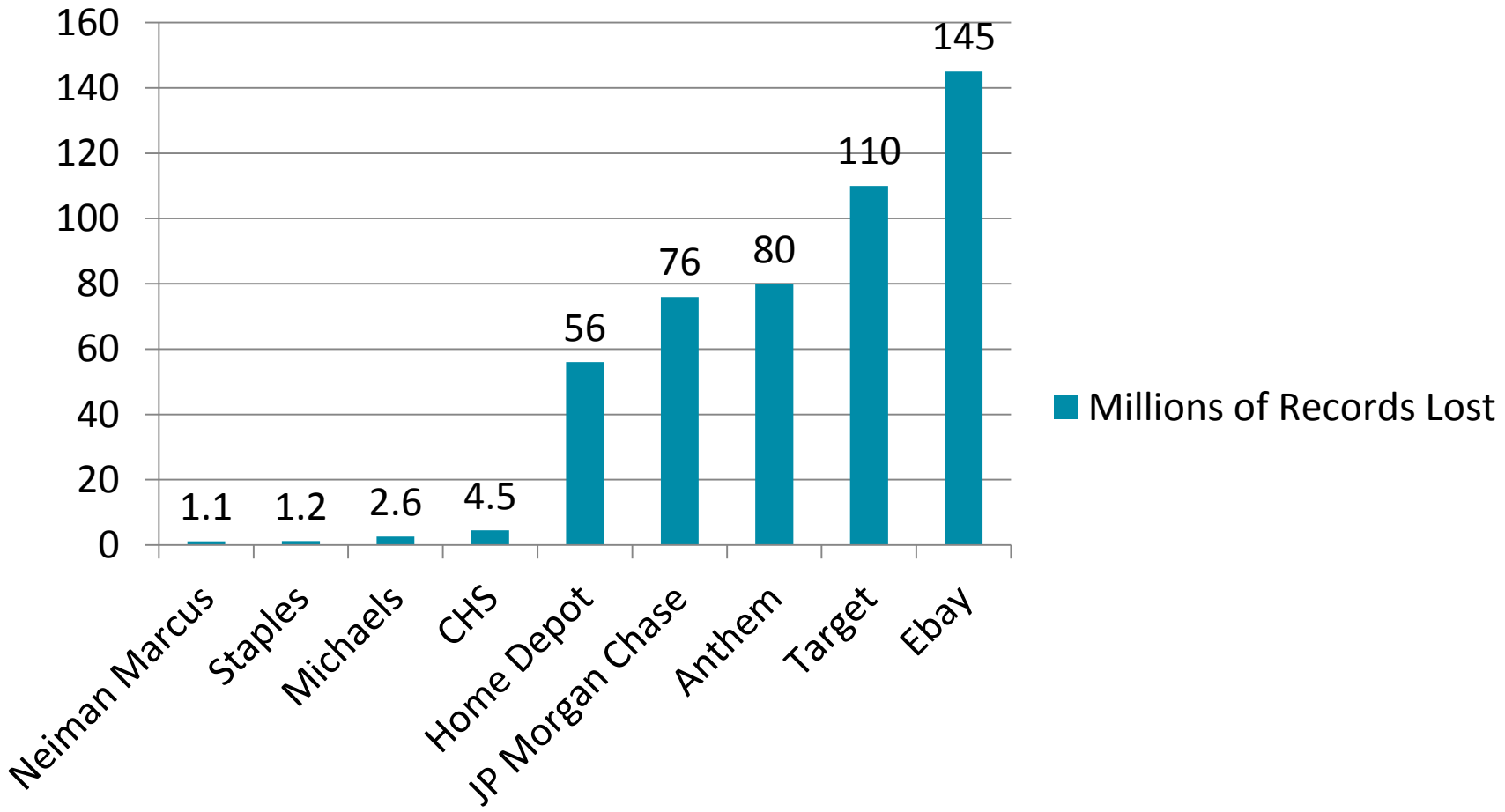
The Business of Cybercrime

Jim Murray
Corporate Information Security Executive
james_murray@ncci.com

Agenda

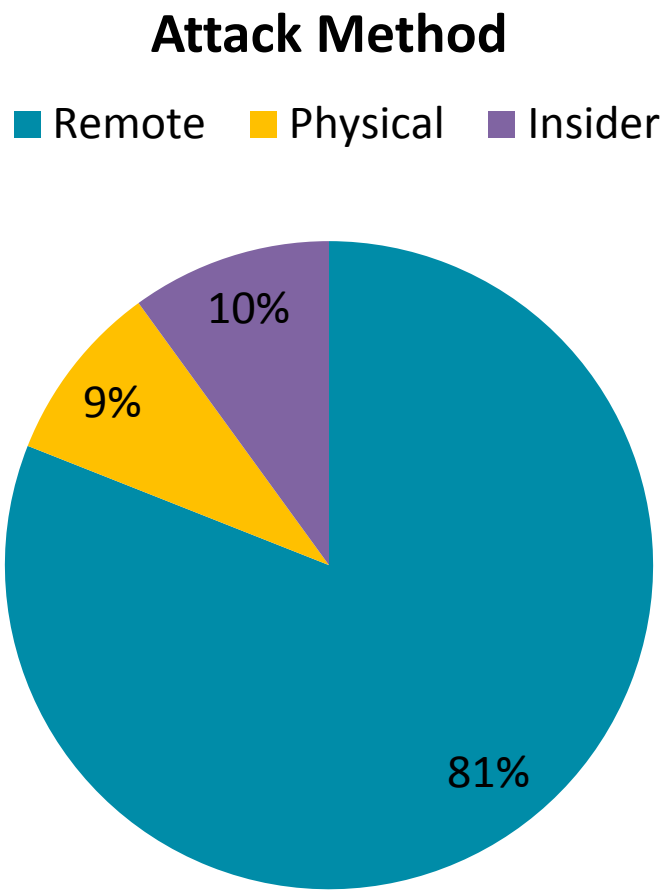
- State of Security
- Security by the Numbers
- Attack Methodology
- Defense Methodology
- Questions

A Year of Mega Breaches



Ponemon Institute, January 2015

Method of Attack



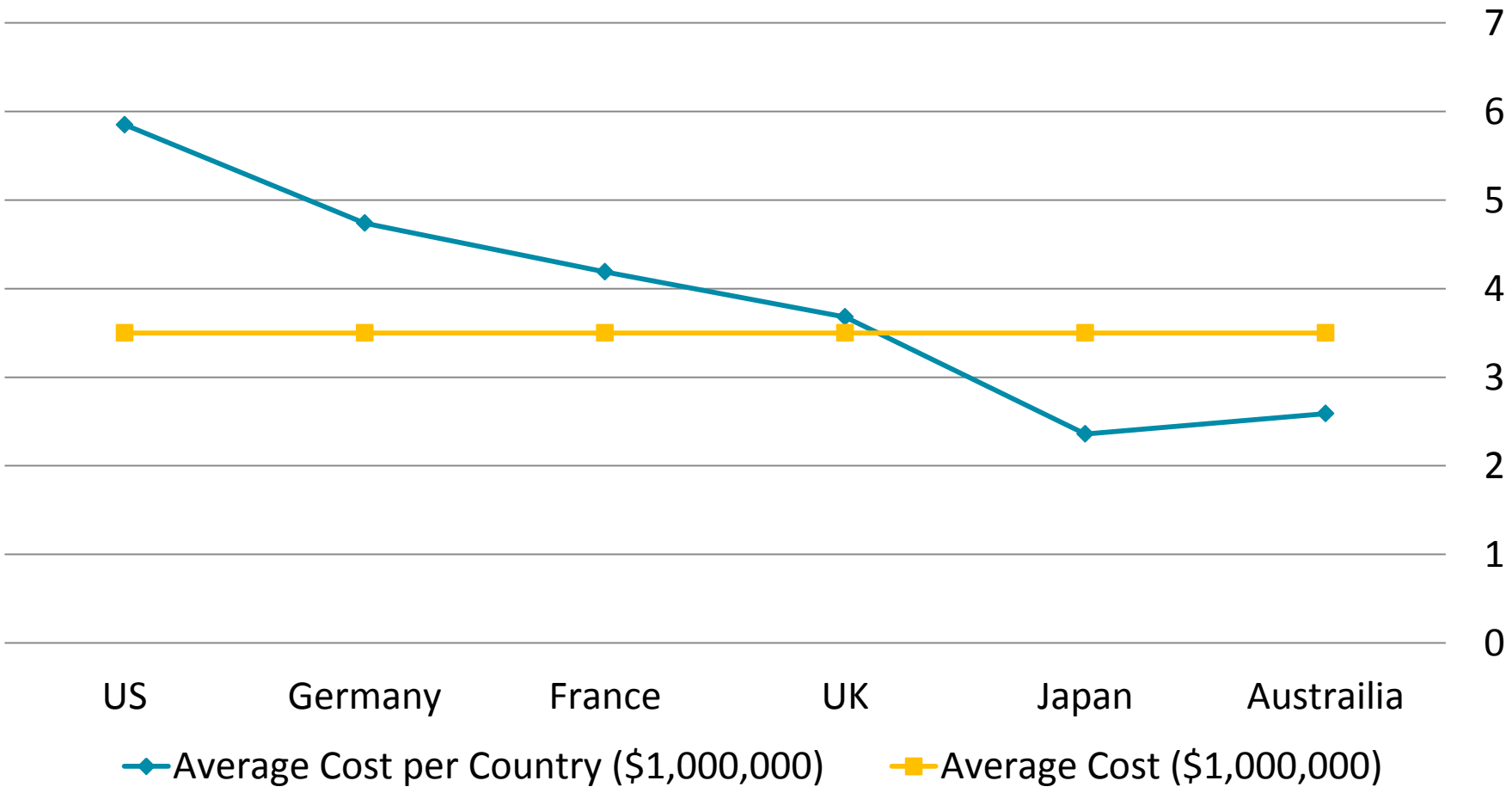
Verizon DBPR, April 2014

Other Disturbing Facts

- ~90% of compromises happen within days
- <20% of compromises are discovered in days
- <20% of compromises are discovered by the organization
  - Most discoveries are reported by:
    - Law Enforcement
    - Third Parties
    - Fraud Detection
- 90% of remote attacks performed via email or web browsing

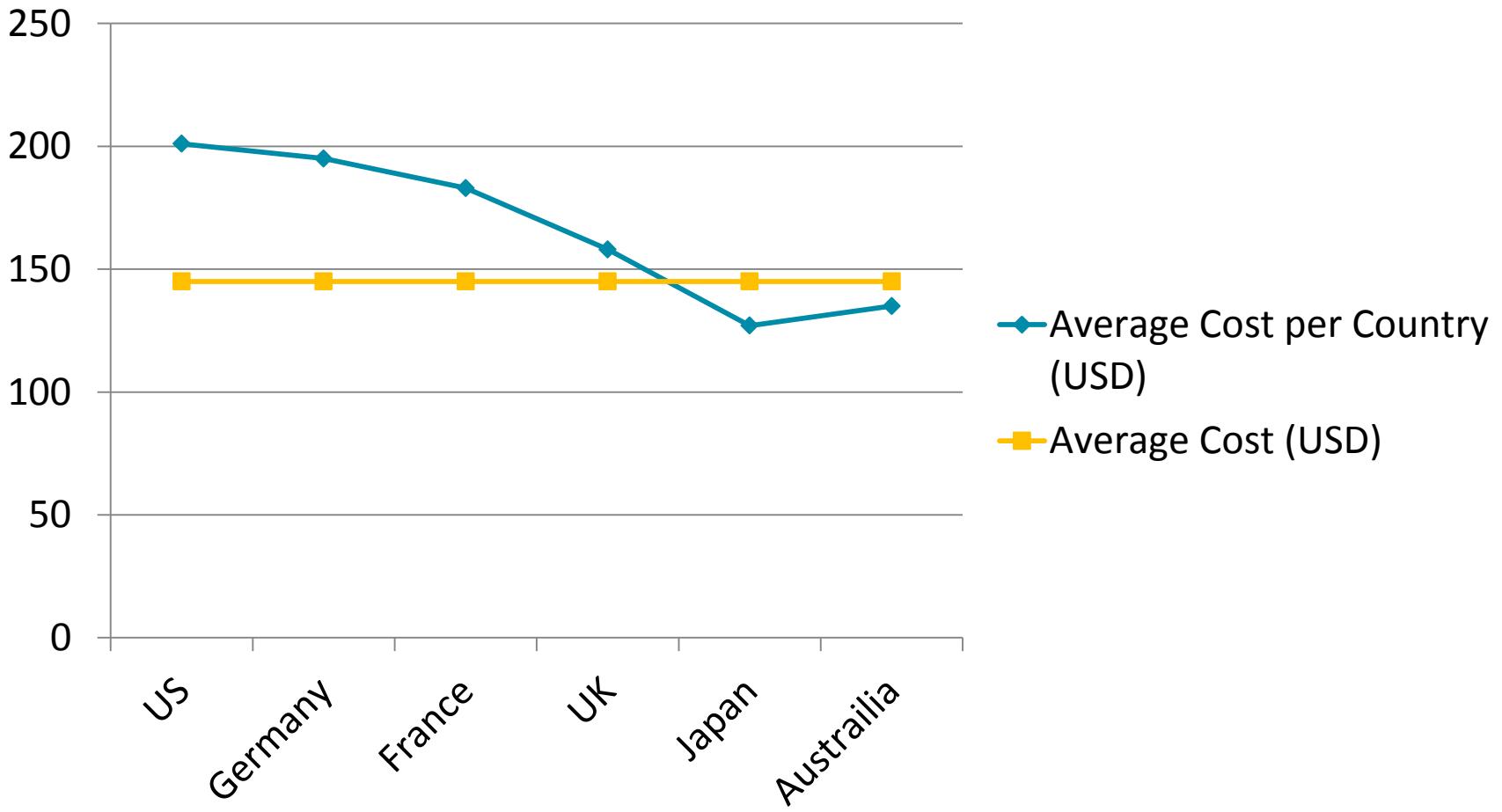
Verizon DBPR, April 2014

Average Cost of Data Breaches



[Ponemon Institute, May 2014]

Cost Per Record Lost



Ponemon Institute, May 2014

Market Value

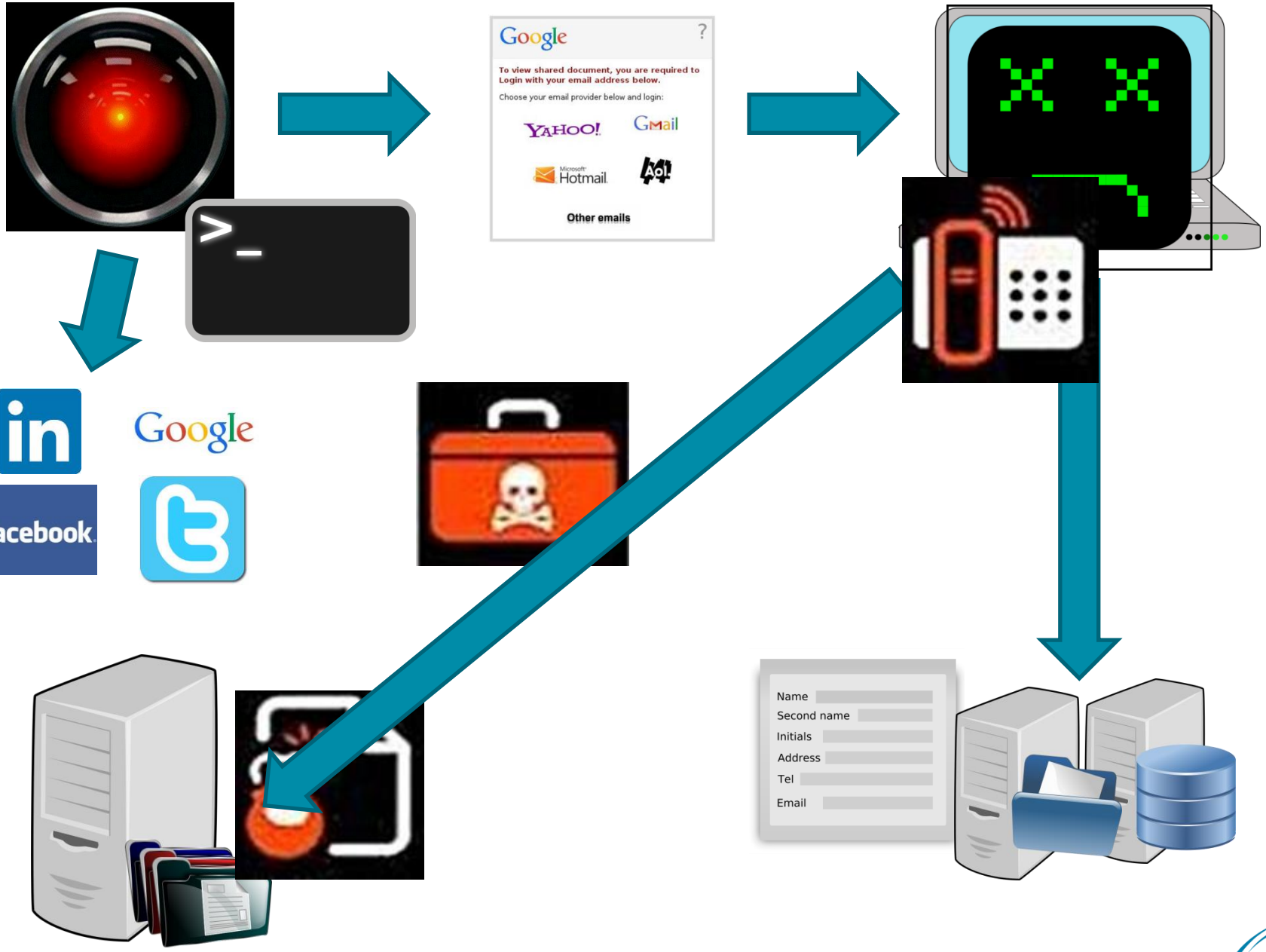
Data Type	Street Value
Valid Email Address	$1 per 10,000
Username/Password/Emails Compromised Website	$1 per 1,000
Credit Card #	$2 - $90
Medical Record	$8 - $20
Bank Credentials	$80+
Rent 100 Botnet Infected Machines	$700+ / month
Celebrity Medical Records	$1,000+
Admin Access to High-Traffic Compromised Website	$3,000+
Company Financials, Intellectual Property	$10,000+ - ???

US intelligence agencies estimate cost of lost business due to theft of technology and business ideas $100 - $250 billion / year

Proofpoint (2014)

7 Stages of Attack

Websense 7 Stages, 2015



Cyber Defense Methodolgy

- Three-Tiered Approach
  - Prevent
    - Implement processes and technologies designed to prevent security vulnerabilities from being exploited
    - Examples: Firewalls, Application Whitelisting, Anti-Virus, Access Control, Patching, Message Hygiene, Device Control
  - Detect
    - Implement processes and technologies designed to detect security incidents as soon as possible, understanding that prevention is not absolute and will ultimately fail
    - Examples: Intrusion Detection, Security Information and Event Management, Vulnerability Scanning, Access Reviews, DLP
  - Respond
    - Implement processes and technologies designed to appropriately respond to security incidents in an effort to minimize the impact of those incidents to the organization.
    - Examples: Incident Handling, Forensic Capabilities, Alerting, Remediation,

Additional Resources

- 2014 A Year of Mega Breaches – Ponemon Institute:
  - http://www.ponemon.org/library/2014-a-year-of-mega-breaches
- Verizon 2014 Data Breach Investigations Report
  - http://www.verizonenterprise.com/DBIR/2014/
- 2014 Cost of Data Breach Global Analysis – Ponemon Institute:
  - http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis
- Intelligence Driven Computer Network Defense – AKA Cyber Kill Chain – Lockheed Martin
  - http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
- 7 Stages of a Cyber Attack – Websense
  - http://www.websense.com/content/seven-stages-recon.aspx

Questions?