Hackers Are Among Us: Start Thinking Like a Bad Guy

Ed Sadeghi, Adjunct Professor
MS, MCSE, CNE, CISA, CEH, CTGA

Keller Graduate School of Management
College of Engineering and Information Sciences
ssadeghi@devry.edu
650-269-9742

Core Competencies - C31

Speaker Profile

- **Professional Summary:**
  - Adjunct Professor
  - Information Security Analyst
  - Information Security Consultant
  - IT Manager/Director
  - Security Architect
  - Network Engineer

- **Professional Experience:**
  - DeVry Univ.
  - Safeway
  - Ross Stores
  - ST. Mary's College HS
  - ITT Technical Institute
  - 3Com
  - Applied Material
  - National Semiconductor

Agenda

- Information Security Terminologies
- Telecommunications and Networking in Today's World

- Defense in Depth Strategy
  - Risk Management, Vulnerability Management and Threat Assessment.

- Verizon Data Breach Investigation Report
- Intrusion Kill Chain Framework
  - Intelligence-Driven Computer Network Defense
  - Action Matrix

- A Stenography Video Clip

InfoSec Terminologies

Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from unauthorized access.

Threat – any potential danger to information life cycle
Threat agent – an entity that may act on a vulnerability

Advanced Persistent Threat - represents a well-resourced and trained adversaries that conduct multi-year intrusion campaigns targeting highly sensitive economic, proprietary or national security information.

Vulnerability – a weakness or flaw that my provide an opportunity to a threat agent

InfoSec Terminologies (Cont'd)

Asset – Both tangible and intangible features of your organization including hardware, software, information, people, facilities, brand, reputation, etc.

Risk – The likelihood of a threat agent exploits a discovered vulnerability

- Total Risk = Threats X Vulnerability X Asset Value

Countermeasure/Safeguard – an administrative, operational or logical mitigation against potential risk(s)

InfoSec Terminologies (Cont'd)

Hackers - Unauthorized user who attempts to or gains access to an information system

Crackers – Professional hackers (Bad Guy) who gains access to an information system for specific purposes such as espionage or fraud.

Stenography - The practice of concealing messages or information within other non-secret text or data

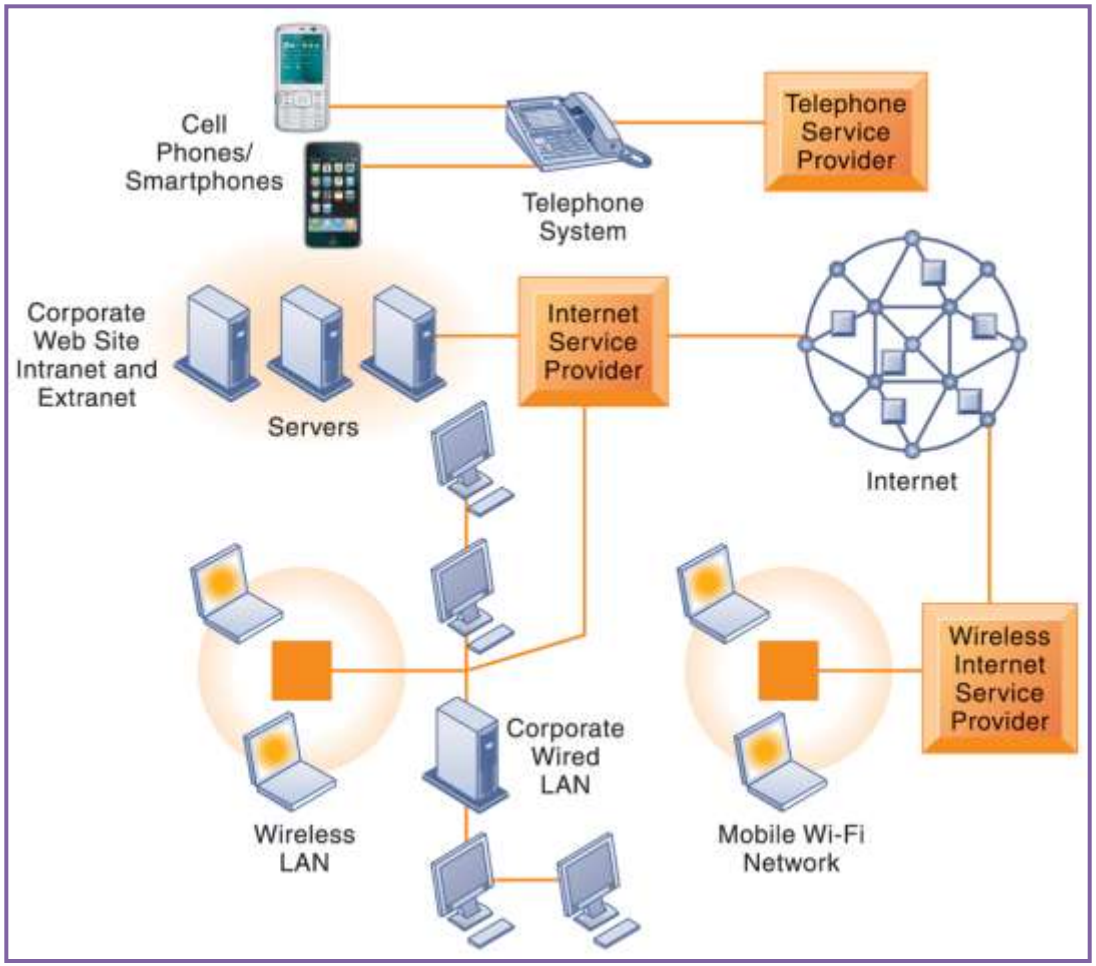
Examples of Assets Needing Protection

- Sales Profits
- Promotions
- Advertising
- Strategies
- Budget
- Forecasts
- Cardholder information
- PIN

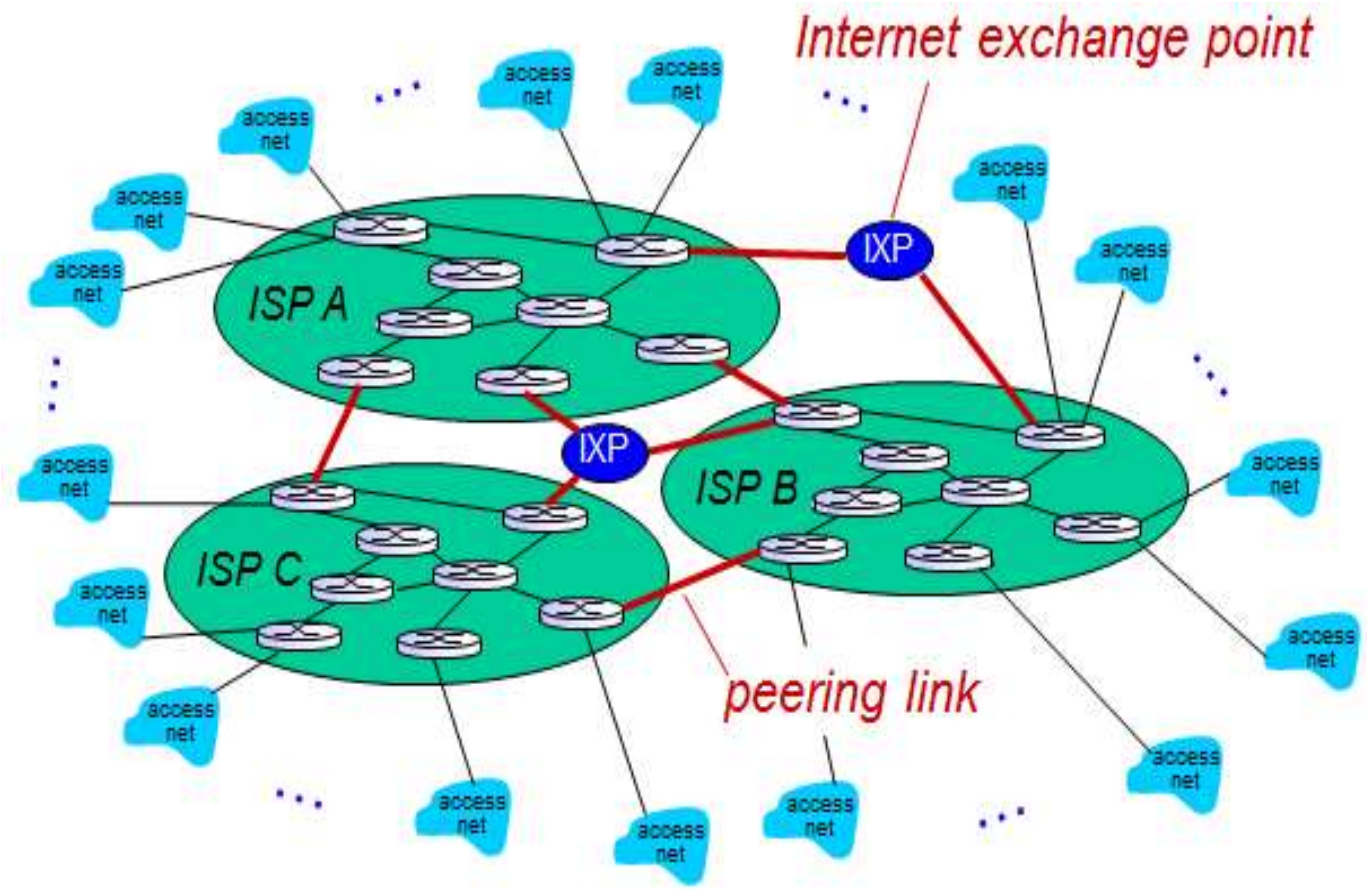
Examples of Threats

- People/Employee
- Hackers/Crackers
- Vendors
- System Failure
- Data Leakage
- Software Bugs
- Spyware
- Spy
- Terrorists

Telecommunications and Networking in Today's Business World



Basic Internet Infrastructure



Defense-in-Depth Strategy

- People
- Operations
- Technology

Defense-In-Depth Solutions

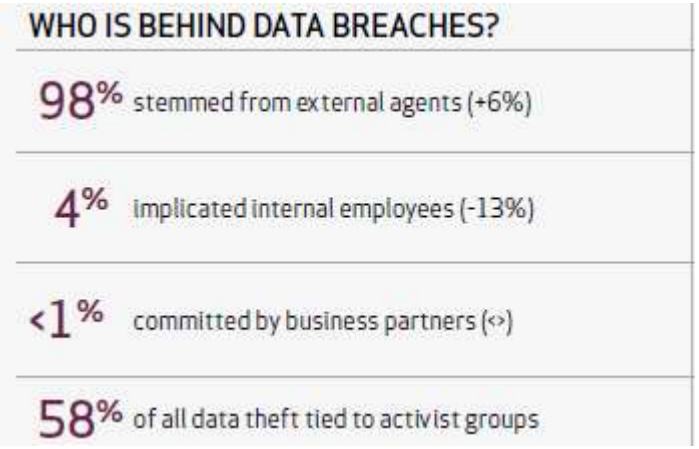
- Vulnerability Management
  - Qualys
  - Tripwire nCircle
- Application Scanner
  - WebInspect
- Patch Management
  - Keseya
- Compliance Management
  - Agiliance
  - Archer Technologies

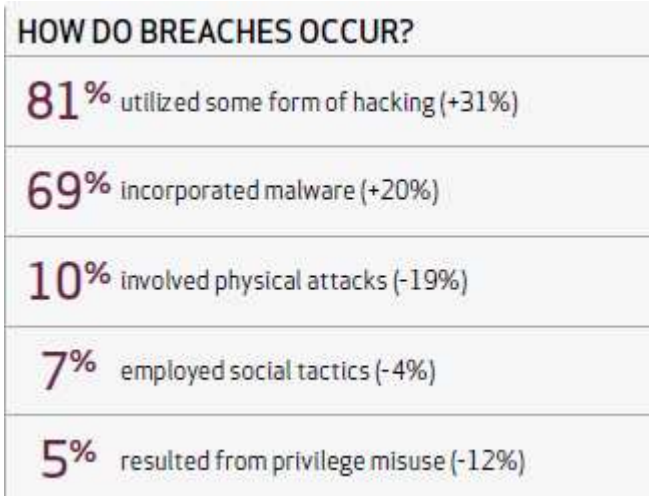
Defense-In-Depth Solutions (Cont'd)

- Enterprise Security Management
  - RedSeal
- Security Information and Event Management
  - Splunk
  - IBM Qradar
  - HP Archsight
- Network Security Monitoring Tool
  - NetWitness

Data Breach Investigation Report

- USSS, NHTCU, AFP, IRISS, PCeU and Verizon collected data based on VERIS (Verizon Enterprise Risk and Incident Sharing).
- DBIR is showing many facets for corporate data theft. (855 incidents, 174 million compromised record). Below, I have a few highlights.





Data Breach Investigation Report (Cont'd)

WHAT COMMONALITIES EXIST?

79% of victims were targets of opportunity (-4%)

96% of attacks were not highly difficult (+4%)

94% of all data compromised involved servers (+18%)

85% of breaches took weeks or more to discover (+6%)

92% of incidents were discovered by a third party (+6%)

97% of breaches were avoidable through simple or intermediate controls (+1%)

96% of victims subject to PCI DSS had not achieved compliance (+7%)

WHERE SHOULD MITIGATION EFFORTS BE FOCUSED?

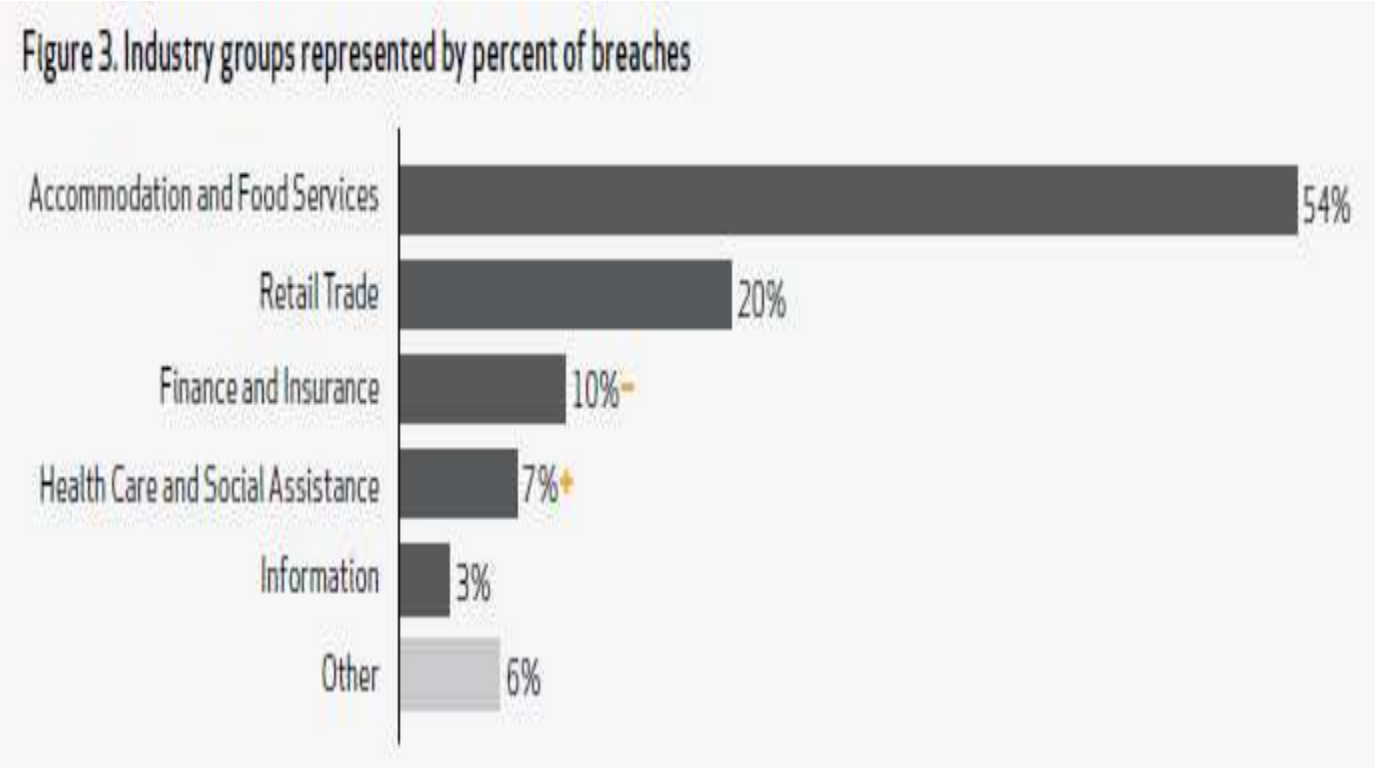
Smaller organizations

- ✔ Implement a firewall or ACL on remote access services
- ✔ Change default credentials of POS systems and other Internet-facing devices
- ✔ If a third party vendor is handling the two items above, make sure they've actually done them

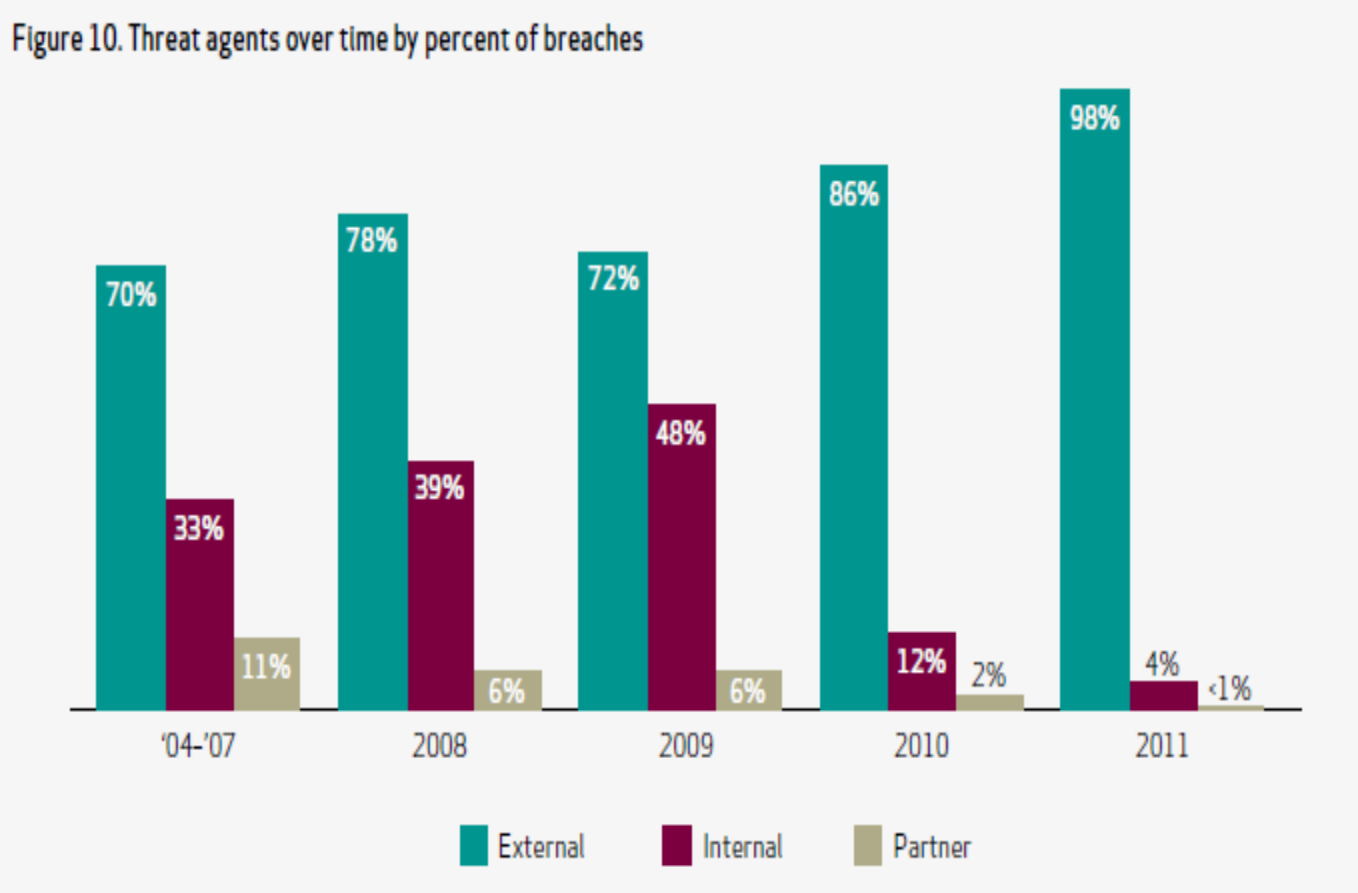
Larger organizations

- ✔ Eliminate unnecessary data; keep tabs on what's left
- ✔ Ensure essential controls are met; regularly check that they remain so
- ✔ Monitor and mine event logs
- ✔ Evaluate your threat landscape to prioritize your treatment strategy
- ✔ Refer to the conclusion of this report for indicators and mitigators for the most common threats

Data Breach Investigation Report (Cont'd)



Data Breach Investigation Report (Cont'd)



Data Breach Investigation Report (Cont'd)

Figure 17.
Number of selected incident classification patterns over time

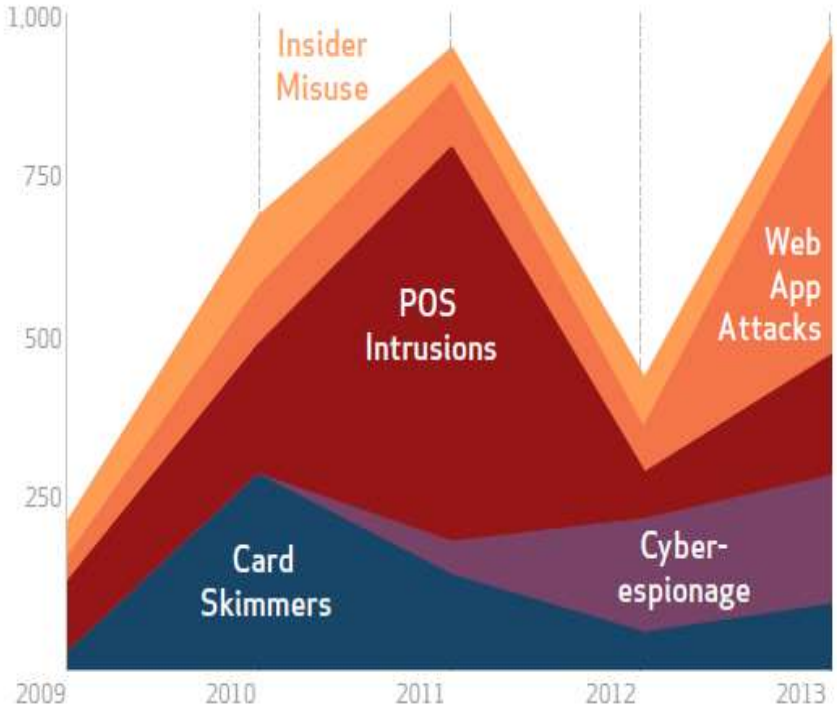
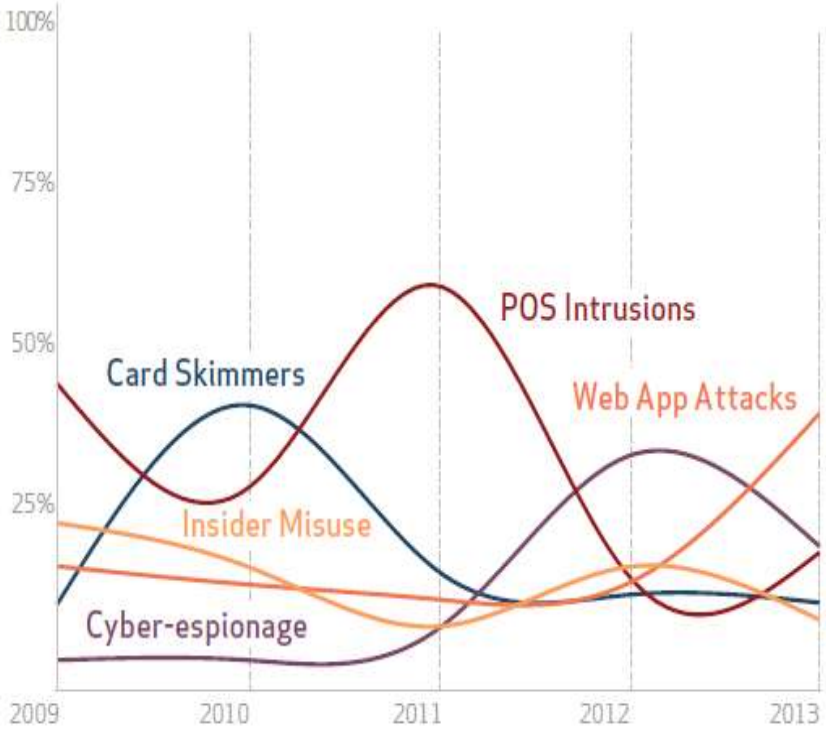
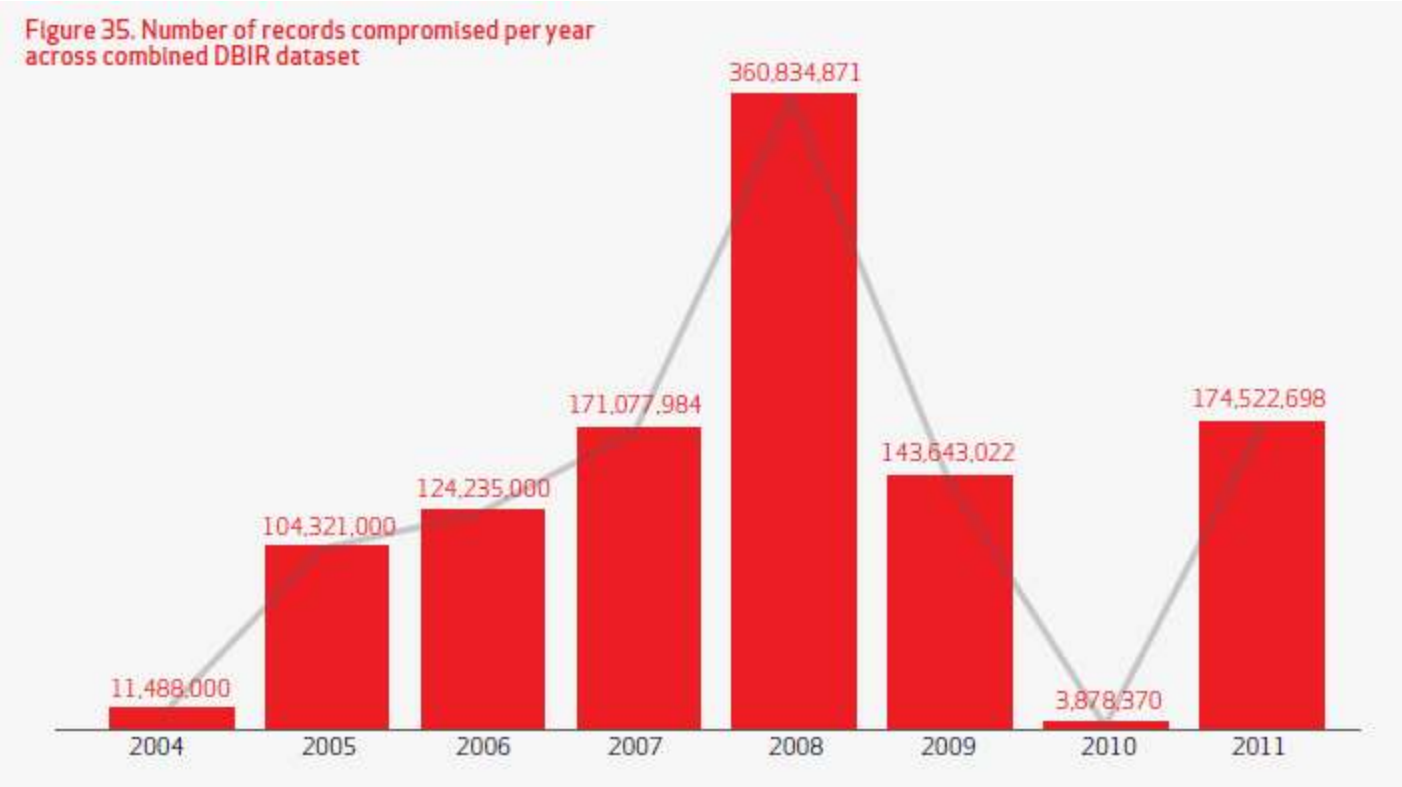


Figure 18.
Percent of selected incident classification patterns over time



Data Breach Investigation Report (Cont'd)



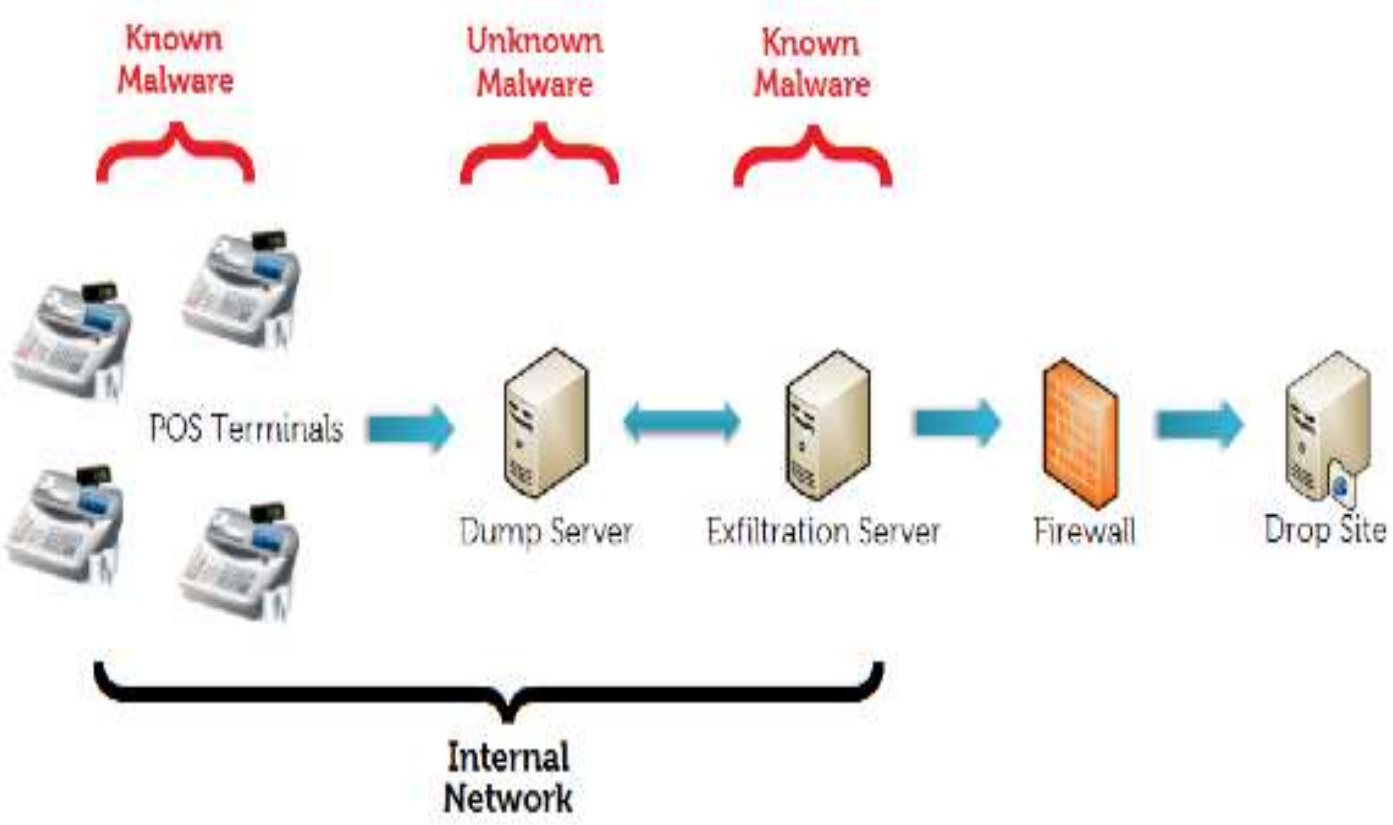
Four Types of Intruders

- Script Kiddies
  - They have a limited knowledge of computer security. They simply cruise along the Internet trying to access any computer they come across.
- Hackers
  - They break into computer networks because they enjoy the challenge and enjoy showing off for friends. Most of the time, they make little attempt to profit from their exploits.
- Crackers
  - They are professional hackers who break into corporate or government computers for specific purposes such as espionage, fraud or intentional destruction.
- Employees
  - These are employees who have legitimate access to the network, but who gain access to information they are not authorized to use.

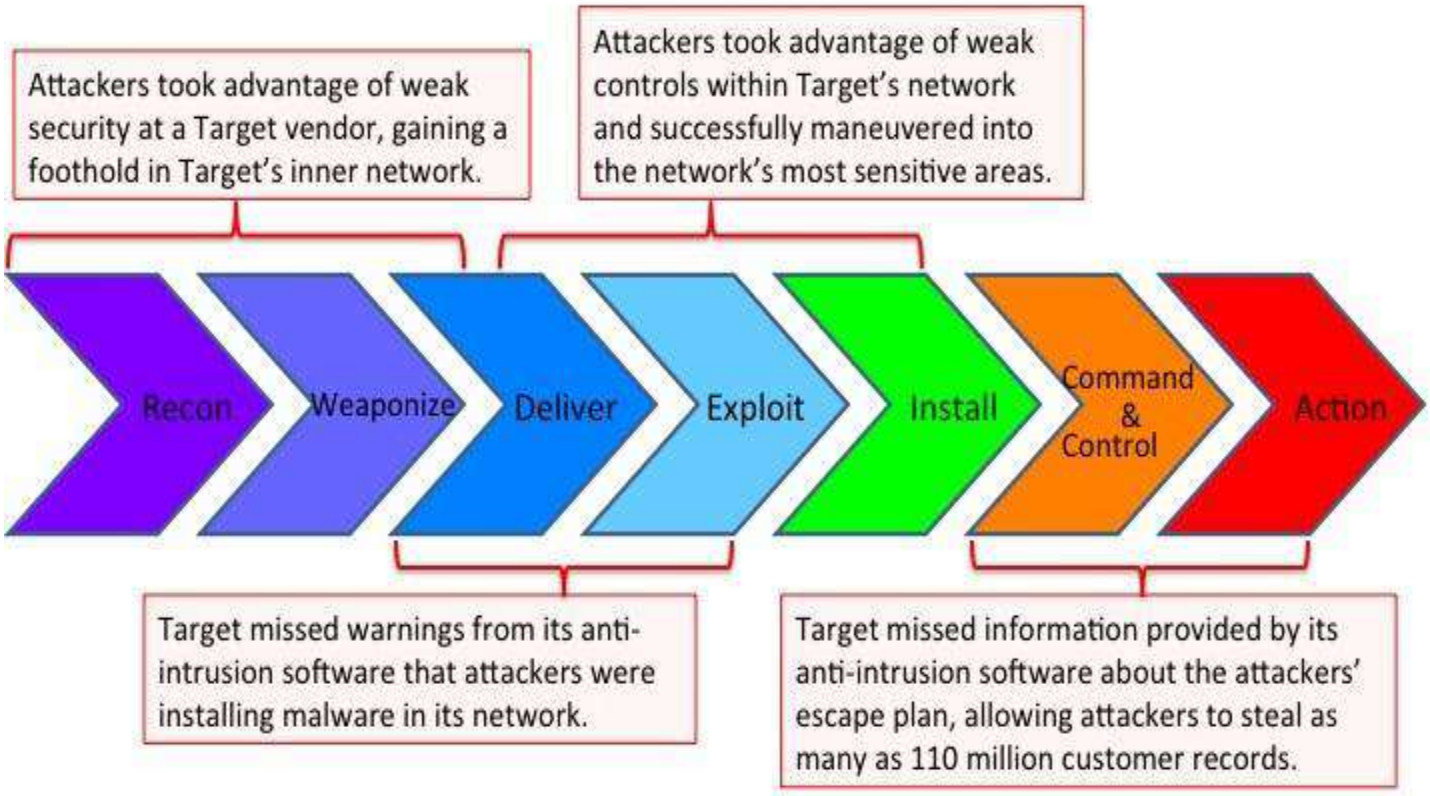
The “Kill Chain “ as a Cybersecurity Defense Tool

Phases of Intrusion Kill Chain

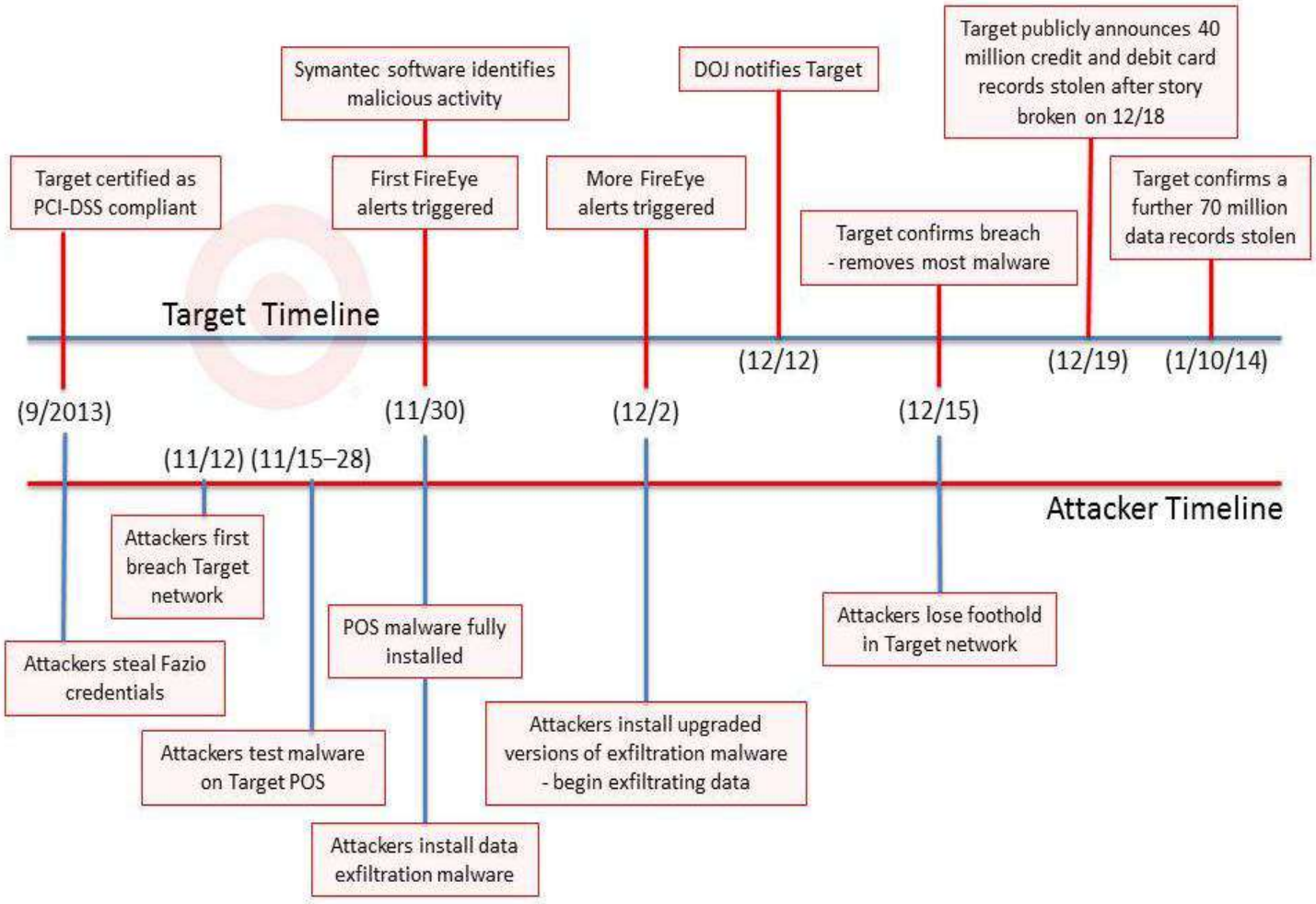
Diagram of Target's Data Exfiltration



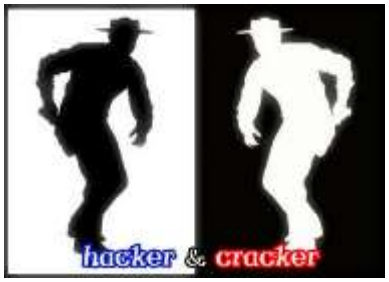
Target's Possible Missed Opportunities



A timeline of the Target Data Breach



Who is Winning the Cyber War?



Intelligence-driven Computer Network Defense

- A risk management strategy that addresses the threat component of risk, incorporating analysis of adversaries, their capabilities, objectives, doctrine and limitations
- Intelligence-driven CND requires a new understanding of the intrusions themselves, not as singular events, but rather as phased progressions

- In a kill chain model, just one mitigation breaks the chain and thwarts the adversary, therefore any repetition by the adversary is a liability that defenders must recognize and leverage

- If defenders implement countermeasures faster than adversaries evolve, the adversary must make more difficult and comprehensive adjustments to achieve their objectives.
- The effect of intelligence-driven CND is a resilient security posture

Courses of Action Matrix

Analysts must reveal indicators through analysis or collaboration, mature these indicators by leveraging them in their tools, and then utilize them when matching activity is discovered.

Table 1: Courses of Action Matrix

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

A Stenography Video Clip

- Hiding something in plain sight
  - https://hub2.devry.edu/node/3386

Key Takeaways…..

- The conventional controls are not sufficient to protect organizations from sophisticated “advanced persistent threats”.
- The kill chain framework must be utilized by information security professionals in both public and private sectors.
- The kill chain is a systematic process to target and engage an adversary to create desired effects.
- Intelligence-driven computer network defense is a necessity in light of advanced persistent threats.
- The kill chain model provides a structure to analyze intrusions, extract indicators and drive the following courses of actions:
  - Intrusion reconstruction
  - Identify indicators of compromise
  - Automate asset management process
  - Educate IT staff about advanced threat vectors
- Defenders goal must be able to move their detection and analysis up the kill chain and more importantly to implement courses of actions across the kill chain.

Questions?

Ed Sadeghi, Adjunct Professor

MS, MCSE, CNE, CISA, CEH, CTGA

ssadeghi@devry.edu

650-269-9742

References

- The International Information Systems Security Consortium
  - www.isc2.com
- Data Breach Investigation Report
  - www.verizonenterprise.com
- Security – Wikipedia
  - http://en.wikipedia.org/wiki/Security
- Intrusion Kill Chain Framework
  - http://www.lockheedmartin.com/
- Business Data Communications and Networking - Dennis Fitzgerald
- Disaster Recover and Planning: Preparing for Unthinkable, 3rd Edition – Jon William Toigo
- Designing Network Security, 2nd Edition - Merike Kaeo
- Management Information Systems - Ken and Jane Laudon
- Security in Computing, 4th Edition - Charles P. Pfleeger