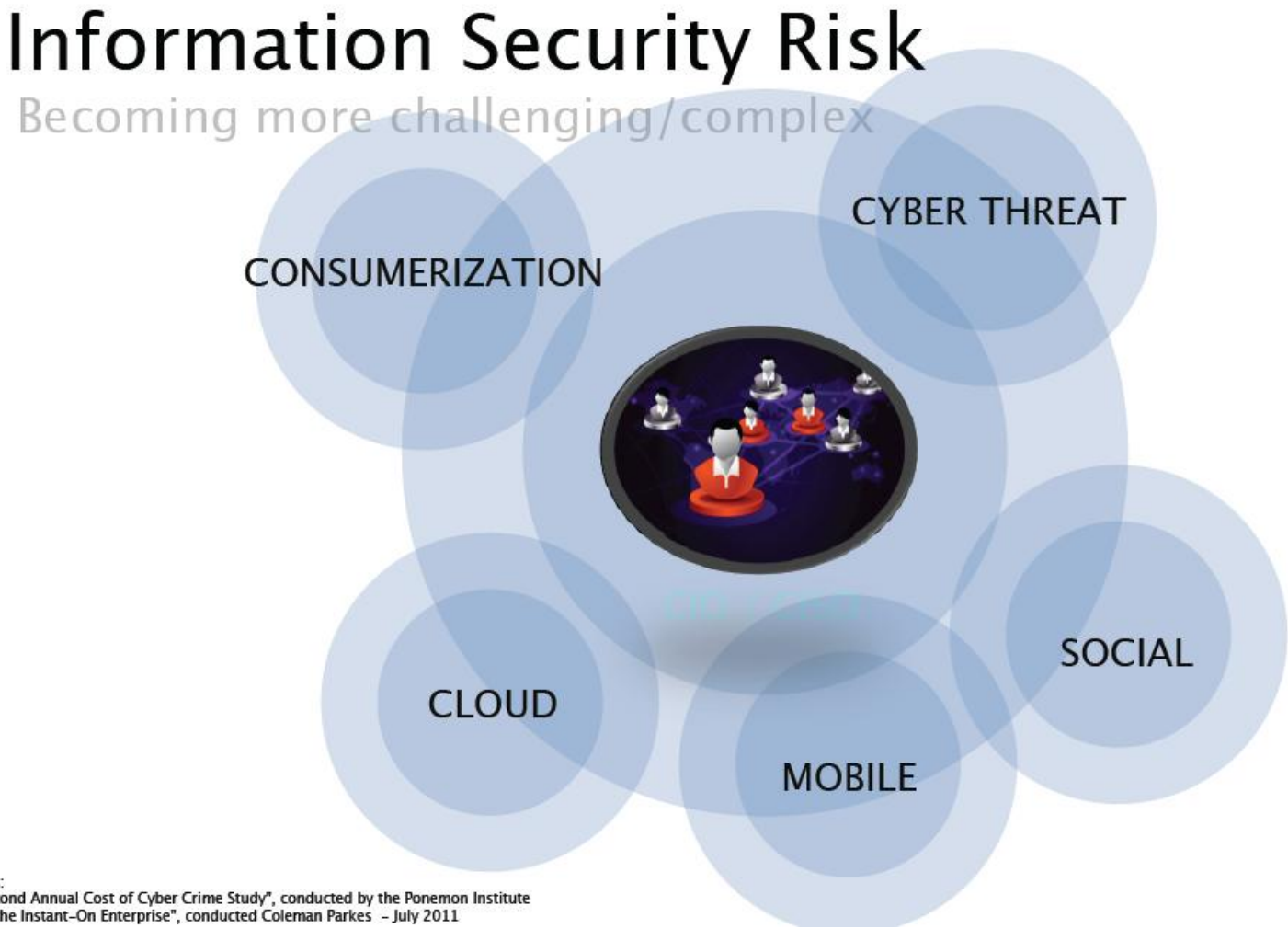
Sirius Security Solutions Presentation

Which way are you looking?

Kevin Russell, MCS, CISSP, CRISC
IT Consultant

Information Security Threats

The IT World is More Complex

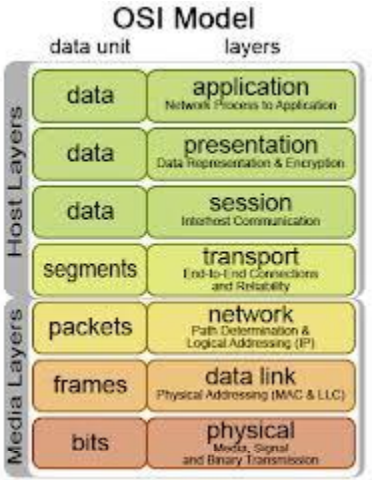


Sources:
"The Second Annual Cost of Cyber Crime Study", conducted by the Ponemon Institute
"Risk & the Instant-On Enterprise", conducted Coleman Parkes – July 2011

Security Trends

- Attacks are moving to the weakest points (and up the OSI stack)
  – Users, Applications, Business Partners, the copier repairman

  The Target Story



- More targeted Custom Malware Attacks (AV still won't save you)

- Social engineering attacks are becoming more sophisticated and widespread

- Social Media will continue to facilitate an increase of the speed and scale of attacks (breaking traditional OODA loop cycles)

- Smartphones, BYOD (bring your own device), and tablets have made havoc on the ever-eroding perimeter; virtualization technology is increasingly providing some safe passage

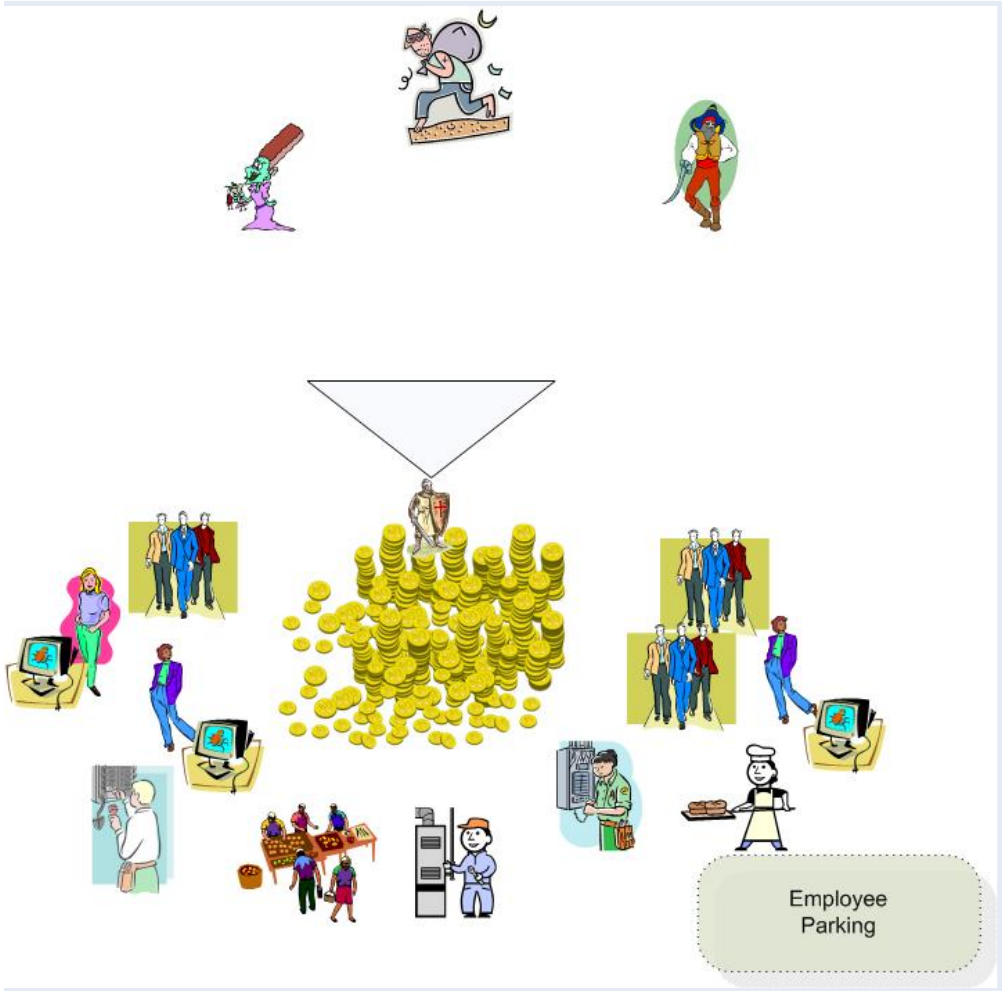
- Compliance is still an issue (PCI, HIPAA – HITECH, etc.)
- Compliance ≠ Security

Early Days of Security

There was the lone security guy

And the GOLD

Early Days of Security



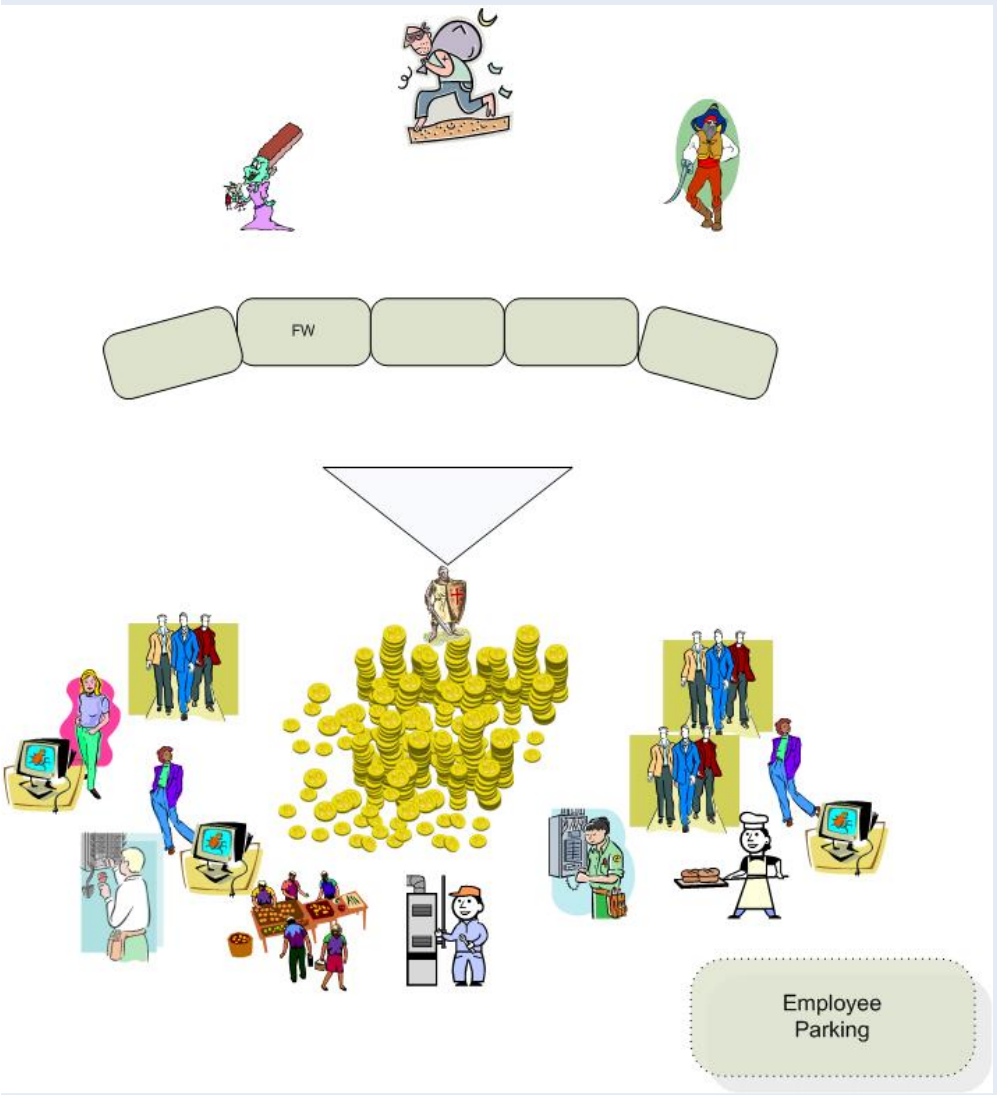
There was the lone security guy

And the perceived threat landscape

Cyber Crime Reports

49,711 in 2001 (est. loss $17.8 M)
75,063 in 2002 (est. loss $54.0M)

Security Field is Growing



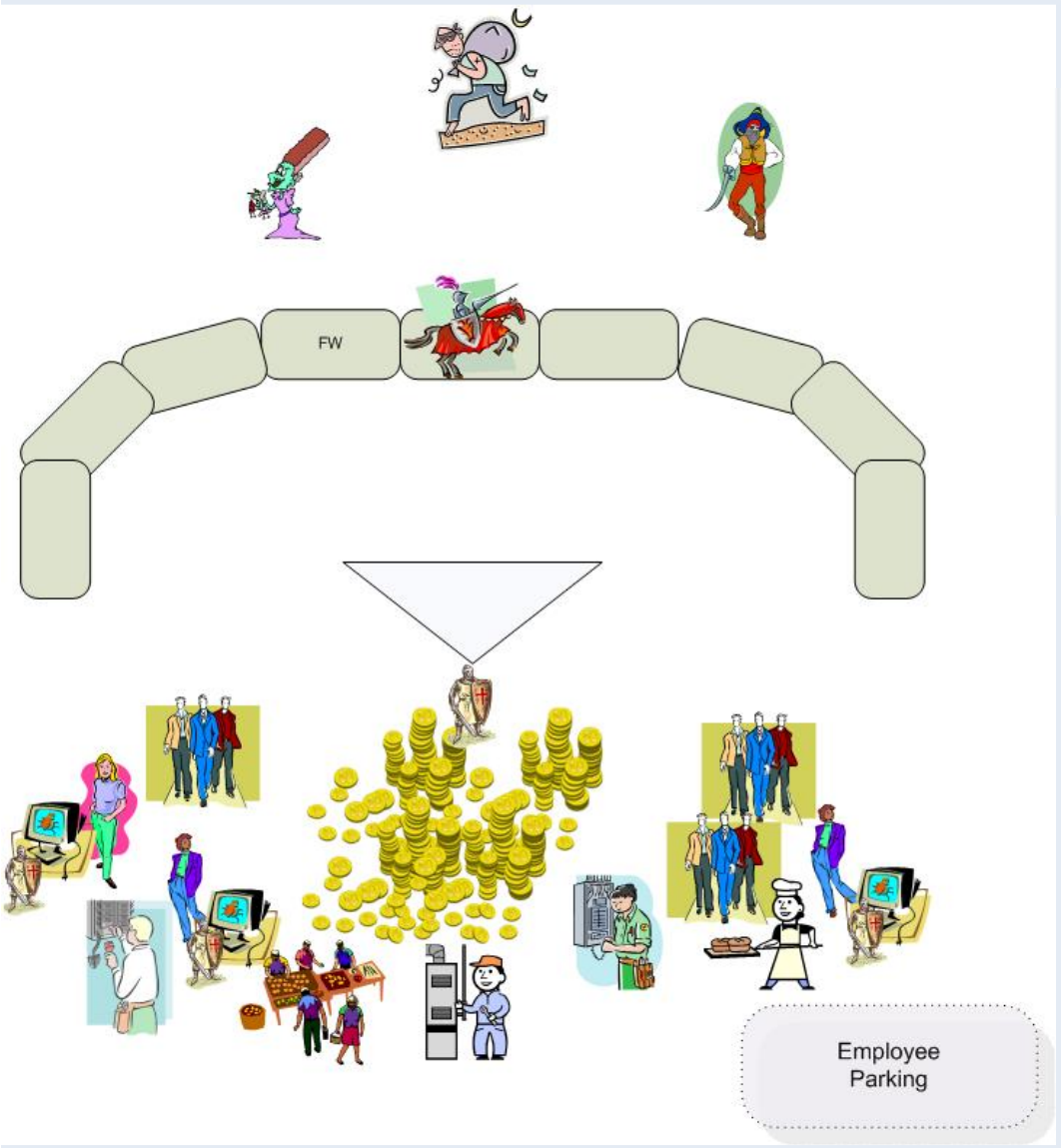
CSI Report– 80% plus attacks from inside
(Often quoted myth from a 2000/2001 report)

So we installed firewalls

Cyber Crime Reports

124,509 in 2003 (est. loss $125.0M)
207,449 in 2004 (est. loss $68.0M)

Cyber Threats are Real



FBI statistics – 2001 real cybercrime statistics (75% individual, 81% male, California, Florida etc)

Number of viruses is growing exponentially

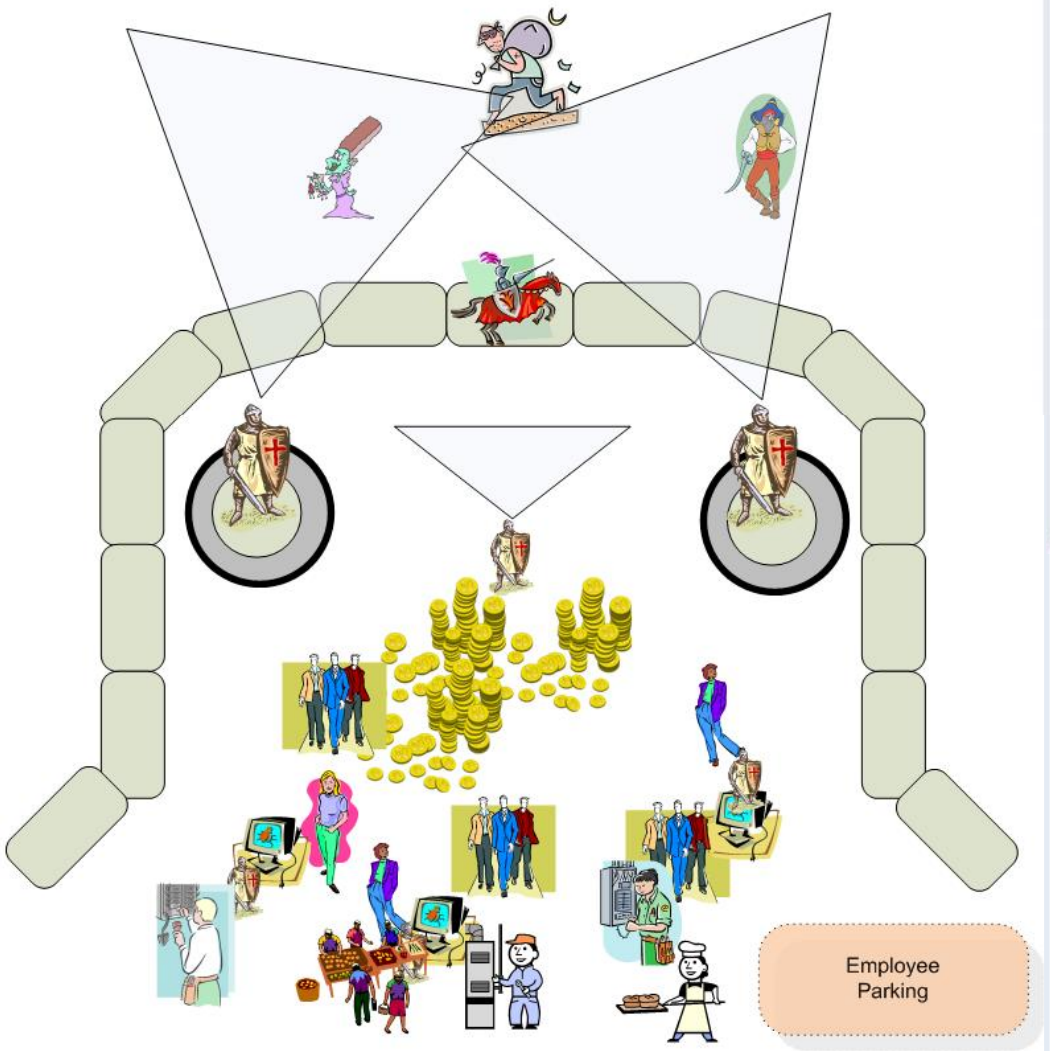
-So we improved our firewalls

-And installed Anti Virus

Viruses Over Time

-1,300 in 1990 to
--50,000 in 2000 to
--More than 200 million in 2010.

Cyber Threats are Increasing



FBI Stats – 2005/6/7 real cybercrime statistics (From 71% to 60% United states, 29% to 40%International)

The threat is more complex and moving

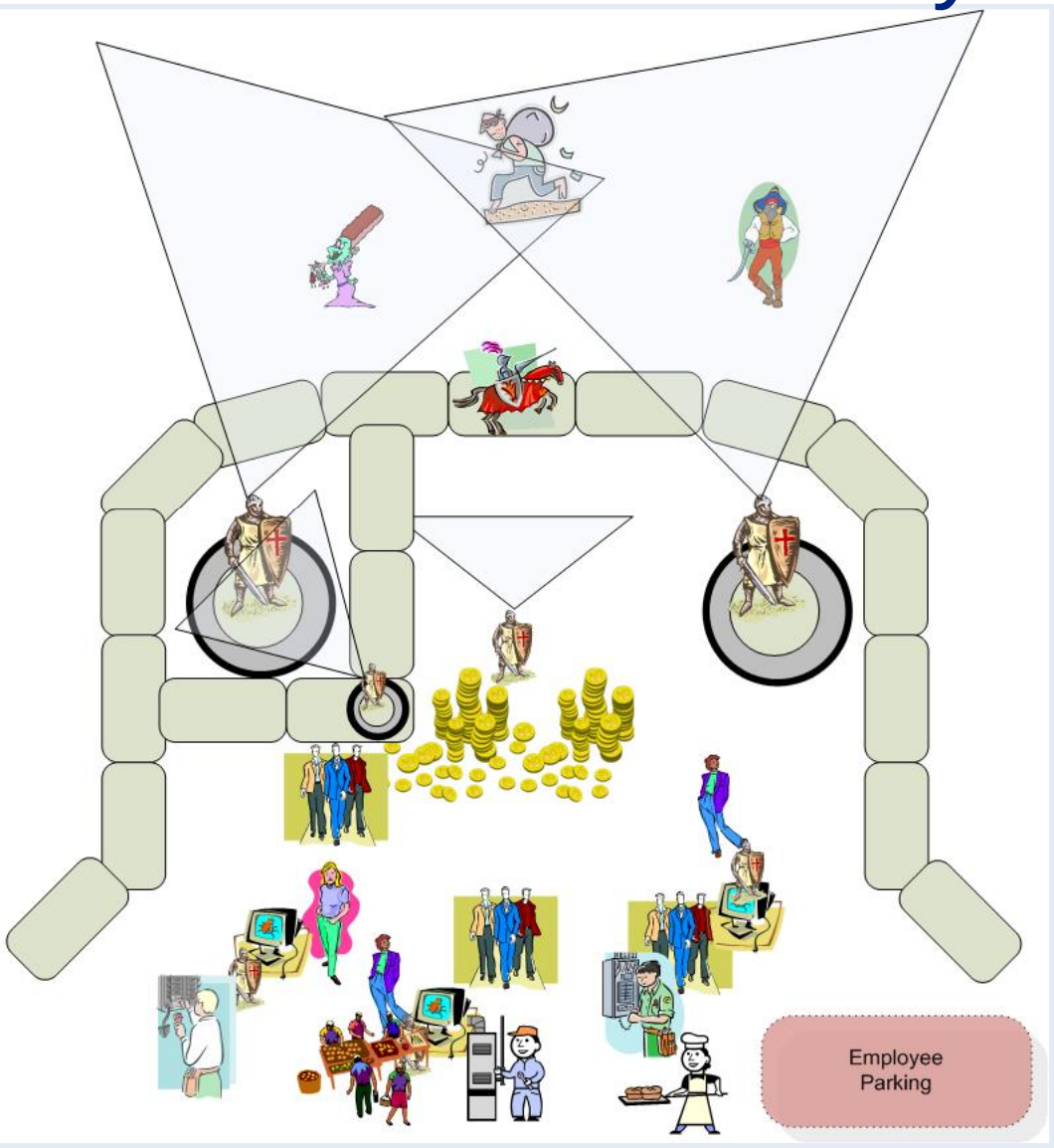
-So we improved our firewalls

-And installed Intrusion Detection

Cyber Crime Reports

231,493 in 2005 (est. loss $183.0M)
207,492 in 2006 (est. loss $198.0M)
206,884 in 2007 (est. loss $239.9M)

Cyber Threats are Increasing



FBI Stats – 2008/9 real cybercrime statistics (65% United states, 35% International)

The threat is more sophisticated

The threat is becoming professional

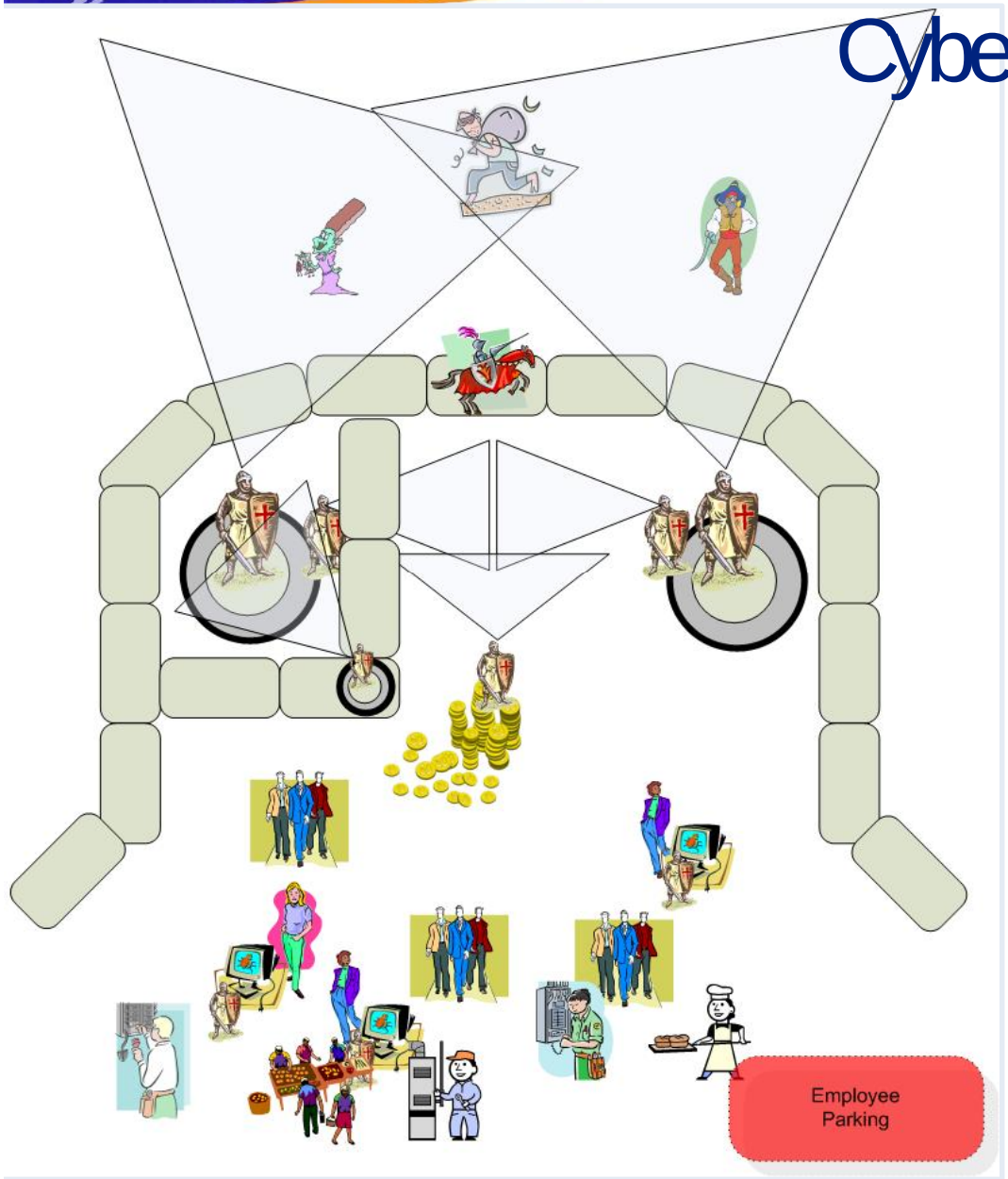
-So we improved our IDS to IPS
-Add log aggregation

- And built DMZs

Cyber Crime Reports

275,284 in 2008 (est. loss $264.0M)
336,655 in 2009 (est. loss $559.0M)

Cyber Threats are Increasing



FBI statistics – The focus is on the type of fraud and not where from. The danger is ubiquitous.

The threat is targeted and specific

The threat is organized and government sponsored

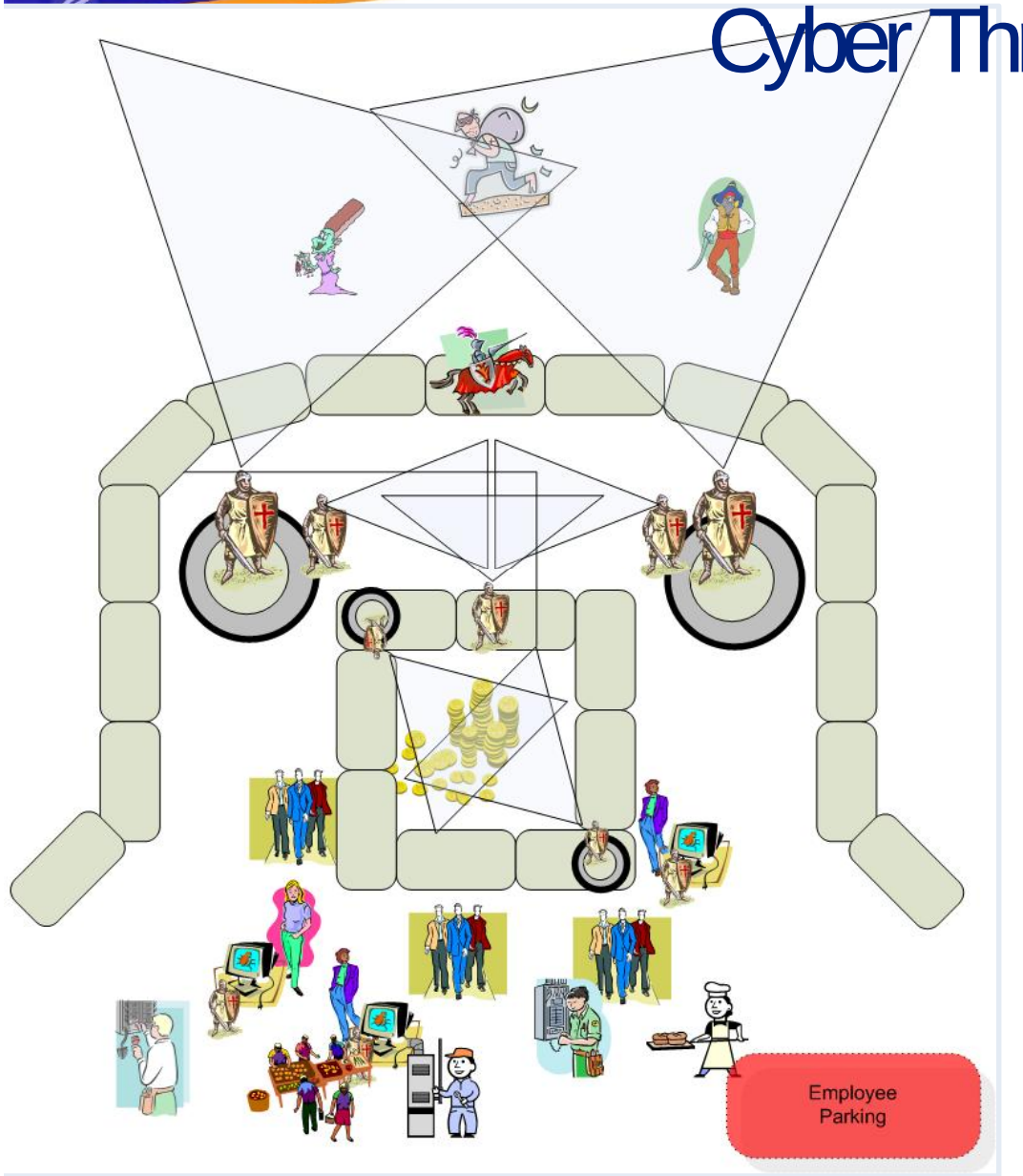
- So we expanded monitoring

- And installed Data Loss Protection

Cyber Crime Reports

314,246 in 2011 (est. loss $485.3M)
289,874 in 2012 (est. loss $525.4M)

Cyber Threats are Commonplace



Today
The threat is from many vectors

What can the security team do?

Protect the assets!

- Logging
- Information gathering
- Blocking
- Monitoring

Cyber Crime Reports

262,813 in 2013 (est. loss $781.8M)

Why this story? Why Now?

Because we can finally do something about it!

- **Finally monitoring at line speed**
- **SIEMS are workable, reliable, and manageable.**
- **Mass log aggregation is a reality**
  Disk Space is cheap and plentiful for all logs

A Practical Defense

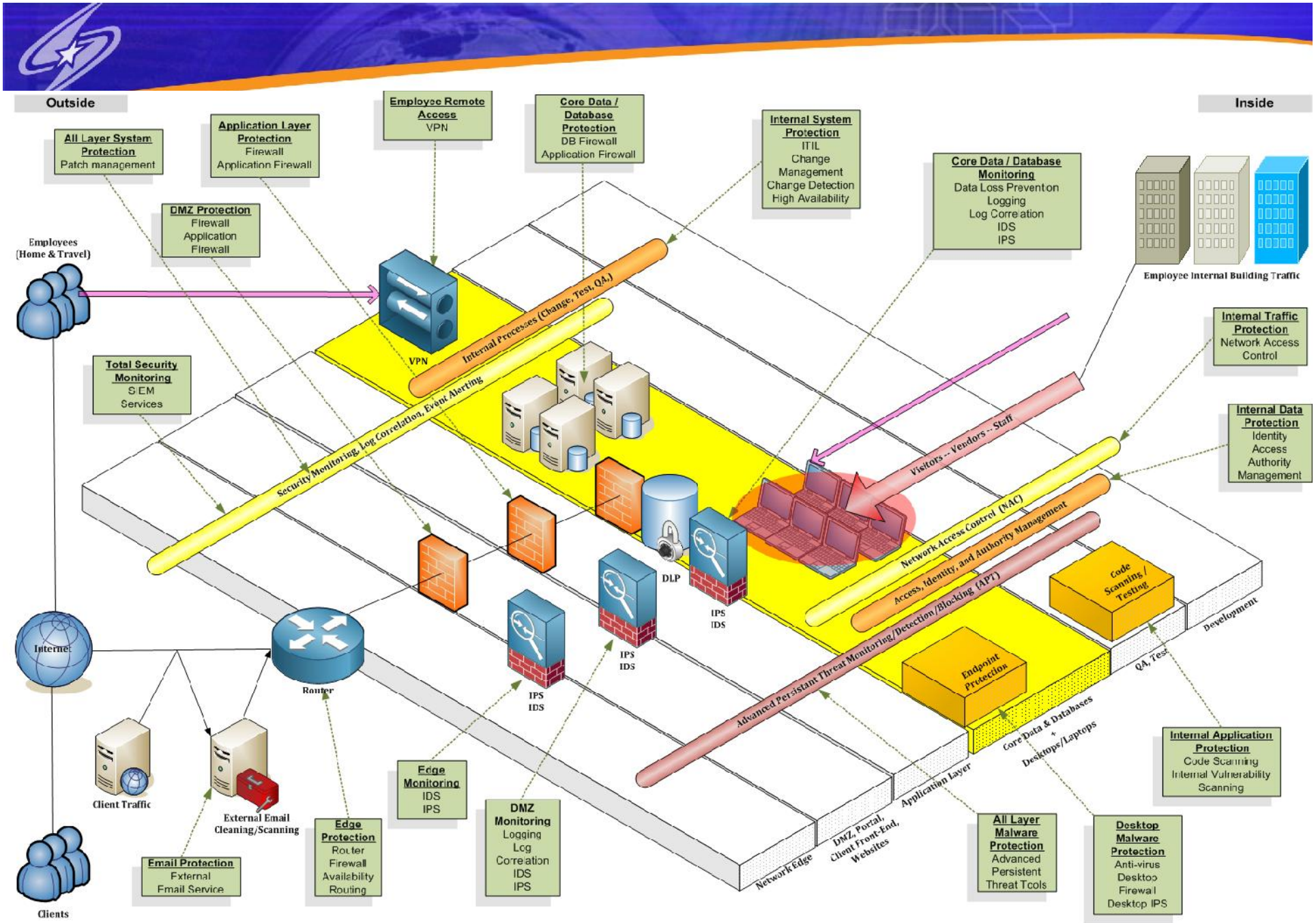
“It is said that if you know your enemies and know yourself, you will not be imperiled in a hundred battles; if you do not know your enemies but do know yourself, you will win one and lose one; if you do not know your enemies nor yourself, you will be imperiled in every single battle.” Sun Tzu 孫子

- Organizations must understand the value of
- Assets and information

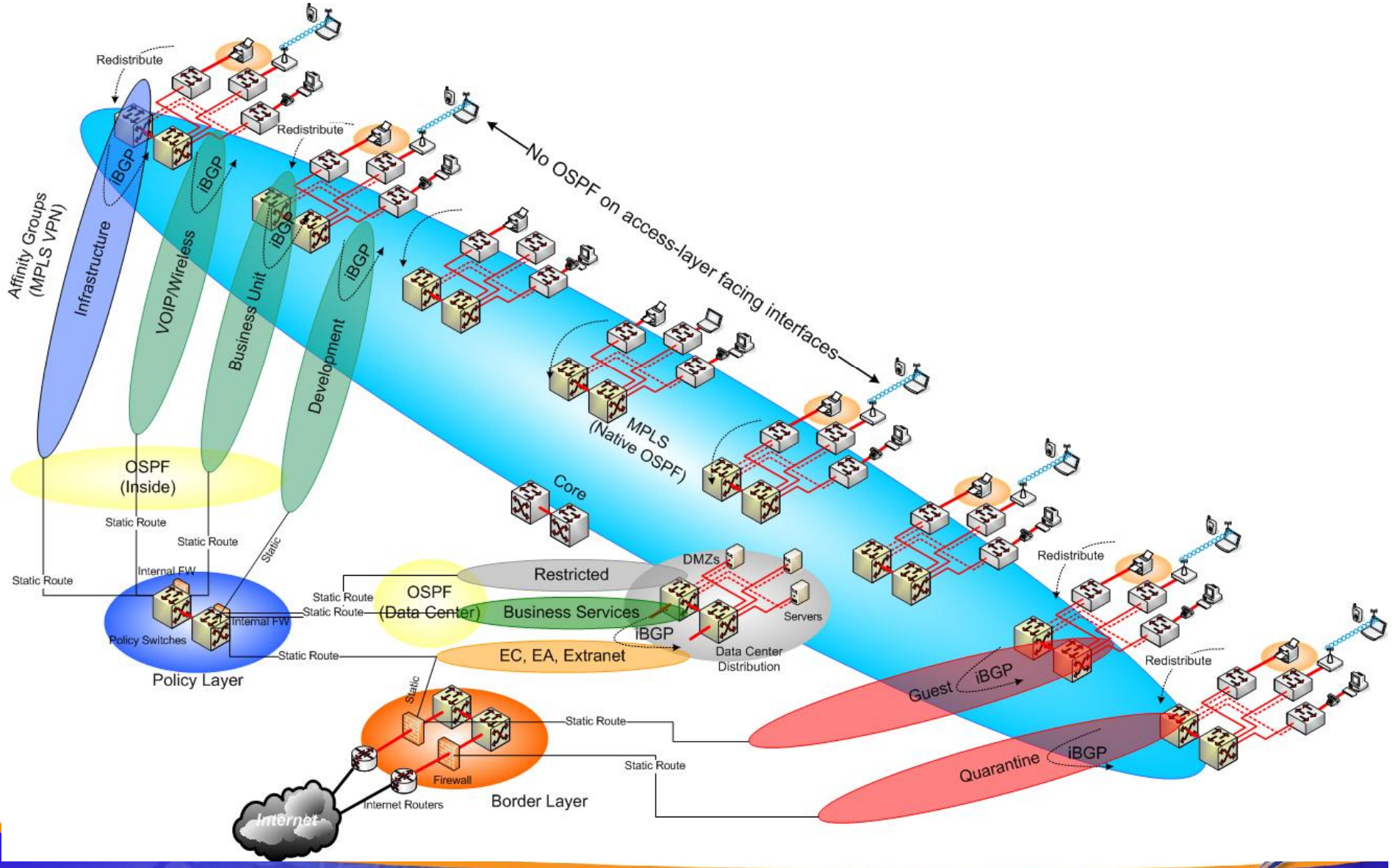
- Organizations must know potential impacts
- of security events

- Organizations must understand the
- defensive capabilities of the organization

Security assessments help organizations understand the enemy and themselves

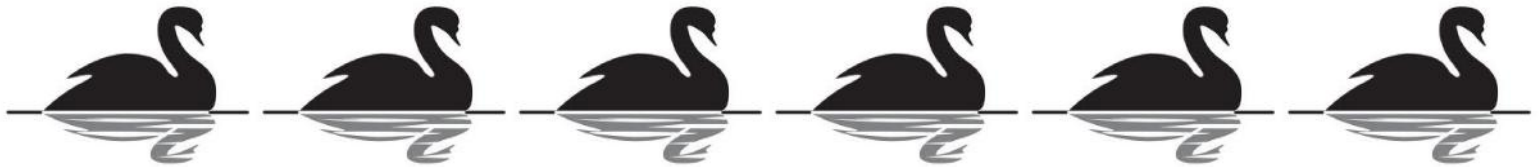

Outside
Inside
All Layer System Protection
Patch management
Application Layer Protection
Firewall
Application Firewall
Employee Remote Access
VPN
Core Data / Database Protection
DB Firewall
Application Firewall
Internal System Protection
ITIL
Change Management
Charge Detection
High Availability
Core Data / Database Monitoring
Data Loss Prevention
Logging
Log Correlation
IDS
IPS
DMZ Protection
Firewall
Application
Firewall
Employees
(Home & Travel)
Employee Internal Building Traffic
Internal Traffic Protection
Network Access Control
VPN
Internal Processes (Change, Test, QA)
Total Security Monitoring
SIEM
Services
Security Monitoring, Log Correlation, Event Alerting
Visitors -- Vendors -- Staff
Internal Data Protection
Identity
Access
Authority
Management
Network Access Control (NAC)
Access, Identity, and Authority Management
Advanced Persistant Threat Monitoring/Detection/Blocking (APT)
DLP
IPS
IDS
Code Scanning / Testing
Development
QA, Test
Endpoint Protection
Core Data & Databases
+
Desktops/Laptops
Application Layer
Internet
Router
IPS
IDS
IPS
IDS
IPS
IDS
Internal Application Protection
Code Scanning
Internal Vulnerability Scanning
Client Traffic
External Email
Cleaning/Scanning
Edge Monitoring
IDS
IPS
DMZ Monitoring
Logging
Log Correlation
IDS
IPS
All Layer Malware Protection
Advanced Persistent Threat Tools
Desktop Malware Protection
Anti-virus
Desktop Firewall
Desktop IPS
Email Protection
External
Email Service
Edge Protection
Router
Firewall
Availability
Routing
Clients
Network Edge
DMZ, Portal, Client Front-End, Websites

Information Security Zone Architecture



A Practical Defense

- **Static Defenses (no human action required)**
  - Static security works best against copycats who repeat attacks
    - AV, IPS, Malware Detection, Data Execution Protection
  - Defense in Depth, Data Decentralization and Compartmentalization
- **Active Defenses and Detection (labor saving tools and force multipliers)**
  - Security Event and Incident Monitors (SIEMs)
  - Incident Detection and Response (1 responder to 7,500 systems for enterprise – SANS)
  - Hybrid models for IR through managed services
- **Risk Reduction and resiliency (reduce the impact of possible bad events)**
  - Reduce target value, eliminate or modify activities that have spectacular failure modes



Statistics in this Presentation

Viruses Over Time

-1,300 in 1990 to
--50,000 in 2000 to
--More than 200 million in 2010.

Cyber Crime Reports

49,711 in 2001 (est. loss $17.8 M)
75,063 in 2002 (est. loss $54.0M)
124,509 in 2003 (est. loss $125.0M)
207,449 in 2004 (est. loss $68.0M)
231,493 in 2005 (est. loss $183.0M)
207,492 in 2006 (est. loss $198.0M)
206,884 in 2007 (est. loss $239.9M)
275,284 in 2008 (est. loss $264.0M)
336,655 in 2009 (est. $559.0M)
303,809 in 2010
314,246 in 2011 (est. loss $485.3M)
289,874 in 2012 (est. loss $525.4M)
262,813 in 2013 (est. loss $781.8M)

SIRIUS
COMPUTER SOLUTIONS

Thank You