

REUTERS/Eloy Alonso

Information Security – Read the news, don't make the news

October 3, 2015

Ellen Kroehler – VP, Information Security Risk Management
Thomson Reuters – Legal

© 2015 Thomson Reuters.

This is an informational and educational report distributed by the International Municipal Lawyers Association during its 2015 Annual Conference, held October 3-7, 2015 in Las Vegas, NV. IMLA assumes no responsibility for the policies or positions presented in the report or for the presentation of its contents.

THOMSON REUTERS

What is your most embarrassing moment?

"Wardrobe Malfunction" at the Super Bowl in 2004

Oscars, 2013, Best Actress Award

Now think about it in terms of information security.

Many industries were impacted and had their "moments":

- Retail
- Government
- Health
- Financial
- Food/restaurants

Read the news, don’t make the news
Agenda – Start with the basics

- Know your data
- Proactive measures
- Reactive measures

Know your data

What should you protect?

- Classify your data
  - Data classification system
  - What type of data do you have (sensitive, confidential, public)?
- Know where your data is
  - On your premise/your data center
  - At third-party data center
  - Neither?
- Know where your data flows
  - Data doesn't typically just sit in one database



Proactive measures to protect your data

"But I don't have enough budget…." Do the basics!

- Lock the front door
  - Lock down your network (firewalls, secure wireless/guest access, network segregation)
  - Encrypt sensitive data (at rest and in transit)
  - Be compliant (depending on what type of data, PCI)
- Lock the back door
  - Get a baseline – self assessment compared to ISO standards, hire an ethical hacker to do a manual penetration test, do a risk assessment
  - Security Awareness training
- Lock the windows
  - Prioritize and remediate what you find from your baseline



Reactive measures

It's going to happen - be prepared

- Statistics on data breaches
- Have an Incident response plan
  - Practice it
  - Roles: who's doing what/when
  - Communication plan
- Here's what the IT guys are doing:
  - Verify
  - Containment & mitigation
  - Investigate & analysis



What can you do?

Getting started today

- Think like a hacker – what do they want of yours
- Ask your IT partner
  - What are we doing?
  - What should we be doing?
- Protect yourself/your PC – strong passwords, change your passwords, don't click on that link, don't give out your credentials, encrypt your data

Summary

- Know your data
- Put in reasonable proactive measures
- Have an incident response plan