“Cyber Certainty”

Paul Laurent, J.D., M.S., CISSP, CISA
Director of Cybersecurity Strategy

An Introduction:

Conversations with:

- Business leadership
- Security
- Audit
- Legal
- Law Enforcement
- Opposing Counsel

(Ranked in descending order of “fun”)

Pregame Routine:

APTs

Wall Street Journal Announces That It, Too, Was Hacked by the Chinese

Published: January 31, 2013

One day after The New York Times reported that Chinese hackers had infiltrated its computers and stolen passwords for

The Washington Post **Technology**

Chinese hackers suspected in attack on The Post's computers

By Craig Timberg and Ellen Nakashima, February 01, 2013

A sophisticated cyberattack targeted The Washington Post in an operation that resembled intrusions against other major American news organizations and that company officials suspect was the work of Chinese hackers, people familiar with the incident said.

Post company officials confirmed the broad outlines of the infiltration, which was discovered in 2011 and first reported by an

Smart grid company Telvent struck by Chinese hackers

hackers disrupted energy output, gain access to customer information.

By Ben Weitzenkorn, SecurityNewsDaily

Mon, Oct 01 2012 at 2:41 PM EST

+1 0 Like 0

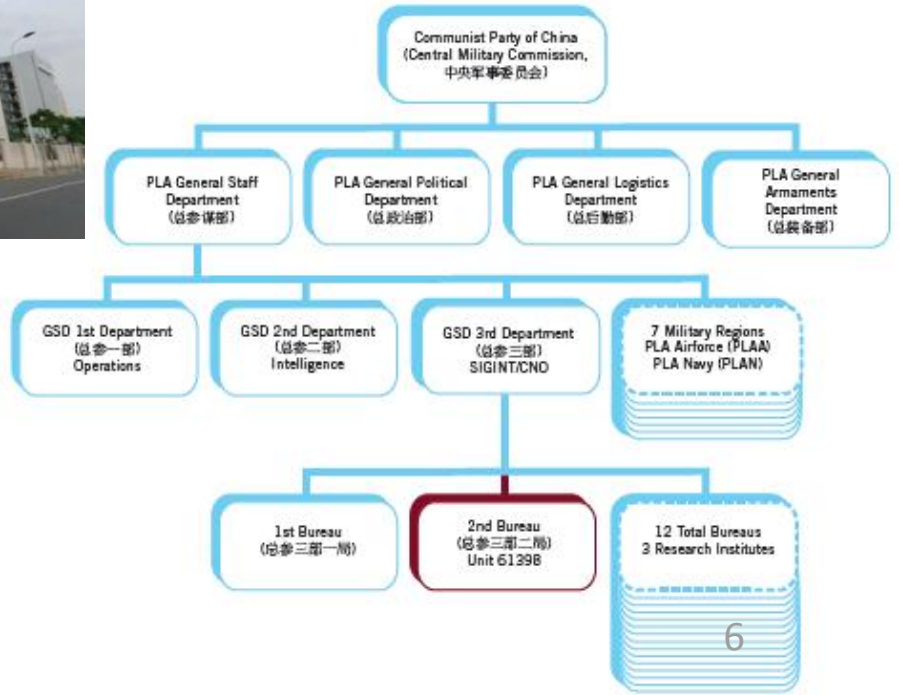
N.Y. Times hacked: How large is China's campaign to control, intimidate?

The list of media outlets infiltrated by Chinese cyberspies doesn't end with The New York Times or Wall St. Journal, cybersecurity experts say. Anyone reporting on China is a potential target.

Meet PLA Unit 61398…

- “Quality Intrusions – Since 2006”
- >1000 Servers
- >2000 Employees
- 3 “personas”

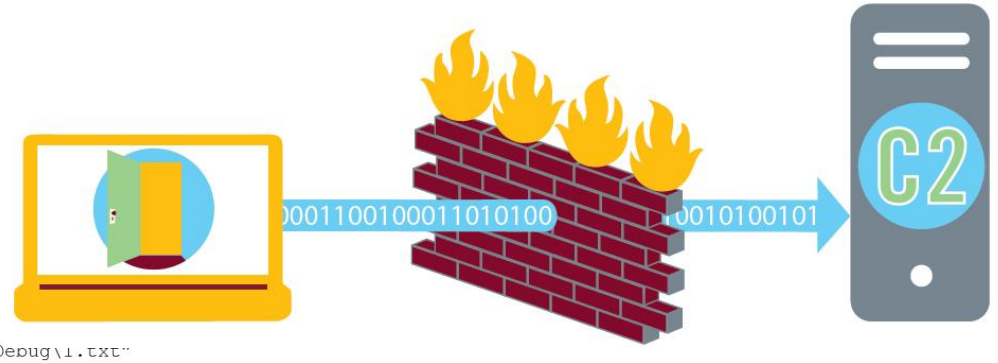
FIGURE 26: Professor Zhang (张召忠) 16 Jan 2004, source http://www.chinamil.com.cn/site1/gflt/2004-09/30/content_705216.htm



Modus Operandi

- Spearphish
- Recon
  - Persistent
  - Privileges
  - Auditing
- Package up and remove EVERYTHING

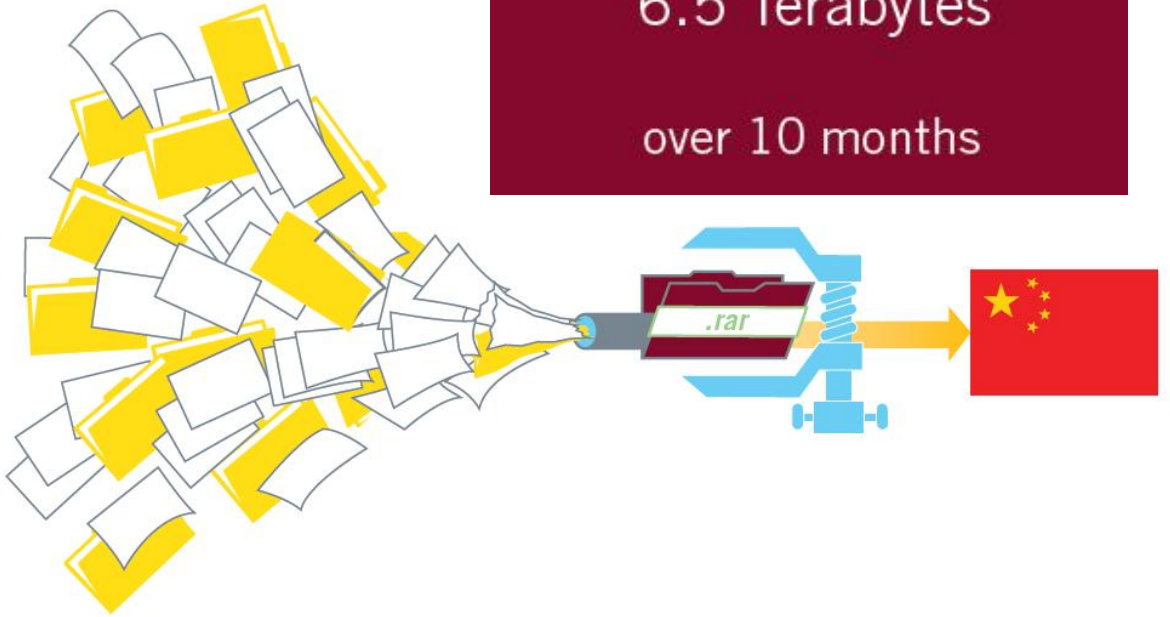
```
@echo off
ipconfig /all>>"C:\WINNT\Debug\1.txt"
net start>>"C:\WINNT\Debug\1.txt"
tasklist /v>>"C:\WINNT\Debug\1.txt"
net user >>"C:\WINNT\Debug\1.txt"
net localgroup administrators>>"C:\WINNT\Debug\1.txt"
netstat -ano>>"C:\WINNT\Debug\1.txt"
net use>>"C:\WINNT\Debug\1.txt"
net view>>"C:\WINNT\Debug\1.txt"
net view /domain>>"C:\WINNT\Debug\1.txt"
net group /domain>>"C:\WINNT\Debug\1.txt"
net group "domain users" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain admins" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain controllers" /domain>>"C:\WINNT\Debug\1.txt"
net group "exchange domain servers" /domain>>"C:\WINNT\Debug\1.txt"
net group "exchange servers" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain computers" /domain>>"C:\WINNT\Debug\1.txt"
```



Largest APT1 data theft from a single organization:

6.5 Terabytes

over 10 months



Even If: Lone Wolves & Insiders

- **Immense fallout from leaks**
- **3x as likely to target Public Sector's "Crown Jewel" Data Sets**
- **Curiosity, Ideology, Fame, Challenge, Advantage**

Threat Vectors: The Expanding Possible*

- USPS

- Large scale health care intrusions

- USIS

- OPM

Threat Vectors: Can’t Make These Up…

Hackers Threaten to Expose 37 Million Cheating AshleyMadison Users

Chris Mills
Filed to: HACKING 7/20/15 1:24am

503,954 40

stl today.com

2015 PULITZER PRIZE WINNER

ST. LOUIS POST-DISPATCH

Cardinals fire scouting director as hacking investigations continue

July 03, 2015 12:00 pm • By Robert Patrick, Derrick Goold

ST. LOUIS • The St. Louis Cardinals have terminated the contract of their scouting director, Chris Correa, as investigations continue into alleged hacking of a Houston Astros database.

A Cardinals’ lawyer, James G. Martin, confirmed the move

Threat Vectors: File Under??

04 Sources: Trump Hotels Breached Again

APR 16

Banking industry sources tell KrebsOnSecurity that the **Trump Hotel Collection** — a string of luxury properties tied to business magnate and Republican presidential candidate **Donald Trump** — appears to be dealing with another breach of its credit card systems. If confirmed, this would be the second such breach at the Trump properties in less than a year.

The First Person to Hack the iPhone Built a Self-Driving Car. In His Garage

George Hotz is taking on Google and Tesla by himself.

By Ashlee Vance | December 16, 2015

Photographs by Peter Bohler

Video by David Nicholson

From Bloomberg Businessweek

Hacktivists

Before “The Interview” & Incentives

“Anonymous” attacks Sony to protest PS3 hacker lawsuit

Outraged by Sony's lawsuit against PS3 hacker George Hotz, the hacker …

by **Nate Anderson** - Apr 4 2011, 12:42pm CST

The Day I Stopped Doing Vector Analysis…

Defamer

Sony Leak: Studio Exec Calls Kevin Hart a Greedy "Whore"

The Saddest Email: Paul Reiser Wants More *Mad About You* on DVD

Leaked: The Nightmare Email Drama Behind Sony's Steve Jobs Disaster

Sam Biddle
Yesterday 5:35pm

738,394 56

The permanently upcoming Steve Jobs biopic has been hotly anticipated since it was first

What's More Preposterous?

GAWKER

Hudson Hongo

Filed to: SONY HACK Sunday 12:22pm

North Korea Denies Role in "Righteous," Totally Bitchin' Sony Hack

30,043 3

Dennis Rodman to go back to North Korea – again

The former NBA star and self-styled 'basketball diplomat' says he plans to take pro-wrestling to the secretive state in November. We look back at his previous, controversial visits

What's typically missing?

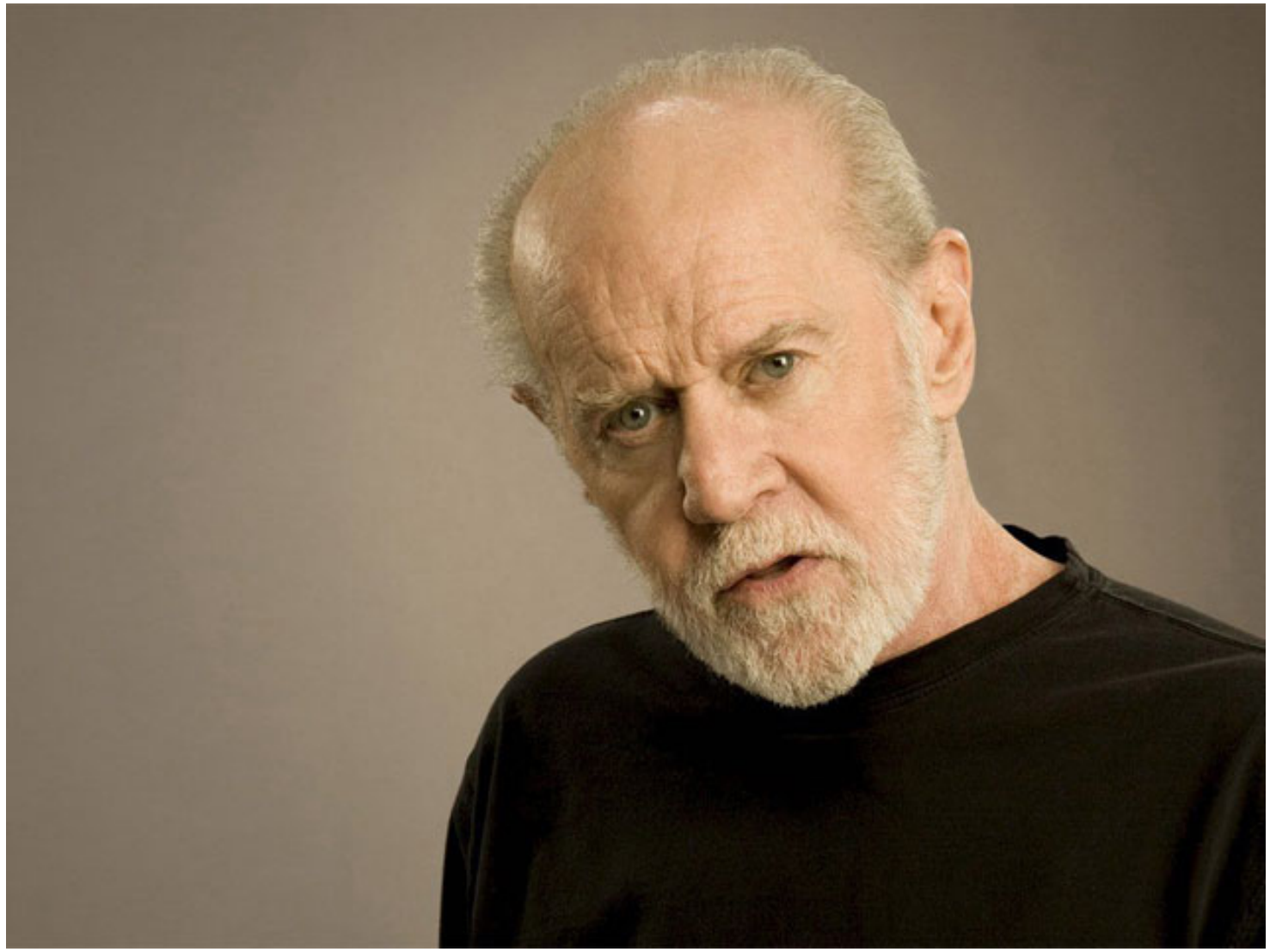
- Clear understanding of the *business* objectives & priorities (risk)
- **Risk Optics**
- The most granular unit of risk?
  - "RBAC"
- Impact on:
  - Policy
  - Process
  - Enterprise Architecture

SECURE GOVERNMENT powered by ORACLE

Involving Business

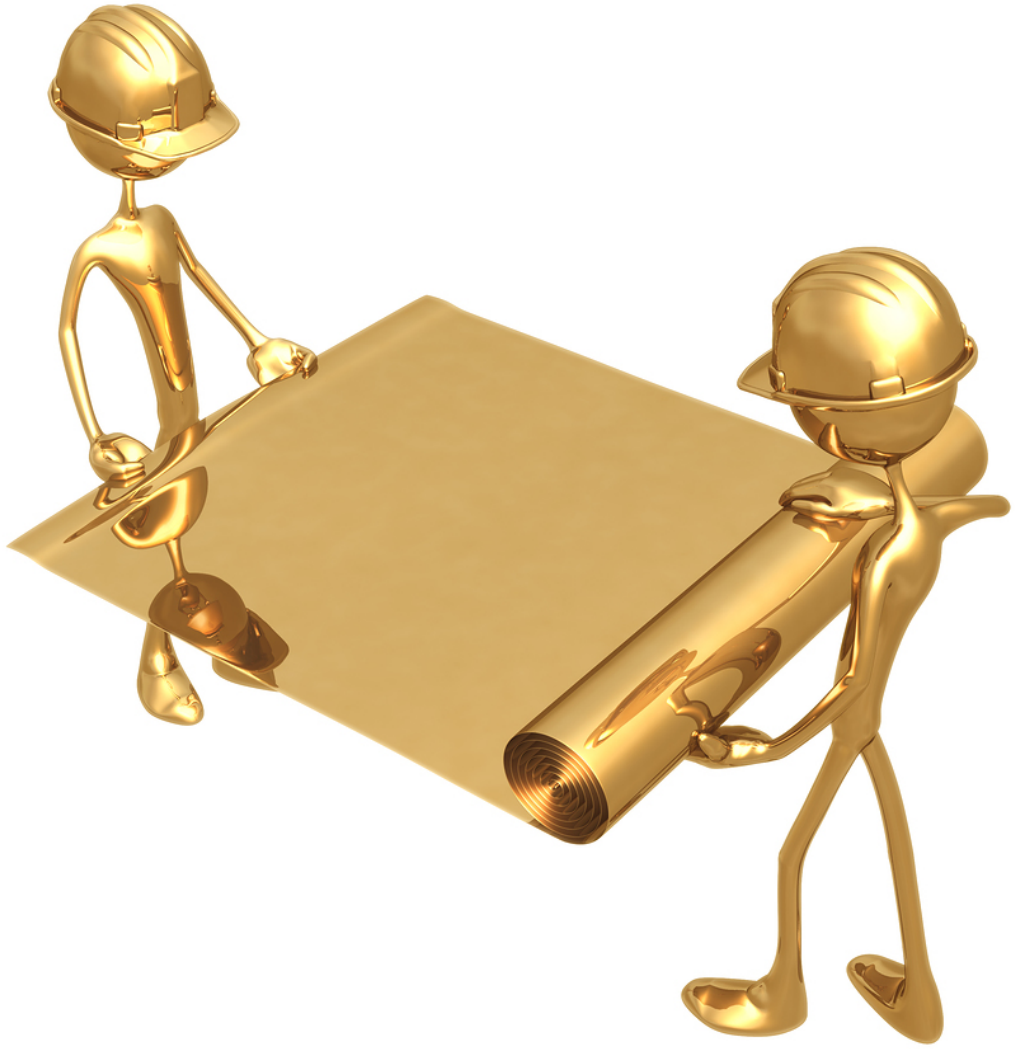
Field	Data Type	Associated System	Overall Impact	Confidentiality Impact	Integrity Impact	Availablity Impact
PII {Whole Column}			**HIGH**	**HIGH**	**HIGH**	**HIGH**
SSN	PII - Citizen	Support Enforcement	MOD/HIGH	MOD/HIGH	MOD	MOD
DOB	PII - Citizen	Support Enforcement	MOD	LOW	MOD	MOD
Address	PII - Citizen	Support Enforcement	HIGH	MOD/HIGH*	HIGH	HIGH
Name	PII - Citizen	Support Enforcement	HIGH	MOD/HIGH*	MOD/HIGH*	MOD/HIGH*
Phone #	PII - Citizen	Support Enforcement	MOD	LOW/MOD	MOD	MOD
Gender	PII - Citizen	Support Enforcement	LOW	LOW	LOW	LOW
Race	PII - Citizen	Support Enforcement	LOW	LOW	LOW	LOW
Maiden Name	PII - Citizen	Support Enforcement	MOD	MOD	LOW	LOW
Email	PII - Citizen	Support Enforcement	LOW	LOW	LOW	LOW
Driver's License	PII - Citizen	Support Enforcement	MOD	MOD	LOW/MOD	LOW/MOD
FTI {Whole Column}			**MOD**	**MOD**	**LOW**	**MOD**
Payment Type	FTI	Support Enforcement	LOW	LOW	LOW	LOW
Refund Amt	FTI	Support Enforcement	MOD	MOD	LOW	LOW
Refund Date	FTI	Support Enforcement	LOW	LOW	LOW	LOW
EIN	FTI	Support Enforcement	MOD	MOD	MOD	MOD
FIN {Whole Column}			**HIGH**	**MOD**	**HIGH**	**HIGH**
Payment Amt	FIN	Support Enforcement	MOD	LOW	MOD	MOD
Arrearages	FIN	Support Enforcement	MOD	LOW	MOD	MOD
EFT/ACH	FIN	Support Enforcement	MOD/HIGH	MOD	MOD/HIGH	MOD/HIGH
SVC	FIN	Support Enforcement	MOD	LOW	MOD	MOD

FCC v. Pacifica Foundation



The Security/Privacy Ratio

Having a Plan…



Key Takeaway 1: Even with the *best* statistical chance…

Your Hand	Dealer's Upcard									
	2	3	4	5	6	7	8	9	10	A
5-8	H	H	H	H	H	H	H	H	H	H
9	H	D	D	D	D	H	H	H	H	H
10	D	D	D	D	D	D	D	D	H	H
11	D	D	D	D	D	D	D	D	D	H
12	H	H	S	S	S	H	H	H	H	H
13	S	S	S	S	S	H	H	H	H	H
14	S	S	S	S	S	H	H	H	H	H
15	S	S	S	S	S	H	H	H	H	H
16	S	S	S	S	S	H	H	H	H	H
17-20	S	S	S	S	S	S	S	S	S	S
A,2	H	H	H	D	D	H	H	H	H	H
A,3	H	H	H	D	D	H	H	H	H	H
A,4	H	H	D	D	D	H	H	H	H	H
A,5	H	H	D	D	D	H	H	H	H	H
A,6	H	D	D	D	D	H	H	H	H	H
A,7	S	Ds	Ds	Ds	Ds	S	S	H	H	H
A,8	S	S	S	S	S	S	S	S	S	S
A,9	S	S	S	S	S	S	S	S	S	S
Pairs										
2,2	P	P	P	P	P	P	H	H	H	H
3,3	P	P	P	P	P	P	H	H	H	H
4,4	H	H	H	P	P	H	H	H	H	H
5,5	D	D	D	D	D	D	D	D	H	H
6,6	P	P	P	P	P	H	H	H	H	H
7,7	P	P	P	P	P	P	H	H	H	H
8,8	P	P	P	P	P	P	P	P	P	P
9,9	P	P	P	P	P	S	P	P	S	S
10,10	S	S	S	S	S	S	S	S	S	S
A,A	P	P	P	P	P	P	P	P	P	P

Key:

- H = Hit
- S = Stand
- P = Split
- D = Double (hit if not allowed)
- Ds = Double (stand if not allowed)

SECURE GOVERNMENT powered by ORACLE

Key Takeaway 2: "Risk" has multiple meanings

Field	Data Type	Associated System	Overall Impact	Confidentiality Impact	Integrity Impact	Availablity Impact
PII {Whole Column}			**HIGH**	**HIGH**	**HIGH**	**HIGH**
SSN	PII - Citizen	Support Enforcement	MOD/HIGH	MOD/HIGH	MOD	MOD
DOB	PII - Citizen	Support Enforcement	MOD	LOW	MOD	MOD
Address	PII - Citizen	Support Enforcement	HIGH	MOD/HIGH*	HIGH	HIGH
Name	PII - Citizen	Support Enforcement	HIGH	MOD/HIGH*	MOD/HIGH*	MOD/HIGH*
Phone #	PII - Citizen	Support Enforcement	MOD	LOW/MOD	MOD	MOD
Gender	PII - Citizen	Support Enforcement	LOW	LOW	LOW	LOW
Race	PII - Citizen	Support Enforcement	LOW	LOW	LOW	LOW
Maiden Name	PII - Citizen	Support Enforcement	MOD	MOD	LOW	LOW
Email	PII - Citizen	Support Enforcement	LOW	LOW	LOW	LOW
Driver's License	PII - Citizen	Support Enforcement	MOD	MOD	LOW/MOD	LOW/MOD
FTI {Whole Column}			**MOD**	**MOD**	**LOW**	**MOD**
Payment Type	FTI	Support Enforcement	LOW	LOW	LOW	LOW
Refund Amt	FTI	Support Enforcement	MOD	MOD	LOW	LOW
Refund Date	FTI	Support Enforcement	LOW	LOW	LOW	LOW
EIN	FTI	Support Enforcement	MOD	MOD	MOD	MOD
FIN {Whole Column}			**HIGH**	**MOD**	**HIGH**	**HIGH**
Payment Amt	FIN	Support Enforcement	MOD	LOW	MOD	MOD
Arrearages	FIN	Support Enforcement	MOD	LOW	MOD	MOD
EFT/ACH	FIN	Support Enforcement	MOD/HIGH	MOD	MOD/HIGH	MOD/HIGH
SVC	FIN	Support Enforcement	MOD	LOW	MOD	MOD

Key Takeaway 3: Speak the Same Language (Use Wheels)

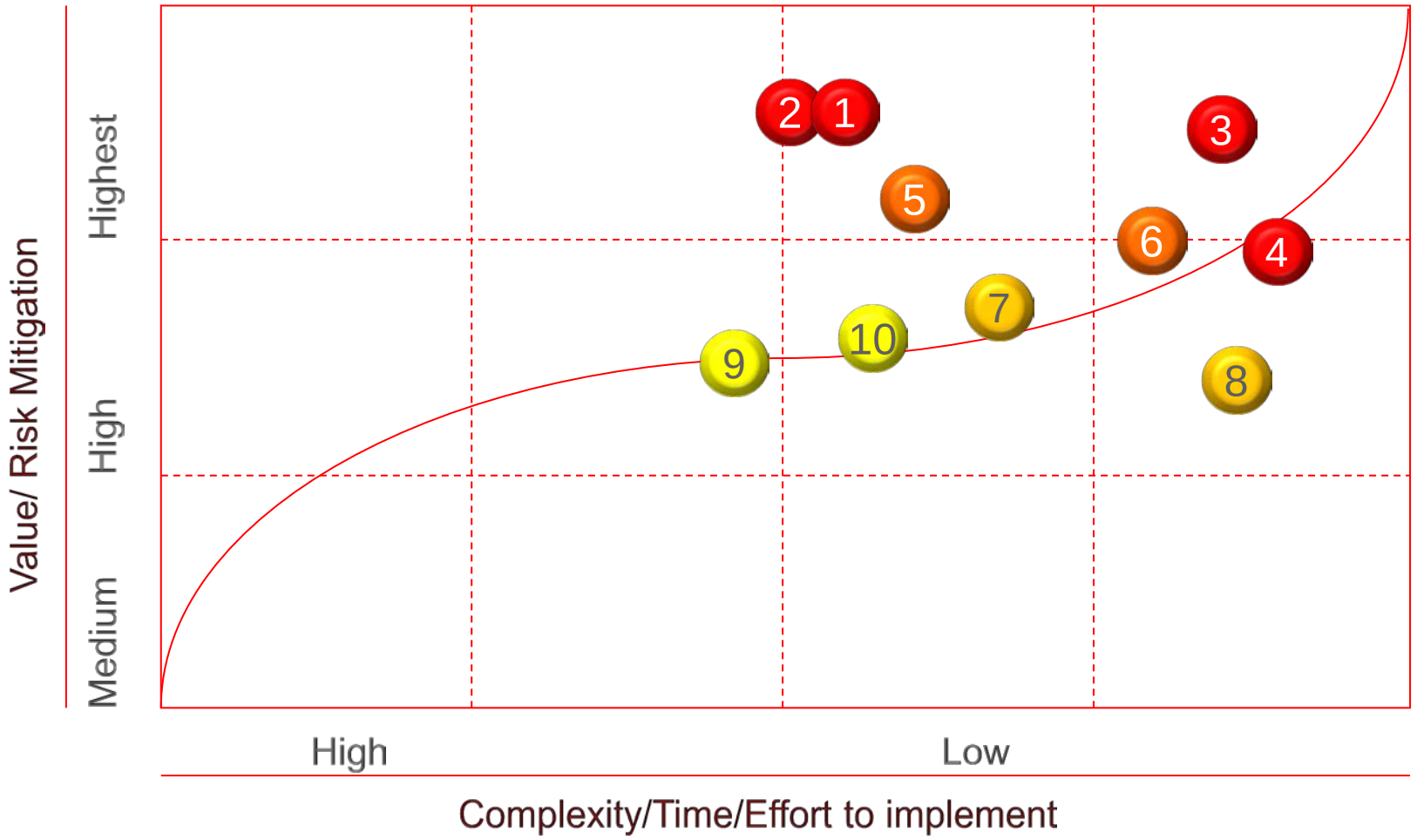
	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Sample Objectives

- Connect data to business risk
- Common taxonomy for data
  - Relation to business impact, not overly complex
  - Seek for commonality in interoperability, participation in programs, & grant applications
- Methodology
  - Common risk/data taxonomy Ranks risk to confidentiality, integrity, & availability into 3 categorizations
  - Controls based on risk/impact

A little help: Database Security Methodology Overview

Mapped to a strategy: e.g. Value/Effort Map



Recommendations	
1	Protect Sensitive Data
2	Enhance Auditing and Alerting of Database Activity
3	Encrypt Data at Rest
4	Password Controls
5	Separation of Duties/Control Authorized Access
6	Update Patching
7	Revoke Privileges on Sensitive Packages From “PUBLIC”
8	Server Security – file privileges
9	SQL Injection Prevention
10	Minor configuration issues

Granular specifics & configuration detail

Oracle Database Risk Assessment Report

Risk Category Breakdown

Severe	3
Significant	0
Some	2
Informational	0

Enviroment Overview

Data Collection Version	1.1
Analyze Version	20150326
Data Collection Date	18-APR-2015 14:05
Data Analyzed Date	20/04/2015 00:07
Database Name	DB01
Database Version	11.2.0.4.0
Database Platform	Linux x86 64-bit

Found The Following Security Concerns

The following is a list of checks that require attention. You MUST still review the raw data separately. Do NOT rely on this report solely for assessment.

Found Excessive Number Of Users With DBA Role	Details
Found Excessive Number Of Users With Alter or Drop Privilege	Details
Found Excessive Number Of Users With Deadly System Privileges	Details
Found Excessive Number Of Users With Deadly Roles	Details
Found Weak Security Parameters With Severity of SEVERE	Details
Found Excessive Number Of Users With Direct System Rights	Details
Found Excessive Number Of Users With Excessive Roles	Details
Found Users With Access To Senistive Packages	Details
Found Users With Default Passwords	Details
No Encrypted Tablespaces	Details
Found Excessive Number Of Users With DBA Role	Details

Questions