2016 Data Protection & Breach Readiness Webinar Will Start Shortly

please download the guide at https://otalliance.org/breach

2016 Data Protection & Breach Readiness Guide
February 3, 2016

Craig Spiezle
Executive Director & President
Online Trust Alliance

Madelon Smith
VP, Strategic Initiatives
Online Trust Alliance

Jeff Wilbur
VP Marketing
Iconix
Who is OTA?

Mission to enhance online trust and empower users, while promoting innovation and the vitality of the internet.

- Goal to help educate businesses, policy makers and stakeholders while developing and advancing best practices and tools to enhance the protection of users' security, privacy and identity.
- Collaborative public-private partnerships, benchmark reporting, meaningful self-regulation and data stewardship.
- U.S. based 501(c)(3) tax-exempt charitable organization.
- Global focus & charter.
- Supported by dues, donations and grants.
2016 Breach Report Highlights

- 91% of 2015 breaches were preventable!
- Actionable advice to enhance data protection and to be prepared for a data loss incident
- Includes:
  - Summary of Key Learnings
  - Risk Assessment Guides
  - Security Best Practices
  - Forensics Do’s & Don'ts
  - Cyber Insurance Considerations
  - Law Enforcement Report Template
- [https://otalliance.org/breach](https://otalliance.org/breach)
Key Metrics* (page 8)

- 29% increase in publically disclosed breaches
- 91% of incidents could have been prevented
- 30% due to lack of internal employee controls
- Anthem led with 78.8 million records compromised
- $3.8 MM cost / breach
- $154 cost per record
- <50% have adequate cyber insurance coverage

* Analysis based on review of public breaches through 9/30/15.

What is “Preventable”?

- Not patching known / public vulnerabilities
- Misconfigured devices / servers
- Unencrypted data and/or keys disclosed
- End of life devices, operating systems and applications
- Employee errors
  - Lost data, files, drives, devices, computers
  - Accidental disclosure via email, posting on public sites
- Business Email Compromise & social exploits
The Realities of a Loss Incident
What We Have Learned? (page 10)

1. There needs to be a critical shift in attitude regarding roles and responsibilities of data stewardship and security.

2. Data is often a company’s most valuable asset requiring the appropriate level of protection.

3. The level of data security you apply must be commensurate with the data held.

4. Only collect and retain data that has a purpose.

What We Have Learned?

5. Everyone needs to consider the consequences of an incident and what could happen.

6. Security and privacy are not absolutes and must evolve.

7. Security and privacy is beyond your walls.

8. Being prepared is not just for Boy Scouts.
   - Needs to incorporate both planning and training to help prevent, detect, mitigate and respond.
   - Planning is the key to maintaining online trust and business continuity.
What is Your Risk Appetite?

Risk Assessment (pp. 11-13)

- Board, Officers & Investors
  - What is the worst-case scenario your “crown jewels” that could be compromised?

- Internal Operation Risk
  - Are your practices defendable?

- Cloud, Vendors & Service Providers
  - Who owns the relationship
  - Do you know who they are?
  - What are their notification triggers?
Learn From Mistakes of Others!

Laws of Data

• Your data includes “covered information”
• You have regulatory requirement(s)
• You will have a data incident
• If you are unprepared it will cost you
  ◦ Direct Expenses
  ◦ Remediation
  ◦ Partners
  ◦ Brand
  ◦ Business Shock
  ◦ Your Reputation
Security Best Practices (pp.14–16)

1. Encryption & Key Management
   - At rest, storage and in some cases “in use”
2. Password Management
3. Least privilege user access (LUA)
4. Security design and code reviews including penetration tests and vulnerability scans
5. Deploy multi-layered firewall protections
6. Authenticate on all mail servers
   - Outbound & inbound
   - SPF, DKIM & DMARC
   - Sub-domains, active & parked domains

Security Best Practices, cont’d

7. Mobile device (and IoT) management program
8. Continuous monitoring in real-time
   - SSL/TLS Configurations
   - Log reports
9. Web application firewalls
10. Permit only authorized wireless devices
11. Implement “https” EVERYWHERE
Security Best Practices, cont’d

12. Review server certificates for vulnerabilities
   • Consider Extended Validation Certs
   • Upgrade Domain Validated to Organizational Validated Certs

13. Develop, test and continually refine your response plan

14. Establish and manage a vulnerability / threat intelligence reporting program

Embrace Data Stewardship

© 2016 All rights reserved. Online Trust Alliance (OTA)
Plan Fundamentals (page 24)

- Create and Empower a Team
  - Designate First Responders
  - Create a Notification “Tree”
- Develop Law Enforcement Relationships
- Create Communication Templates
- Training
- Regulatory and Legal Review
- Cyber Insurance
- Testing, Critique and Refinement
Cyber Insurance – Realities (p. 30)

- Liability (defense costs, settlements, judgments)
- Incident response (including forensics, public relations, breach notification, credit monitoring)
- Loss/replacement of electronic data
- Expenses for cyber extortion
- Regulatory fines
- Business interruption, including lost revenue
- Areas for potential claims denial – negligence?

Communications (p. 34)

Know your audience
- Internal
- Key partners & customers
- Regulators
- Law enforcement,
- Impacted parties
- Press, media and analysts

4 T’s
- Tactic
- Tone
- Timing
- Technology
Remediation (page 35)

- Move beyond the minimum; it has been a race to the bottom.
- Consider ID theft counseling and “case managers”
- Partner with community based resources
- Benefits impacted parties, your reputation and the court!

Consumer Attitudes

"BETWEEN THE NSA, TARGET AND SEIMAN MARCUS, I'M WORRIED THERE WON'T BE ENOUGH OF MY IDENTITY LEFT TO STEAL."
Evolving Regulatory Landscape

• Where do the impacted parties now reside?
  • EU – Data Protection Directive
  • Canada
  • Australia
  • New Zealand

EU-US Privacy Shield

• Feb 2\textsuperscript{nd} the European Commission announced new agreement to replace Safe Harbour
  ▫ Strong obligations on companies handling Europeans' personal data, robust enforcement
  ▫ Safeguards and transparency obligations
  ▫ Effective protection of EU citizens' rights with redress
• EC drafting details over next few weeks
• Article 29 Working Group will review and comment
• US Dept of Commerce released statement of support
Regulatory Landscape (page 38)

- Opt-in v. Opt Out
- Honor “Do-Not-Track”
- Safe Harbor Provisions
- Reasonable Security
- Adequate Notice
- “Right to be Forgotten”
- Data Server Locations
- Definition of PII
- Government Access

Apply What You Have Learned

- **Next week you should:**
  - Identify data owners
  - Identify external service providers
  - Identify and connect law enforcement contacts

- **In the 90 days you should:**
  - Complete an internal & external assessment
  - Identify security & privacy investments
  - Identify forensics resources

- **In six months you should:**
  - Have an updated security & privacy roadmap
  - Make security & privacy part of your value position
  - Updated your response plan and employee review
Webinar Series – Starting March 9

- Security & Responsible Privacy Best Practices
- Cyber Insurance Considerations
  - Understanding the Landscape
- Risk Assessment Fundamentals
  - Internal & with Service / Cloud Providers
- Remediation Services & Considerations
- Breach Regulatory Landscape
- Working With Law Enforcement;
  - Before, During & After An Incident
- Cyber Forensics Realities; CSI or Mr. Robot?

Schedule @ https://otalliance.org/Breach

Resources & Tool

- UK Information Commissioner's Office
Summary of the Guide

- Executive Summary
- Risk Assessment
- Security Best Practices
- Data Lifecycle & Stewardship
- Incident Response Fundamentals
- Cyber Insurance Considerations
- Notification Requirements
- Training, Testing & Budgeting
- Regulatory Landscape
- Resources/Templates

More Information

- Join OTA [https://otalliance.org/membership](https://otalliance.org/membership)
- IoT Framework [https://otalliance.org/IoT](https://otalliance.org/IoT)
- Data Breach Readiness Guide [https://otalliance.org/breach](https://otalliance.org/breach)
- Contact us +1 425-455-7400 admin@otalliance.org
- Follow OTA on Twitter @otalliance