Security Essentials

Miguel (Mike) O. Villegas
CISA, CISSP, GSEC, CEH, QSA, PA QSA, ASV
Director - K3DES LLC

Core Competencies – C24

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

2013 Fall Conference – "Sail to Success"

CRISC
CGEIT
CISM
CISA

Abstract

The adage **"Security is everyone's business"** has not changed but what has changed is security itself. The implementation of security is often disparate primarily due to a lack of understanding, support or wherewithal with those responsible for protecting critical assets.

This course will cover the essentials of information security. It is meant to be offered to those with low to medium level knowledgeable attendees; however, more advanced attendees might profit from a refresher, if for nothing else, to confirm their understanding of information security essentials.

Due to time constraints and possibly offered in other courses at this conference, this will not cover Physical Security, Business Continuity Planning, or Laws, Investigations and Ethics.

Table of Contents

- Security Basics
- Security Models
- Security Architecture
- Network Security
- Internet Security
- Cloud Security
- Operating System Security
- Database Security
- Application Security
- Web Application Security
- Encryption
- Security Monitoring
- Compliance

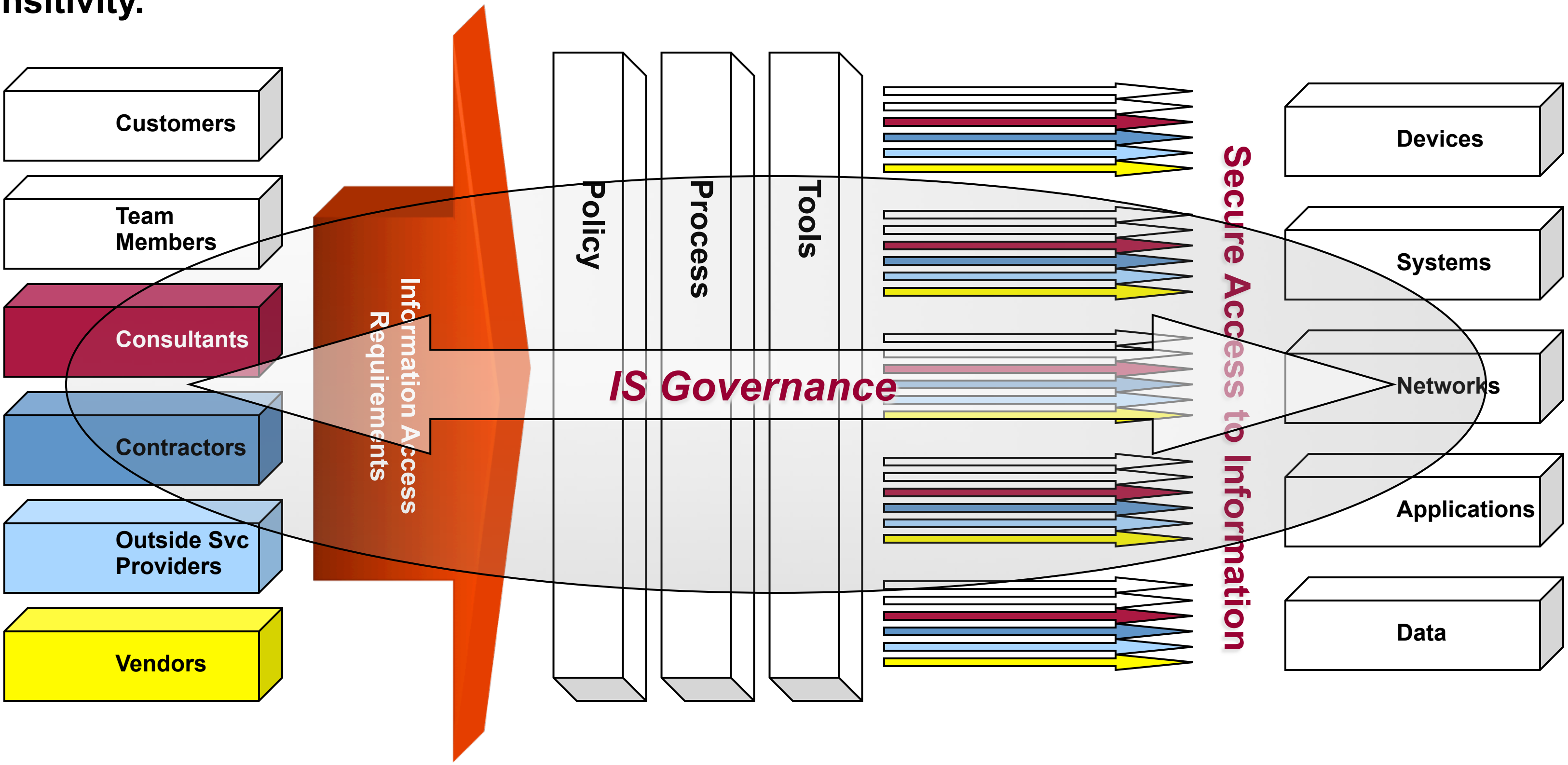
Not Covered: Although Important, these will not be covered strictly due to time constraints.

- Mobile Security
- Physical Security
- Vendor Management
- Personnel Security

- Risk Assessment – clearly needs to be performed FIRST but we will never ~~finish~~ start if we cover RA

Sample Information Security Vision

IS VISION: Policies, business processes, and technical infrastructure are aligned to effectively and efficiently protect information based on its value, vulnerability and sensitivity.



Security Basics

"Data security refers to protection of data against accidental or intentional disclosure to unauthorized persons, or unauthorized modifications or destruction."

-James Martin (1973 – "Security, Accuracy and Privacy in Computer Systems")

"Data security is the protection of data from accidental or malicious modification, destruction, or disclosure."

-Official (ISC)2 Guide to the CISSP Exam (2012)

What Has Changed?

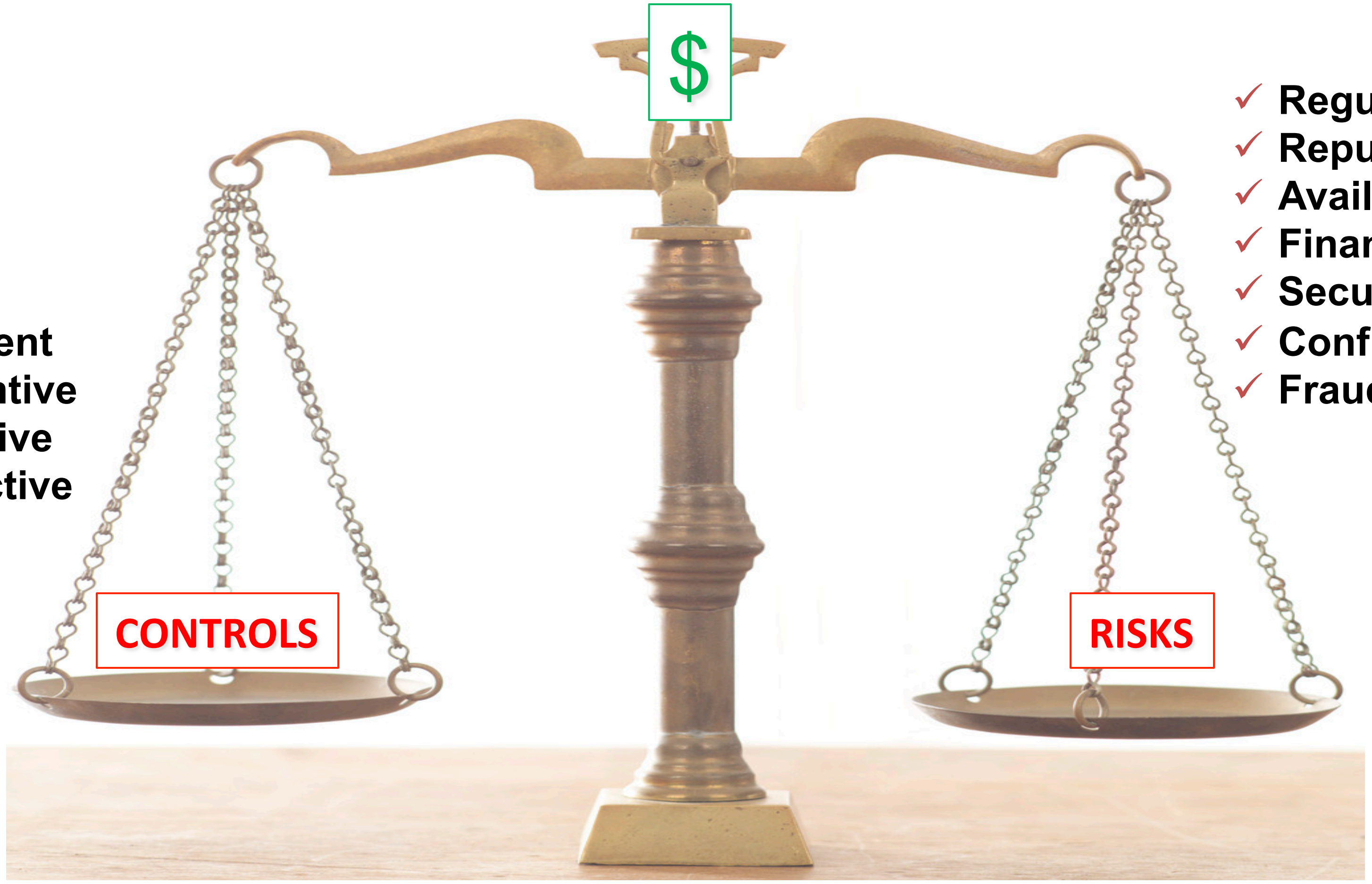
- Technology
- User Technical Skillset (CBOK)
- Teenage Hacker to Nation State Backed Hackers
- Ubiquitous Mobile Technology (PC/Smart Phone/Pads)
- Cyberlaws / Cybercrime
- Strict Standards Compliance
- Everything talks to everything: “any-to-any”
- Multi-Platform/Multi-System/Multi-Application/ Multi-User Environments
- Security Software: AV, ESM, Layer 3 security devices (FW/ Router/Switches), WAF, DLP (Network/DB/EndPoint), FIM, IDS/IPS, SIEM, MDM

Absolute Security Does Not Exist

But We Still Put in Controls

- Alarms
- Locks
- Sensors
- Video Cameras
- Guard Dogs
- Alert Authorities
- Insurance
- Security Awareness
- Training
- Contingency Procedures
- Stay informed / trained

Balanced View of Information Security



- ✓ Deterrent
- ✓ Preventive
- ✓ Detective
- ✓ Corrective

- ✓ Regulatory
- ✓ Reputation
- ✓ Availability
- ✓ Financial
- ✓ Security
- ✓ Confidentiality
- ✓ Fraud

STRATEGIC BUSINESS OBJECTIVES

I - A - A

IDENTIFICATION - AUTHENTICATION - AUTHORIZATION -

Information

- **IDENTIFICATION – I AM MIKE**
- **AUTHENTICATION – PROVE IT**
  - **Something I KNOW**
  - **Something I HAVE**
  - **Something I AM**
- **AUTHORIZATION – ACCESS TO WHAT?**
  - **Access Level**
  - **Information Requested**
  - **Approval**

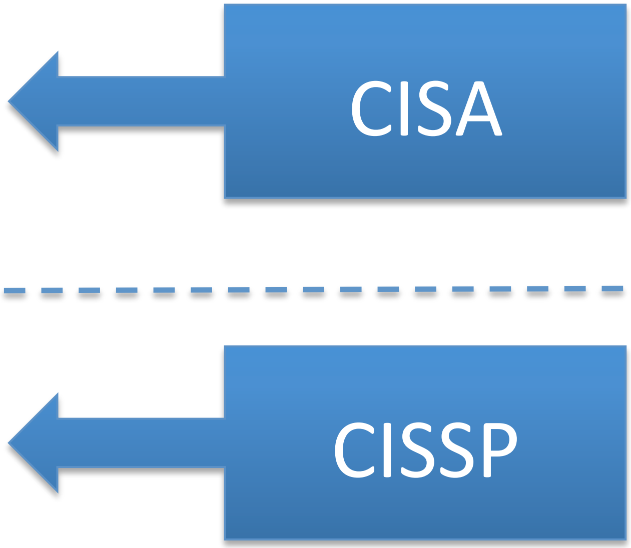
Identification and Authentication

- Logon IDs and passwords
- Features of passwords
- Password syntax (format) rules
- Token devices, one-time passwords
- Biometric
- Single Sign-On (SSO)

Types of Controls

- Preventive
- Detective
- Corrective

- Directive
- Recovery



CISA

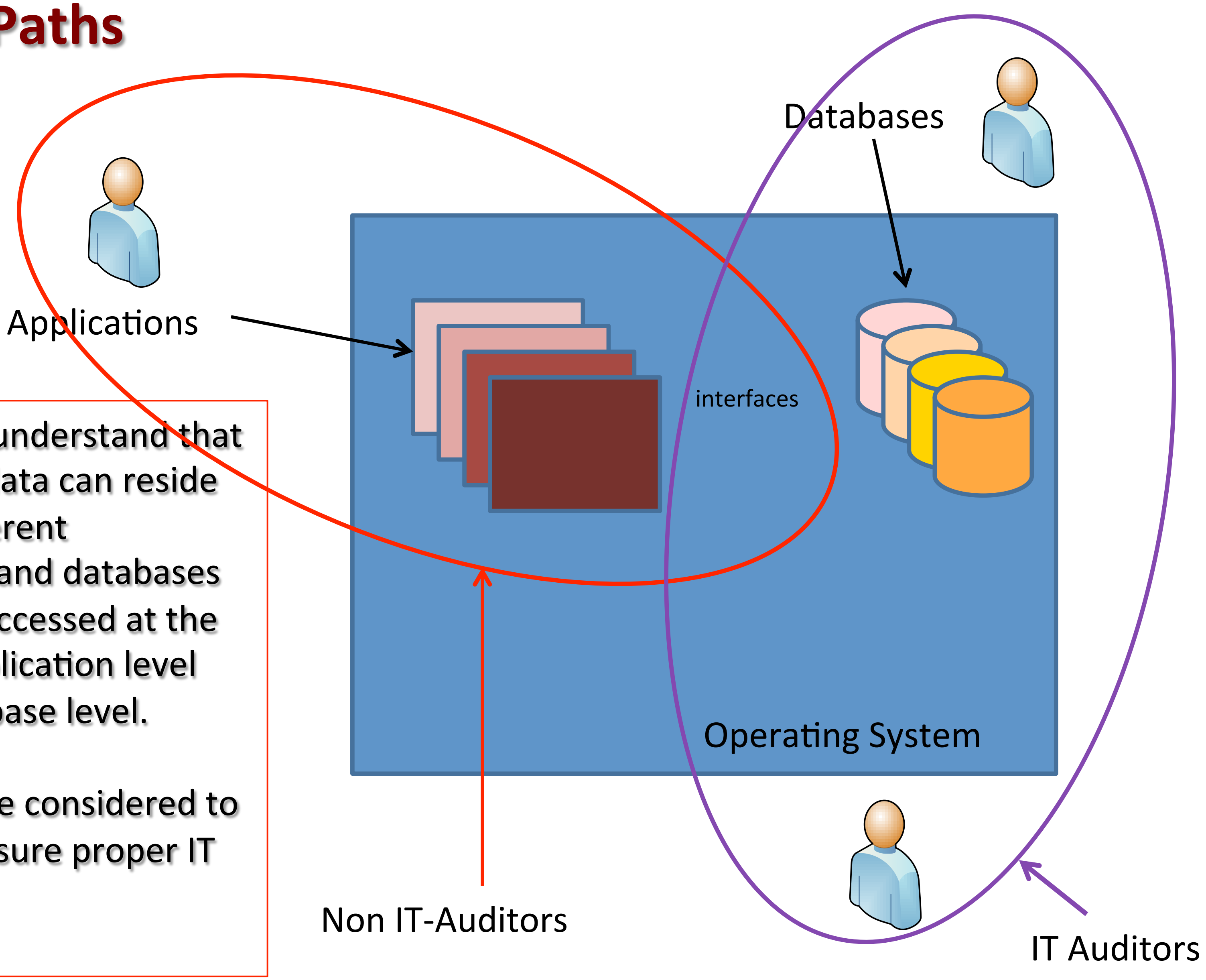
CISSP

Authorization

- Access rules (authorization) specify who can access what.
- Access control is often based on **Principle of Least**, which refers to the granting to users of only those accesses required to perform their duties.
- Access should be on a documented need-to-know and need-to-do basis by type of access.

Access Paths

- Hardware
- Software



We need to understand that application data can reside in many different applications and databases and can be accessed at the OS level, application level and/or database level.

All need to be considered to adequate ensure proper IT controls.

Security Models

Basically there are two ways to implement security:

1. Discretionary
2. Mandatory

Bell-LaPadula

- Simple Security Property
- Star Property
- Strong Star Property

Biba Security

- Simple Integrity Property
- Integrity Star Property

Clark-Wilson

- Unauthorized Users Should Make No Changes
- System should Maintain Internal/External Consistency
- Authorized Users Should Make No Unauthorized Changes

Security Models

Access Control Matrix

- Access is based on Users vs Objects
- Axis of these two states the access privilege
- No Access, Read, Execute, Read, Write, Delete, Create

Information Flow

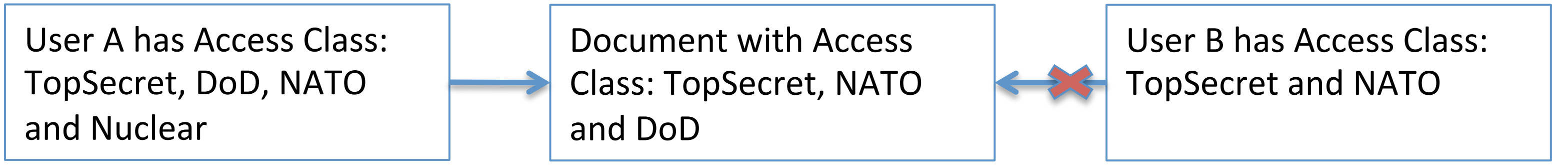
- Simple Integrity Property
- Integrity Star Property

Chinese Wall

- Typically where analysts are dealing with different clients
- There must not be any information flow potentially causing a conflict of interest

Lattice

- Dominates are defined as "greater than or equal to"



User A has Access Class: TopSecret, DoD, NATO and Nuclear

Document with Access Class: TopSecret, NATO and DoD

User B has Access Class: TopSecret and NATO

Security Architecture

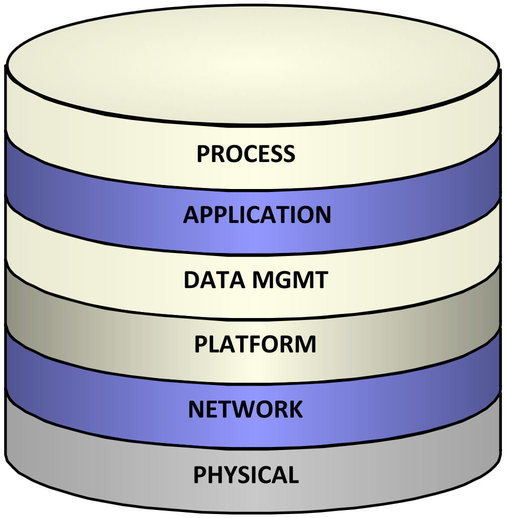
- Security architecture provides insight into the security services, mechanisms, technologies and features that can be used to satisfy security requirements
- Security architecture is not a description of functions of the system
- Security architecture describes the relationships between key elements of the
  - Hardware
  - Operating systems
  - Applications
  - Network
  - Other required components to protect the organization's interest

ISO/EIC 27001:2005

- Security Policy
- Organization of information security
- Asset Management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access Control Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance

Information Security Architecture

Information Security Architecture can be viewed in six (6) distinct layers. This facilitates linking the business risk to an Information Technology Layer in order to address information security related business risks



Before you begin looking at an architecture, you first need to understand the business model, business risk and strategic business objectives.

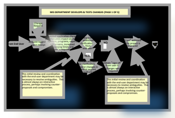
Without this, it becomes a technical exercise without much meaning.

Balanced View of Security

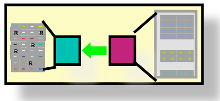
Information Security Architecture

IT Layers

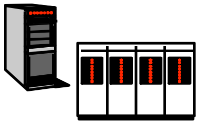
PROCESS - Business functions and processes that use IT



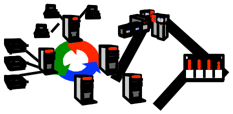
APPLICATION - Application software and functions



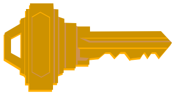
DATA MANAGEMENT - File structure and DBMS software controls



PLATFORM - Hardware platform including OS and system software



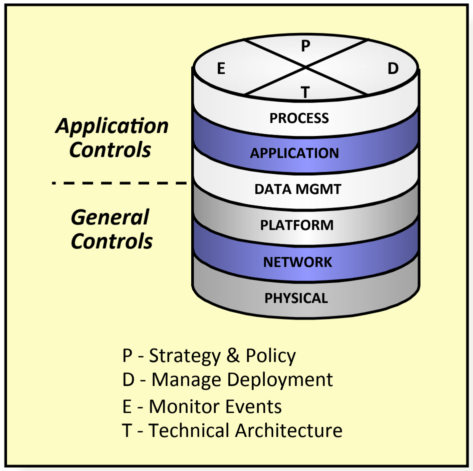
NETWORK - LAN, WAN, Internet, Intranet and support systems

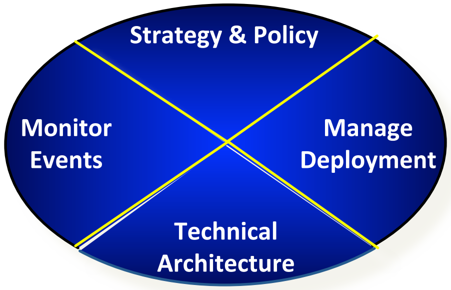


PHYSICAL - Components that house, support and process IT

Information Security Architecture

CONTROL ELEMENTS





Management policies set the tone for the effectiveness of the entire security program.

A series of processes that include managing the technical architecture (networks), maintaining users, and security training and awareness.

Business processes that include identifying security activities, ensuring compliance with policies, and detected breeches and abnormalities.

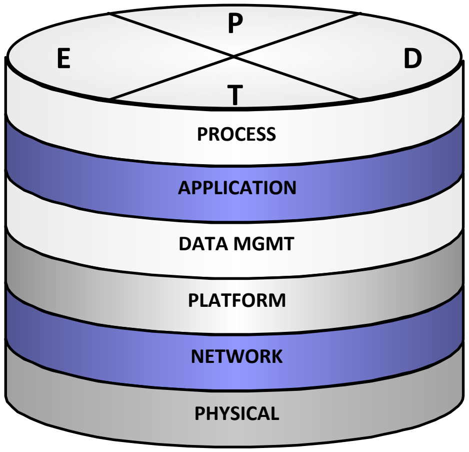
Hardware and software implementation and configuration used to establish a controlled environment.

Information Security Architecture

Putting It All Together

Application Controls

General Controls



Strategies & Policies	Manage Deployment	Monitor Events	Technical Architecture
—	—	—	—
Limited	Limited	—	—
—	—	—	—
✓	✓	✓	✓
✓	✓	✓	✓
—	✓	—	✓

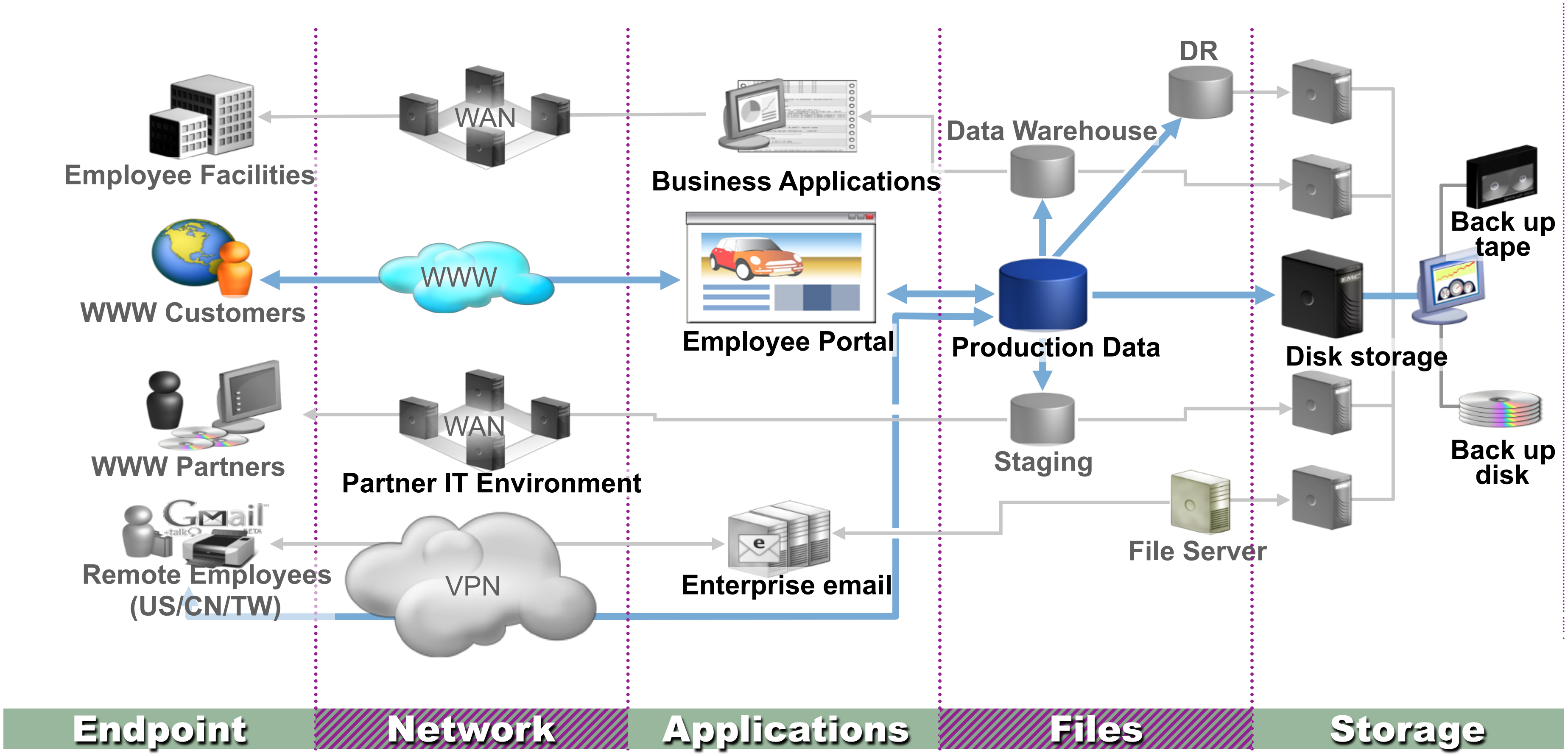
✓	In scope
—	Not in scope

P – Strategies & Policies
D – Manage Deployment
E – Monitor Events
T – Technical Architecture

IT Controls Topology

Why IT Controls So Difficult?

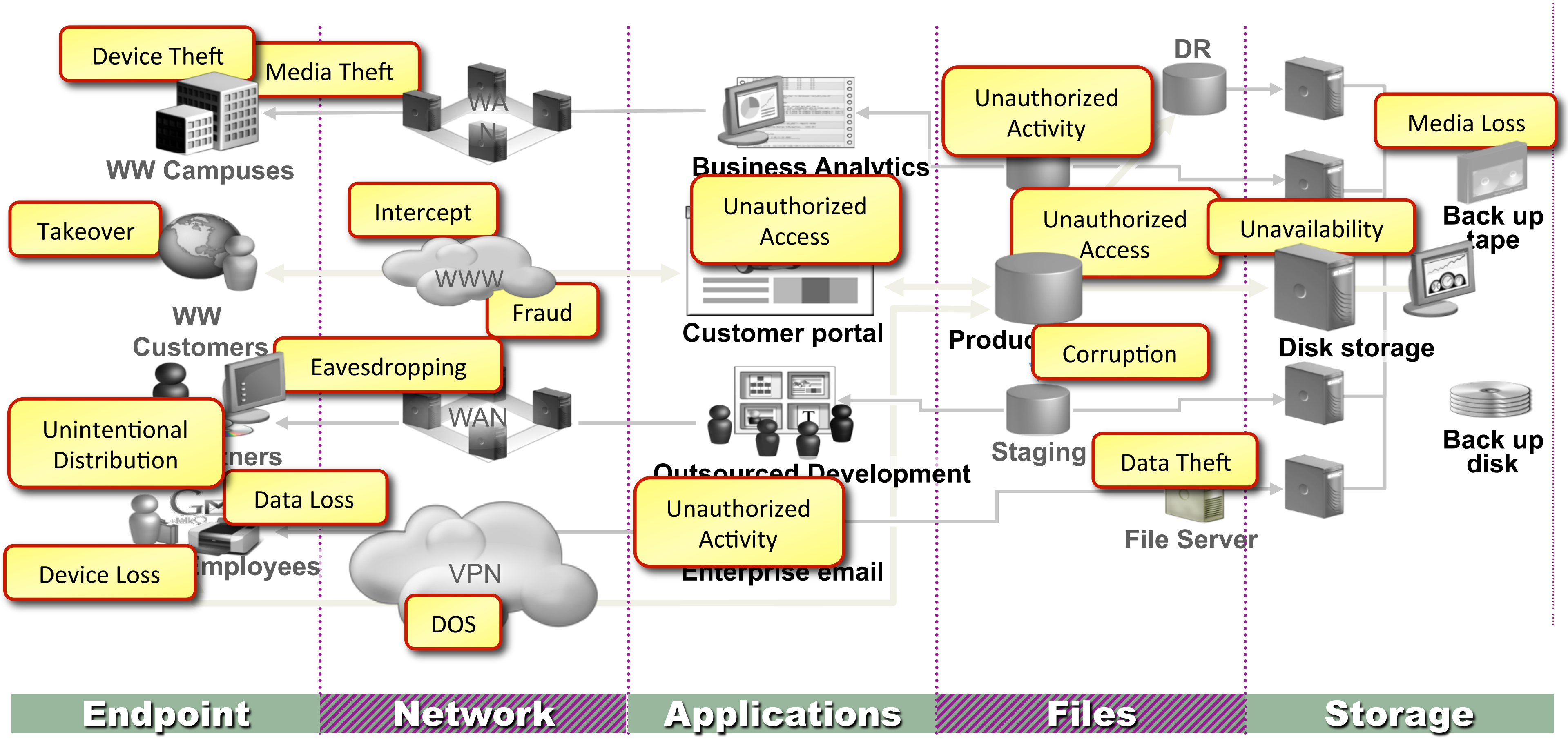
…because sensitive information is always moving and transforming



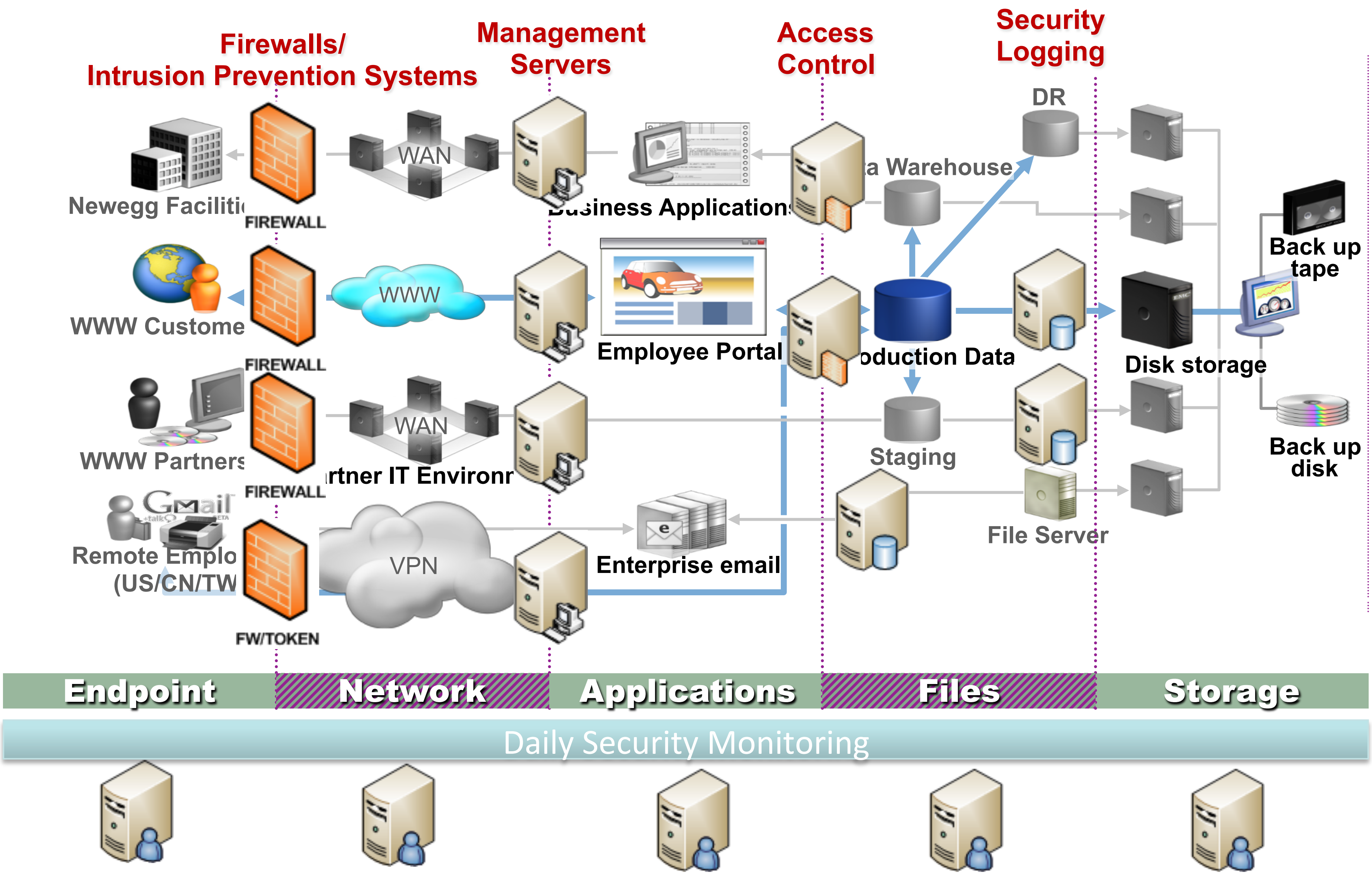
IT Controls Topology

Why are IT Controls So Difficult?

…because sensitive information is always moving and transforming



How to Manage IT Controls



Network Security

- A network is simply two or more computers connected so that they can exchange information (such as e-mail messages or documents) or share resources (disk storage or printers)
- Network security ensures the following goals:
  - Security and accessibility of transmission channels and services
  - Interoperability of network mechanisms are operational
  - Messages sent are the actual messages received
  - A given message link is between valid source and destination
  - Message non-repudiation
  - Prevent unauthorized disclosure of messages
  - Prevent unauthorized traffic flows
  - Secure remote access mechanisms
  - Transparent to users
  - Easy to implement and maintain

Internet Security

Passive attacks

- **Network analysis** - The intruder applies a systematic and methodical approach known as footprinting to create a complete profile of an organization's network security infrastructure
- **Eavesdropping** - The intruder gathers the information flowing through the network with the intent of acquiring and releasing the message contents for either personal analysis or for third parties who might have commissioned such eavesdropping
- **Traffic analysis** - The intruder determines the nature of traffic flow between defined hosts, and through an analysis of session length, frequency and message length, he/she is able to guess the type of communication taking place.

Internet Security

Active attacks

- Brute-force attack
- Masquerading
- Packet replay
- Phishing
- Message modification
- Unauthorized access through the Internet or web-based services (OWASP TOP 10)
- Denial of service
- Dial-in penetration attacks
- E-mail bombing and spamming
- E-mail spoofing

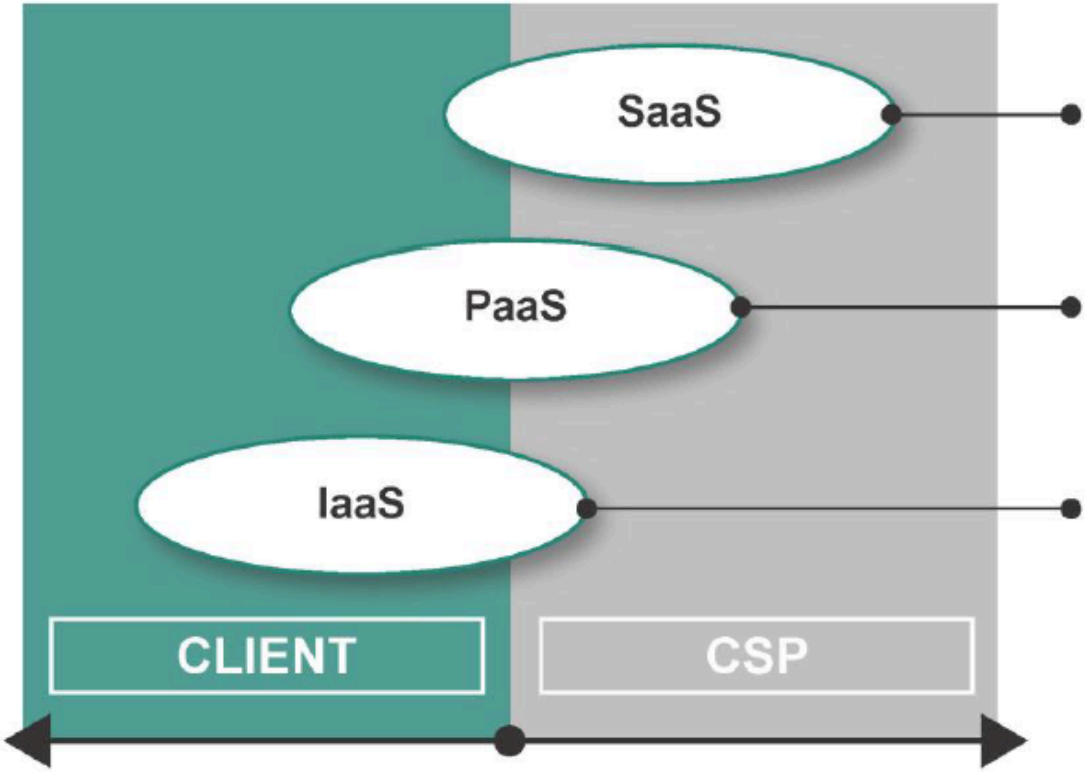
Internet Security

- Factors for Internet attacks
  - Availability of tools and techniques on the Internet
  - Lack of security awareness and training
  - Exploitation of security vulnerabilities
  - Inadequate network security
    - Firewalls
    - Routers
    - Switches
    - IDS/IPS
    - Security Monitoring

Cloud Security

- Flavors of “Cloud”
  - Infrastructure-as-a Service (IaaS)
  - Platform-as-a-Service (Paas)
  - Software-as-a-Service (Saas)
  - Security-as-a-Service (SECaas)
- Deployment Type
  - Public Cloud
  - Private Cloud
  - Community Cloud
  - Hybrid Cloud

Cloud Security Role/Responsibility



Level of control/responsibility for client and CSP across different service models

Saas
The client may have limited control of user-specific application configuration settings.

PaaS
The client has control over the deployed applications and possibly configuration settings for the application-hosting environment.

IaaS
The client has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Cloud Challenges

- Clients have little or no visibility into CSP’s underlying infrastructure and related security controls
- Clients have limited or no oversight over data storage
- Some virtual components do not have the same level of control, logging and monitoring as their physical counterparts
- Perimeter boundaries between client environments can be fluid
- Public cloud environments are usually designed to allow access from anywhere in the Internet
- Many large CSP’s might not support right-to-audit for their clients.

Source: PCI SSC – Information Supplement: PCI-DSS Cloud Computing Guidelines – Feb 2013

Cloud Security Options

- Physical firewalls and network segmentation at the infrastructure level
- Firewall at the hypervisor and VM level
- VLAN tagging or zoning in addition to firewalls
- IPS at the hypervisor and VM level
- DLP at the hypervisor level and VM level
- Controls to prevent out-of-band communications via the underlying infrastructure
- Segmented data stores for each client
- Continuous logging and monitoring of perimeter traffic, and real-time response
- Do not store, process or terminate sensitive data (e.g., payment card data) in the cloud

Source: PCI SSC – Information Supplement: PCI-DSS Cloud Computing Guidelines – Feb 2013

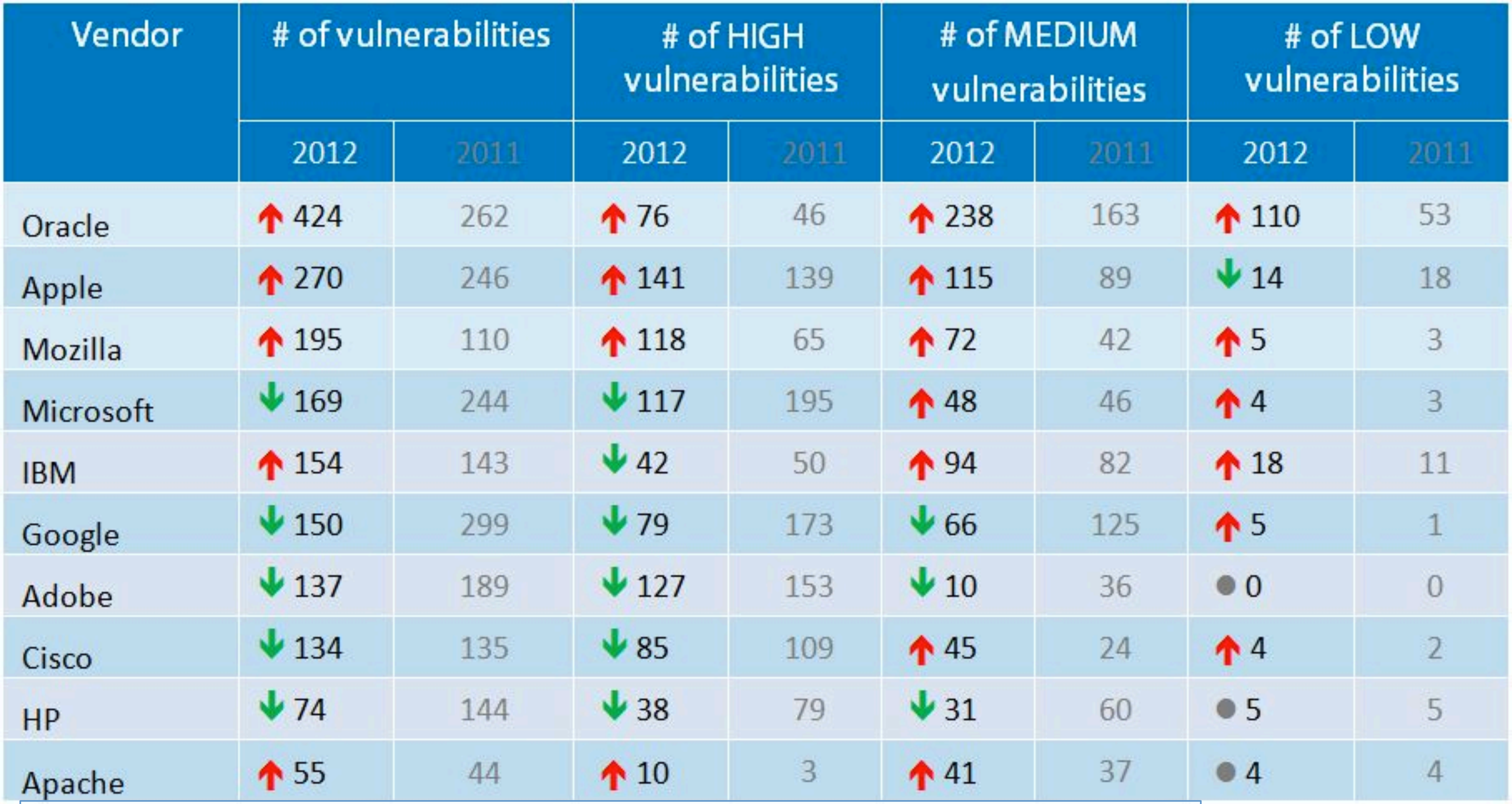
Operating Systems

- Operating System Software and Utilities
- Memory Management
- Supervisor State / Problem State
- Task Management
- Virtual Processing
- Device Management
- Job Scheduling
- File System (files, objects, directories)
- I - A - A

Operating System Security

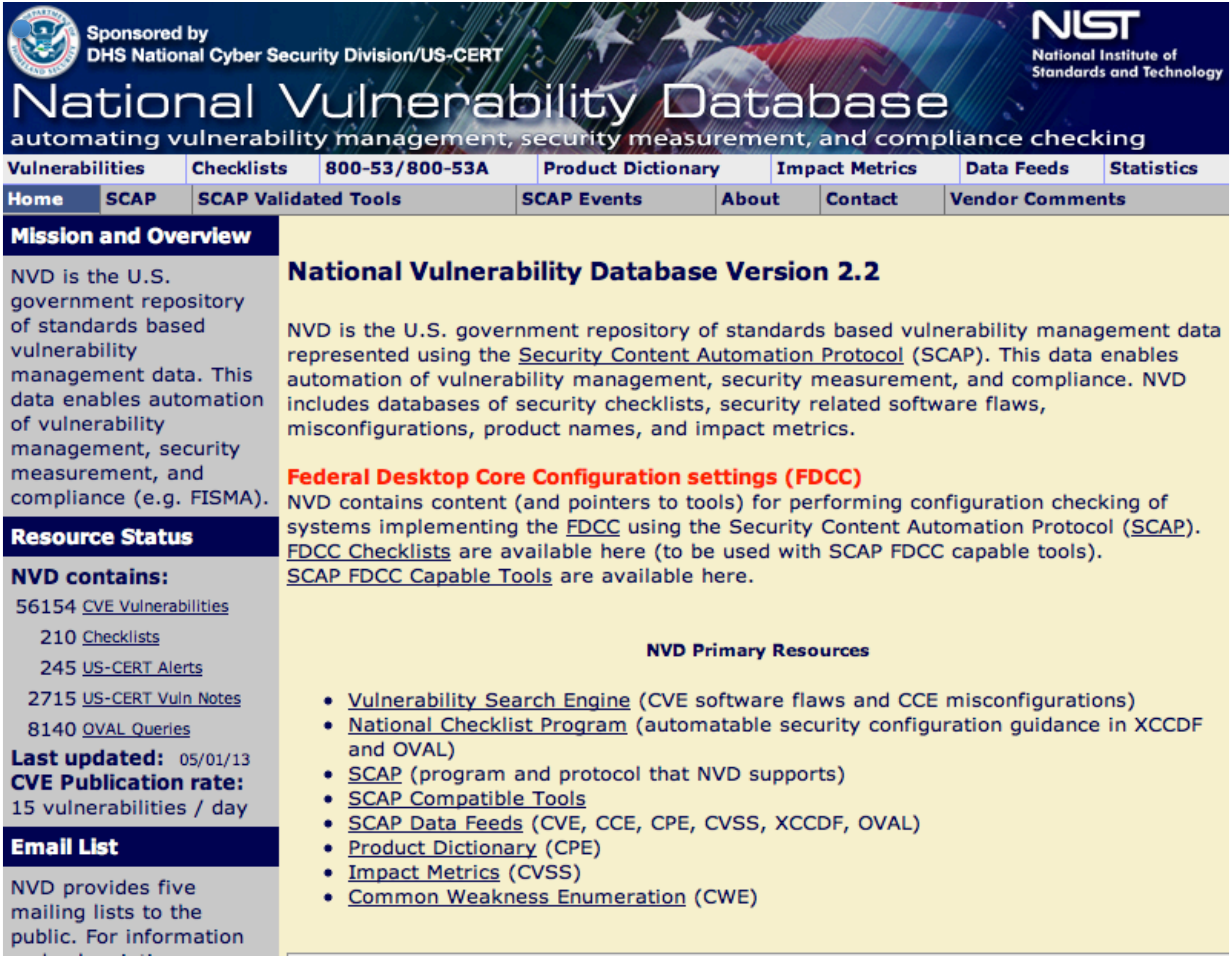
- Identification – typically primary for "user" access to OS - AD, applications, databases
- Authentication – OS passwords, password controls, augmented by two-factor
- Authorization – none, read, write, create, delete
- Mandatory / Discretionary
- External Security Managers – ESM
- OS logging

2013 OS Vulnerabilities



Vendor	# of vulnerabilities		# of HIGH vulnerabilities		# of MEDIUM vulnerabilities		# of LOW vulnerabilities	
	2012	2011	2012	2011	2012	2011	2012	2011
Oracle	↑ 424	262	↑ 76	46	↑ 238	163	↑ 110	53
Apple	↑ 270	246	↑ 141	139	↑ 115	89	↓ 14	18
Mozilla	↑ 195	110	↑ 118	65	↑ 72	42	↑ 5	3
Microsoft	↓ 169	244	↓ 117	195	↑ 48	46	↑ 4	3
IBM	↑ 154	143	↓ 42	50	↑ 94	82	↑ 18	11
Google	↓ 150	299	↓ 79	173	↓ 66	125	↑ 5	1
Adobe	↓ 137	189	↓ 127	153	↓ 10	36	● 0	0
Cisco	↓ 134	135	↓ 85	109	↑ 45	24	↑ 4	2
HP	↓ 74	144	↓ 38	79	↓ 31	60	● 5	5
Apache	↑ 55	44	↑ 10	3	↑ 41	37	● 4	4

Source: TalkToMe Web Site - Report: The Most Vulnerable Operating Systems and Applications in 2012, *Cristian Florian on February 5, 2013*


Sponsored by
DHS National Cyber Security Division/US-CERT
NIST
National Institute of Standards and Technology
National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking
Vulnerabilities
Checklists
800-53/800-53A
Product Dictionary
Impact Metrics
Data Feeds
Statistics
Home
SCAP
SCAP Validated Tools
SCAP Events
About
Contact
Vendor Comments

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

56154	CVE Vulnerabilities
210	Checklists
245	US-CERT Alerts
2715	US-CERT Vuln Notes
8140	OVAL Queries

Last updated: 05/01/13
CVE Publication rate:
15 vulnerabilities / day

Email List

NVD provides five mailing lists to the public. For information

National Vulnerability Database Version 2.2

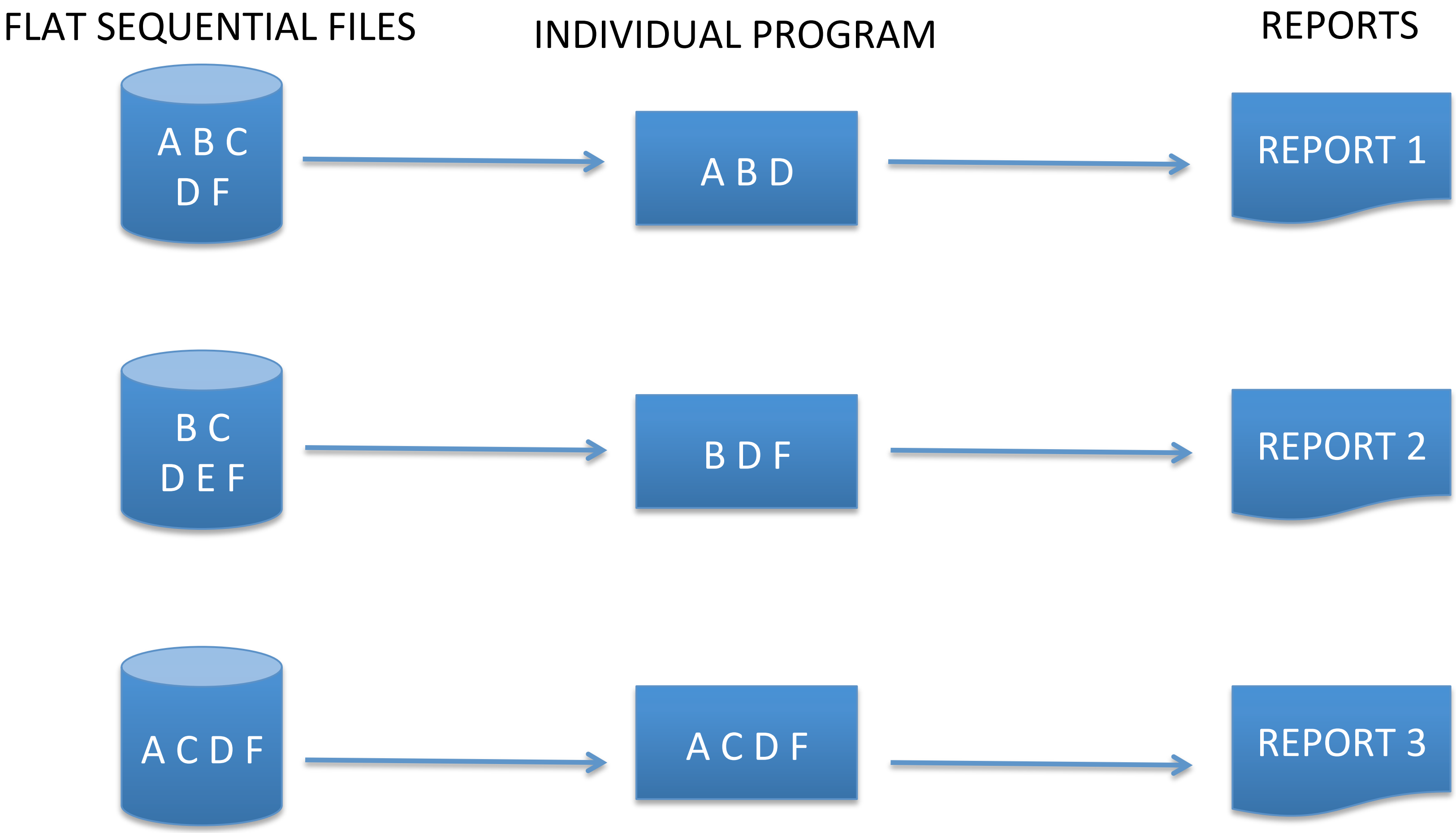
NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

Federal Desktop Core Configuration settings (FDCC)
NVD contains content (and pointers to tools) for performing configuration checking of systems implementing the FDCC using the Security Content Automation Protocol (SCAP). FDCC Checklists are available here (to be used with SCAP FDCC capable tools). SCAP FDCC Capable Tools are available here.

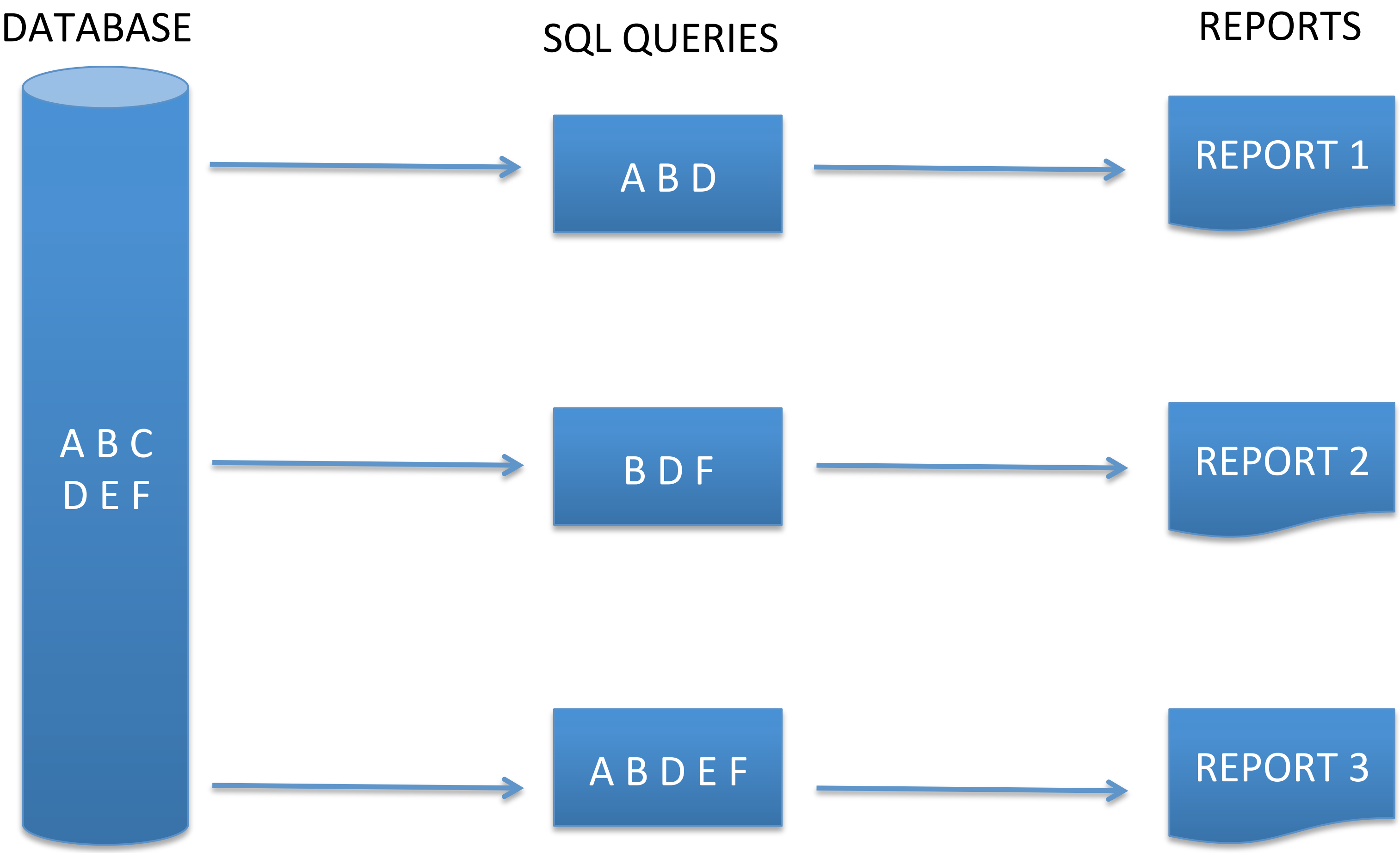
NVD Primary Resources

- Vulnerability Search Engine (CVE software flaws and CCE misconfigurations)
- National Checklist Program (automatable security configuration guidance in XCCDF and OVAL)
- SCAP (program and protocol that NVD supports)
- SCAP Compatible Tools
- SCAP Data Feeds (CVE, CCE, CPE, CVSS, XCCDF, OVAL)
- Product Dictionary (CPE)
- Impact Metrics (CVSS)
- Common Weakness Enumeration (CWE)

DATABASE SECURITY



DATABASE SECURITY



DATABASE

A B C
D E F

SQL QUERIES

A B D

B D F

A B D E F

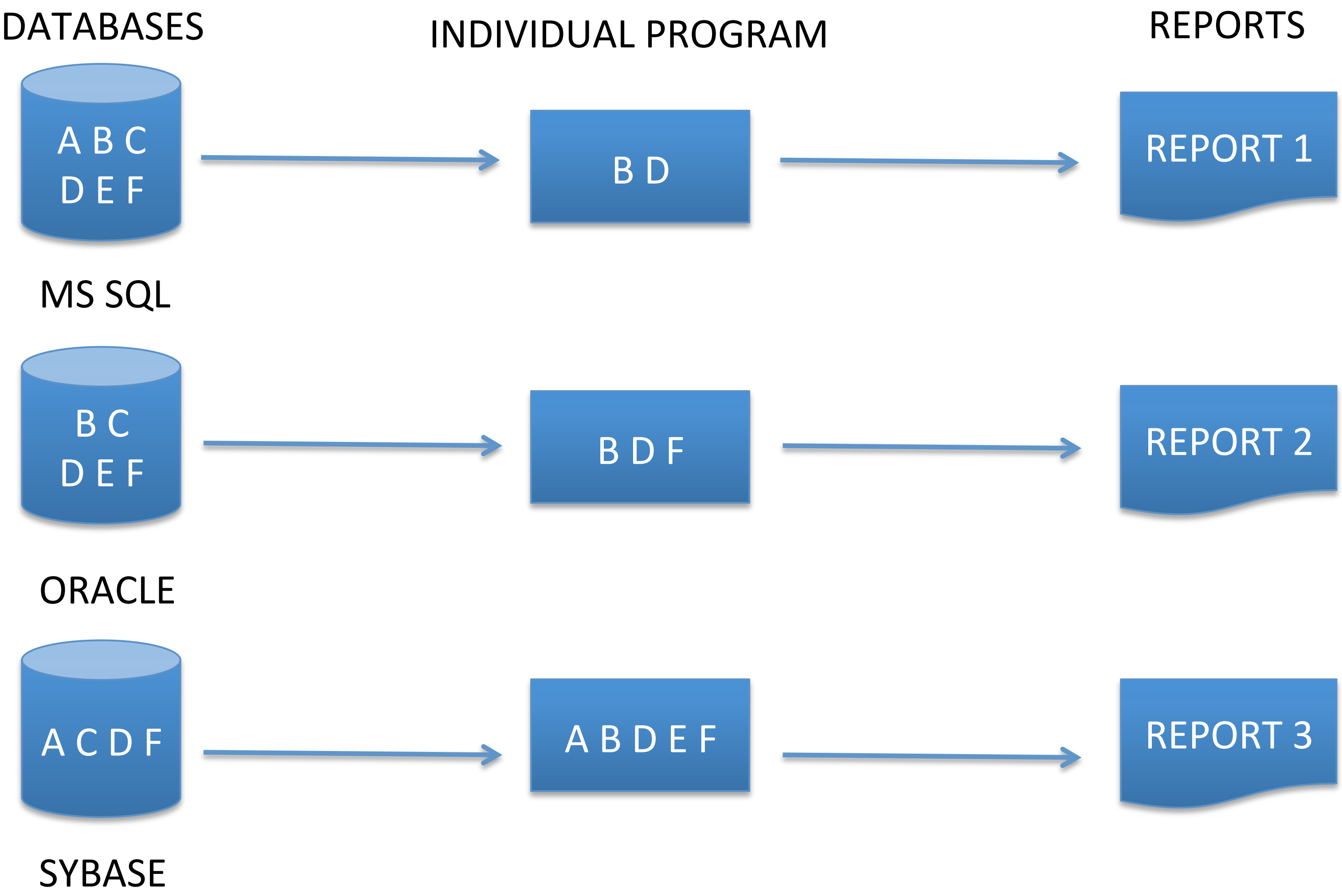
REPORTS

REPORT 1

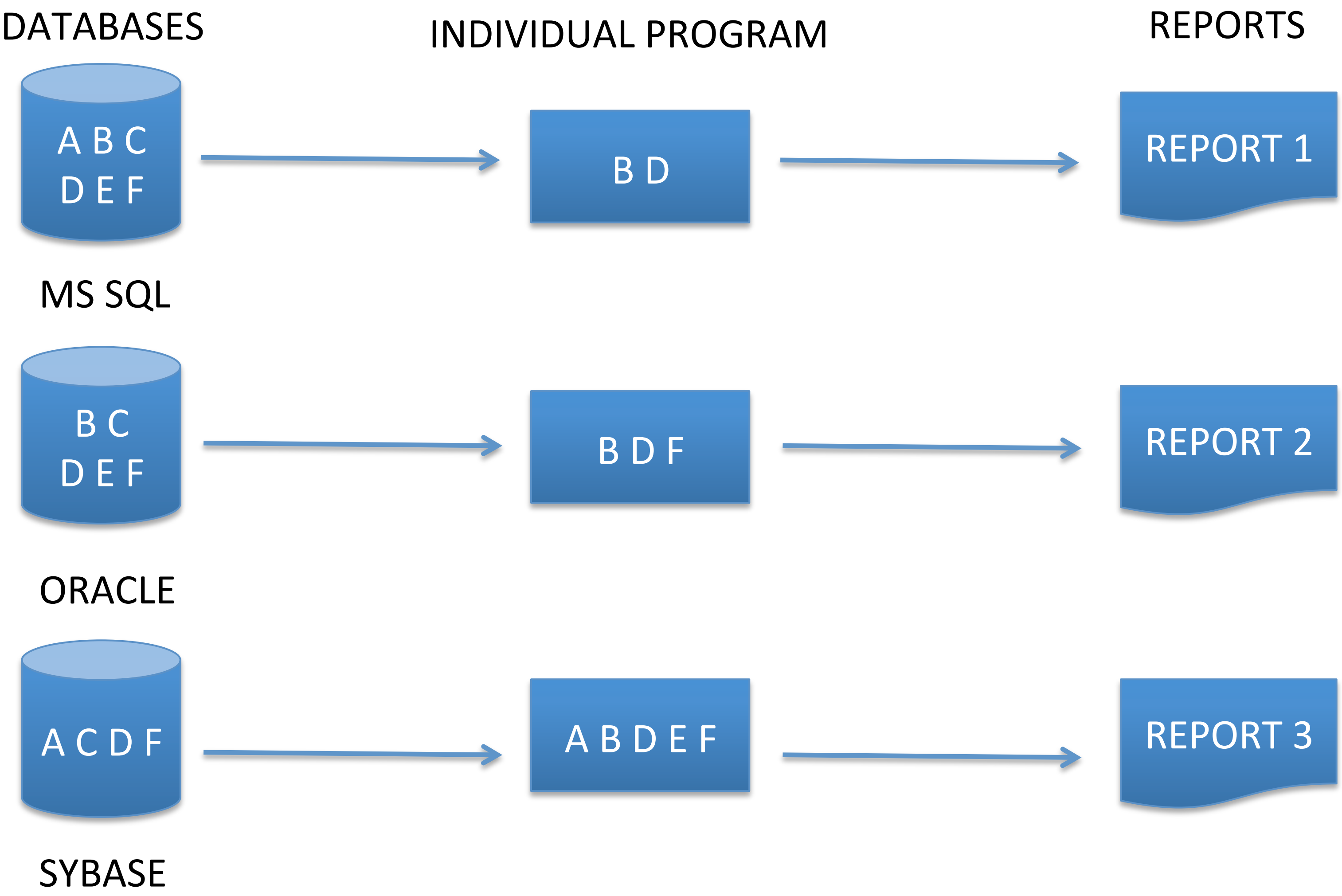
REPORT 2

REPORT 3

DATABASE SECURITY



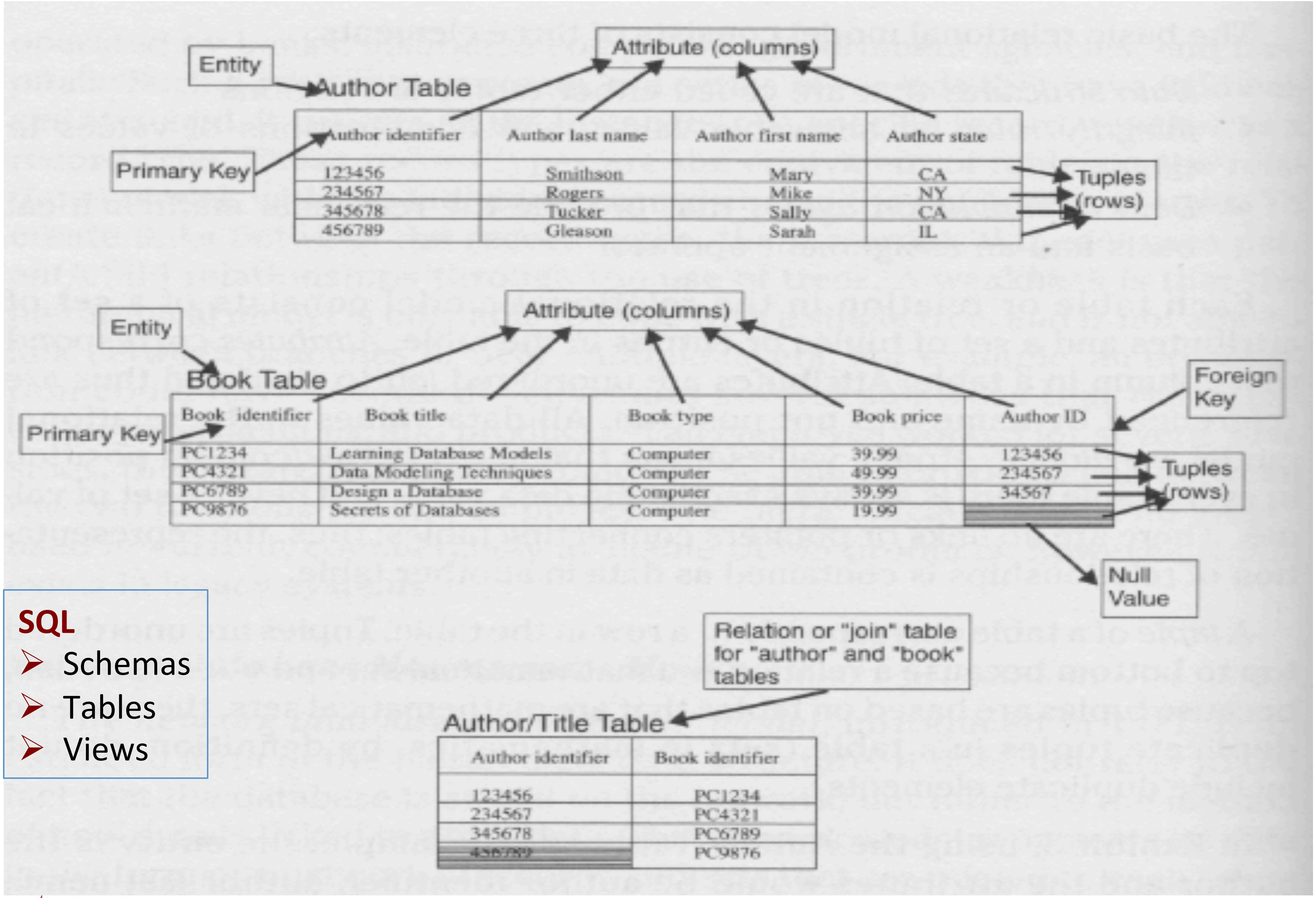
DATABASE SECURITY



Database Architectures

- Hierarchical Database Management Systems (IMS - mainframe)
- Relational Database Management Systems (Oracle, DB2)
- Network Database Management Systems
- Object-Oriented Database Management Systems
- End-User Database Management Systems (dBase, Paradox, MS Access)
- Spreadsheets (MS Excel)

RELATIONAL DATABASE



Author Table

Author identifier	Author last name	Author first name	Author state
123456	Smithson	Mary	CA
234567	Rogers	Mike	NY
345678	Tucker	Sally	CA
456789	Gleason	Sarah	IL

Book Table

Book identifier	Book title	Book type	Book price	Author ID
PC1234	Learning Database Models	Computer	39.99	123456
PC4321	Data Modeling Techniques	Computer	49.99	234567
PC6789	Design a Database	Computer	39.99	34567
PC9876	Secrets of Databases	Computer	19.99	

Author/Title Table

Author identifier	Book identifier
123456	PC1234
234567	PC4321
345678	PC6789
456789	PC9876

SQL

- Schemas
- Tables
- Views

Database Security

- Risk Assessment – use and contents
- Identification/Authentication – AD, OS, DB
- Authorization – database, table, field (tuple)
- Access – READ, WRITE, CREATE, DROP, CREATE, GRANT
- Aggregation – combination of non-sensitive data to create sensitive data
- Support Access – developers, DBA, anyone else
- Security Monitoring – SIEM, SQL Logging, who reviews
- Segmentation – ACL, Proxy Server, V-Lans

APPLICATION SECURITY

Internal Control Objectives

- Safeguarding of IT assets
- Compliance to corporate policies or legal requirements
- Input
- Authorization
- Accuracy and completeness of processing of data input/ transactions
- Output
- Reliability of process
- Backup/recovery
- Efficiency and economy of operations
- Change management process for IT and related systems

IT Control Objectives

Internal control objectives apply to all areas, whether manual or automated. Therefore, conceptually, control objectives in an IT environment remain unchanged from those of a manual environment.

- Safeguarding assets
- Assuring the integrity of general operating system environments
- Assuring the integrity of sensitive and critical application system environments through:
  - Authorization of the input
  - Accuracy and completeness of processing of transactions
  - Reliability of overall information processing activities
  - Accuracy, completeness and security of the output
  - Database integrity

IT Control Objectives

- Ensuring appropriate identification and authentication of users of IS resources
- Ensuring the efficiency and effectiveness of operations
- Complying with requirements, policies and procedures, and applicable laws
- Developing business continuity and disaster recovery plans
- Developing an incident response plan
- Implementing effective change management procedures

IT Audit Methodology

- Understanding of the audit area/subject
- Risk assessment and general audit plan
- Define audit scope
- Detailed audit planning
- Preliminary review of audit area/subject
- Evaluating audit area/subject
- Verifying and evaluating controls
- Compliance testing
- Substantive testing
- Reporting (communicating results)
- Follow-up

- **I – O - P**

INPUT

OUTPUT

PROCESSING

Input / Origination Controls

Input control procedures must ensure that every transaction to be processed is entered, processed and recorded accurately and completely.

The controls should ensure that only valid and authorized information is input and that these transactions are only processed once.

- Input Authorization
    - Signatures on batch forms or source documents
    - Online access controls
    - Unique passwords
    - Terminal or client workstation identification
    - Source documents
- Batch Controls and Balancing
    - Total monetary amount
    - Total items
    - Total documents
    - Hash totals
    - Batch registers
    - Control accounts
    - Computer agreements

Input / Origination Controls

- Error Reporting and Handling
  - Rejecting only transactions with errors
  - Rejecting whole batch of transactions
  - Holding the batch in suspense
  - Accepting the batch and flagging error transactions
- Input Control Techniques
  - Transaction log
  - Reconciliation of data
  - Documentation
  - Error correction procedures
    - Logging of errors
    - Timely corrections
    - Upstream resubmissions
    - Approval of corrections
    - Suspense file
    - Error file
    - Validity of correction
  - Transmittal log
  - Cancellation of source documents

Output Controls

Output controls are meant to provide assurance that the data delivered to users will be presented, formatted and delivered in a consistent and secure manner.

- Logging and storage of negotiable, sensitive and critical forms in a secure place
- Computer generation of negotiable instruments, forms and signatures
- Report distribution
- Balancing and reconciling
- Output error handling
- Output report retention
- Verification of receipt of reports – to provide assurance that sensitive reports are properly distributed, the recipient should sign a log (manual or electronic) as evidence of receipt of output

Processing Controls

Processing controls are meant to ensure the reliability of application program processing. Auditors need to understand the procedures and controls that can be exercised over processing to evaluate what exposures are covered by these controls and what exposures remain.

- Data Validation and Editing (see next page for descriptions)
- Processing Controls
  - Manual recalculations
  - Editing
  - Run-to-run totals
  - Programmed controls
  - Reasonable verification of calculated amounts
  - Limits checks on amounts
  - Reconciliation of file totals
  - Exception reports
- Data file controls
  - System control parameters
  - Standing data
  - Master data/balance data
  - Transaction files

Processing Controls

Data Validation and Edit Controls

Edits	Description Examples
Sequence checks	Invoice numbered sequentially
Limit checks	Data should not exceed a predetermined amount (not > $4,000)
Range checks	Product type codes range from 100 – 250
Validity checks	Payroll record with marital status can only be M or S
Reasonableness checks	Input are matched to predetermined limits (order not > 20 items)
Table lookups	Input clerk enters a city code of 1 -10 corresponding city name
Existence check	Valid transaction code must be entered in the transaction field
Key verification	Keying process is repeated by a separate individual – re-verification
Check digit	Calculated numerical value of field to prevent transposition errors
Completeness check	Value is not left blank and complies with expected data format
Duplicate check	Invoice numbers not entered twice to prevent vendor paid twice
Logical relationship check	Employee hire date must be more than 16 years past his date of birth

OWASP Top 10

Top 10 – 2004	Top 10 - 2007
1. Unvalidated Input	A1 – Cross Site Scripting (XSS)
2. Broken Access Control	A2 – Injection Flaws
3. Broken Authentication and Session Management	A3 – Malicious File Execution
4. Cross Site Scripting	A4 – Insecure Direct Object Reference
5. Buffer Overflow	A5 – Cross Site Request Forgery (CSRF)
6. Injection Flaws	A6 – Information Leakage and Improper Error Handling
7. Improper Error Handling	A7 – Broken Authentication and Session Management
8. Insecure Storage	A8 – Insecure Cryptographic Storage
9. Application Denial of Service	A9 – Insecure Communications
10. Insecure Configuration Management	A10 – Failure to Restrict URL Access

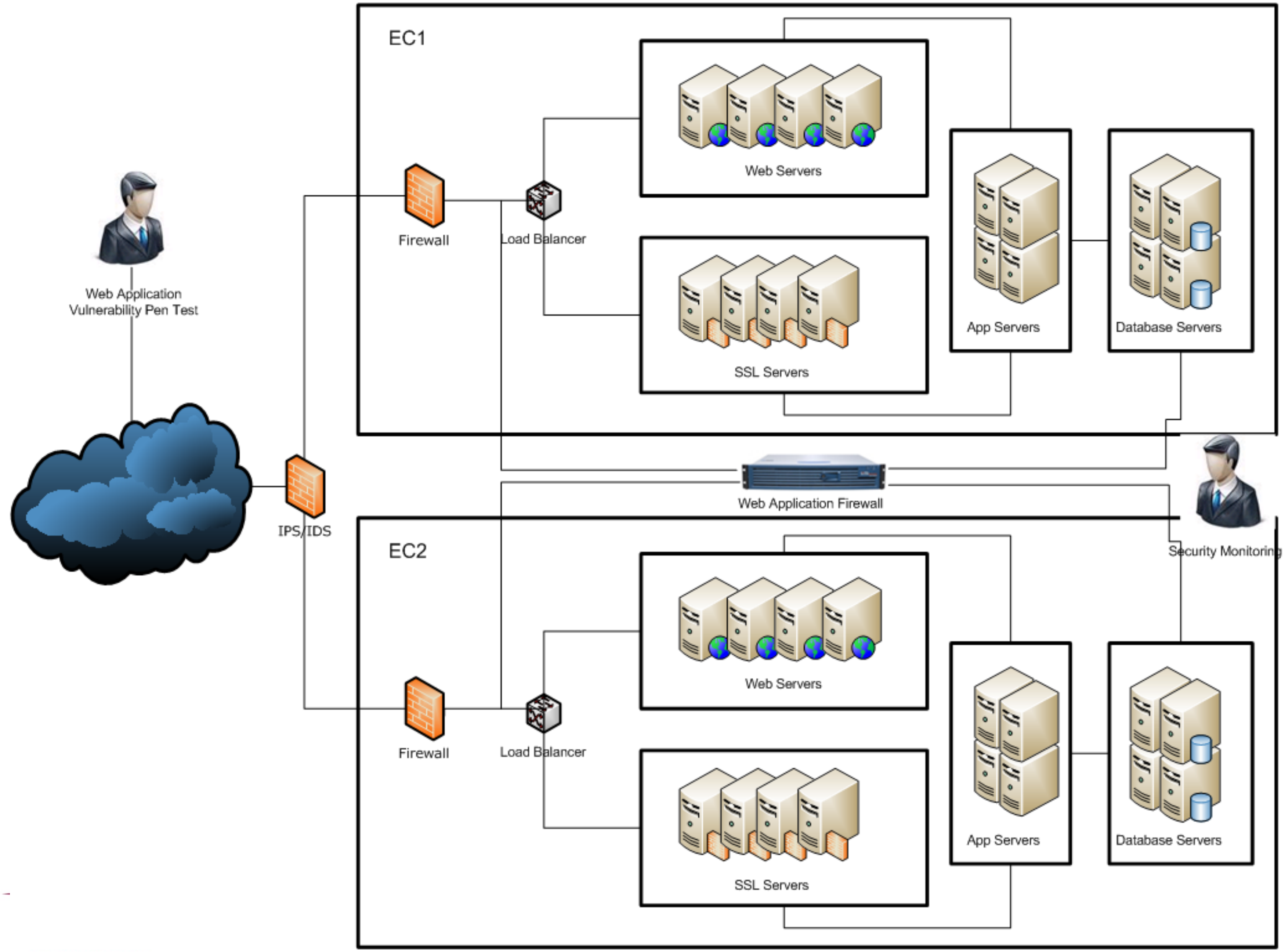
OWASP Top 10 - 2010

Top 10 – 2010
A1 – Injection
A2 – Cross Site Scripting (XSS)
A3 - Broken Authentication and Session Management
A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)
A6 – Security Misconfiguration (NEW)
A7 – Failure to Restrict URL Access
A8 – Unvalidated Redirects and Forwards (NEW)
A9 - Insecure Cryptographic Storage
A10 – Insufficient Transport Layer Protection (NEW)

I DON'T ALWAYS TEST MY CODE
BUT WHEN I DO, I DO IT IN PRODUCTION
memegenerator.net

...NOT...

Sample EC Architecture



Input Validation (Encoding)
How many ways can you say ➔

- http://www.cnn.com ➔ (enter url on browser address bar)
- http://157.166.240.11/ (IP address. Everyone knows it…)
- http://0x9DA6F00B/ (Hex representation)
- http://2644963339/ (Decimal representation)
- http://0235.0246.0360.0013/(Octal representation)
- http://157.0xA6.0360.11/ (You can mix them too!)

Each of these point to the same location. Input validation should consider encoding possibilities to properly secure your web site.

A1 – Injection

Injection flaws allow attackers to relay malicious code through a web application to another system. These attacks include calls to the operating system via system calls, the use of external programs via shell commands, as well as calls to backend databases via SQL (i.e., SQL injection).

Whole scripts written in perl, python, and other languages can be injected into poorly designed web applications and executed.

Any time a web application uses an interpreter of any type there is a danger of an injection attack.

A1 – Injection

SELECT ProductName, ProductDescription FROM Products
WHERE ProductNumber = ProductNumber
	Request sent to the database to retrieve the product’s name and description

sql_query= "SELECT ProductName, ProductDescription FROM Products WHERE ProductNumber " & Request.QueryString("ProductID“)	an ASP code that generates an SQL query.
http://www.mydomain.com/products/products.asp?productid=123	When a user enters URL

SELECT ProductName, ProductDescription
FROM Products WHERE ProductNumber = 123
	This SQL is generated

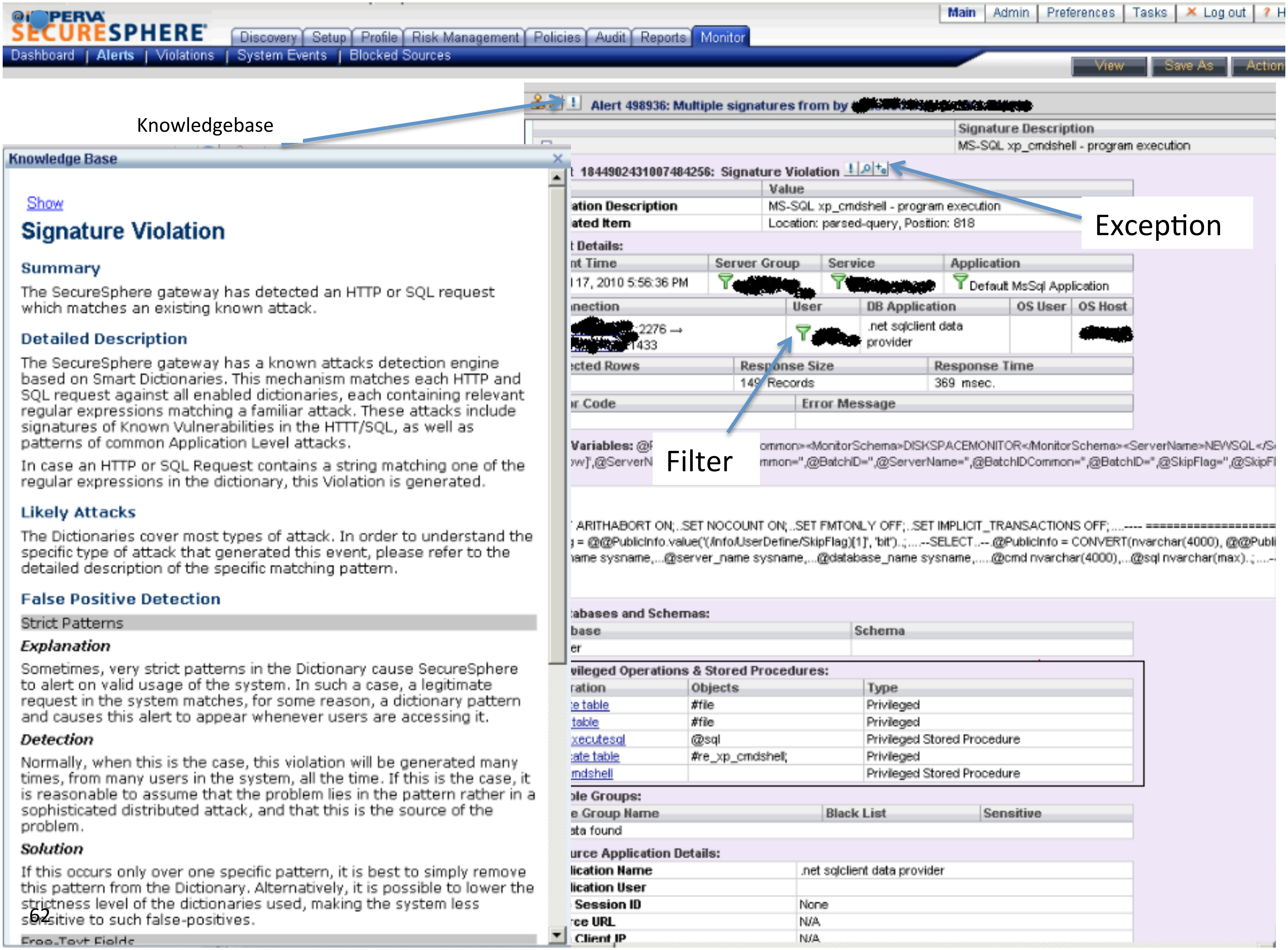
http://www.mydomain.com/products/products.asp?productid=123 or 1=1	Attacker could enter this value
SELECT ProductName, Product Description From Products WHERE ProductNumber = 123 OR 1=1	This SQL is generated

A1 – Injection

http://www.mydomain.com/products/products.asp?productid=123;DROP TABLE Products	←	Attacker could put in this URL and drop tables

SELECT ProductName, ProductDescription
FROM Products WHERE ProductID = &rsquor;123’
UNION SELECT Username, Password FROM Users;
	←	&rsquor;UNION SELECT allows the chaining of two separate SQL SELECT queries that have nothing in common

http://www.mydomain.com/products/products.asp?productid=123 UNION SELECT user-name, password FROM USERS	←	This is the same as a URL. The result is a two column table containing result of first and second query
…ProductID = “123;EXEC master..xp_cmdshell dir—”	←	Extended stored procedure xp cmdshell executes OS commands in the context of a MS SQL Server



IMPERVA SECURESPHERE
Main | Admin | Preferences | Tasks | Log out | ? H
Discovery | Setup | Profile | Risk Management | Policies | Audit | Reports | Monitor
Dashboard | Alerts | Violations | System Events | Blocked Sources
View | Save As | Action

Knowledgebase

Exception

Filter

Knowledge Base

Show

Signature Violation

Summary

The SecureSphere gateway has detected an HTTP or SQL request which matches an existing known attack.

Detailed Description

The SecureSphere gateway has a known attacks detection engine based on Smart Dictionaries. This mechanism matches each HTTP and SQL request against all enabled dictionaries, each containing relevant regular expressions matching a familiar attack. These attacks include signatures of Known Vulnerabilities in the HTTT/SQL, as well as patterns of common Application Level attacks.

In case an HTTP or SQL Request contains a string matching one of the regular expressions in the dictionary, this Violation is generated.

Likely Attacks

The Dictionaries cover most types of attack. In order to understand the specific type of attack that generated this event, please refer to the detailed description of the specific matching pattern.

False Positive Detection

Strict Patterns

Explanation

Sometimes, very strict patterns in the Dictionary cause SecureSphere to alert on valid usage of the system. In such a case, a legitimate request in the system matches, for some reason, a dictionary pattern and causes this alert to appear whenever users are accessing it.

Detection

Normally, when this is the case, this violation will be generated many times, from many users in the system, all the time. If this is the case, it is reasonable to assume that the problem lies in the pattern rather in a sophisticated distributed attack, and that this is the source of the problem.

Solution

If this occurs only over one specific pattern, it is best to simply remove this pattern from the Dictionary. Alternatively, it is possible to lower the strictness level of the dictionaries used, making the system less sensitive to such false-positives.

Free-Text Fields

Alert 498936: Multiple signatures from by [redacted]

Signature Description
MS-SQL xp_cmdshell - program execution

t 1844902431007484256: Signature Violation

	Value
ation Description	MS-SQL xp_cmdshell - program execution
ated Item	Location: parsed-query, Position: 818

t Details:

nt Time	Server Group	Service	Application
l 17, 2010 5:56:36 PM	[redacted]	[redacted]	Default MsSql Application

nection	User	DB Application	OS User	OS Host
[redacted]:2276 → [redacted]1433	[redacted]	.net sqlclient data provider		[redacted]

cted Rows	Response Size	Response Time
	149 Records	369 msec.

r Code	Error Message

```
Variables: @P                ommon><MonitorSchema>DISKSPACEMONITOR</MonitorSchema><ServerName>NEWSQL</S
ow]',@ServerN                mmon='',@BatchID='',@ServerName='',@BatchIDCommon='',@BatchID='',@SkipFlag='',@SkipFl

' ARITHABORT ON;..SET NOCOUNT ON;..SET FMTONLY OFF;..SET IMPLICIT_TRANSACTIONS OFF;....---- ===================
g = @@PublicInfo.value('(/info/UserDefine/SkipFlag)[1]', 'bit')..;....--SELECT..--.@PublicInfo = CONVERT(nvarchar(4000), @@Publi
name sysname,...@server_name sysname,...@database_name sysname,.....@cmd nvarchar(4000),...@sql nvarchar(max)..;....--
```

abases and Schemas:

base	Schema
er	

vileged Operations & Stored Procedures:

ration	Objects	Type
e table	#file	Privileged
table	#file	Privileged
xecutesql	@sql	Privileged Stored Procedure
ate table	#re_xp_cmdshell;	Privileged
ndshell		Privileged Stored Procedure

ble Groups:

e Group Name	Black List	Sensitive
ata found		

urce Application Details:

lication Name	.net sqlclient data provider
lication User	
Session ID	None
rce URL	N/A
Client IP	N/A

A1 – Injection (Remediation)

$sql = 'UPDATE #__mytable SET `id` = ' . (int) $int;	←	if you are expecting an integer, force it to be an integer (or a float). So, if you have a variable that you are expecting to be an integer, cast it to an integer.
$date =& JFactory::getDate($mydate); $sql = 'UPDATE #__mytable SET `date` = ' . $db->quote($date->toMySQL(), false);	←	If you want to insert a date, then use JDate, and it'll give you back a valid mysql date each time
$sql = 'UPDATE #__mytable SET `string` = ' . $db->quote($db->getEscaped($string), false);	←	anytime you take a string from user input (always escape everything from a variable, it's extra insurance), you should escape it using this
master..Xp_cmdshell, xp_startmail, xp_sendmail, sp_makewebtask	←	Delete stored procedures that you are not using. Document and monitor those that you are.
single quote, double quote, slash, back slash, semi colon, extended character like NULL, carry return, new line, etc,	←	Filter out character in all strings from: - Input from users - Parameters from URL - Values from cookie

Regular Expressions (regex)

Regular expressions are a syntactical shorthand for describing patterns. They are used to find text that matches a pattern, and to replace matched strings with other strings. They can be used to parse files and other input, or to provide a powerful way to search and replace. The following link is a regex primer.

http://docs.activestate.com/komodo/4.4/regex-intro.html

```
part="515", rgxp="[^\d]515\d[-\.\s\\\/=]?\d{4}[-\.\s\\\/=]?\d{4}[-\.\s\\\/=]?\d{4}[^\d]{1}"
```

This is a regex that will match strings for a Mastercard Credit Card number that starts with "515".

Searching for Credit Cards

- Visa: ^4[0-9]{12}(?:[0-9]{3})?$ All Visa card numbers start with a 4. New cards have 16 digits. Old cards have 13.
- MasterCard: ^5[1-5][0-9]{14}$ All MasterCard numbers start with the numbers 51 through 55. All have 16 digits.
- American Express: ^3[47][0-9]{13}$ American Express card numbers start with 34 or 37 and have 15 digits.
- Diners Club: ^3(?:0[0-5]|[68][0-9])[0-9]{11}$ Diners Club card numbers begin with 300 through 305, 36 or 38. All have 14 digits. There are Diners Club cards that begin with 5 and have 16 digits. These are a joint venture between Diners Club and MasterCard, and should be processed like a MasterCard.
- Discover: ^6(?:011|5[0-9]{2})[0-9]{12}$ Discover card numbers begin with 6011 or 65. All have 16 digits.
- JCB: ^(?:2131|1800|35\d{3})\d{11}$ JCB cards beginning with 2131 or 1800 have 15 digits. JCB cards beginning with 35 have 16 digits.

The Need For Encryption

- Today' s method for communications to legacy and client server applications allows the flow of information that traverses our networks in clear text.
- Authentication systems use encryption for id and passwords/tokens, however, once authenticated, invariably NPPI (Non-Public Private Information) is not encrypted.
- SSL is used to encrypt web application access by encrypting the tunnel, however, it also encrypts "hacker' s" sessions – not sufficient.
- NPPI residing on stolen laptops could compromise the confidentiality of customer information.
- Unauthorized access to systems behind DMZ could also subject NPPI exposures.

Encryption defined

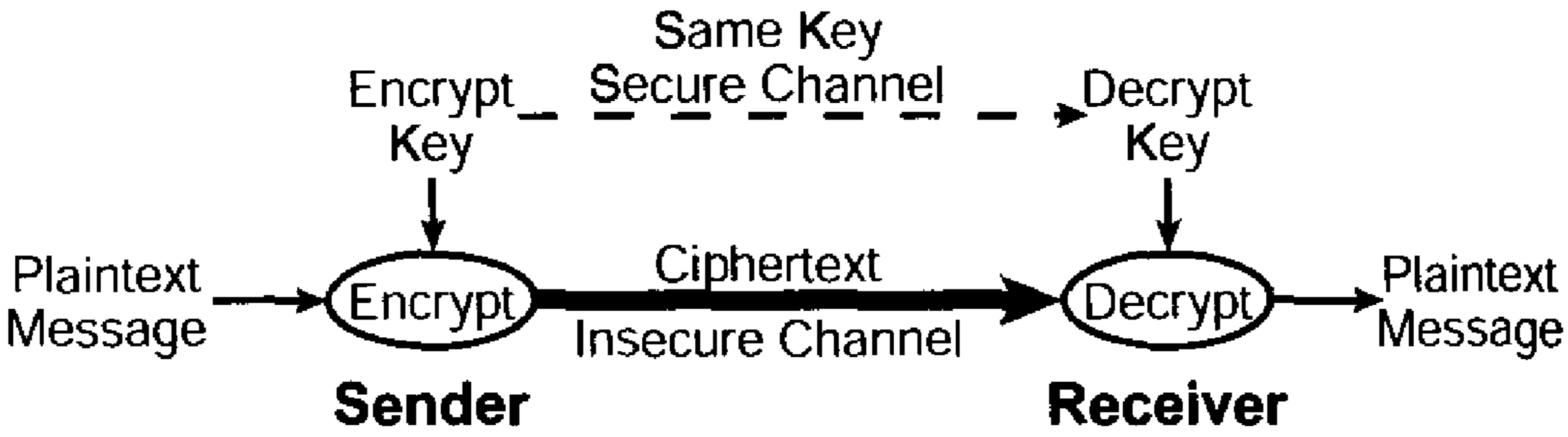
The reversible transformation of data from the original (the plaintext) to a difficult-to-interpret format (the ciphertext) as a mechanism for protecting its confidentiality, integrity and sometimes its authenticity. Encryption uses an encryption algorithm and one or more encryption keys.

Encryption Standards and Algorithms

- Data Encryption Standard (DES) was developed by IBM and the US government in 1970 using the Data Encryption Algorithm (DEA).
- In 1976 public key encryption was developed by Whitfield Diffie and Martin Hellman, separately.
- In 1977, Ronald Rivest, Adi Shamar and Leonard Adleman developed the RSA algorithm.
- In 1990, IDEA (International Data Encryption Algorithm) was developed by two Swiss engineers.
- In 1991, Phil Zimmerman developed PGP (Pretty Good Privacy) using Blowfish.
- In 2000, after NIST coordinated an international competition, AES won, developed by two Belgium cryptographers, Joan Daeman and Vincent Rijmen. AES is expected to eventually replace DES and 3DES, however, the investment into the DES standards may delay it.

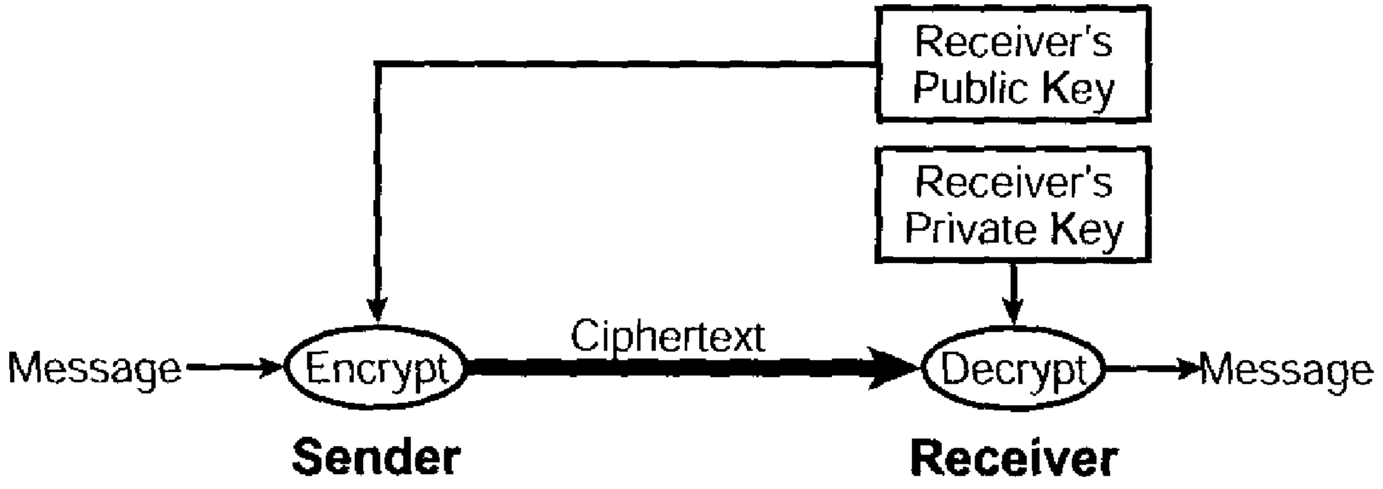
Symmetric vs. Asymmetric

Symmetric Encryption – this is where a single key is used to encrypt and decrypt a message



Symmetric vs. Asymmetric

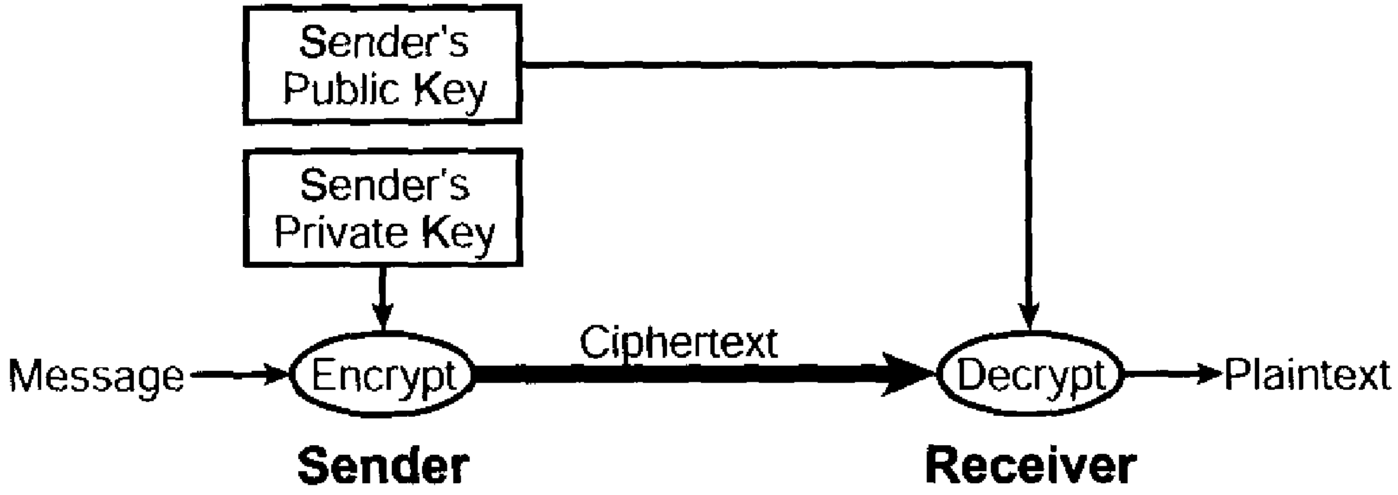
Asymmetric Encryption – this is where the sender uses the receiver's public key to encrypt the message and the receiver would use his private key to decrypt the message and read it.



(Secure Message)

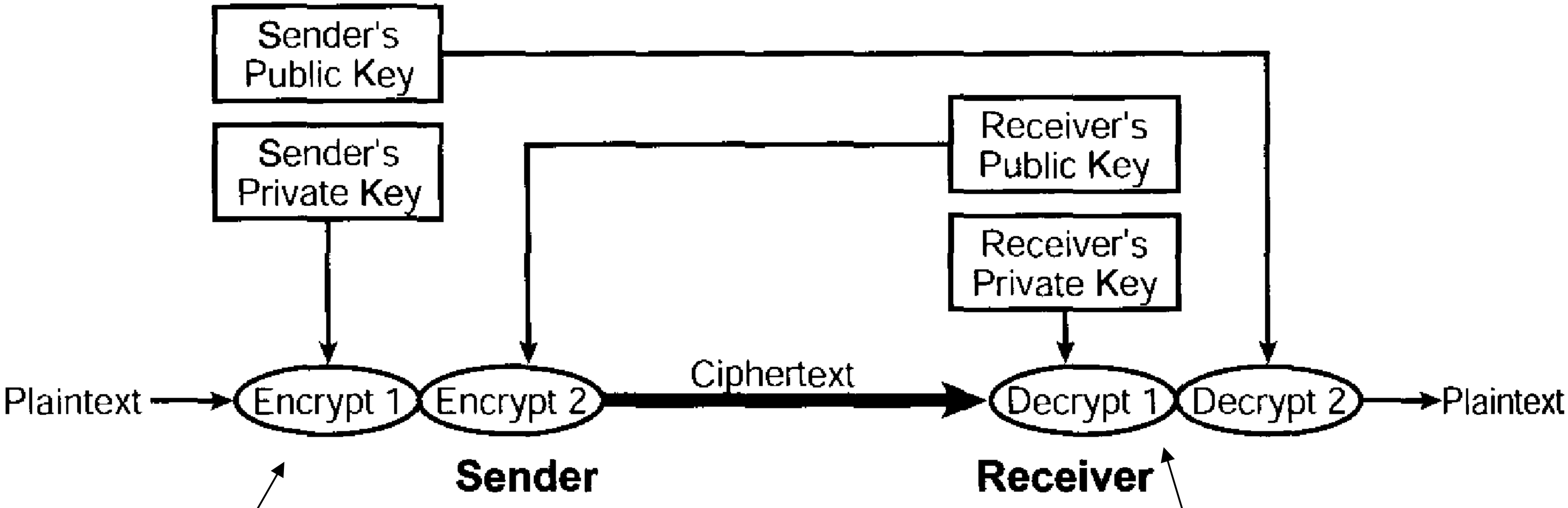
Symmetric vs. Asymmetric

Asymmetric Encryption – this is where the sender uses his own private key to encrypt a message and sends his public key to the receiver so he can decrypt the message.



(Open Message)

Public Key Infrastructure



Digital signature

Digital signature

Other Forms of Encryption

- Use of encryption in OSI protocols
  - Secure sockets layer (SSL)
  - Secure Hypertext Transfer Protocol (S/HTTP)
  - IP security (IPSEC)
  - SSH
  - Secure multipurpose Internet mail extensions (S/MIME)

Security Monitoring

- Basically there are two major threat vectors
  - External and organized crime
  - Insider threats
- Users are becoming more technology literate so the risk goes beyond IT and MIS personnel
- Monitoring required by regulation or laws
  - PCI is not a law but carries just as much weight
  - Sarbanes Oxley
  - HIPPA
  - Regulatory Bodies: OCC, FDIC, PUC, FISMA, many more
- Stakeholder/Executive Management Directives

Policies for Monitoring

- Once you see a cockroach in your home, rest assured there are more lurking around
- The tendency is to bring in an exterminator and fumigate the house to rid yourself of the pest
- When you turn on monitoring, you see incidents (cockroaches) that lead you to believe you are being infected or attacked
- Not everything on your network is a cockroach
- You need to plan or a policy to know the difference or to know what to do
  - When to investigate
  - When to log for further analysis
  - When to ignore as normal or insignificant

Policies for Monitoring

- Blacklist Monitoring – creating a list of prohibited events. This is the most common method of security monitoring.
- Whitelist Monitoring - only entities on the list will be accepted, approved, and/or recognized.
- Anomaly Monitoring – this is where one is looking for events that fall out of what is expected to be normal traffic
- Policy Monitoring – monitoring that is driven by laws, regulations, best practices, internal policies

Know Your Environment

- **Industry Knowledge** – know what laws and regulations you are governed or measured by. These will be critical for you to know what needs to be monitored and protected
- **Organization Culture** – management and business key objectives. Internal politics, key decision makers, strategic committees, problem areas, management view of information security
- **Organization Chart** - know key roles and responsibilities. IT/MIS org chart.
- **Network** – what is your network topology? Get an inventory of Layer 3 devices and their uses. Who manages them?
- **External Facing Web Sites** – do you take financial transactions from your web site? PCI requirements?
- **Wireless Network** – inventory known access points; rouge access points.
- **VPN Access** – do you have home or external access to internal network?
- **Legacy Environment** – inventory mainframes, servers, mid-range computers, internal network topology, database technologies

Know Your Environment

- **Information Security Risk Assessment** – perform a risk assessment to determine critical applications, IT environments, key personnel, mission critical processes, high level attack vectors
- **Log Management -** what is currently being logged? Log repositories; retention; monitoring; by whom.
- **Incident Response Program –** does it exist? When last tested?
- **SIEM (Security Incident Event Manager) -** what SIEM is your company using? What logs are being fed into it?
  - **IPS**
  - **Firewalls**
  - **Windows Events**
  - **Database Events**
  - **VPN Events**
  - **Network Vulnerability Scans (Internal and External)**
  - **ERP – SAP, JDE, PeopleSoft, etc.**
  - **DLP**
  - **Anti-Virus/Malware Detection Software**
  - **File Integrity Monitoring (FIM)**

Select Targets for Monitoring

- **Methods for Selecting Targets**
  - **Business Impact Analysis (BIA) –** key business processes
  - **Financial Impact Analysis (FIA) –** revenue/expense apps
  - **Legal Requirements –** external audit, SOX, PCI, HIPPA, GLBA, etc
  - **Sensitivity Profile –** PII, confidential information, M&A
  - **Risk Profile –** key apps/environments without proper IAA
  - **Visibility Profile –** external ingress/egress portals (web, FTP, VPN, etc)
- **Best Practice Methods**
  - **BIA –** identify time-critical business processes
  - **Information Security Risk Assessment –** examination of regulatory compliance, contractual /legal requirements and systems that access sensitive data

THREAT VECTORS

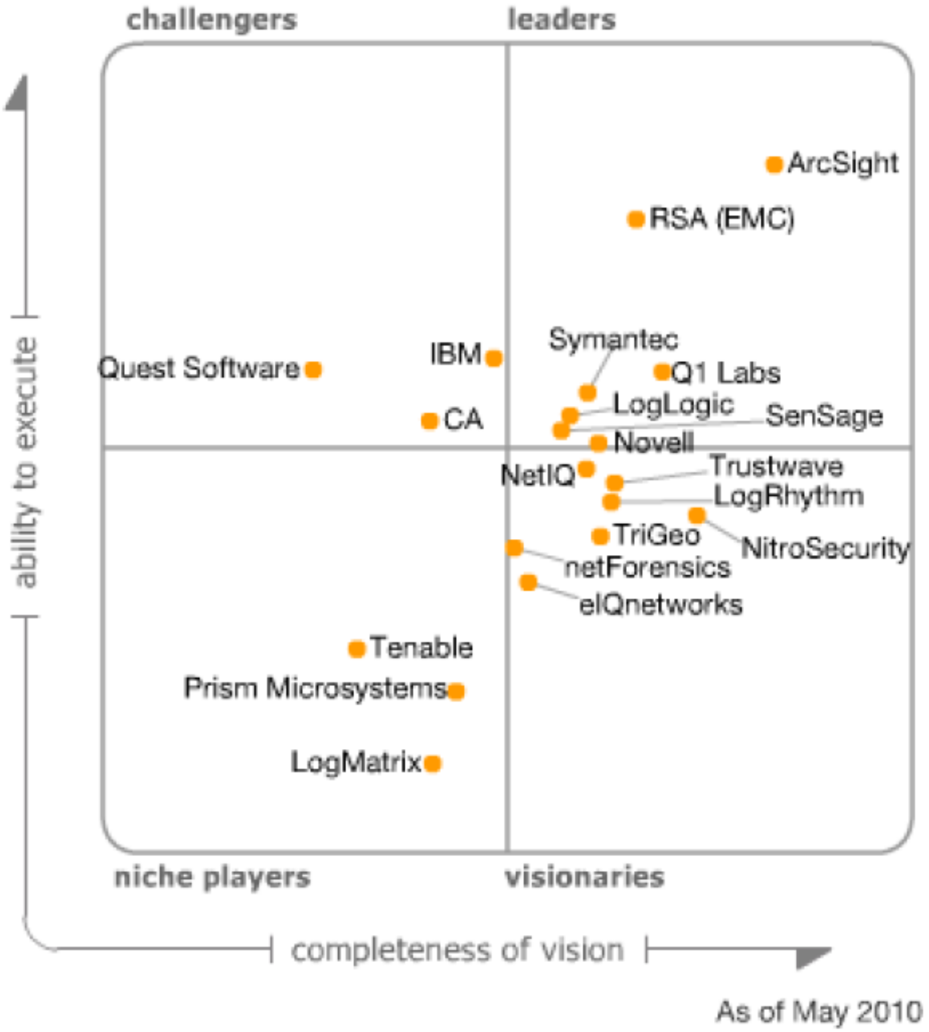
EXTERNAL

- Network
  - Distributed Denial of Service Accounts (DDOS)
  - Network Device Configuration Vulnerabilities
  - Wireless Rogue Access Points
- WEB Application
  - SQL Injections
  - Directory Traversals
  - Cross Site Scripting (XSS)
  - Exploiting Operating Systems from SQL databases
  - Improper Authentication and Session Management
  - Improper Error Handling
- Phishing Attacks
- Sharing Information with Third Party Service Providers
- Malware (virus, trojans, spyware, worms, SPAM, man-in-the-middle)
- Cyberlaws (Federal and State)
- Stolen Laptops
- Payment Card Industry (PCI) Compliance
- External Audit Issues

INTERNAL

- Network
  - User/Developer access to production domains
  - Sharing of Logon IDs
  - Generic IDs
  - Users Loading NE docs on Public Web Sites
- File System
  - Access to production servers
  - Access to production source code
  - Access to customer information (credit cards, account numbers, etc.)
- WEB Application
  - Developer SQL Access to production databases
  - Improper secure coding practices
  - Developers not passing secure code exams
- Legacy Application
  - Separation of Duties
  - Developer Access to Production
- End-Point
  - USB/CD/DVD
  - Improper configurations

Gartner Magic Quadrant: SIEM



Source: Gartner (May 2010)

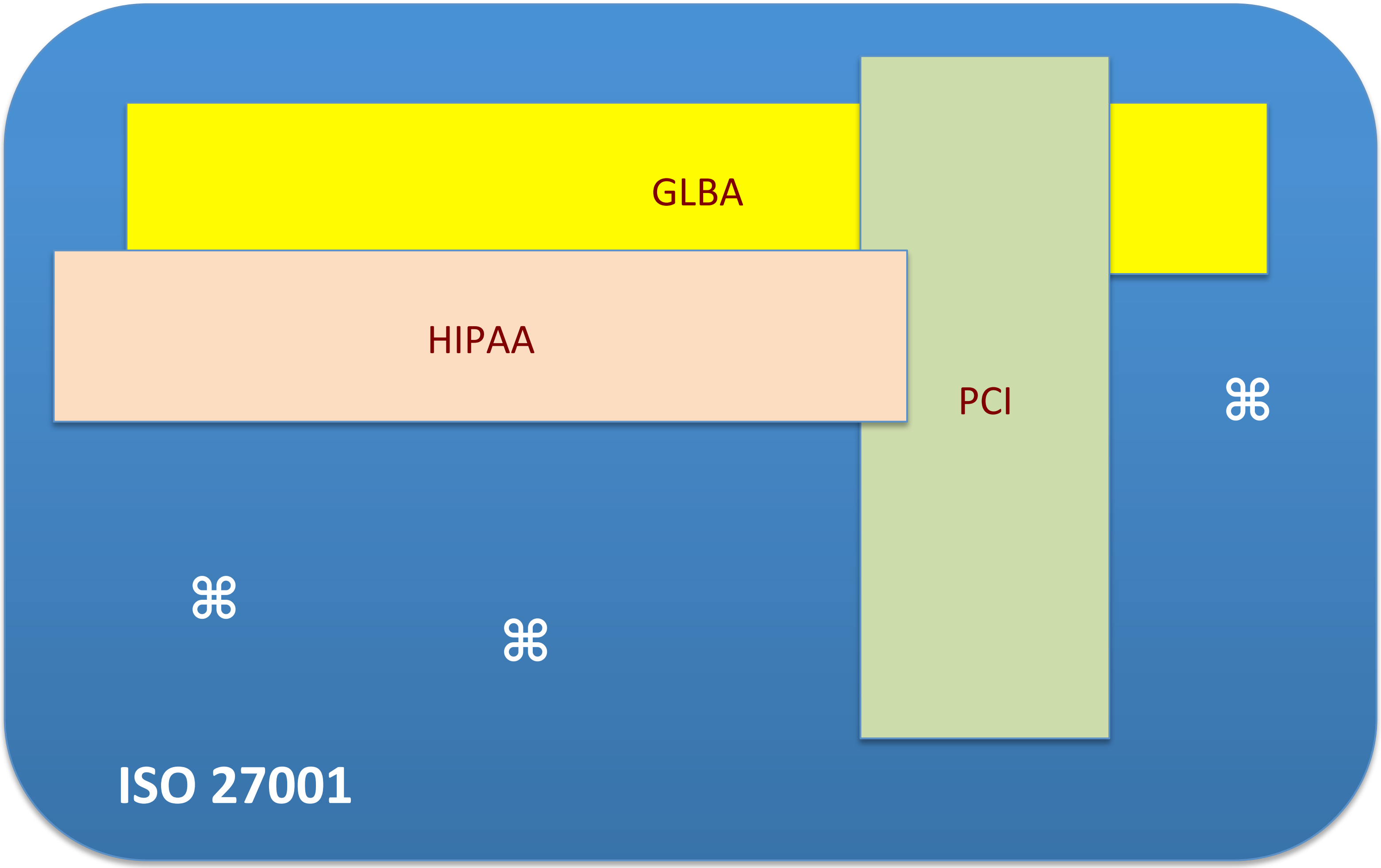
Compliance

Risk Management VS Compliance

Unfortunately or Maybe not…

WHO WINS?

Compliance



Not to Scale – For Illustrative Purposes Only

Compliance

- Gramm-Leach-Blylie – GLBA
- HIPAA – Health Insurance Portability & Accountability Act
- Payment Card Industry Data Security Standard – PCI DSS
- Sarbanes-Oxley – SOX
- FISMA
- HIGH TECH
- Many others

THANK YOU

BIO

Miguel (Mike) O. Villegas is the Director for K3DES LLC. He QA's and performs PCI-DSS and PA-DSS assessments for K3DES clients. He also manages the K3DES ISO/IEC 27001:2005 program. Mike was previously Director of Information Security at Newegg, Inc.

Mike has over 30 years of Information Systems security and IT audit experience. Mike was previously Vice President & Technology Risk Manager for Wells Fargo Services responsible for IT Regulatory Compliance and was previously a partner at Arthur Andersen and Ernst & Young for their information systems security and IS audit groups over a span of nine years. Mike is a CISA, CISSP, GSEC and CEH. He is also a QSA, PA-QSA and ASV as Director for K3DES.

Mike was past president of the LA ISACA Chapter during 2010-2012 and was the SF ISACA Chapter President during 2005-2006. He was the SF Fall Conference Co-Chair from 2002–2007 and also served for two years as Vice President on the Board of Directors for ISACA International. Mike has taught CISA review courses for over 15 years.