Technology, Threats, Turmoil, Tenacity & Trust

Craig Spiezle
Executive Director & President
Online Trust Alliance
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 Collaboration
Overview

- Challenges & Lesson Learned
- Prevention, Detection & Response
- Evolving Threats & Challenges
  - Malvertising
  - Business Email Compromises (BEC)
  - Ransomware
  - IoT
- Online Trust Audit

What Keeps Me Up

© 2016 All rights reserved. Online Trust Alliance (OTA)
What Keeps Me Up

- Mistrust in the privacy, security and the online experience are resulting in chilling effects.
- Need to move beyond compliance to stewardship.
- Inaction will stifle economic growth and the benefits to society at large.
- For Internet to thrive, users must trust their information will be secure and privacy respected.

Challenges & Realities

- Technology
- Threats
- Turmoil
- Tenacity
- Trust
Challenges

• Moving target
• Under resourced & funded
• Expanded scope of data loss incidents
• Evolution of cybercrime - Increased precision, decreasing a crime of opportunity
• Evolving Regulatory Landscape
• Beyond your 4 walls

The Realities

• 29% increase in publically disclosed breaches
• 93% of incidents could have been prevented
• 30% due to lack of internal employee controls
• <50% have adequate cyber insurance
• 47% increase in identity theft complaints
• Impact is not only financial or PII
  ◦ Cyber vandalism
  ◦ Hactavisim
  ◦ Social engineered exploits
  ◦ ACH withdraws
Learn From Mistakes of Others!

What We Have Learned?

1. Needs for a critical shift regarding roles
2. It is not about compliance!
3. Yesterdays approaches are often inadequate
4. Security and privacy is beyond your walls
Risk Assessment

- 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?

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
What is “Preventable”?

Data Stewardship Lifecycle
Data Collection Considerations

Data Management Fundamentals
The ABCs of a Response Plan

- 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

Communications

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

4 T’s
- Tactic
- Tone
- Timing
- Technology
Remediation

- 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!

Regulatory Landscape

- Opt-in v. Opt Out
- Honor “Do-Not-Track”
- Privacy Shield
- FTC / FCC
- Reasonable Security
- Adequate Notice
- “Right to be Forgotten”
- Data Server Locations
- Definition of PII
- Government Access
Cyber Insurance – Realities

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

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
Evolving Risks

- Increasing Threats & Challenges
  - Ransomware
  - Malvertising
  - IoT

Ran$omware

- Shift from Trojans
- No longer a crime of opportunity
- Increased precision and targeting via spear phishing and malvertising
- Beyond consumer data
  - Surge pricing
  - Doubling in demands; decreasing time to respond
  - Professional services, CPA, financial services, engineering firms
  - Proprietary & client data
Defense & Containment

- Implement Phishing / Social Engineering counter measures
- DMZ Hardening / Ongoing Port Scans
- Authenticate All Inbound email
- Block ads from critical systems
- Imped lateral movement and propagation
  - VLAN and subnet segmentation
  - Gateway /firewall segmentation
  - App blocking / whitelisting
  - Role base permission (least privilege)
- Offline backups

Malvertising

1. User visits a trusted website via a link, types the URL directly or uses their favorites
2. Ad tricks user / or auto downloads ("driveby") a program that installs malware
3. Captures & forwards data back to creator, turns into bots, installs ransomware and other
4. Used for identity theft, ACH fraud, account take over, corporate espionage and other crimes

All site visitors

Impact

Plus the reputation of advertisers, sites & brands
Increased Precision & Reach

Malicious advertising offers broad reach and quick rewards for malware perpetrators
Dynamic, expanding advertising scene opening juicy targets for Internet bandits

By John P. Mello Jr.
March 12, 2014 — CSO — A burgeoning and dynamic online advertising market is creating an abundance of opportunity for cyber criminals.

Advertising outstrips porn as top malware gateway
Porn is now the third leading threat vector, driving users to malware 16 per cent of the time

The IoT landscape

Samsung Fails To Secure Thousands Of SmartThings Homes From Thieves

ASUS Settles FTC Charges That Insecure Home Routers and “Cloud” Services Put Consumers’ Privacy At Risk

Nest to ‘brick’ working Revolv smart home hubs in May

Wearables, apps disclose user passwords and location: Symantec
Challenges - IoT Ecosystem

- Highly personal, dynamic, persistent collection and transfer of data
- Combination of devices, apps, platforms & services
- Data flows, touch points & disclosures
- Lack of defined standards
- **Sustainability**
  - Lifecycle Supportability
  - Data retention / ownership

Overview – IoT Trust Framework

- **Focus – Phase 1**
  - Connected Home
  - Wearables (Health & Fitness)
- **Code of Conduct**
  - Foundation for certification
- **30 Principles Addressing:**
  - Security
  - Privacy
  - Sustainability *from purchase to “end-of-life”*
Framework – 30 Baseline Criteria

<table>
<thead>
<tr>
<th>IoT Trust Framework</th>
<th>Required</th>
<th>Recommended</th>
<th>N/A – Not Applicable</th>
<th>Connected</th>
<th>Wearable</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECURITY</td>
<td></td>
<td></td>
<td></td>
<td>Home</td>
<td>Tech</td>
</tr>
<tr>
<td>1. Ensure devices support current generally accepted security transmission protocols. All personally identifiable data in transit and in storage must be encrypted using current generally accepted security standards. This is including but not limited to wired, Wi-Fi and Bluetooth connections.</td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. All authentication credentials, including but not limited to passwords shall be salted and hashed and/or encrypted.</td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. All IoT support websites must fully encrypt the user session. Current best practices include HTTPS or HTTP Strict Transport Security (HSTS) by default, also known as AOS SSL or Always On SSL.</td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. IoT support sites must implement regular monitoring and continual improvement of site security and server configurations to acceptably reduce the impact of vulnerabilities. Perform generally accepted penetration tests at least annually.</td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Establish and maintain processes and systems to receive, track and promptly respond to external vulnerabilities reports from third parties including the research community. Remediate post product release design vulnerabilities and threats in a publically responsible manner either through remote updates and/or through actionable consumer notifications, or other effective mechanism(s).</td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Major Sections Include:
- Security
- User Access & Credentials
- Privacy Transparency & Disclosures

IoT – Why You Need To Care

- Impact to industrial controls & critical infrastructure
- BYOB – Employee IoT devices Privacy & Data Collection Practices
- Long-Term Risks
Online Trust Audit

Objectives:

• Move from a “compliance” mindset to “stewardship”
• Recognize leadership brands, sites & apps that implement security and privacy practices protecting users’ data
• Incentivize businesses and developers to enhance their security, data protection and privacy practices
• Make security & privacy part of a brand’s value proposition
• Increase awareness and preference for best practices

Honor Roll Overview

• Audit of 1,000 web sites
  ◦ FDIC Banking 100
  ◦ Internet Retailer 500
  ◦ Top 100 Consumer Services
  ◦ Top 100 News/Media
  ◦ Top 100 Federal & State Gov’t
  ◦ OTA Members
  ◦ 2016 Presidential Candidates

• Scoring
  ◦ Up to 100 points in each category
  ◦ Bonus & Penalty points for
  ◦ Honor Roll = 80% of total points, 55% or better in each category

• Results to be released June 14th
Summary

- Mistrust in the privacy, security and the online experience are resulting in chilling effects.
- Need to move beyond compliance to stewardship.
- Inaction will stifle economic growth and the benefits to society at large.
- For Internet to thrive, users must trust their information will be secure and privacy respected.

More Information

- Data Breach Readiness Guide https://otalliance.org/breach
- Online Trust Honor Roll https://otalliance.org/HonorRoll
- IoT Framework https://otalliance.org/IoT
- Contact us
  - Craig Spiezle, Executive Director, craigs@otalliance.org
- Follow OTA on Twitter @otalliance