2017 Cyber Incident & Breach Readiness Webinar Will Start Shortly

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

Craig Spiezle
Executive Director & President
Online Trust Alliance

Jeff Wilbur
VP, Research
Online Trust Alliance
Vision

• To enhance online trust and empower users, while promoting innovation and the vitality of online services
  ▫ Accelerate the adoption of security enhancing standards, technologies and best practices
  ▫ Convene and embrace public-private partnerships and meaningful self-regulation and data stewardship.
  ▫ Educate businesses, policy makers and stakeholders while developing and advancing best practices
  ▫ Promote transparent and responsible privacy practices
  ▫ Benchmark reports and affirmation to orgs who “walk-the-talk”
  ▫ 501c3 charitable non-profit

Key Initiatives

• IoT Trust Framework – Set of Strategic Principles
  advancing privacy, security, safety & sustainability

• Online Trust Audit & Honor Roll
  recognizing leadership in consumer protection, data security and responsible privacy practices

• Vision for a Trustworthy Internet; email, advertising & IoT
“An ecosystem built on trust and innovation where benefits to society and commerce are realized by prioritizing security, privacy and safety.”

What is an Incident?

“Traditional consumer data breaches” plus...

- Unauthorized access to a system or device and its data,
- Unauthorized extraction, deletion or damage to any form of data,
- Disruption of availability and/or integrity of any business operation,
- Unauthorized activity causing financial or reputational harm
A Recent Incident

Sundance Hack Acts as a Warning to Small and Mid Sized Businesses

Amanda McGuinness – January 26, 2017

This past Saturday, January 21st, the 2017 Sundance Film Festival was underway with its first weekend of screenings when it was interrupted by a cyberattack that disabled its online box office as well as internet access throughout Park City, Utah. The attack is reportedly being investigated by the FBI as a denial of service (DDoS) attack, and Sundance representatives assured that no artist or customer information was compromised. In addition to the online box office, many local businesses were hampered as they were forced to accept cash only, and most ATMs were disabled from the attack.

Ransomware

The Romantik Seehotel Jägerwirt 4-Star Superior Luxury Hotel was hit by a ransomware attack that locked guests in and out of the rooms.

Another singular incident involved a ransomware, the victims are hundreds of guests of a luxurious hotel in Austria, the Romantik Seehotel Jägerwirt 4-Star Superior Hotel. The guests were locked in or out of their rooms. The malware infected the systems at the hotel and its administration opted to pay the ransom to restore a normal operation.
OTA Incident Methodology

Review of data from leading sources:

- Risk Based Security, Privacy Rights Clearing House, Identity Theft Resource Center...
- Government Agencies – DHS, FBI, Secret Service & international agencies
- Information Sharing & Analysis Centers (ISAC’s)
- Industry, including Microsoft, Symantec & Verisign

2016 Key Metrics

82,000 Incidents – 20x of “traditional breaches”

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>90% + preventable (OTA)</td>
<td>1300% increase in BEC losses</td>
</tr>
<tr>
<td>4,149 confirmed breach's worldwide</td>
<td>35% rise in business ransomware</td>
</tr>
<tr>
<td>4.2 billion records disclosed</td>
<td>$75 billion cost of ransomware</td>
</tr>
<tr>
<td>58% increase in DDoS attacks</td>
<td>78% increase in phishing sites</td>
</tr>
</tbody>
</table>

Incidents Across All Sectors

- Business
- Non-Profits / NGOs
- Healthcare / Medical
- Government / Military
- Education
- Banking / Credit / Financials
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

2017 Incident Response Guide

Providing Prescriptive Guidance for...

- Risk Assessment
- Adopting Security Best Practices
- Data Lifecycle & Stewardship
- Incident Response Fundamentals
- Cyber Insurance Considerations
- Notification Requirements
- Training, Testing & Budgeting
- Regulatory Landscape
- Resources/Templates
The Realities of a Loss Incident

Incident Fundamentals

- No perfect security
- Data stewardship, privacy and incident readiness are everyone’s responsibility
- Practices need continual review
- All organizations collect some form of sensitive information
- Cyber incidents will occur
- Every organization needs to have a current and tested plan
- Ongoing employee training is a critical key to success
- Security must be priority; those that fail will be held accountable
Learn From Mistakes of Others!

Checklist (pg 9)

- Complete risk assessments (pg 11)
- Review security best practices (pg 14)
- Data management and stewardship (pg 17)
- Complete an audit of insurance (pg 22)
- Establish an end-to-end incident response plan (pg 24)
- Establish/confirm relationships with law enforcement (pg 25)
- Review and establish forensic capabilities (pg 26)
- Review notification processes and plans (pg 29)
- Develop communication strategies by audience (pg 30)
- Review remediation programs & alternatives (pg 31)
- Implement employee training for incident response (pg 32)
- Establish employee data security awareness. (pg 32)
- Understand the regulatory requirements (pg 34)
Risk Assessments (pg 11-13)

- Board & Executive Leadership
- Internal & Operational
  - Throughout an organization
- Third Parties
  - Vendors
  - Cloud Service Providers

Security Best Practices (pg 14)

1. Encryption of data at rest / in storage and in transit
2. Multi-factor authentication
3. Enforce effective password management policies
4. Least privilege user access (LUA)
5. Regular security design, pen tests and vulnerability scans
Security Best Practices

6. Secure client devices with multi-layered firewall protection
7. Email authentication – inbound & outbound
8. Implement a mobile device management program
9. Continuously monitor systems in real-time
10. Deploy web application firewalls

Security Best Practices

11. Permit only authorized wireless devices
12. Implement Always On Secure Socket Layer (AOSSL)
13. Review server certificates for vulnerabilities
14. Ensure all updates and patches verified/signed
15. Back up key data to offline storage
Security Best Practices

16. Develop, test and continually refine response plans
17. Establish a vulnerability reporting program
18. Complete an inventory
19. Security third-party assessments
20. Bake DDoS protection into incident response plan

Data Stewardship (pg 17-21)
Cyber Insurance (pg 22-23)

- 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 – negligence?

Plan Fundamentals (pg 24-28)

- 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
Notification Requirements (pg 29)

- Expanded Definition of “Personal Information”
  - Login Credentials - California, Florida, Illinois, Nebraska, North Dakota, Nevada, Rhode Island & Wyoming
  - Biometric Data - Illinois & Oregon
  - License Plate Data - California

- Encryption
  - Defined - Rhode Island & California
  - Key Compromises - California, Nebraska & Illinois

- Consumer Notice - Rhode Island & California
- Notice to State AG’s - Oregon, Nebraska & Rhode Island
- Notice Deadlines - Rhode Island & Tennessee

Communications (pg 30)

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

4 T’s
- Tactic
- Tone
- Timing
- Technology
Regulatory Landscape (pg 34)

- International Implications – GDPR
- US patchwork of 46 State laws
- Framework for National Legislation
  - Preempt States; *providing it meets the California / Mass bar*
  - State Attorney General right to enforce, (aka CANSPAM)
  - FTC rule making capabilities as it pertains to reasonable security standards and practices
  - Minimal standard of care including credit monitoring, ID theft protection and ID theft counseling / case workers
  - Timing for Notification
  - Converge for SMBs / Homebased businesses

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
2017 Incident Response Guide

Providing Prescriptive Guidance Aiding in ….

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

- Incident Response Guide [https://otalliance.org/Incident](https://otalliance.org/Incident)
- Vision for Trust [https://otalliance.org/Vision](https://otalliance.org/Vision)
- Identity Guard / Intersections Inc. [https://identityguard.com](https://identityguard.com)
- LifeLock Inc. [https://lifelock.com](https://lifelock.com)
- Symantec [https://Symantec.com](https://Symantec.com)
- Verisign [https://verisign.com](https://verisign.com)