



**OTA**  
Online Trust Alliance

# 2012 Data Protection & Breach Readiness Guide

Webinar Jan 25, 2012

**Tim Rohrbaugh**  
CSO  
Intersections Inc.

**Michelle Kisloff**  
Partner  
Hogan Lovells, LLP

**Craig Spiegle**  
Executive Director  
Online Trust Alliance



LEARN • INNOVATE • COLLABORATE

## Agenda

---

- OTA Overview
- 2011 Data Loss Highlights
- OTA Laws of Data
- Security & Privacy by Design
- Fundamentals of a Plan
- Additional Best Practices



© 2012 All rights reserved. Online Trust Alliance (OTA)

Slide 2

LEARN • INNOVATE • COLLABORATE

# OTA Mission

- To develop and advocate best practices and public policy which mitigate emerging privacy, identity and security threats to online services, brands, government, organizations and consumers

*enhancing online trust and confidence,  
innovation and the vitality of commerce.*



© 2012 All rights reserved. Online Trust Alliance (OTA)

Slide 3

LEARN • INNOVATE • COLLABORATE

# Public / Private Collaboration



© 2012 All rights reserved. Online Trust Alliance (OTA)

Slide 4

LEARN • INNOVATE • COLLABORATE

# 2011 Data Breach Highlights

---

- 558 breaches
- 126 million records
- 76% server exploits
- 92% avoidable
- \$318 cost per record
- \$7.2 million average cost of each breach
- \$6.5 billion impact to U.S. businesses

(See pages 4-6)

© 2012 All rights reserved. Online Trust Alliance (OTA)

Slide 5



LEARN • INNOVATE • COLLABORATE

# Recent Headlines

---

- A EU proposal to simplify and toughen data-protection rules will require companies to disclose breaches within 24 hours
- 97% of data breaches worldwide are due to SQL injections, according to Barclaycard.
- "Data breaches have become a statistical certainty"
- "You need the trust of customers to build a successful business..." said Stefan Gross-Selbeck, CEO, Xing AG

## References

<http://www.bloomberg.com/news/2012-01-22/eu-s-reding-says-users-to-be-told-of-data-hacks-within-24-hours.html>

<http://news.techworld.com/security/3331283/barclays-97-percent-of-data-breaches-still-due-sql-injection/>

© 2012 All rights reserved. Online Trust Alliance (OTA)

Slide 6



LEARN • INNOVATE • COLLABORATE

# What do they have in common?

© 2012 All rights reserved. Online Trust Alliance (OTA) Slide 7

LEARN • INNOVATE • COLLABORATE

© 2012 All rights reserved. Online Trust Alliance (OTA) Slide 8

## Why Care?

---

- “We have spent over 12 years building our reputation and trust. It is painful to see us take so many steps back due to a single incident”  
*said Zappos CEO Tony Hsieh*

© 2012 All rights reserved. Online Trust Alliance (OTA)

Slide 9



LEARN • INNOVATE • COLLABORATE

## Why Care?

---

### What has changed?

- Data driven economy – “Big Data”
- Multi-Channel & blurring of on & off-line data.
- Evolving definitions of PII and coverage information.
- Complexity and dynamic regulatory environment.
- Reliance of service providers & cloud services.
- Shift from a PC centric to users with multiple devices
- Increased sophistication of the cyber-criminal

© 2012 All rights reserved. Online Trust Alliance (OTA)

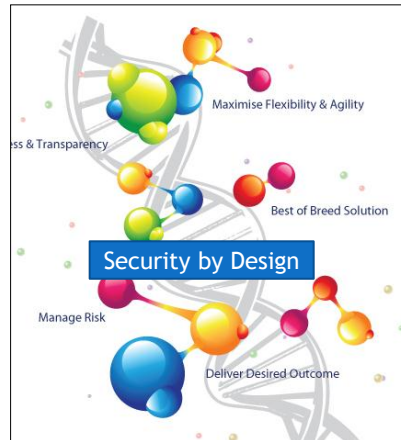
Slide 10



LEARN • INNOVATE • COLLABORATE

# Law of Data & Security by Design

- Needs to be part of your corporate culture (DNA)
- Fundamental truths:
  - Your data contains sensitive and private data.
  - Data protection is everyone's responsibility.
  - You will incur a data incident.
  - You fall under one of more regulatory agencies.
  - An incident can have a significant impact



© 2012 All rights reserved. Online Trust Alliance (OTA)

Slide 11



LEARN • INNOVATE • COLLABORATE

# Critical Elements

- Inventory & Risk Assessment
- Data Governance, Minimization & Prevention
- Incident Response Planning
- Training, Testing & Continuous Improvement

© 2012 All rights reserved. Online Trust Alliance (OTA)

Slide 12



LEARN • INNOVATE • COLLABORATE



**OTA**  
Online Trust Alliance

# Step 1

## Risk Assessment

### Key Questions for Every Executive

(See pages 6-7)

© 2012 All rights reserved. Online Trust Alliance (OTA)

Slide 13



**OTA**  
Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

## Risk Assessment

1. Do you know what sensitive information is maintained by your company, where it is stored and how it is kept secure?
2. Do you have an incident response team in place ready to respond 24/7?
3. Are you up-to-date with all of the regulatory & legal reporting requirements (*including partners / customers*)?

© 2012 All rights reserved. Online Trust Alliance (OTA)

Slide 14



**OTA**  
Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

# Risk Assessment

---

4. Have you completed a privacy and security audit of all data collection activities including cloud and outsourced services?
5. Are you prepared to communicate to customers, partners and stockholders?
6. Do you have readily available access codes and credentials to critical systems in the event key staff are not available or are incapacitated?

# Risk Assessment

---

7. Are employees trained and prepared to notify management in the case of accidental data loss or a malicious attack?

Do your policies require notification to management?

Are employees reluctant to report such incidents for fear of disciplinary action or termination?

# Risk Assessment

---

8. Have you coordinated with all necessary departments with respect to breach readiness?
9. Do you have a privacy review and audit system in place for third-party service providers? Have you taken necessary or reasonable steps to protect users' confidential data?
10. Do you review the plan on a regular basis to reflect key changes?



## Elements of a Data Protection & Breach Readiness Plan



# Data Governance & Prevention

---

1. Data Classification
2. Audit & Validate Access
3. Forensics, Instruction Analysis & Auditing
4. Data Loss Prevention - Best Practices
5. Data Minimization
6. Data Destruction
7. Inventory System Access & Credentials

(See pages 7-11)

© 2012 All rights reserved. Online Trust Alliance (OTA)

Slide 19



LEARN • INNOVATE • COLLABORATE

# Incident Response Planning

---

8. Creating an Incident Response Plan
9. Establishing vendor & law enforcement relationships
10. Creating a project plan
11. Define Notification Requirements
12. Draft communications
13. Assistance & Remedies

(See pages 12-16)

© 2012 All rights reserved. Online Trust Alliance (OTA)

Slide 20



LEARN • INNOVATE • COLLABORATE

# Training, Testing & Budget

---

14. Employee Training
15. Analyze legal landscape
16. Funding & budgeting
17. Ongoing critique and post mortem analysis

(See pages 16-17)

© 2012 All rights reserved. Online Trust Alliance (OTA)

Slide 21



LEARN • INNOVATE • COLLABORATE

# #18 Technical Remedies

---

1. Require approved browsers for all employees & partners
2. Adopt both SPF and DKIM (inbound & outbound)
3. Encrypt files which are transmitted externally or stored on portable devices / media
4. Upgrade to Always On SSL & EV SSL certificates
5. Password Management
6. Enable automatic patch management
7. Monitor third-party code, links and advertising
8. Enable encryption on routers and access points
9. Domain Name System Security Extension (DNSSEC).
10. Move to consumer centric data privacy statements

(See page 18)

© 2012 All rights reserved. Online Trust Alliance (OTA)

Slide 22



LEARN • INNOVATE • COLLABORATE



**OTA**  
Online Trust Alliance

## Regulatory Landscape Update

**Michelle Kisloff**

Partner, Hogan Lovells, LLP



© 2012 All rights reserved. Online Trust Alliance (OTA)

Slide 23



**OTA**  
Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

## What has changed .....

- Broader call for data governance
- More aggressive lawsuits by State AG's
- Redefinition of what is PII & adequate notification
- Call for allowing for private right of action except for approved safe harbor program.
- Failure of business taking reasonable steps
- ESPs & Ad supply chain being exploited (Malvertising compromised)

© 2012 All rights reserved. Online Trust Alliance (OTA)

Slide 24



**OTA**  
Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

# Data Breach Regulatory Update

---

- Call for National Breach Legislation
  - Senate Judiciary Chair Patrick Leahy (D-Vt.)
- Section 5 of the FTC Act
- Security & Exchange Commission
- Enforcement
- International Implications & Considerations

Reference:

<http://thehill.com/blogs/hillicon-valley/technology/206137-leahy-urges-congress-to-pass-data-breach-legislation>

(See pages 18)

© 2012 All rights reserved. Online Trust Alliance (OTA)

Slide 25



LEARN • INNOVATE • COLLABORATE

# EU Update

---



- [http://ec.europa.eu/justice/newsroom/data-protection/news/120125\\_en.htm](http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm)
- Proposal to simplify and toughen the region's data-protection rules will require companies to disclose data breaches within 24 hours.
  - Companies must inform the data protection authorities and the individuals concerned, and they must do so without undue delay.
  - Includes stricter sanctions to equip authorities to levy sanctions and fines, will "become a trademark people recognize and trust worldwide."
  - Will require "specific and explicit" consent to store information, and delete data unless there is a "legitimate and legally justified interest" to keep them on their servers.
  - Recommended Recap from Hogan Lovells  
<http://www.hldataprotection.com/2012/01/articles/international-eu-privacy/european-commission-releases-official-draft-of-groundbreaking-data-protection-regulation/index.html>

© 2012 All rights reserved. Online Trust Alliance (OTA)

Slide 26



LEARN • INNOVATE • COLLABORATE

## Summary – Key Principles

---

- Acknowledge the data you collect contains one or more forms of PII or sensitive data.
- Accept you will experience a data loss incident or breach.
- Understand your company falls under multiple government regulations requiring notice and remedies.
- Being unprepared can significantly add to the direct and indirect costs including management resources and lost productivity.
- A data incident can result in significant damage to your business's brand reputation.

© 2012 All rights reserved. Online Trust Alliance (OTA)

Slide 27



LEARN • INNOVATE • COLLABORATE

## Resources

---

- 2012 Data Protection & Breach Incident Planning  
<https://otalliance.org/breach.html>
- Online Trust Guidelines  
<https://otalliance.org/resources/principles.html>
- Anti-Malvertising - <https://otalliance.org/malvertising.html>
- Email Authentication  
<https://otalliance.org/resources/authentication/index.html>
- Browser Upgrades – <https://otalliance.org/browser>
- Privacy - <https://otalliance.org/resources/initiatives.html>
- [Staff@otalliance.org](mailto:Staff@otalliance.org) +1 425-455-7400

© 2012 All rights reserved. Online Trust Alliance (OTA)

Slide 28



LEARN • INNOVATE • COLLABORATE

## More Information

---

### **Michelle Kisloff**

Partner, Hogan Lovells, LLP

[michelle.kisloff AT hoganlovells.com](mailto:michelle.kisloff@hoganlovells.com)

### **Tim Rohrbaugh**

CSO, Intersections Inc

[Trohrbaugh AT intersections.com](mailto:Trohrbaugh@intersections.com)

### **Craig Spiezele**

Executive Director, Online Trust Alliance

[Craigs AT otalliance.org](mailto:Craigs@otalliance.org)

+ 1 425-455-7400

© 2010. All rights reserved. Online Trust Alliance (OTA)  
Slide 29



LEARN • INNOVATE • COLLABORATE

## Resources

---

- Slides & Recording will be posted on the OTA Member Site
- Feb 8 - Update on the European Union Cookie Directive
  - Justin Weiss, Sr. Director, International Privacy & Policy Yahoo!
- Feb 15 - State of Email Authentication and Evolving Standards – OTA Webinar
- Feb 16 - Planning for Failure: Data Breach Risk in the New Threat Landscape – *Webinar sponsored by Debix*
- Visit <https://otalliance.org/events/>

© 2012. All rights reserved. Online Trust Alliance (OTA)

Slide 30



LEARN • INNOVATE • COLLABORATE