

WAKING UP THE C-SUITE TO PRIVACY AND SECURITY RISKS

Daniel J. Solove

**John Marshall Harlan Research Professor of Law
George Washington University Law School**

President & CEO, TeachPrivacy



CRISIS

Ad



30-YR FIXED MORTGAGE

3.875% RATE **1.000** POINTS **4.062%** APR

60 Day **FREE** Rate Lock

Rates current as of 9/10/2014

LEARN MORE

Morning Mix

Chinese hackers may have stolen your medical records




Capital One **BANK MOBILE**

START SAVING

Member FDIC

BANK ANYWHERE



By **Gail Sullivan** August 19   Follow @g_forcewinds

Chinese hackers have stolen medical records for 4.5 million patients, according to a regulatory



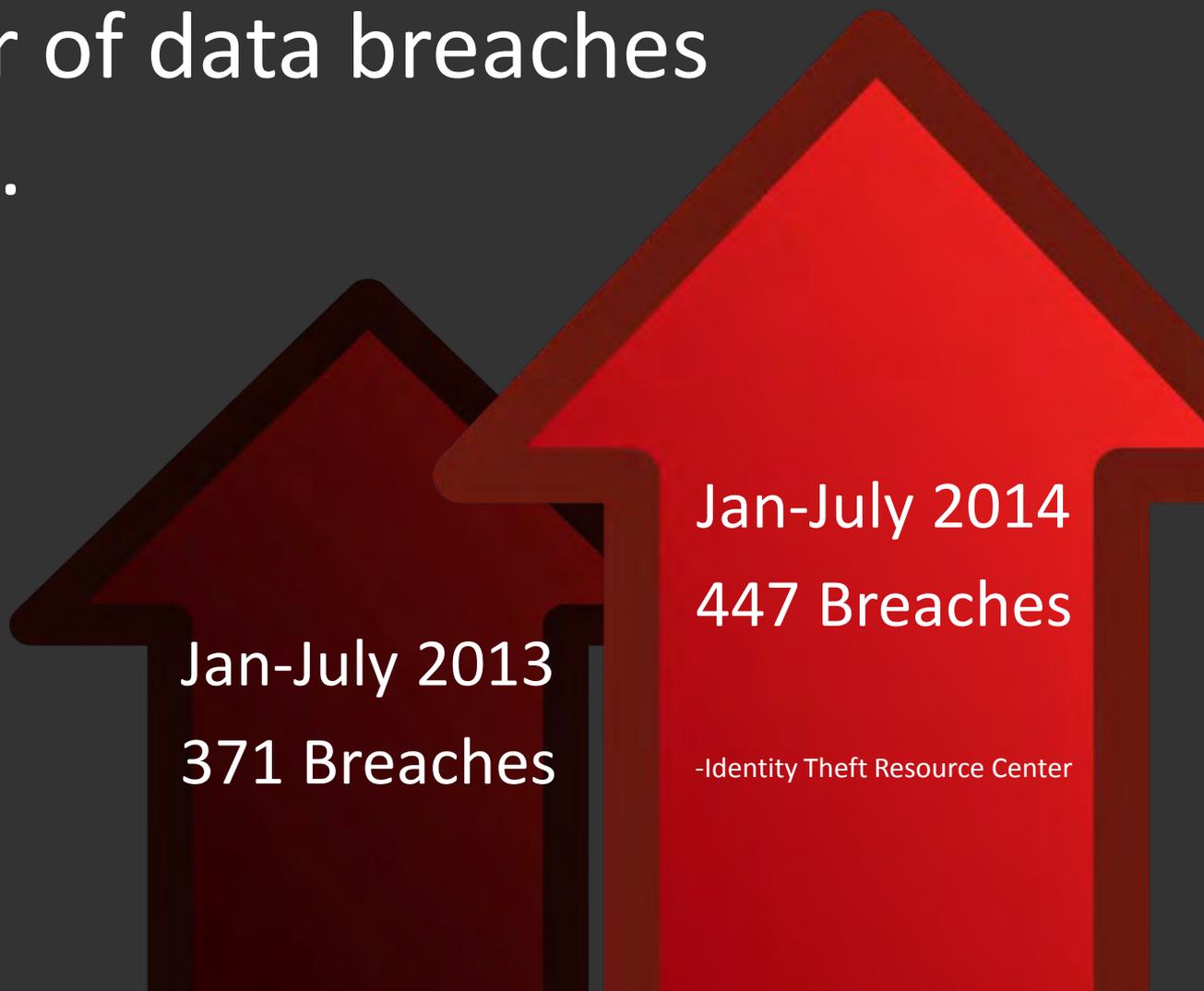
Advertisement



PENFED

Your "home" for mortgages

The number of data breaches keeps rising.



Data breaches cost healthcare institutions \$5.6 billion

90% had 1 breach within the past 2 years

38% had more than 5 breaches within the past 2 years

The C-Suite must understand the risks, the law, and the importance of compliance.



The workforce must know how
to protect PHI.



THE C-SUITE MUST CARE



THE WORKFORCE MUST BE AWARE



DATA PROTECTION MUST BE
FELT IN THE
BONES
OF AN ORGANIZATION



WAKING UP THE C-SUITE

The C-Suite doesn't fully appreciate the risks

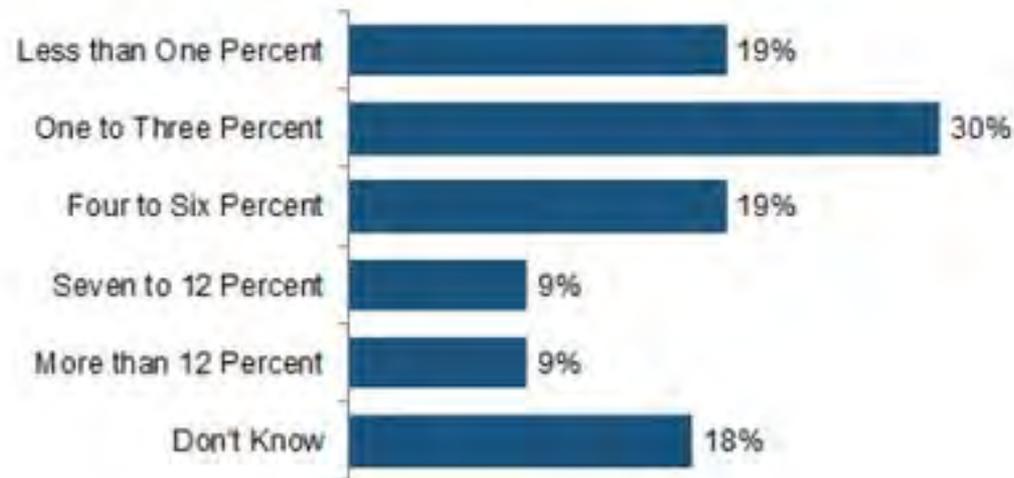


Needs a better understanding of the law

Some troubling facts...

- **Only 32%** of IT practitioners believe companies are “vigilant in protecting regulated data on mobile devices.”
- **1/3** of IT security teams never speak to company executives about data security.
- **Just 52%** of healthcare organizations have a full-time resource for security.

Percent of IT Budget Dedicated to Information Security









MONEY

Privacy and security risks are costly!

- Target's profit dropped from **\$961 million** to **\$520 million** in the same quarter after the breach.
- Target could face fines of between **\$400 million** to **\$1.1 billion**.



Lawsuits keep coming – Settlements can be substantial.

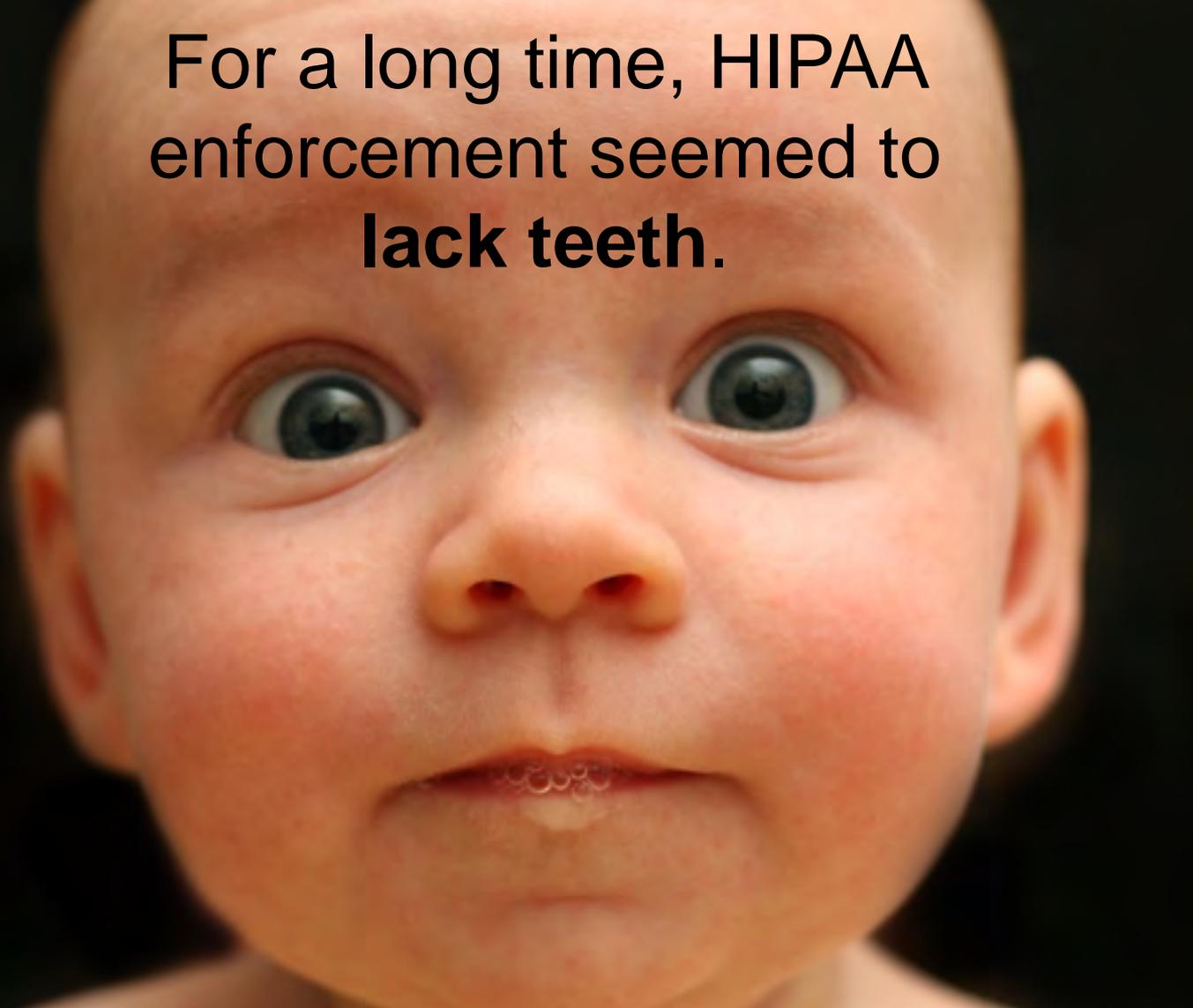
Settlement rates hover
around 50%.

Average settlement is
\$2,500 per plaintiff.





HIPAA



For a long time, HIPAA
enforcement seemed to
lack teeth.



HIPAA enforcement post-HITECH

problems
contracting with
covered entities
and other
business
associates





privacy and security training that makes people remember and care

Fines can be up
to \$1.5 million
per provision of
HIPAA violated.

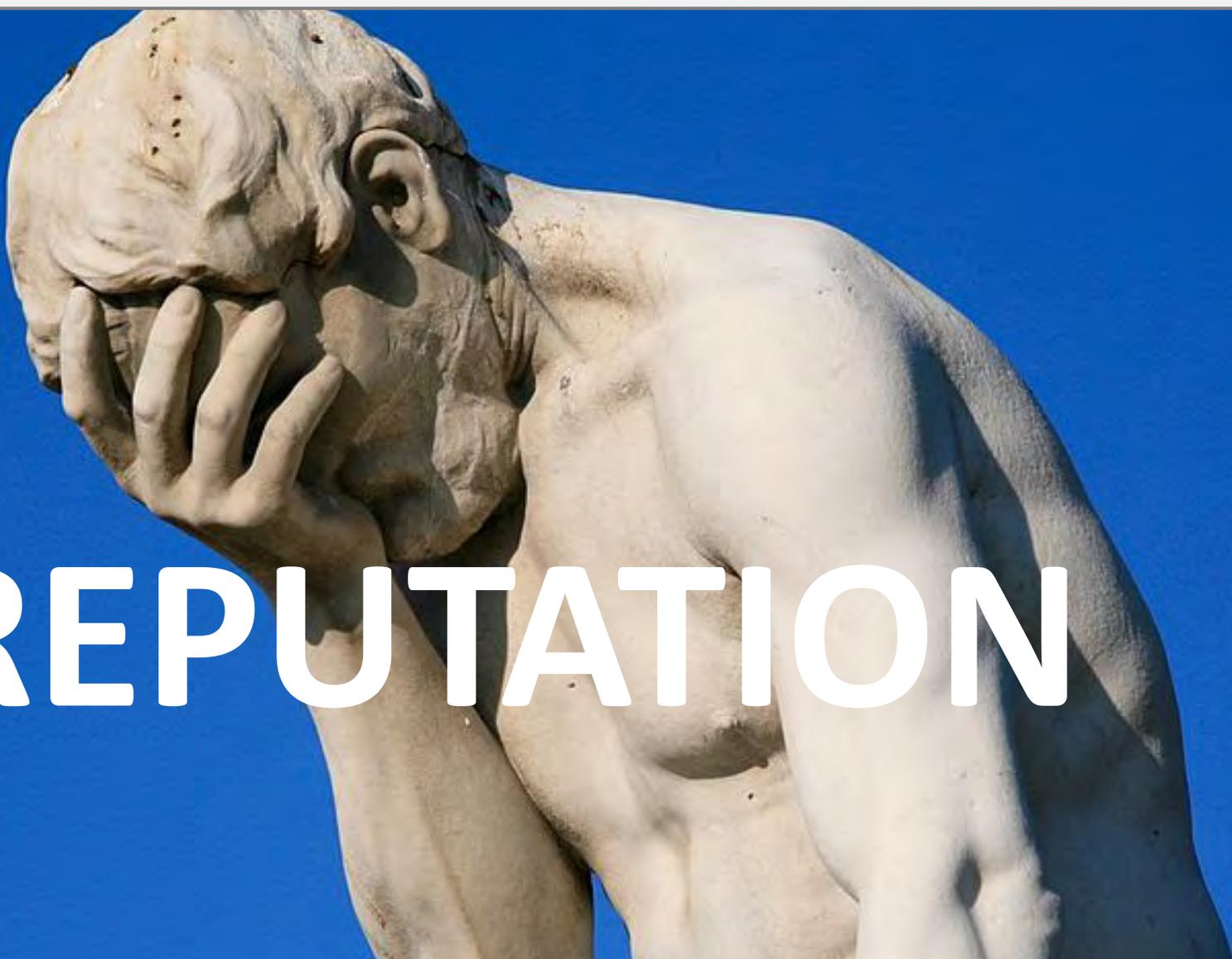


TIME





**Incidents take
time and attention.**



REPUTATION



THE WALL OF SHAME

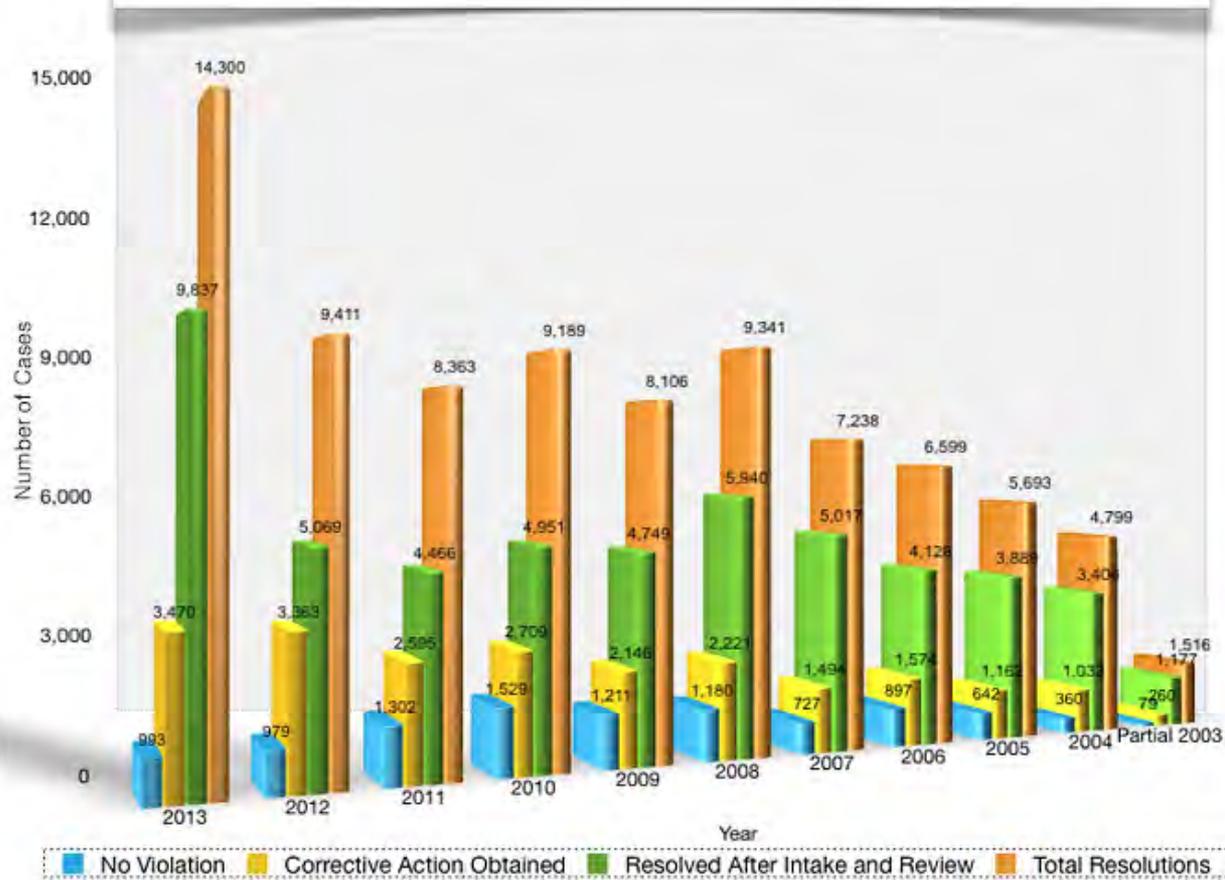
**The cost of incidents is
INCREASING**

**Enforcement is
INCREASING**



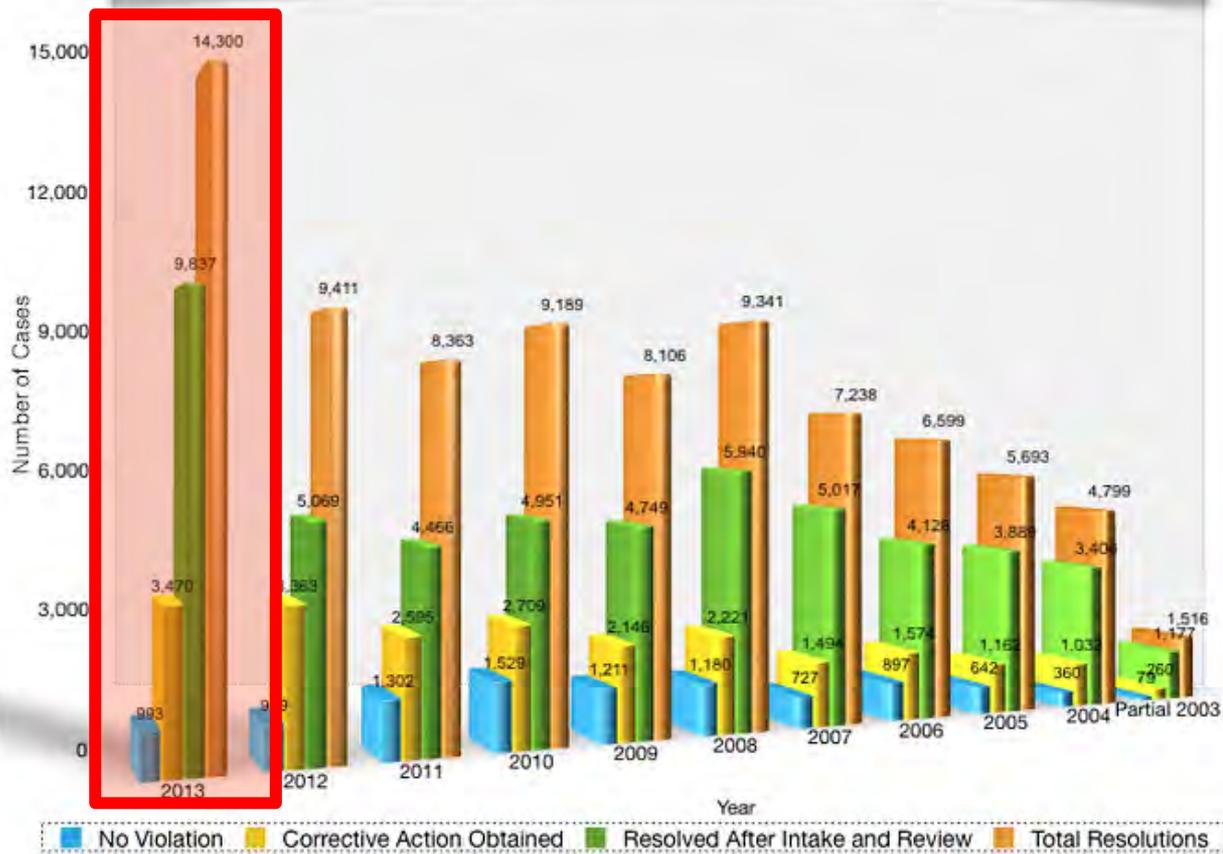
Resolutions by Year and Type

April 14, 2003 through December 31, 2013



Resolutions by Year and Type

April 14, 2003 through December 31, 2013



Data Breach Notification Laws

- 47 States plus DC.
- Law differ significantly and change frequently.
- States are raising fines, shortening notification times, and making notifications more likely.



The law is
ratcheting up the
pain.

THE C-SUITE MUST CARE



THE WORKFORCE MUST BE AWARE





The Workforce is the biggest security threat.

90% of malware requires a human interaction to infect.

Employees who don't receive training engage in risky data security practices.

- 33% of workers use the same password for work and personal devices.
- 35% have clicked on email links from unknown senders.
- 59% have stored work information in the cloud.



All it takes is
ONE
person



**How do you control
human behavior?**



**Impose
more
control?**

Awareness and Training



If you can't *force* them to do the right thing,
then you must *teach* them to do the right thing.



56% of employees don't receive any data security awareness training.

And a lot of existing training isn't very effective.



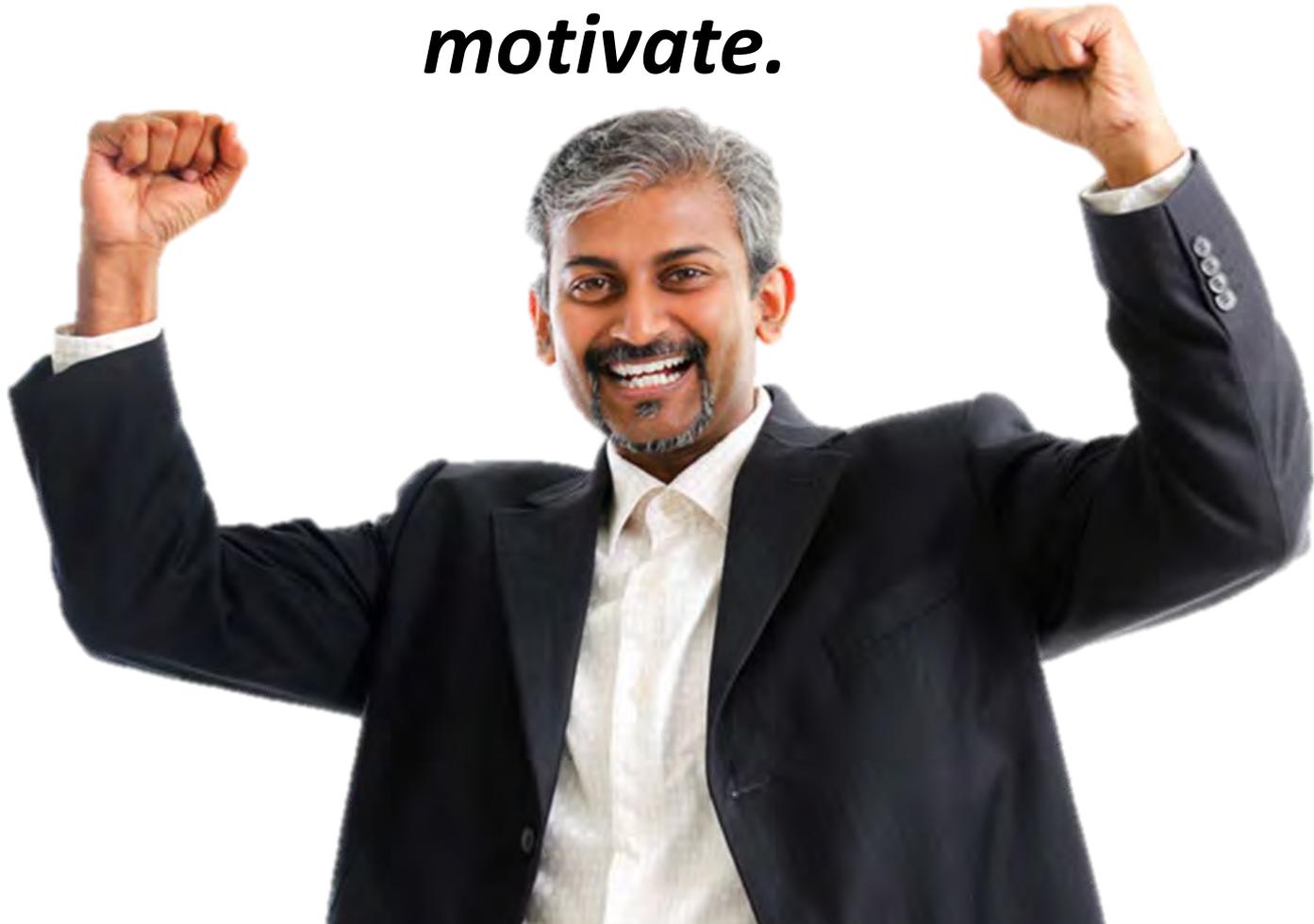
Use stories.





Training should make an emotional connection.

**Training should not just educate, but
*motivate.***







**Preventative medicine
works for health
and also for data.**



Scholarship

<http://danielsolove.com>

LinkedIn INfluencer Blog

<https://www.linkedin.com/today/author/2259773>

Privacy/Security Training

<http://teachprivacy.com>