OTA
Online Trust Alliance
DATA PRIVACY & PROTECTION DAY
2017

Congressional Cyber Breach & Incident Briefing

https://otalliance.org/Incident

2016 Incident Highlights

- 82,000+ total cyber incidents in 2016 (OTA)
- 90%+ of incidents preventable (OTA)
- 4,149 confirmed breach worldwide (RBS)
- 4.2 billion consumer records disclosed (RBS)
- 58% increase in DDoS attacks (Verisign)
- 1300% increase in BEC losses (FBI)
- 78% increase in phishing sites (APWG)
- 35% rise in business ransomware (Symantec)
- $75 billion cost of ransomware (Symantec)

Incidents Include

- 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.

Top Cyber Security Tenets

1. There is no perfect security and any organization is at risk; most organizations hold data of interest.
2. Organizations must make security a priority; those that fail will be held accountable.
3. Organizations need to look beyond the impact and cost of a "traditional data breach" to the life safety and physical impact of an incident, damage to an organization's reputation and risks to users.
4. Business incentives are needed to accelerate "security by design" along with the need for annual security assessments of sites, applications services and devices.
5. Signaling of commitment to security and privacy can become product and brand differentiators.
6. Employee training and awareness must be addressed to help close the security technology gaps.

Readiness Checklist

- ☐ Complete risk assessments for executive review, operational process and third party vendors (pg 11)
- ☐ Review security best practices and validate adoption or reasoning for not adopting (pg 14)
- ☐ Audit data management and stewardship programs including data life-cycle management (pg 17)
- ☐ Complete an audit of insurance needs including exclusions and third party coverage (pg 22)
- ☐ Establish an end-to-end incident response plan including empowering 24/7 first-responders (pg 24)
- ☐ Establish/confirm relationships with law enforcement and incident service providers (pg 25)
- ☐ Review and establish forensic capabilities and resources (internal and third-party providers) (pg 26)
- ☐ Review notification processes and plans (pg 29)
- ☐ Develop communication strategies and tactics tailored by audience (pg 30)
- ☐ Review remediation programs, alternatives and service providers (pg 31)
- ☐ Implement employee training for incident response (pg 32)
- ☐ Establish employee data security awareness. Provide education on privacy, incident avoidance (password practices, how to recognize social engineering, etc.) and incident response (pg 32)
- ☐ Understand the regulatory requirements, including relevant international requirements (pg 34)

U.S. Government & State Agencies

Federal Trade Commission
- Breaches - https://www.ftc.gov/news-events/blogs/business-blog/2016/10/responding-data-breach
- Complying with the FTC's Health Breach Notification Rule https://www.ftc.gov/healthbreachnotificationrule

Dept. of Education, Breach Kit - http://ptac.ed.gov/document/data-breach-response-training-kit

Dept. of Homeland Security, Cybersecurity - https://www.dhs.gov/topic/cybersecurity

Federal Bureau of Investigation (FBI) Cyber Resources - https://www.fbi.gov/investigate/cyber

Secret Service Electronic Crimes Task Force - http://www.secretservice.gov/investigation/

Department of Commerce Privacy Shield: https://www.commerce.gov/page/eu-us-privacy-shield

NIST Cybersecurity Framework - https://www.nist.gov/cyberframework

State of California
- Breach reporting https://oag.ca.gov/ecrime/databreach/reporting
- Privacy https://oag.ca.gov/privacy
- Breach Reports https://.oag.ca.gov/privacy/privacy-reports

State of Massachusetts- http://www.mass.gov/ocabr/data-privacy-and-security/data/

State of New York - https://its.ny.gov/eiso/breach-notification

State of Ohio - http://infosec.ohio.gov/Business/DataBreachNotificationandResponse.aspx

State of Rhode Island - http://webserver.rilin.state.ri.us/BillText15/SenateText15/S0134B.pdf

State of Washington - http://www.atg.wa.gov/data-breach-notifications

Canada

Personal Information Protection and Electronic Documents Act (PIPEDA) - https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

Privacy Toolkit - https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/guide_org/

Office of the Privacy Commissioner of Canada - https://priv.gc.ca/en/

Non-Profits

Anti-Phishing Working Group (APWG)
- Research & Whitepapers http://apwg.org/resources/apwg-reports/whitepapers
- Educating Your Consumers http://apwg.org/resources/Educate-Your-Customers/

Consumer Federation of America - http://consumerfed.org/issues/privacy/id-theft/

Council of Better Business Bureaus - www.bbb.org/cybersecurity
- Data Security Guide - http://www.bbb.org/data-security

Identity Theft Council - https://www.identitytheftcouncil.org/

InfraGard - https://www.infragard.org/

Internet Society, Global Internet Report 2016 - https://internetsociety.org/globalinternetreport/2016/

Internet Crime Complaint Center (IC3) - http://www.ic3.gov/default.aspx

OWASP Incident Response - https://www.owasp.org/index.php/OWASP_Incident_Response_Project

Online Trust Alliance

Cyber Incident & Breach Response Resource Center - https://otalliance.org/incident

Email Security & Authentication (SPF, DKIM & DMARC) – https://otalliance.org/eauth

Internet of Things Trust Framework & Checklists – https://otalliance.org/IoT

Online Trust Audit & Honor Roll – https://otalliance.org/TrustAudit

Security & Privacy Best Practices - https://otalliance.org/resources/security-privacy-best-practices

Visions for Online Trust - https://otalliance.org/Vision

Identity Guard / Intersections Inc.

Consumer ID Theft Resources - http://www.identityguard.com/news-insights/category/tools/

Breach Readiness –http://www.intersections.com/library/7stepstodatabreach_040611%20FINAL.pdf

Learnings- https://www.identityguardbusiness.com/resource-center/learning-from-a-recent-data-breach-case/

Breach Response Solutions https://www.identityguardbusiness.com/breach-services

Identity Guard - http://www.identityguardbusiness.com/

LifeLock Inc.

Overview - https://www.lifelock.com/education/

Online Risk Calculator - https://www.lifelock.com/risk-calculator/

Breach Solutions - https://www.lifelockbusinesssolutions.com/industries/lifelock-breach-solutions/

Symantec

Symantec Cyber Insurance - https://www.symantec.com/solutions/insurance

Security Internet Security Threat Report - https://www.symantec.com/security-center/threat-report

Symantec Encryption Solutions - http://www.symantec.com/encryption

Symantec File Share Encryption - http://www.symantec.com/file-share-encryption/

Symantec Website Security - https://www.symantec.com/website-security/

Verisign

DDoS Mitigation Support - https://www.verisign.com/en_US/forms/underattackrequestform.xhtml

Reports - https://www.verisign.com/en_US/internet-technology-news/published-reports/index.xhtml

Verisign Blog - https://blog.verisign.com/

DDoS - https://www.verisign.com/en_US/security-services/ddos-protection/ddos-report/index.xhtml