COMPLIANCE WEEK WEST

NOV 14-15 2013 ROSEWOOD SAND HILL MENLO PARK CA

THE INTERSECTION OF ETHICS, COMPLIANCE, PRIVACY & BIG DATA

#CWWEST13

Recovering From a Privacy Breach

Kirsten Daru, Head of Global Privacy, Electronic Arts

Jacki Monson, Chief Privacy Officer, Sutter Health

Andrea White, Chief Compliance Counsel & Privacy Officer, Toyota USA

Moderated by **Joseph McCafferty**, Executive Editor, Compliance Week

COMPLIANCE WEEK WEST

NOV 14-15 2013 ROSEWOOD SAND HILL MENLO PARK CA

Two Factors Of Preparation

Preparation for a data breach requires both knowledge of the law and *good business sense*.

Breach Notification Laws: Did you know?

- Acquisition of a user's first initial and last name plus DOB, alone, can result in affirmative obligation to notify.

- California law will change as of January 1, imposing an affirmative duty to notify upon unauthorized access to usernames and passwords.

The Element of Business Sense

What are you going to do if the law doesn't require notification but…

- Contractual obligations require that you notify a partner?
- Some laws require notification and others don't?
- There's some risk of harm (economic or reputational) to your consumers or employees, or notification is just the right thing to do.
- The threat landscape is such that disclosure is beneficial to industry or even your own company?

In the event of a crisis, is there anything else you can do to protect your consumers and employees other than tell them what happened?

You have the elements down. **Now what?**

- Create a comprehensive data breach response plan.

It's more than documenting the two foregoing elements of preparedness.

- Contract in advance with a seasoned data breach response firm.

EA's Plan In Action: April through June 2011

June 14, 2011: EA's Turn

18,000 Accounts Compromised

EA was able to reset passwords and send detailed notifications to all 18,000 affected consumers, train customer support advisers and take down the affected forums…

In less than one day.

Why send notifications?

- Legal Obligation?
- Landscape? PR Risk?
- Harm to Consumers?

Jacki Monson
Chief Privacy Officer
Sutter Health

COMPLIANCE WEEK WEST
NOV 14-15 2013 ROSEWOOD SAND HILL MENLO PARK CA

Sutter Health at a Glance

Sutter Health
We Plus You

Serving more than 100 communities:

- 5,000 physicians (Physician medical foundation model; plus 4 IPAs)
  - Aligned under Sutter Medical Network
- 24 acute care hospitals
- More than two dozen surgery centers
- Approximately 47,000 employees
- $9.6 billion in revenues (2012)
- Home health, hospice, long-term care
- Health care research, development and dissemination program
- Medical education/training
- 24 fundraising organizations

Lessons Learned

- Unencrypted desktop stolen with 4 million patients' information.
- Patient data found during an unrelated law enforcement investigation.

Response to Privacy Incident

- Keep Calm
- Incident Response Plan & Team
  - Key individuals: Communications/PR, Legal, HR, Physical Security, Information Security, eDiscovery, Compliance, Business Owners, Risk
- Complete Thorough Investigation to Obtain Accurate Facts
- Cyber Insurance Policy

Response to Privacy Incident

- Outside Counsel
- Notification to Regulators/Media
- Corrective Action Plans
- Vendor Selected/Agreements in Place

Learnings

- Complete Indemnification in Business Associate Agreements
- Managing the Message
- Key Vendors / Contracts Lined Up
  - Forensics
  - Identity Theft Insurance
  - Call Center – Escalated Process / FAQs
  - Privacy Investigator
  - Outside Counsel
- Keeping Leadership and Governance Committees Updated and Involved

Andrea White

Chief Compliance Counsel & Privacy Officer
Toyota USA

COMPLIANCE WEEK WEST

NOV 14-15 2013 ROSEWOOD SAND HILL MENLO PARK CA

Privacy Breach – A Case Study

Toyota and "Vendor X"

What is your

WORST NIGHTMARE?

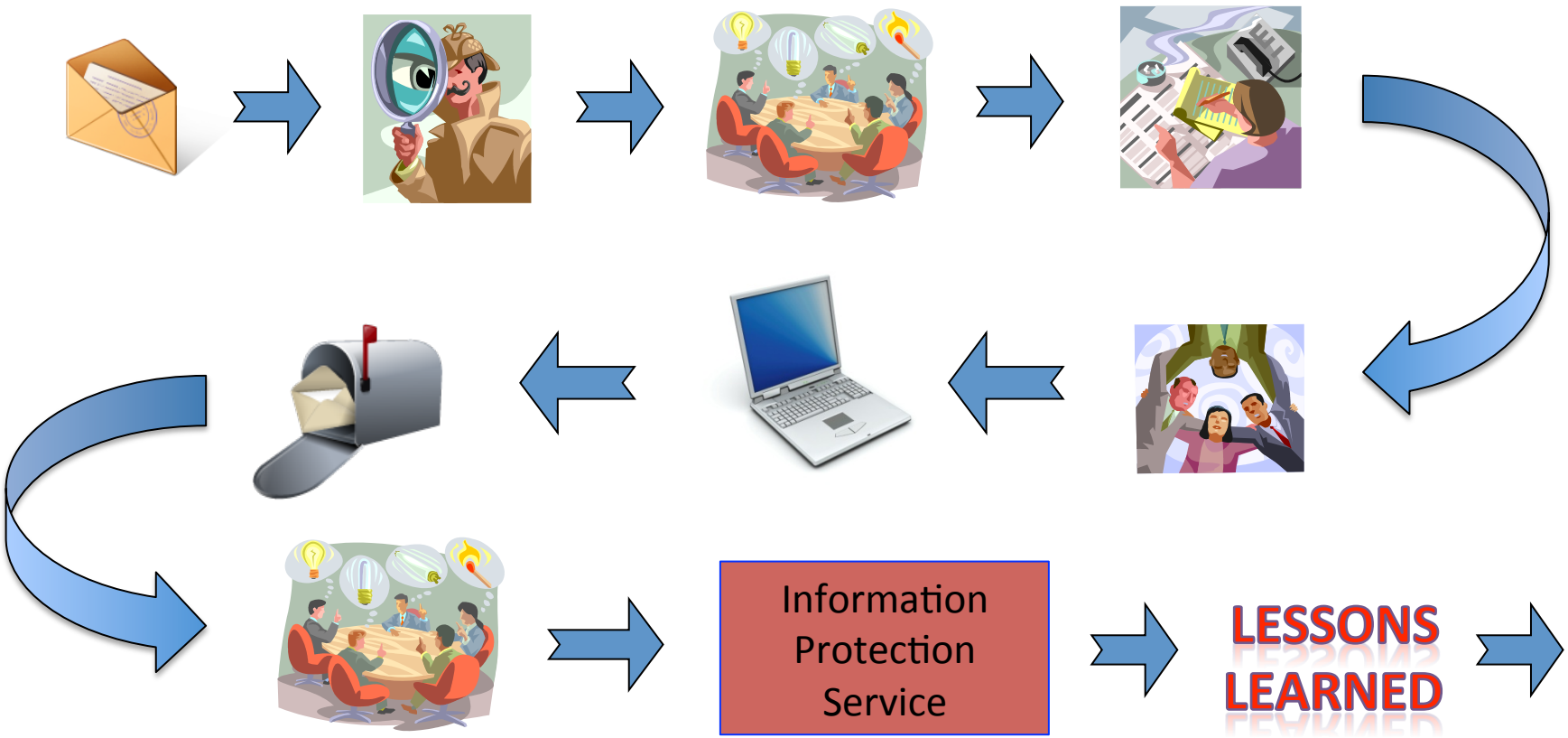
Privacy Breach – A Case Study

November 2008

Paraphrased:

"Dear Sir & Madame, we are holding information on all of your Associates that can be found in **Vendor X's database**. The information includes **Social Security Numbers and health information**. We have enclosed a sampling of the information in our possession. Please kindly remit the sum of $X to the following bank account:_____ in order to avoid any adverse consequences. Signed, "***The Villains***"

Privacy Breach – A Case Study



Privacy Breach – A Case Study

CHECK YOUR CONTRACT, DHA, MSA, ETC.!!!

- Make sure it includes clear provisions regarding the following:
  - Data Ownership
  - Immediate notification to your company of any suspected breach
  - Investigation involvement (including the right to communicate with any law enforcement agencies involved)
  - Vendor follow YOUR lead relative to notification activities (and to reimburse you out of pocket expenses for your notification costs)
  - Depending on your customer/employee approach – require reimbursement for reasonable identity protection services for all impacted individuals