



***Managing Risk:
Keeping Your Agency Off
The Front Page***



***Paul Laurent, J.D., M.S., CISSP
Public Sector Director of Cybersecurity Strategy***

An Introduction:



Remember When...

The Year Was 2006



Remember When...

Veteran's Administration

- WORST CASE SCENARIO
 - Self-inflicted wound

CONSUMER AFFAIRS

VA Loses Data on 26 Million Veterans

Employee Claims Laptop With Sensitive Data Was Stolen

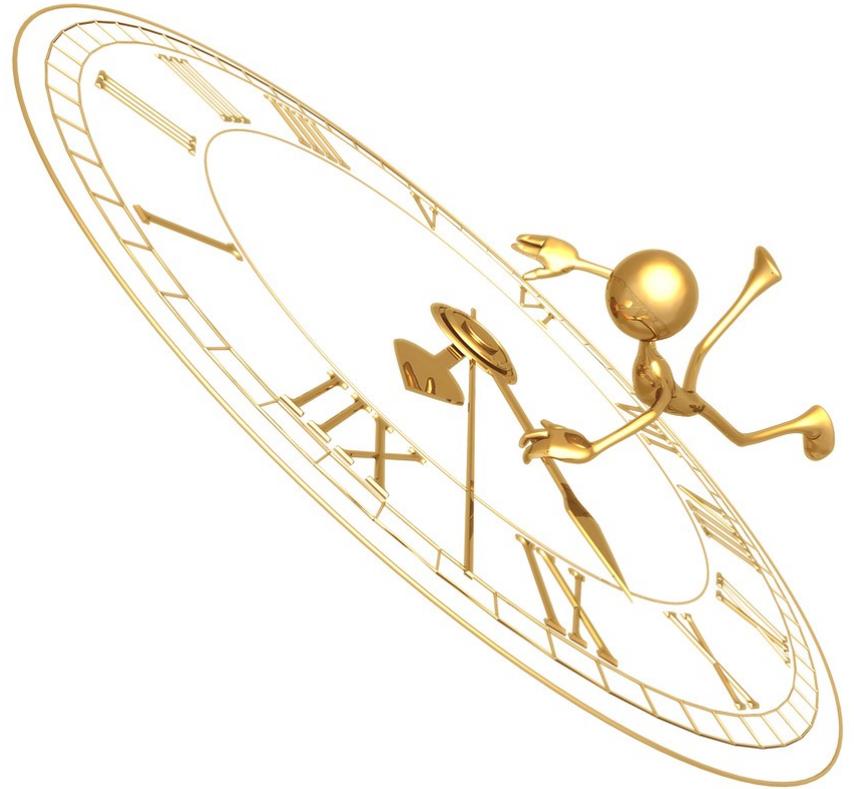
05/22/2006 | ConsumerAffairs | [Laptop Data Theft](#)



As Time Passed...

The Situation Evolved

- An “Impact Catalyst” (2002)
- National Importance (2005)
- Growth in Scale (2005-2009)
- “Cyber rioting” (2010)
- Architectural Impacts (ongoing)



There oughta' be a law...

WORST CASE: Public Sector ROI



Tech

▪ [E-mail this story](#) ▪ [Subscribe to the newspaper](#) ▪ [Sign-up for e-mail news](#)

05/29/2002 - Updated 12:55 PM ET

Hearing set on Calif. hacking incident

SACRAMENTO, Calif. (AP) — State senators said Tuesday they would investigate why it took weeks for 260,000 government employees to be notified that a hacker accessed a computer system containing their personal financial information.

Growing Awareness

WORST CASE: “Going Deep”



ChoicePoint ID theft victims span U.S.

By Carolyn Pritchard, MarketWatch

Last Update: 2:50 PM ET Feb 21, 2005

SAN FRANCISCO (MarketWatch) - ChoicePoint Inc. said Monday that a recently detected case of identification theft may have affected people across the country, not just certain residents of California, as was previously thought.

Indication of Scale

WORST CASE: Mega-opportunism

SECURITY

TJX suspect indicted in Heartland, Hannaford breaches

Networks pierced by garden-variety exploit

By Dan Goodin, 17 Aug 2009

Hacktivists

WORST CASE: Threat Modeling



“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 Architectural Revolution

Adapting Security for New Business Models

- Paper to Digital
- Mobile
- Shared Services
- Cloud
- SaaS
- Big Data
- BYOD



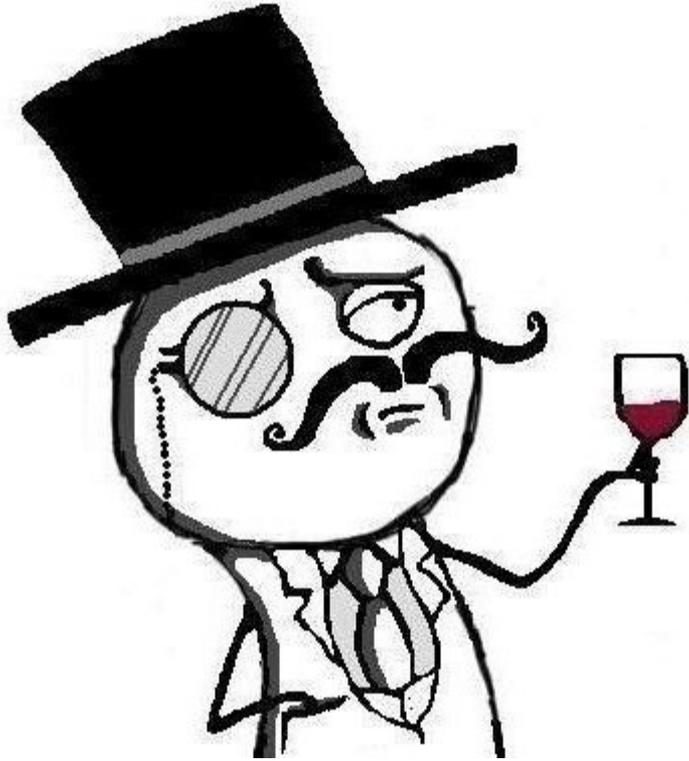
How to Plan for the Future?

Trend Analysis & Lessons Learned

- Adapt
 - Threat Modeling
 - Cyber Capabilities
 - Guidance
 - Best/Appropriate Practices
 - Compliance
 - Impact on Enterprise Architecture
 - “Getting there from here”



“Hacktivists”



- Decentralized “movements”
- Hack targets for political reasons
- No clear financial motivation
- Highly visible, large scale attacks
- They stay busy (58% of all data theft busy*): CIA, FBI, Infragard, US Senate, Scientology, PBS, Israel, Paypal, Visa, Mastercard and even Wikileaks!

Specifically Target Public Sector Orgs

WORST CASE: Busy Bees with a “Thing” for Government

P A S T E B I N | #1 PASTE TOOL SINCE 2002

CREATE NEW PASTE | TOOLS | API | ARCHIVE



P A S T E B I N

CREATE NEW PASTE | TRENDING PASTES



Operation Anti-Security

BY: A GUEST | JUN 19TH, 2011 | SYNTAX: NONE | SIZE: 1.83 KB | VIEWS: 174,886 | EXPIRES: NEVER

[COPY TO CLIPBOARD](#) | [DOWNLOAD](#) | [RAW](#) | [EMBED](#) | [REPORT ABUSE](#)

Welcome to Operation Anti-Security (#AntiSec) - we encourage any vessel, large or small, to open fire on any government or agency that crosses their path. We fully endorse the flaunting of the word “AntiSec” on any government website defacement or physical graffiti art. We encourage you to spread the word of AntiSec far and wide, for it will be remembered. To increase efforts, we are now teaming up with the Anonymous collective and all affiliated battleships.

Top priority is to steal and leak any classified government information, including email spools and documentation. Prime targets are banks and other high-ranking establishments. If they try to censor our progress, we will obliterate the censor with cannonfire anointed with lizard blood.

Insiders Inflict Incredible Injury



- Immense fallout from leaks
- 3x as likely to target Public Sector's "Crown Jewel" Data Sets
- Curiosity, Ideology, Fame, Challenge, Advantage
- **WORST CASE: Deal Crushing Blows to Most Sensitive Initiatives & Programs. Know Where It Hurts.**



APT's



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 New York Times

Business Day
Technology

Chinese Army Unit Is Seen as Tied to Hacking Against U.S.

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.

The Washington Post Politics Opinions Local Sports National

Chinese cyberspies have hacked most Washington institutions, experts say



Internet

NSA: China is Destroying U.S. Economy Via Security Hacks

Jason Mick (Blog) - March 28, 2012 7:06 PM

Jential

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

DOD: Hackers Breached U.S. Critical Infrastructure Control Systems

Defense secretary Leon Panetta says cyberattacks against critical infrastructure at home and abroad--some of which he called the worst to date--should spark urgent action against the hacker threat.

By J. Nicholas Hoover InformationWeek
October 12, 2012 01:04 PM

Smart grid company Telvent struck by Chinese hackers

hackers disrupted energy output, gain access to customer information.

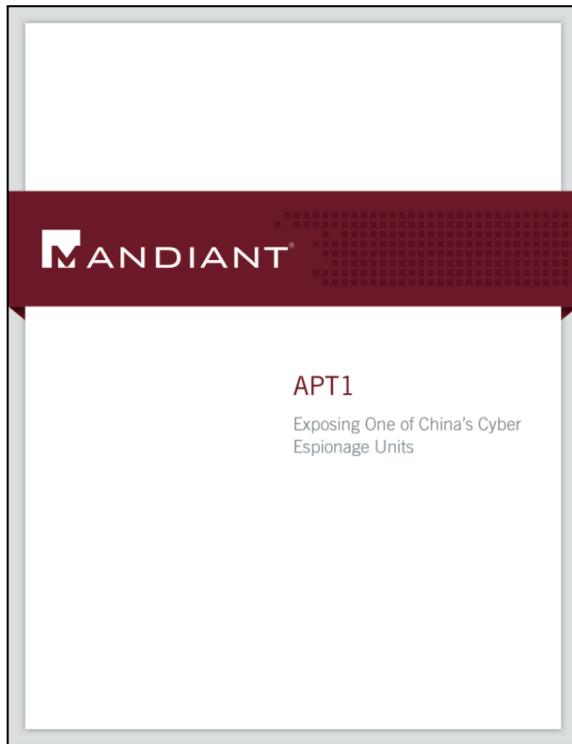
By Ben Weitzenkorn,
SecurityNewsDaily

Mon, Oct 01 2012 at 2:41 PM EST



ACLE

Ever Adapting Threat Landscape



Stealthy
Zero Day
Polymorphic
Coordinated
Targeted
Persistent

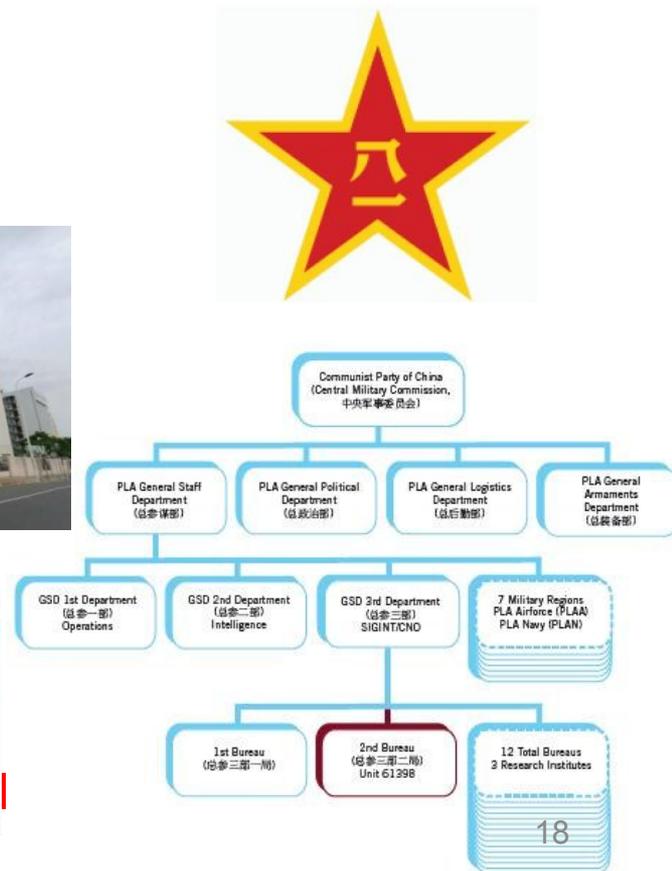


Meet PLA Unit 61398...

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



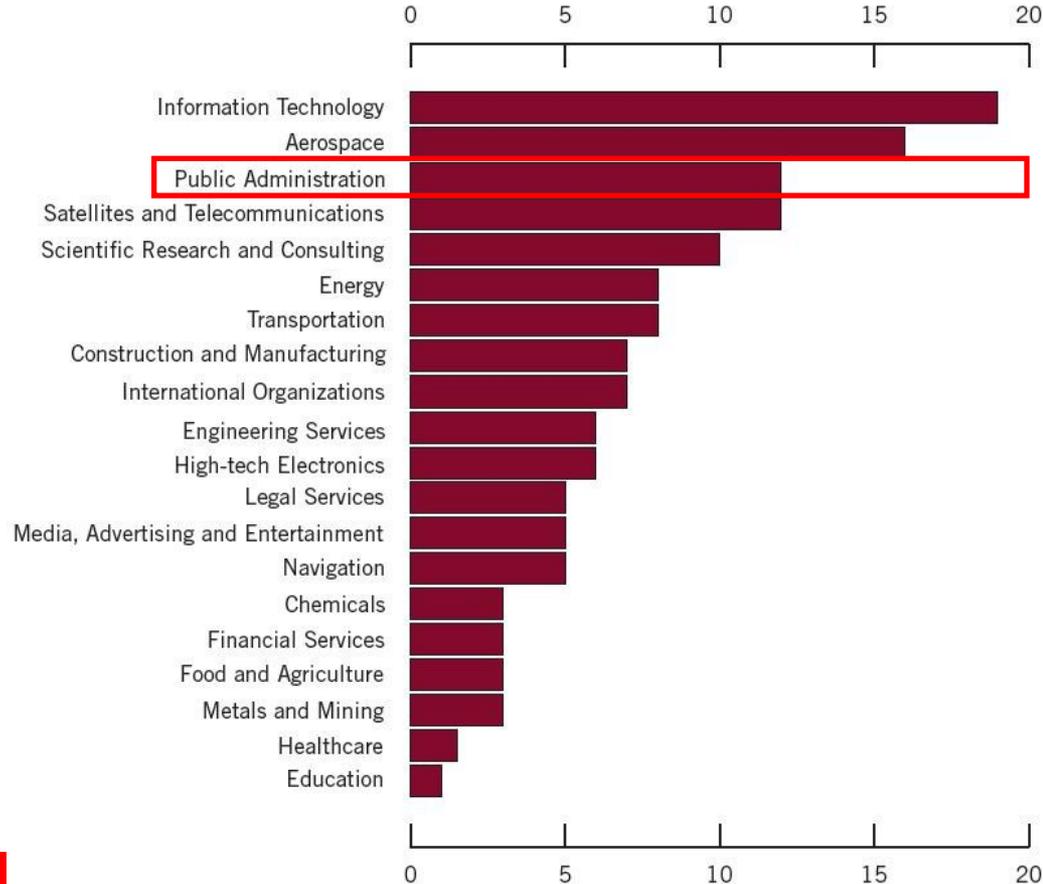
FIGURE 26: Professor Zhang (张召忠) 16 Jan 2004, source http://www.chinamil.com.cn/site1/gff/2004-09/30/content_705216.htm



On Closer Inspection...

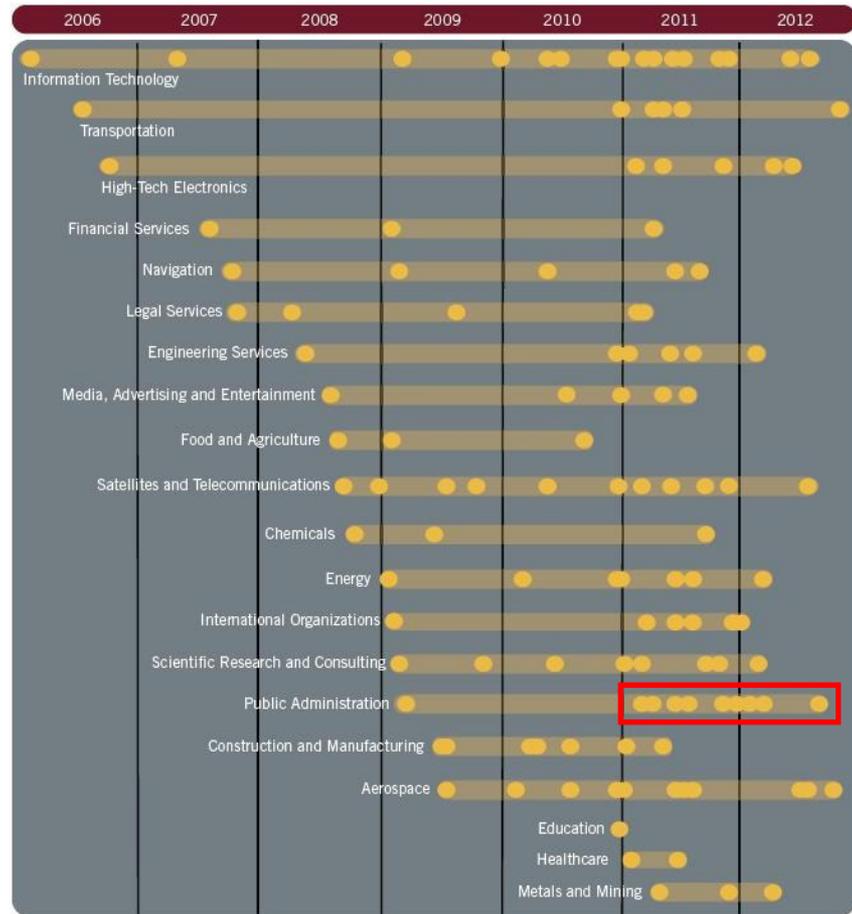
Total # of attacks by industry vertical

A number of other categories that are related.



Closer still.

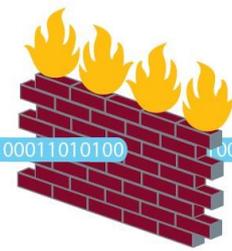
Most targeted vertical since 2011



Modus Operandi (in a nutshell)

- Spearphish
- Recon
 - Persistent
 - Privileges
 - Auditing
- Package up and remove EVERYTHING
- **WORST CASE: Will Require Unprecedented Security Capabilities to Stop**

```
@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 "exchad" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain"
```



0001100100011010100

0010100101



Largest APT1 data theft from a single organization:
6.5 Terabytes
over 10 months



Cybercriminals:

- Delivery vs. Development
- Leaving Breaching for Building Tools
- Targets of Opportunity (75% trend)
- High Proportion of Automation

(Reuters) - The website for the Washington State court system has been hacked and up to 160,000 Social Security numbers and a million driver's license numbers may have been accessed, officials said on Thursday.

OCTOBER 29, 2012

South Carolina reveals massive data breach of Social Security Numbers, credit cards

State governor said she wants the hacker who exposed approximately 3.6 million SSNs and 387,000 credit and debit card numbers 'slammed to the wall'

Utah: Data breach may include 750,000 people

AP By JOSH LOFTIN | Associated Press - Mon, Apr 9, 2012

SALT LAKE CITY (AP) — Health officials in Utah say 750,000 additional people, including many children, may have had personal information stolen by hackers.

Utah Department of Health spokesman Tom Hudachko (HU'-dak-ko) said Monday that about 250,000 Social Security numbers were part of the tens of thousands of stolen files, although many numbers didn't include other information.

Hudachko says the victims could be Medicaid and Children's Health Insurance Program recipients as well as anyone whose healthcare provider submitted their information to the state for possible Medicaid coverage within the last four months.

Utah Department of Technology Services Executive Director Stephen Fletcher says the hackers accessed a health department server that didn't have a secure password. The agency originally thought the hackers stole 24,000 Medicaid claims but now estimate more than 200,000 files were stolen.



ORACLE

WORST CASE: Learning from All Other Players



The SCDOR Hack: Great Security Theater in Five Stages

Hal Berghel, *University of Nevada, Las Vegas*

The South Carolina governor's response to the SCDOR hack represents a textbook application of Elisabeth Kübler-Ross's "five stages of grief" to cybersecurity.

Pick up a paper, any paper...

Profound IMPACT of Cybersecurity

- “Those that have been breached...”
- Lives, programs, fortunes...changed
- The questions *every*:
 - CIO
 - Board
 - Governor

needs to ask

OCTOBER 29, 2012

South Carolina reveals massive data breach of Social Security Numbers, credit cards

State governor said she wants the hacker who exposed approximately 3.6 million SSNs and 387,000 credit and debit card numbers 'slammed to the wall'



Up to 160,000 Social Security numbers exposed in Washington state court hack

RACHEL LA CORTE, The Associated Press

May 9, 2013 at 4:06 PM ET

OLYMPIA, Wash.—The Washington state Administrative Office of the Courts was hacked sometime between last fall and February, and up to 160,000 Social Security numbers and 1 million driver's license numbers may have been accessed during the data breach of its public website, officials said Thursday.

Utah: Data breach may include 750,000 people

AP By JOSH LOFTIN | Associated Press – Mon, Apr 9, 2012

SALT LAKE CITY (AP) — Health officials in Utah say 750,000 additional people, including many children, may have had personal information stolen by hackers.

Utah Department of Health spokesman Tom Hudachko (HU'-dak-ko) said Monday that about 250,000 Social Security numbers were part of the tens of thousands of stolen files, although many numbers didn't include other information.

Hudachko says the victims could be Medicaid and Children's Health Insurance Program recipients as well as anyone whose healthcare provider submitted their information to the state for possible Medicaid coverage within the last four months.

Utah Department of Technology Services Executive Director Stephen Fletcher says the hackers accessed a health department server that didn't have a secure password. The agency originally thought the hackers stole 24,000 Medicaid claims but now estimate more than 200,000 files were

Target Earnings Slide 46% After Data Breach

Updated Feb. 26, 2014 6:36 p.m. ET



Making Adjustments

What have *recent* activities shown us?

- Hacktivists: Unpredictable, Eschew modeling
- Insiders: May know your weaknesses & sensitive data better than you do
- APTs: Advanced. Persistent. Motivated.
- Cybercriminals: Quick Learners & Up the Ante
- **WORST CASE: An amalgam of ALL, stakes continue to grow**



New threats call for a new security roadmap

Accounting for complexity, scale, lessons learned...

- New Considerations

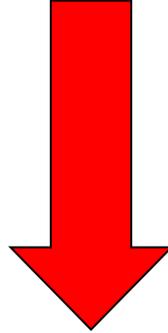
- Stealth, Covering Audit Trails
- Cross Boundary Compromises, Non-prod Environments
- Privileged Users & Privilege Escalation
- Zero Day
- Architecture & Delivery



A Little Help Please?



Convergence



NLST

NIST Special Publication 800-53R4

Specific controls and granular capabilities

- Adjustments
 - Audit protection & proactive alerting
 - Superuser access
 - Continuous monitoring
 - Secure configurations

NIST Special Publication 800-53
Revision 4



**National Institute of
Standards and Technology**

U.S. Department of Commerce

Security and Privacy Controls
for Federal Information Systems
and Organizations

CITIZEN LICENSE CHECK SYSTEM - NIST SPECIAL PUBLICATION 800-53 MAPPING					
CNTL NO.	CONTROL NAME	CURRENT CAPABILITY	RISK ASSESSMENT	EXISTING POLICY	CAPABILITY
AWARENESS AND TRAINING					
AT-1	Security Awareness and Training Policy	3	Not performed		There is a sit
AT-2	Security Awareness	3	Not performed		There is a sit
AT-3	Security Training	1	Not performed		There is a sit
AT-4	Security Training Records	1	Not performed		There is a sit
AT-5	Contacts with Security Groups and	2	Not performed		Designated i
AUDIT AND ACCOUNTABILITY					
AU-1	Audit and Accountability Policy and	0	Not performed		There are no
AU-2	Auditable Events	0	Not performed		Control not i
AU-3	Content of Audit Records	1	Not performed		The CLCS app
AU-4	Audit Storage Capacity	1	Not performed		DBAs monitc
AU-5	Response To Audit Processing Failures	1	Not performed		Audits are w
AU-6	Audit Review, Analysis, and Reporting	0	Not performed		Control not j
AU-7	Audit Reduction and Report Generation	0	Not performed		Control not j
AU-8	Time Stamps	1	Not performed		Time stamps
AU-9	Protection of Audit Information	0	Not performed		Auditing is n
AU-10	Non-repudiation	0	Not performed		Non-repudia
AU-11	Audit Record Retention	1	Not performed		Audit record
AU-12	Audit Generation	1	Not performed		Not docum
AU-13	Monitoring for Information Disclosure	0	Not performed		No monitorii
AU-14	Session Audit	0	Not performed		Information
AC-21	User Based Collaboration and Informatio	0	Not performed		Handled by 1
AC-22	Publicly Accessible Content	NA	Not performed		Unknown, m

Priority and Baseline Allocation:

P1	LOW AC-18	MOD AC-18 (1)
----	-----------	---------------

NIST Risk Management Framework

Integration, Management Processes, Iterative Improvement

- Adjustments
 - Top down framework for most specs
 - Risk-based decision making
 - Lifecycle of adjustments
 - Doesn't count on preventing all attacks
 - Baselining
 - “Continuous monitoring & controls”

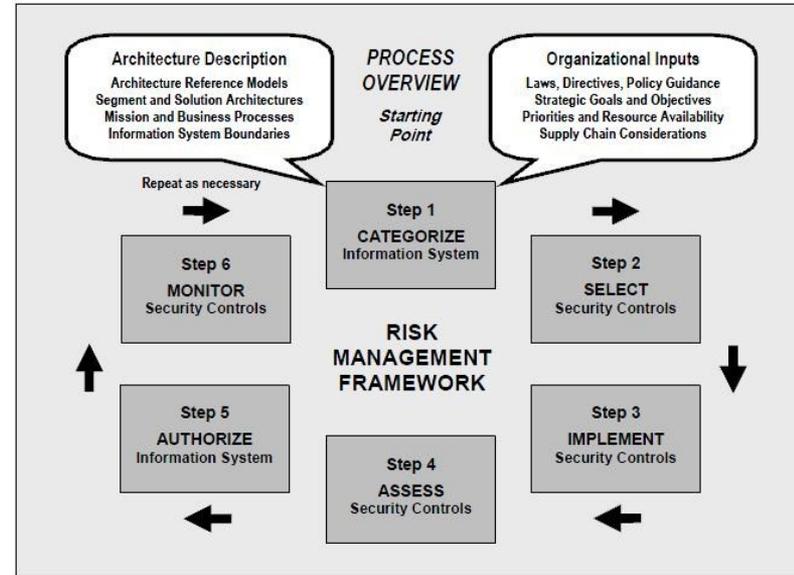
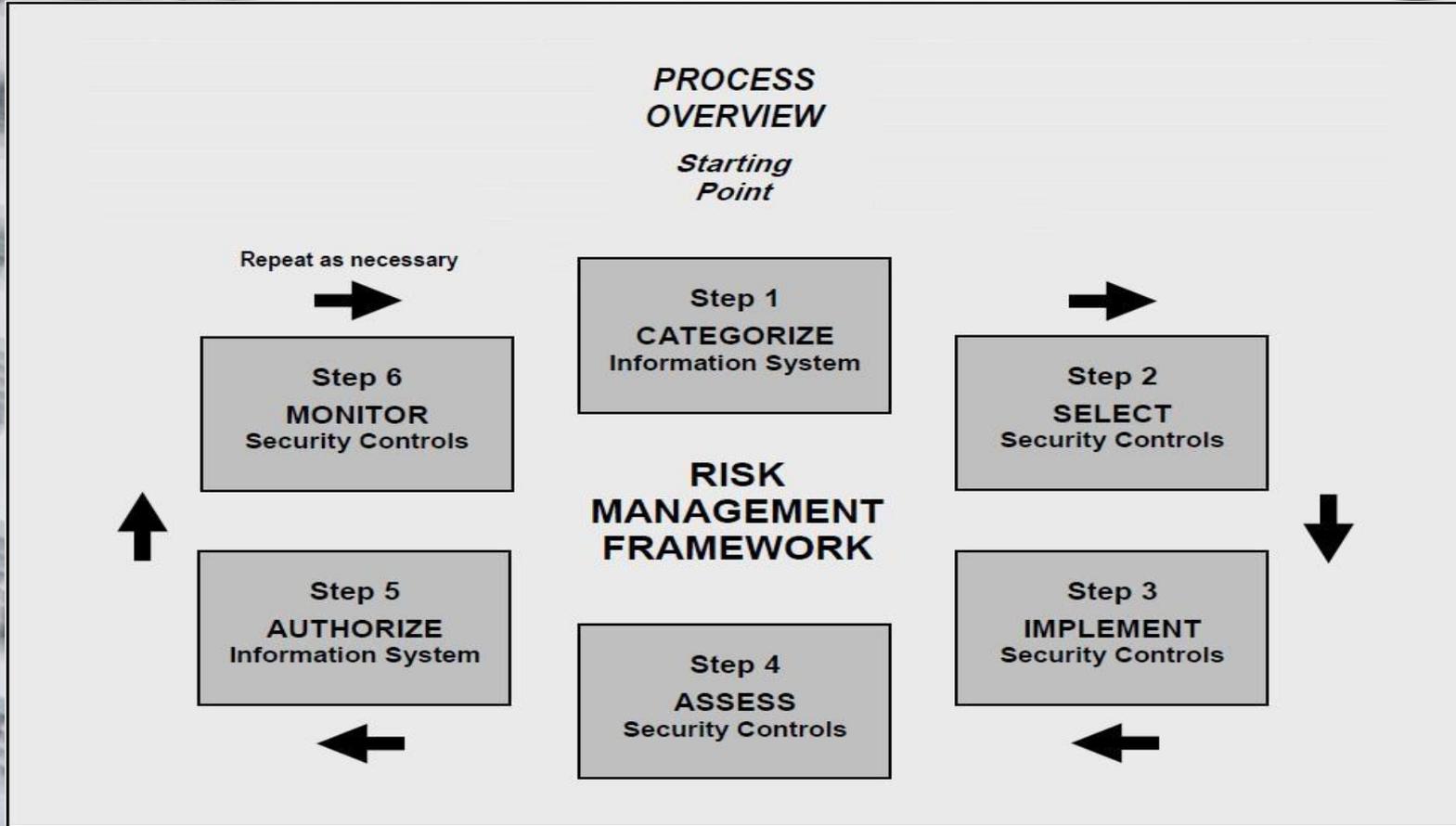
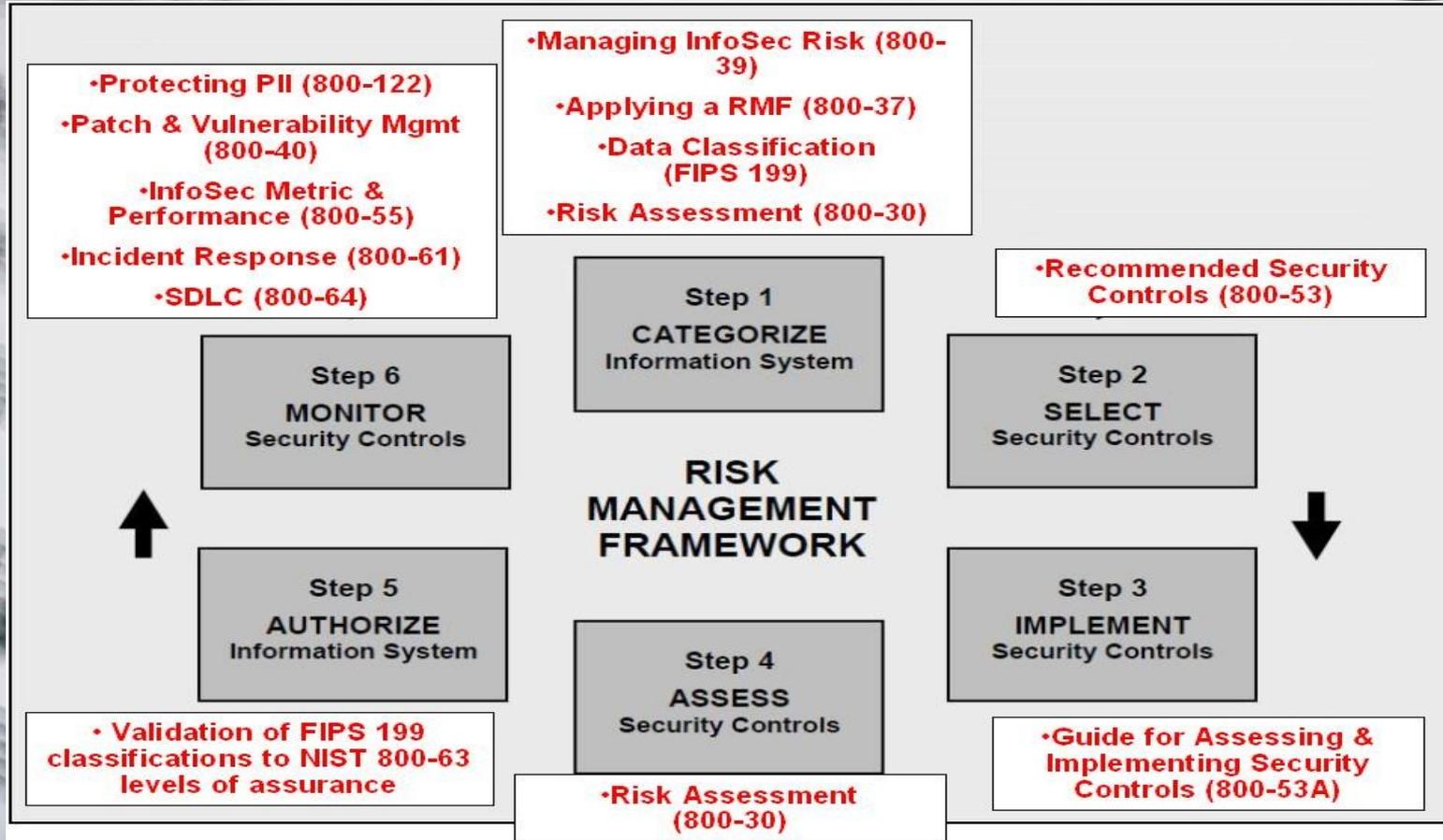


FIGURE 2-2: RISK MANAGEMENT FRAMEWORK

Convergence in Standards



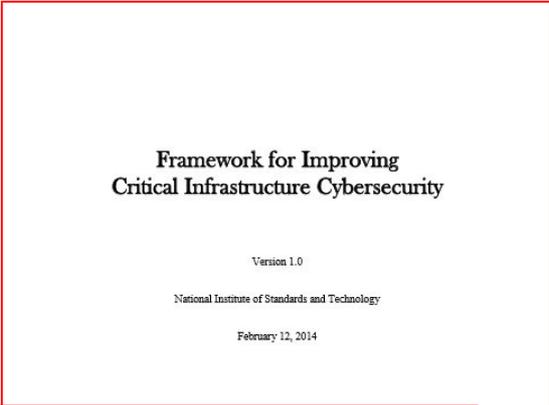
Prescriptive



The NIST Cybersecurity Framework

How'd We Get Here?

- Executive Order 13636
 - SERIOUS threats!
 - “Critical Infrastructure Protection”
- NIST tasked with writing the framework
- Voluntary
- Public/private
- Flexible



Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014

Presidential Documents

Executive Order 13636 of February 12, 2013

Improving Critical Infrastructure Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Who's affected?

“Critical Infrastructure”

- Directly S&L: I.T., Energy, Food & Agriculture, Government Facilities, Transportation, Water Treatment, First Responders
- Likely Related: Health Care, Dams, Nuclear/Materials/Waste, Communications



Government Facilities Sector

The Department of Homeland Security and the General Services Administration are

designated as the Co-Sector-Specific Agencies for the Government Facilities Sector.



Healthcare and Public Health Sector

The Department of Health and Human Services is designated as the Sector-Specific Agency for the

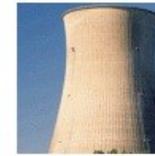
Healthcare and Public Health Sector.



Information Technology Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the

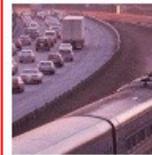
Information Technology Sector.



Nuclear Reactors, Materials, and Waste Sector

The Department of Homeland Security is designated as the Sector-

Specific Agency for the Nuclear Reactors, Materials, and Waste Sector.



Transportation Systems Sector

The Department of Homeland Security and the Department of Transportation are

designated as the Co-Sector-Specific Agencies for the Transportation Systems Sector.



Water and Wastewater Systems Sector

The Environmental Protection Agency is designated as the Sector-

Specific Agency for the Water and Wastewater Systems Sector.

Business Impacts

More adjustments

- Reinforces several security frameworks
- Public Sector still uses NIST
 - IRS 1075, HIPAA/HITECH, CJIS, etc.
- Early Supporters
- De Facto Standard?

Why Businesses Can't Ignore US Cybersecurity Framework

Industry leaders and President Obama call the framework just a first step in creating a cybersecurity playbook for 16 US critical infrastructure sectors. But this is more than just a reference manual.

For immediate release: February 12, 2014

NASCIO Supports Adoption of the NIST Cybersecurity Framework

LEXINGTON, Ky., Wednesday, February 12 — NASCIO applauds the

Virginia quickly adopts National Cybersecurity Framework



By [David Stegon](#) · Wednesday, February 12, 2014 · 3:33 pm

Under the Covers

Identify. Protect. Detect. Respond. Recover.

- Framework Core (activities/outcomes)
- Implementation Tiers (processes)
- Framework Profile (detailed guidance)

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

PROTECT (PR)	<p>Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.</p>	<p>PR.AC-1: Identities and credentials are managed for authorized devices and users</p>	<ul style="list-style-type: none"> CCS CSC 16 COBIT 5 DSS05.04, DSS06.03 ISA 62443-2-1:2009 4.3.3.5.1 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 NIST SP 800-53 Rev. 4 AC-2, IA Family
		<p>PR.AC-2: Physical access to assets is managed and protected</p>	<ul style="list-style-type: none"> COBIT 5 DSS01.04, DSS05.05 ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
			<ul style="list-style-type: none"> COBIT 5 APO13.01, DSS01.04, DSS05.03 ISA 62443-2-1:2009 4.3.3.6.6 ISA 62443-3-3:2013 SR 1.13, SR 2.6 ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1

- NIST SP 800-53 Rev. 4 AC-2, IA Family**

Identify

Identify. Protect. Detect. Respond. Recover.

- Identify is NOT referring to threats
- Assets, Risks, Policies
- Actionable intelligence, Privilege/role modeling

ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy

Protect

Identify. Protect. Detect. Respond. Recover.

- Locking down access (data, identity, remote access)
- Also secure environments (backup, non-prod, maintenance)
- Where most of the 800-53 capabilities are organized

PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology

Detect

Identify. Protect. Detect. Respond. Recover.

- Requires full-stack visibility
- Actionable intelligence difficult to cull from disparate systems
- System, infrastructure, data, access nodes in security context
- An integration project in itself

DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes

Respond

Identify. Protect. Detect. Respond. Recover.

- Analysis, Alerting, Segmentation
- Should be reflected in Enterprise Architecture
- Cyber analytics/reporting and mitigation

RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements

Recover

Identify. Protect. Detect. Respond. Recover.

- Resiliency
- Recovery
- Business Continuity
- Iterative Adjustment

RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

“Getting There from Here”

Cybersecurity looks different for every organization

- Threats require a holistic approach
- Multiple-disciplines
 - People
 - Process
 - Policy
 - Technology
 - Enterprise Architecture



Most Common WORST CASE Prescriptions

Helping where it hurts...

- Comprehensive DB Security
- Secure & Complete Audit Platform
- Masking Sensitive Data in Non-Production
- Identity Management & RBAC
- Security Policy Enforcement
- Secure configuration/management
- Continuous monitoring/alerting



Resources & Support

How Oracle can help

- Assistance in mapping to Cyber specs
 - Data classification
 - Risk assessment
 - NIST based data security workshop
- RBAC/Identity Modeling
 - SICAM Infrastructure
- Mobile Security/BYOD Architecture
- Secure Government Resource Center
 - Cybersecurity White Paper

Field	Data Type	Associated System	Overall Impact	Confidentiality Impact	Integrity Impact	Availability 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

CITIZEN LICENSE CHECK SYSTEM - NIST SPECIAL PUBLICATION 800-53 MAPPING					
CNTL NO.	CONTROL NAME	CURRENT CAPABILITY	RISK ASSESSMENT	EXISTING POLICY	CAPABILITY
AWARENESS AND TRAINING					
AT-1	Security Awareness and Training Policy	3	Not performed		There is a st
AT-2	Security Awareness	3	Not performed		There is a st
AT-3	Security Training	1	Not performed		There is a st
AT-4	Security Training Records	1	Not performed		There is a st
AT-5	Contacts with Security Groups and	2	Not performed		Designated
AUDIT AND ACCOUNTABILITY					
AU-1	Audit and Accountability Policy and	3	Not performed		There are no
AU-2	Auditable Events	3	Not performed		Control not
AU-3	Content of Audit Records	1	Not performed		The CLCS app
AU-4	Audit Storage Capacity	1	Not performed		DBAs monito
AU-5	Response To Audit Processing Failures	1	Not performed		Audits are w
AU-6	Audit Review, Analysis, and Reporting	3	Not performed		Control not
AU-7	Audit Reduction and Report Generation	3	Not performed		Control not
AU-8	Time Stamps	1	Not performed		Time stamps
AU-9	Protection of Audit Information	3	Not performed		Auditing is r
AU-10	Non-repudiation	3	Not performed		Non-repudia
AU-11	Audit Record Retention	1	Not performed		Audit record
AU-12	Audit Generation	1	Not performed		Not docum
AU-13	Monitoring for Information Disclosure	3	Not performed		No monitori
AU-14	Session Audit	3	Not performed		Information
AC-21	User Based Collaboration and Informati	3	Not performed		Handled by
AC-22	Publicly Accessible Content	NA	Not performed		Unknown, m

More Resources for the Most Important TLA's

CLM's & RGE's



Have a Plan

By the Time You Need It...

- Hope
- The Plan
- The Team (“Makin’ a List”)
 - The Lead?
 - CISO? CPO? CIO? Counsel?
 - HR? Call Center? Law Enf?
 - Partners? PR?
- Drill, Baby, Drill!!!
 - “Checkin’ it Twice” (or 4x)
 - Contracts



“First 24”

Most Critical Steps (Internal)

- Record everything!
 - Detection, Efforts, Notification, Scope
- Stop & Secure
 - Don’t power down!
- Assemble the team
 - You have a contact list, right?
- Interview & more documenting
- Determine priorities
 - Regulations, Conflicts, Obligations



“First 24”

Most Critical Steps (External)

- SME's
 - Law Enforcement
 - Forensics
 - PR/Breach
- Review Notification Protocols/Decisions
 - Language & Templates
- Respond/Report



Resources & Templates

“I see you have a wheel...”

[Company Logo]
[Return Address]
[Date]

[Recipient's Name]
[Address]
[City, State, Zip (shows thru outer envelope window)]

Important Security and Protection Notification.
Please read this entire letter.

Dear [Insert customer name]:

I am contacting you regarding a data security incident that has occurred at [Insert Company Name]. This incident involved your [describe the type of personal information (of your client) that may be potentially exposed due to the breach incident (i.e., Social Security number, etc.)]. As a result, your personal information may have been potentially exposed to others. Please be assured that we have taken every step necessary to address the incident, and that we are committed to fully protecting all of the information that you have entrusted to us.

**An example
notification letter.**

“Ground Zero” at a Glance

A Rough Outline Cadence

- Discover
- Investigate & Abate
- Notify Your Team
- Call in SME's
 - Counsel, Forensics, Law Enforcement?
PR? 3rd Party SME's?
- Begin Notification Cadence
- Announcements, Notifications, Call Center
- RECOVER



Hardware and Software

ORACLE®

Engineered to Work Together

ORACLE®