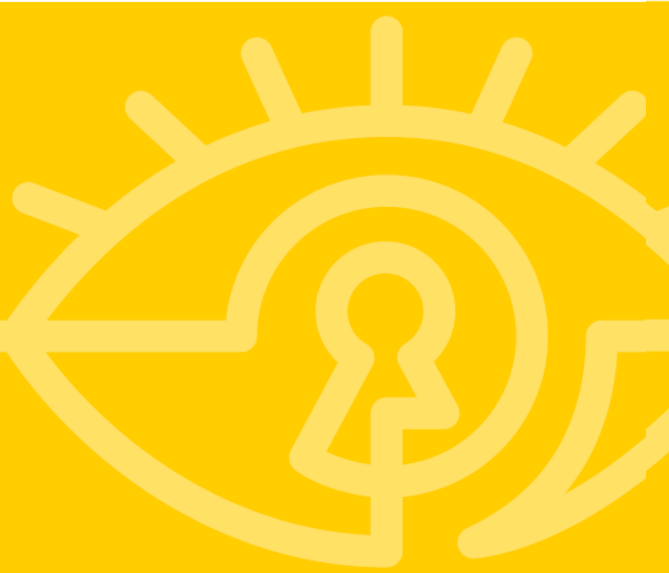
OPM Breach Was Enormous, FBI Director Says

USA TODAY

OPM hack raises questions about security of government contractors

The New York Times

Hackers Took Fingerprints of 5.6 Million U.S. Workers, Government Says



Building relationships

Subhead if needed