Data Breach: Investigations and Readiness

Inno Eroraha, CISSP-ISSAP, CISA, CISM, CHFI
Founder & Chief Strategist
NetSecurity Corporation

ISSA-DC Presentation

February 24, 2015

Abstract

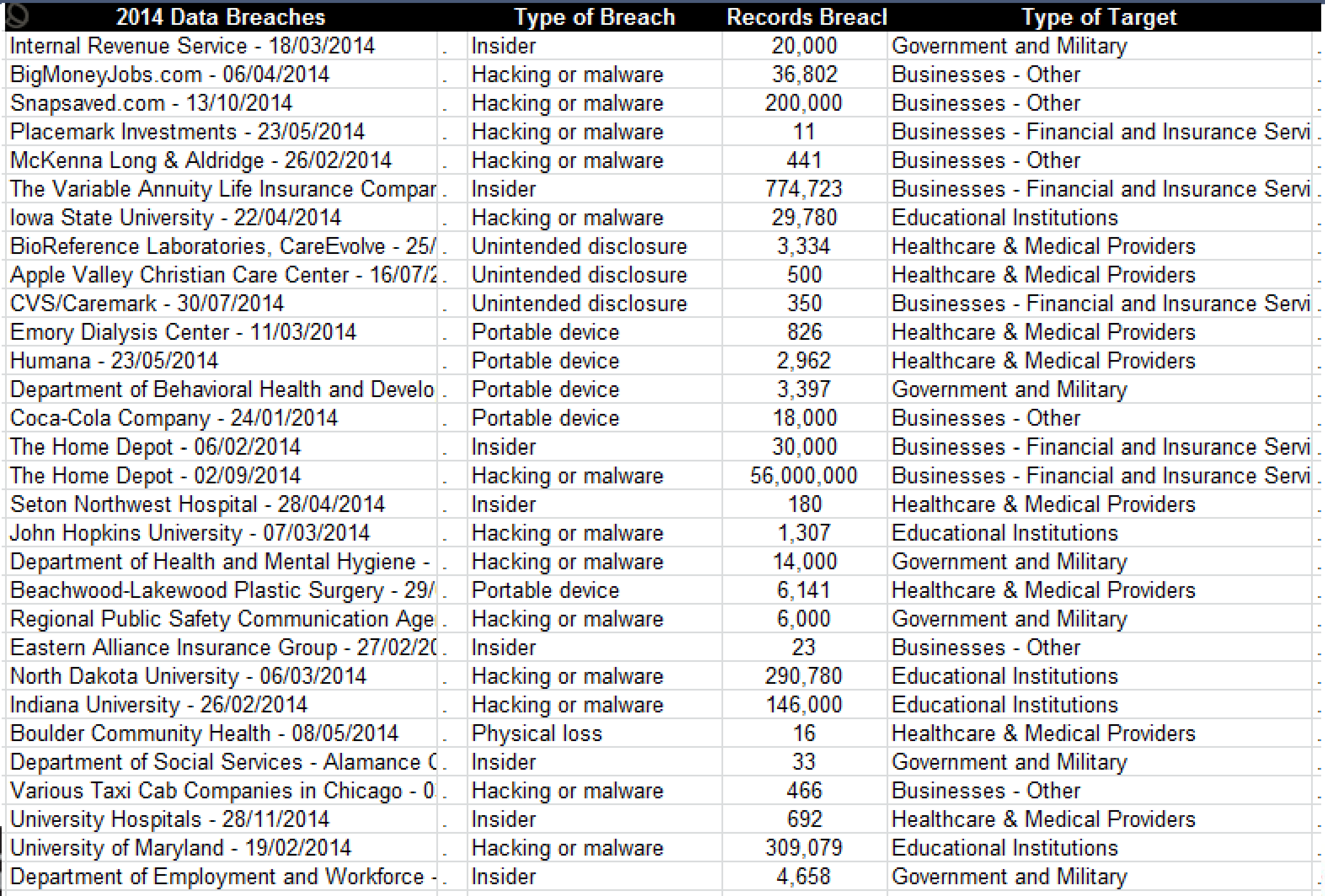
Turn on the television and you are more likely to hear about a data breach than any other security incident. Despite all security measures, data leakage and exfiltration still occur in "well-protected" enterprise networks – bypassing all defensive measures. Unless a viable process exists to protect valuable corporate intellectual property and customers' sensitive information, data breaches and loss will become commonplace rather than an anomaly. Real-world experience gained from preparing high-stake organizations against data loss as well as in conducting high-profile investigations will be shared with participants. These experiences should help attendees anticipate, prepare for, and conduct forensically-sound data breaches investigations timely.

Data Breaches

- Anthem – 80 million records – Linked to China
- Sony
- Target
- Home Depot
- JP Morgan Chase
- Goodwill

Data Breaches

Courtesy: http://data-breach.silk.co/



2014 Data Breaches		Type of Breach	Records Breacl	Type of Target	
Internal Revenue Service - 18/03/2014	.	Insider	20,000	Government and Military	.
BigMoneyJobs.com - 06/04/2014	.	Hacking or malware	36,802	Businesses - Other	.
Snapsaved.com - 13/10/2014	.	Hacking or malware	200,000	Businesses - Other	.
Placemark Investments - 23/05/2014	.	Hacking or malware	11	Businesses - Financial and Insurance Servi	.
McKenna Long & Aldridge - 26/02/2014	.	Hacking or malware	441	Businesses - Other	.
The Variable Annuity Life Insurance Compar	.	Insider	774,723	Businesses - Financial and Insurance Servi	.
Iowa State University - 22/04/2014	.	Hacking or malware	29,780	Educational Institutions	.
BioReference Laboratories, CareEvolve - 25/	.	Unintended disclosure	3,334	Healthcare & Medical Providers	.
Apple Valley Christian Care Center - 16/07/2	.	Unintended disclosure	500	Healthcare & Medical Providers	.
CVS/Caremark - 30/07/2014	.	Unintended disclosure	350	Businesses - Financial and Insurance Servi	.
Emory Dialysis Center - 11/03/2014	.	Portable device	826	Healthcare & Medical Providers	.
Humana - 23/05/2014	.	Portable device	2,962	Healthcare & Medical Providers	.
Department of Behavioral Health and Develo	.	Portable device	3,397	Government and Military	.
Coca-Cola Company - 24/01/2014	.	Portable device	18,000	Businesses - Other	.
The Home Depot - 06/02/2014	.	Insider	30,000	Businesses - Financial and Insurance Servi	.
The Home Depot - 02/09/2014	.	Hacking or malware	56,000,000	Businesses - Financial and Insurance Servi	.
Seton Northwest Hospital - 28/04/2014	.	Insider	180	Healthcare & Medical Providers	.
John Hopkins University - 07/03/2014	.	Hacking or malware	1,307	Educational Institutions	.
Department of Health and Mental Hygiene -	.	Hacking or malware	14,000	Government and Military	.
Beachwood-Lakewood Plastic Surgery - 29/	.	Portable device	6,141	Healthcare & Medical Providers	.
Regional Public Safety Communication Age	.	Hacking or malware	6,000	Government and Military	.
Eastern Alliance Insurance Group - 27/02/2(	.	Insider	23	Businesses - Other	.
North Dakota University - 06/03/2014	.	Hacking or malware	290,780	Educational Institutions	.
Indiana University - 26/02/2014	.	Hacking or malware	146,000	Educational Institutions	.
Boulder Community Health - 08/05/2014	.	Physical loss	16	Healthcare & Medical Providers	.
Department of Social Services - Alamance (	.	Insider	33	Government and Military	.
Various Taxi Cab Companies in Chicago - 0	.	Hacking or malware	466	Businesses - Other	.
University Hospitals - 28/11/2014	.	Insider	692	Healthcare & Medical Providers	.
University of Maryland - 19/02/2014	.	Hacking or malware	309,079	Educational Institutions	.
Department of Employment and Workforce -	.	Insider	4,658	Government and Military	.

Type of Breach

- □ Insider
- □ Hacking or malware
- □ Unintended disclosure
- □ Portable device
- □ Physical loss
- □ Stationary device

Type of Target

- Government and Military
- Businesses - Other
- Businesses - Financial and Insurance Services
- Educational Institutions
- Healthcare & Medical Providers

Security Practices

- Good: Have protection, monitoring practices, don't think they have been compromised
- Bad: Rely on Firewalls and IDS
- Ugly: No one cares about us. We have nothing of value to loose

Anticipate data breach will occur!

Anticipate & Prepare for Data Loss

- Fortify your Security Processes
- Create a Breach Investigation Plan
  - Rehearse the Plan
- Build a Breach Investigation Capability
- Conduct Proactive Threat Response

Fortify Security Processes

Courtesy: https://www.sans.org/critical-security-controls/

- □ 1: Inventory of Authorized and Unauthorized Devices
- □ 2: Inventory of Authorized and Unauthorized Software
- □ 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- □ 4: Continuous Vulnerability Assessment and Remediation
- □ 5: Malware Defenses
- □ 6: Application Software Security
- □ 7: Wireless Access Control
- □ 8: Data Recovery Capability
- □ 9: Security Skills Assessment and Appropriate Training to Fill Gaps
- □ 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Fortify Security Processes (Contd.)

Courtesy: https://www.sans.org/critical-security-controls/

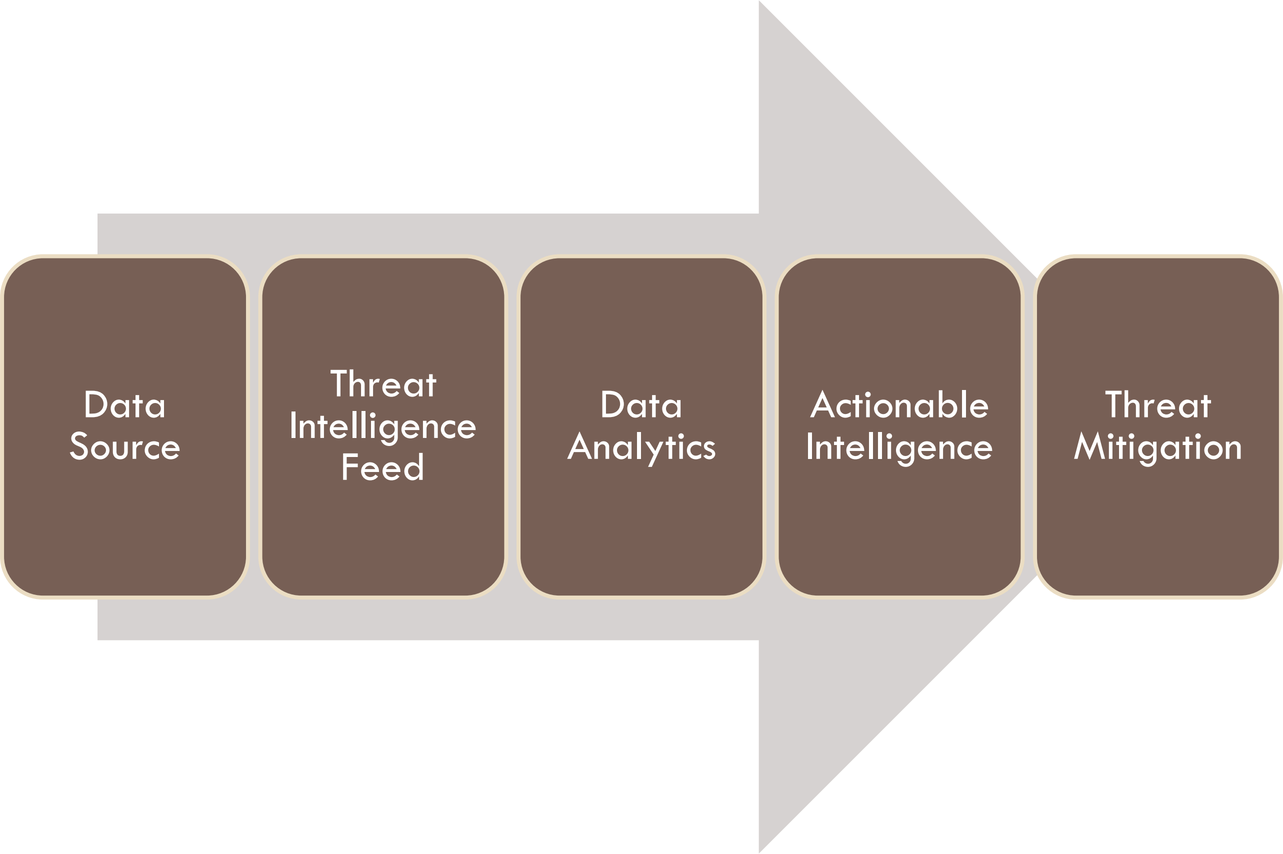
- □ 11: Limitation and Control of Network Ports, Protocols, and Services
- □ 12: Controlled Use of Administrative Privileges
- □ 13: Boundary Defense
- □ 14: Maintenance, Monitoring, and Analysis of Audit Logs
- □ 15: Controlled Access Based on the Need to Know
- □ 16: Account Monitoring and Control
- □ 17: Data Protection
- □ 18: Incident Response and Management
- □ 19: Secure Network Engineering
- □ 20: Penetration Tests and Red Team Exercises

How Do You Know Your Security Process is Working?

Proactive Threat Response

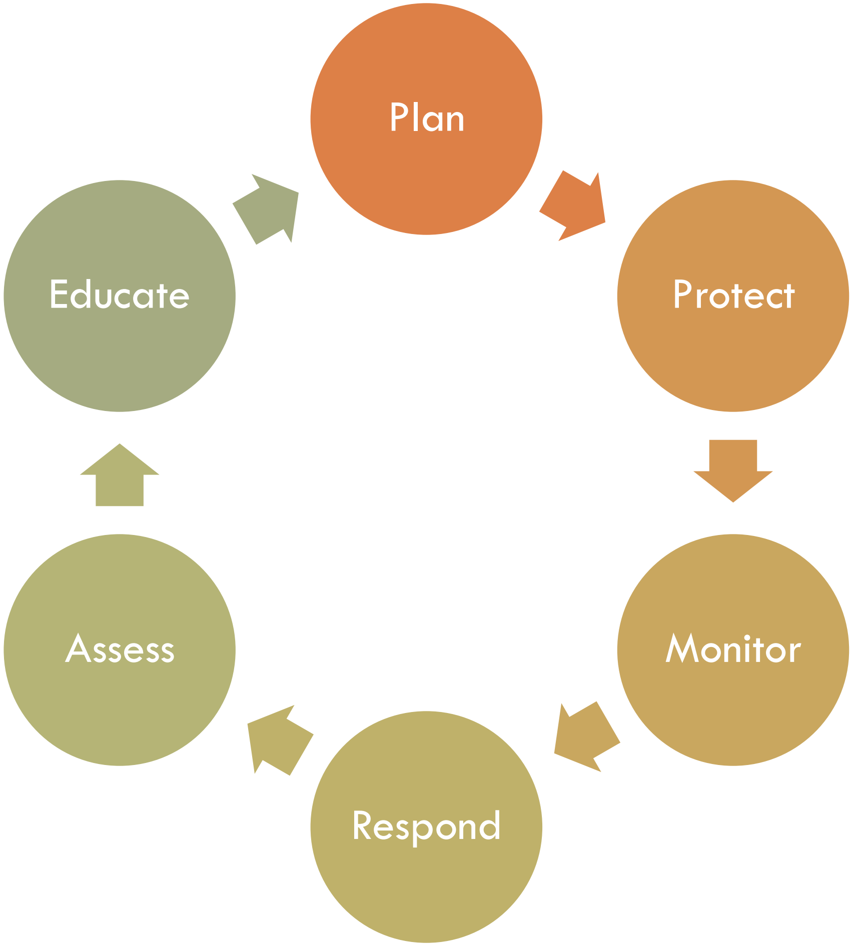
- Continuous threat assessment/detection
- Centralized data feed from endpoints, network devices, applications, SIEM
- Data Analytics
- Threat Intelligence feed (external/internal)
- Actionable Intelligence
- Threat Mitigation

ThreatRESPONDER™



netSecurity®

Breach Readiness



QUESTIONS?