2017 Cyber Incident & Breach Response Briefing

co-hosted by the Congressional Cybersecurity Caucus

Welcome & Opening Comments

Nick Leiserson
Legislative Director
Congressman Jim Langevin (D-RI)
Craig Spiezle
Executive Director & President
Jeff Wilbur
VP, Research

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

- **Data Protection & Privacy Day** – Annual Incident Response Guide

IoT Vision For The Future

“An ecosystem built on trust and innovation where benefits to society and commerce are realized by prioritizing security, privacy and safety.”
IoT Trust Framework

- Multi-stakeholder working group
- 18 month, consensus driven process

Security
- Devices & Sensors
- Applications & Services

Data Privacy
- Transparency & Notice
- Choice & Control

Sustainability
- Lifecycle support
- Portability & Transferability

Online Trust Audit

- 2017 Methodology Released Today

- Audit of 1,000 web sites
  - Internet Retailer Top 500
  - FDIC Banking 100
  - Top 100 Consumer Services
  - Top 100 News/Media
  - Top 50 Federal Gov’t
  - Top 50 ISPs/Carriers/Mail Providers
  - OTA Members

- Scoring
  - 100 baseline points for each category
  - Weighted composite analysis, ~50 criteria
  - Bonus points for emerging practices
  - Penalty points for
    - Vulnerabilities, privacy practices, data loss incident & fines/settlement
Top of The Class in 2016

#1 across all sectors

Twitter (Twitter.com)
HealthCare.gov (healthcare.gov)
Pinterest (pinterest.com)
The White House (whitehouse.gov)
Dropbox (dropbox.com)
FileYourTaxes (fileyourtaxes.com)
LifeLock (lifelock.com)
Instagram (instagram.com)
1040.com (1040.com)
The Gap (gap.com)

Panel of Experts

Scott Behm
VP Cybersecurity Engineering & Operations, LifeLock Inc.

Dena Graziano
Senior Director Federal Government Affairs, Symantec Corp.

Frank Scalzo
Director Security Strategy, Verisign, Inc.

Jerry Thompson
Executive VP, Identity Guard / Intersections Inc.
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

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 breaking incident

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

This past Saturday, January 21st, the 2017 Sundance Film Festival was underway with its first weekend of screenings when it was interrupted by a cyber attack 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. Some ATMs were also out of service.

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.
Challenges With Metrics

- 46 State laws and varying definitions of a breach
  - Was the data encrypted?
  - Was it related to banking credentials?
- Self reporting
- Lack of national definition or central database

OTA Incident Methodology

Review of data from leading sources including:
- Risk Based Security, Privacy Rights Clearing House, Identity Theft Resource Center and others
- Government Agencies – DHS, FBI, Secret Service and international agencies
- Information Sharing and 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

Top Cyber Security Tenets

- There is no perfect security
- Need to make security a priority; those that fail will be held accountable.
- Need to look beyond the impact of a "traditional breach" to the life safety and physical impact of an incident, damage to an organization's reputation and risks to users.
- Incentives are needed to accelerate “security by design” the need for annual security assessments
- Signaling of commitment to security and privacy can become product and brand differentiators.
- Employee training and awareness must be addressed to help close the security gaps and “blind spots”.

LEARN • INNOVATE • COLLABORATE
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.

Security Best Practices

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

National Breach Legislation

- Replace patchwork of 46 State laws
- Considerations -
  - Preempting States; *providing it meets the California / Mass bar*
  - Provides State AGs right to enforce, (aka CANSPAM)
  - Provide FTC rule making capabilities as it pertains to reasonable security standards and practices
  - Define minimal standard of care including credit monitoring, ID theft protection and ID theft counseling / case workers
  - Converge for SMBs / Homebased businesses
Data Stewardship

Data Management
Communications

Discussion Topics

- Evolving Threat Vectors
- Best Practices
  - Prevent
  - Detect
  - Mitigate
  - Respond
- Cyber Insurance
- Regulations / Legislation

“There is no perfect security. Organizations need to recognize they will encounter an incident and they will be judged on how they respond.”
Panel of Experts

Scott Behm  
VP Cybersecurity Engineering & Operations, LifeLock Inc.

Dena Graziano  
Senior Director Federal Government Affairs, Symantec Corp.

Frank Scalzo  
Director Security Strategy, Verisign, Inc.

Jerry Thompson  
Executive VP, Identity Guard / Intersections Inc.

https://otalliance.org/incident
Resources

- Incident Response Guide  https://otalliance.org/Incident
- Vision for Trust  https://otalliance.org/Vision
- Identity Guard / Intersections Inc.  https://identityguard.com
- LifeLock Inc.  https://lifelock.com
- Symantec  https://Symantec.com
- Verisign  https://verisign.com
- Webinar Briefing Feb 7th
  -  https://attendee.gotowebinar.com/rt/2316727454748055298