Cybersecurity Strategy
Defense in Depth!

ISACA South Florida WOW! Event

February 20, 2015

Cybersecurity

cybersecurity

noun | cy·ber·se·cu·ri·ty | \-si-ˌkyu̇r-ə-tē\

Definition of CYBERSECURITY

measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack

First Known Use of CYBERSECURITY

1994

Cybersecurity Exposure

Top Ten Data Breaches

Company Name	Year	Compromised	What happened	How?
Heartland Payment Systems (HPS)	2008-2009	130 million records	Compromised payment systems and network	SQL Injection and applied Sniffer Software
Target Stores (TGT)	2013	110 million records	Unauthorized access to payment card data by failure to properly segregate systems	Malware injected to security and payment system
Sony Online Entertainment Services (SOE)	2011	102 million records	PII compromised through cyberattacks	Distributed denial of service attacks (DDoS)
National Archive and Records Administration (NARA)	2008	76 million records	Potential two hard drives losing containing sensitive information	Unencrypted hard drives, potentially insider threat and poor policies

Top Ten Data Breaches

Company Name	Year	Compromised	What happened	How?
Anthem	2015	69 to 80 million records	Hackers breached IT Systems	TBD, hired FireEye to investigate further
Epsilon	2011	60 to 250 million records	Exposed names and e-mail addresses for customers at dozens of companies	Unauthorized entry into an email system and spear phishing attacks generated from this breach
Home Depot	2014	56 million records	Hackers gained access to network, payment card systems and customer email addresses.	Stolen credentials from a 3rd Party Vendor leading to customized malware deployed on payment card systems.

Top Ten Data Breaches

Company Name	Year	Compromised	What happened	How?
Evernote	2013	50+ million records	Network was compromised and a database breach occurred where hackers stole usernames, associated email addresses and encrypted passwords	Used MD5-hashed passwords that were easy to crack
Living Social	2013	50+ million records	Cyber-attack on their computer systems resulted in unauthorized access to some customer data from our servers	Not disclosed: Likelihood this SQL injection attack or attack that leveraged framework vulnerabilities

Value of Data?

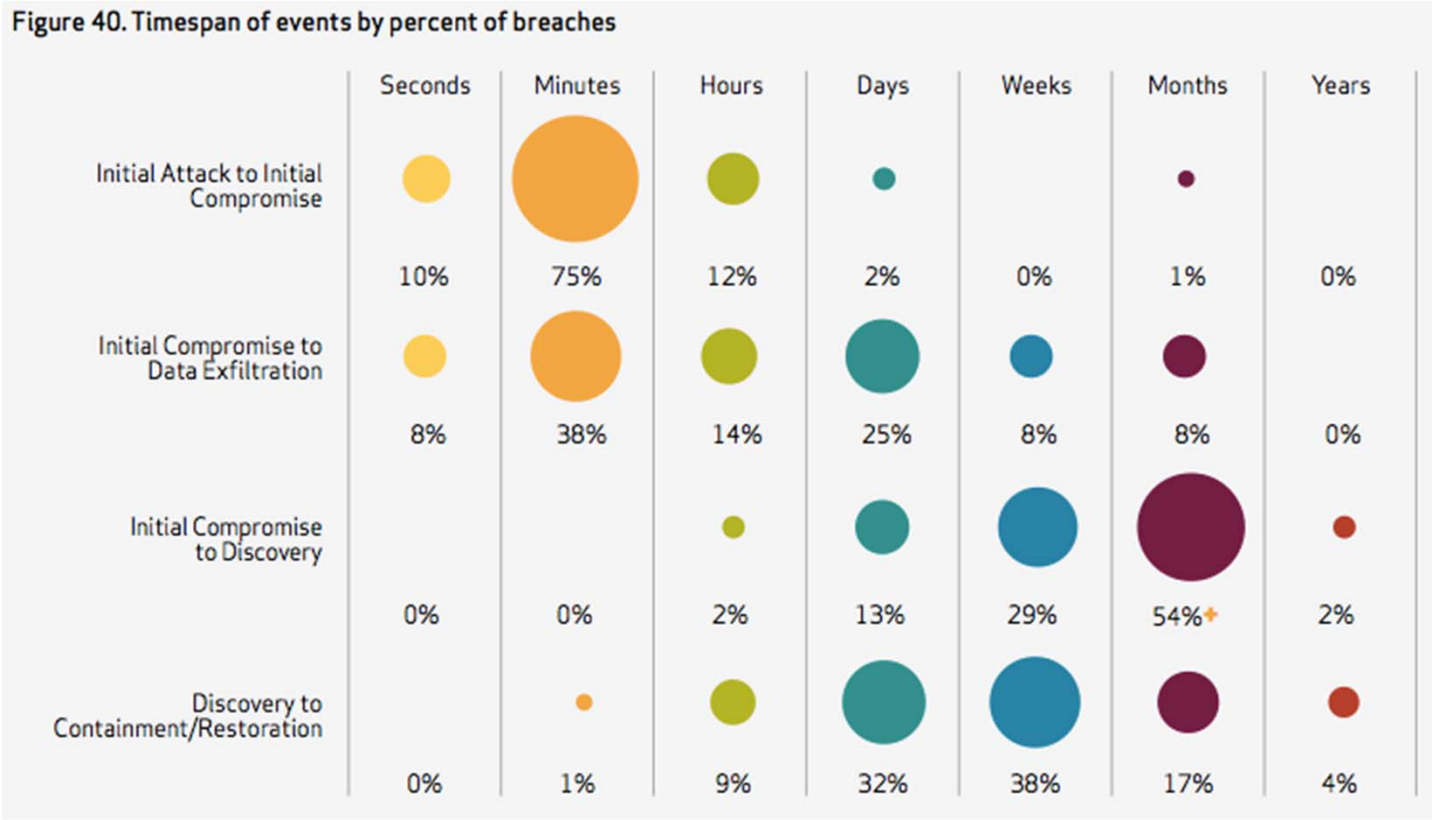
- Personally Identifiable Information (PII)?
- Credit Card Data?
- Protected Health Information (PHI)?
- Sony – Internal Email, Salary Table, Contracts

Who wants your data?

	ORGANIZED CRIME	STATE-AFFILIATED	ACTIVISTS
VICTIM INDUSTRY	Finance Retail Food	Manufacturing Professional Transportation	Information Public Other Services
REGION OF OPERATION	Eastern Europe North America	East Asia (China)	Western Europe North America
COMMON ACTIONS	Tampering (Physical) Brute force (Hacking) Spyware (Malware) Capture stored data (Malware) Adminware (Malware) RAM Scraper (Malware)	Backdoor (Malware) Phishing (Social) Command/Control (C2) (Malware, Hacking) Export data (Malware) Password dumper (Malware) Downloader (Malware) Stolen creds (Hacking)	SQLi (Hacking) Stolen creds (Hacking) Brute force (Hacking) RFI (Hacking) Backdoor (Malware)
TARGETED ASSETS	ATM POS controller POS terminal Database Desktop	Laptop/desktop File server Mail server Directory server	Web application Database Mail server
DESIRED DATA	Payment cards Credentials Bank account info	Credentials Internal organization data Trade secrets System info	Personal info Credentials Internal organization data

Verizon – 2013 Data Breach Investigations Report

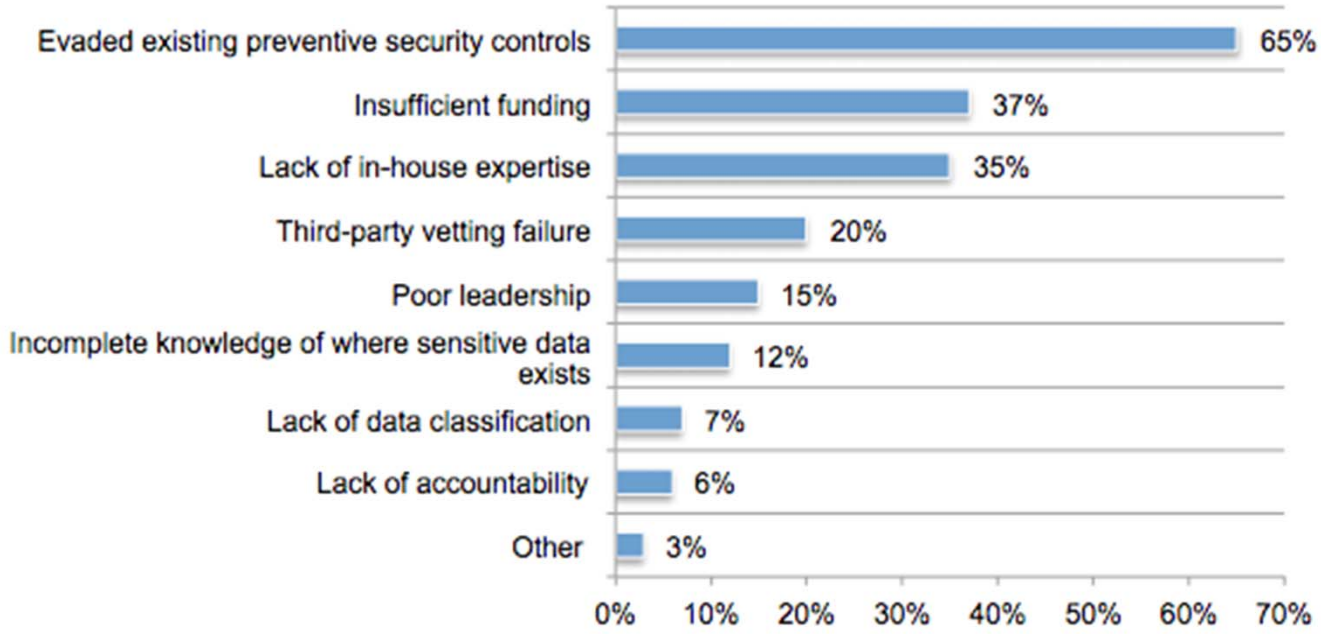
Breach Time Span



Verizon – 2012 Data Breach Investigations Report

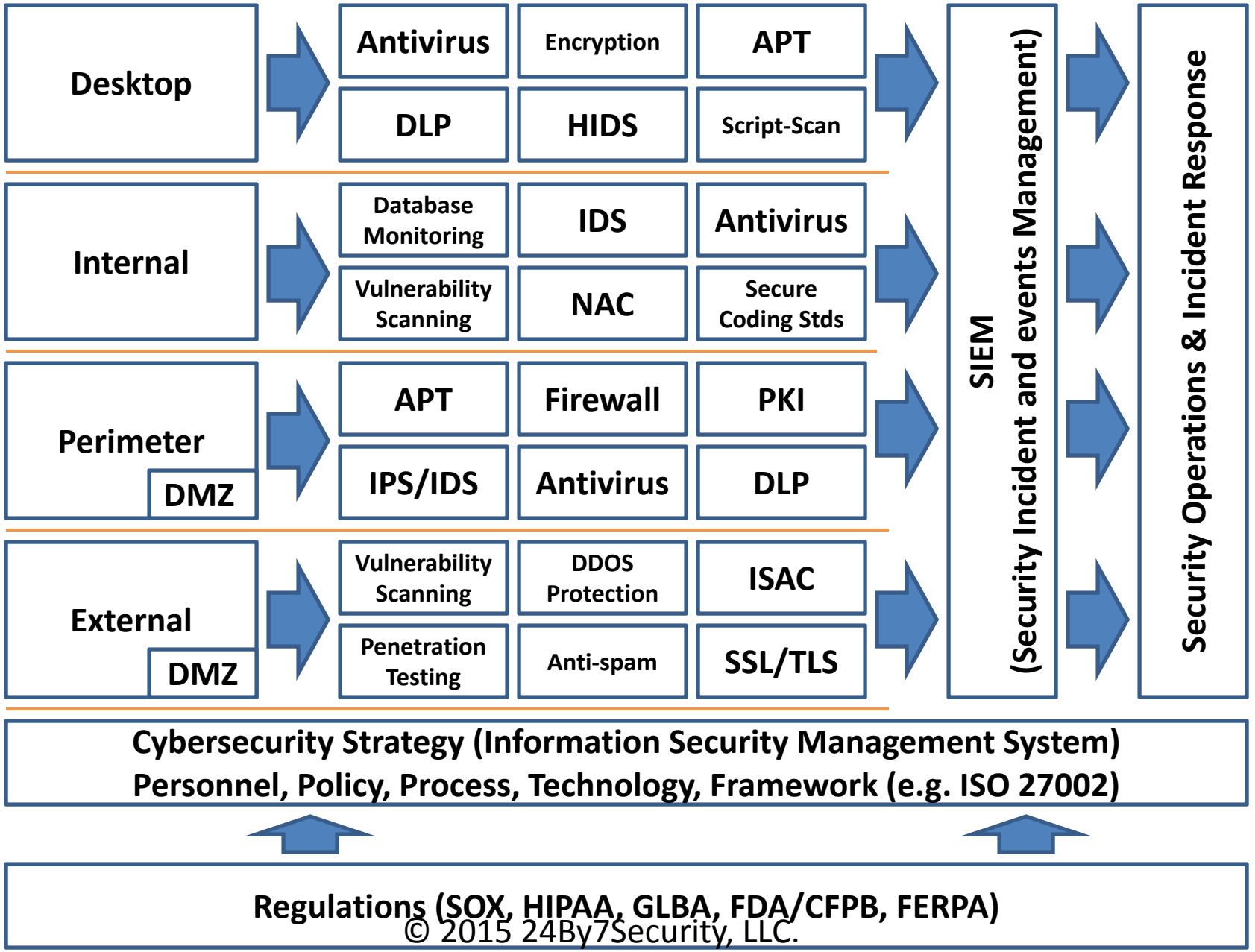
Status of Technology Controls

Figure 11. Why did IT fail to stop the data breach?
Two responses permitted



Ponemon Institute Research Report
2014: A Year of Mega Breaches, Based on a survey of 20,00 IT security practitioners.

Defense in Depth 2.0



Call To Action

- Non-signature based detection
- Controls around firewall, patch management, security monitoring and incident response
- Social Engineering & Security Training
- Skills: In-house vs. Co-source

sanjay.deo@24By7Security.com
24By7security, LLC
facebook.com/24By7Security
@24By7Security