



REDUCING THE LOSS OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

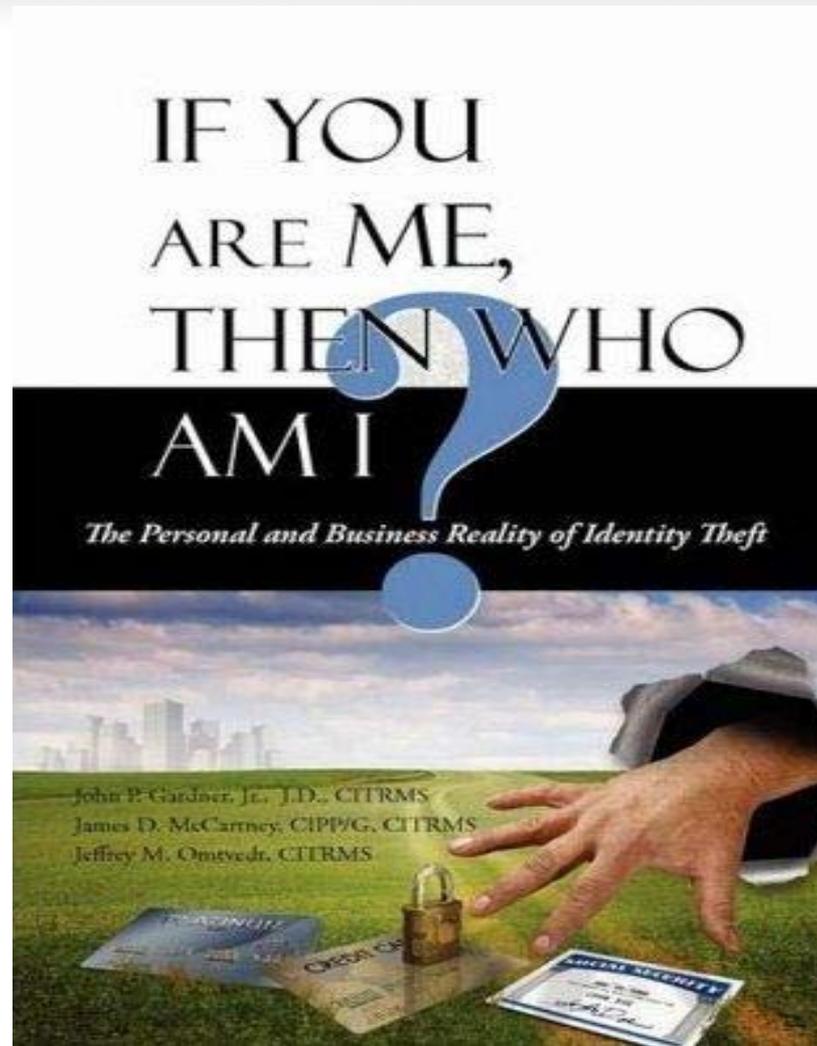
Identity theft tops the Federal Trade Commission's (FTC) list of what consumers complain about most. The number of ID theft complaints increased about 20 percent last year. The commission fielded 313,982 ID theft complaints in 2008, with 20-39-year-olds representing the group most affected by the crime. The most complaints came out of Arizona, California, Florida and Texas. Several factors may be responsible for the overall increase, including the high number of enterprise breaches last year and financial crisis fallout.

Steve Muck CIPP/G
DON CIO Privacy Team Leader
703 602 4412 steven.muck@navy.mil



Overview

- Introductions
- Identity Theft – James McCartney, DMDC
- News from Washington
- Data At Rest Rollout Plan
- High and Low Risk PII
- Response by BUPERS to reduce Breaches
- SSN Reduction Initiative ID cards, forms, IT systems
- DON Breach Metrics and Trends
- DON CIO Web Site and Important Privacy Links



**Presentation by James McCartney, CIPP/G
Co-author of, “If You Are Me, Then Who Am I?”**



News From Washington

- DECLARED UNCONSTITUTIONAL** Child Online Protection Act
 - Too burdensome and violates 1st Amendment
- \$20M **JUDGMENT** in favor of Veterans in '06 VA PII Breach case.
- NEW** ID Theft Enforcement and Restitution Act
 - makes it easier to prosecute thieves and compensate victims
- PROPOSED** Protecting the Privacy of Social Security Numbers Act of '09
 - Prohibits the display, sale, or purchase of Social Security numbers without expressed consent of the individual, w/exceptions.
- PROPOSED** requirement to store all health records electronically
 - \$20B for Health Care IT in American Recovery and Reinvestment Act
- NEW** DoD PIA Template (DoD Form 2930 Nov 08) **NEW** DON Gouge
- Draft** DoD PIA Guidance (signed Feb 09) **Draft** DON guidance soon!
- NEW** PII INFO ALERT (Sign up is in the room)
- NEW** Digital signatures on all emails where CAC/PKI enabled
- NEW** Data at rest encryption being pushed for NMCI seats
- REMINDER** DON IM/IT team or individual award (Nov. submit deadline)
- NEW** SSN Reduction Initiative – Forms and IT system review w/FISMA
- NEW** DON PII Handling Users Guide
- NEW** DON PII Awareness Posters



Data At Rest Rollout

NMCI implementation of DAR solution began mid April 09 and will be completed by Sep 09.

- Allows users to specify a default password or PKI cert to encrypt/decrypt any files created or modified on removable devices
- Places a small utility on removable devices that decrypts data on computers without the encryption software
- For encrypted data stored on removable devices, the user who stored the data will be responsible for providing access control to that device/data for other users
- **If DAR encryption enabled device is lost, stolen or compromised a report to U.S. CERT is required but notifications are not.**
- For more info: www.homeport.navy.mil/support/articles/data-at-rest/
- For computer based training:
www.homeport.navy.mil/training/security/dar/



High and Low Risk PII

“High risk” PII which may cause harm to an individual if lost/compromised

- Financial information- bank account #, credit card #, bank routing #
- Medical Data- diagnoses, treatment, medical history
- Full Social Security Number - use of truncated SSN is better but still a risk
- NSPS/Personnel ratings and pay pool information
- Place and date of birth
- Mother’s maiden name
- Passport #
- Numerous low risk PII elements aggregated and linked to a name

Business related PII, all releasable under FOIA or authorized use under DON policy and considered “low risk”

- Badge number
- Job title
- Pay grade
- Office phone number
- Office address
- Office email address
- Lineal numbers
- Full name

*Cautionary note: Growing problem with email phishing



BUPERS RESPONSE TO PII BREACHES

Presentation by:
David German, BUPERS Privacy Officer





DoD Social Security Number Reduction Plan

Summary of DoD SSN Reduction Plan

- Background
- Acceptable Uses of SSNs
- SSN Reduction for Forms
- SSN Reduction for Systems
- Data included in annual FISMA Report
- IG Review

Broader DON approach includes “high risk PII”

- DON SSN Reduction Plan message forthcoming



Did you know?

DoD will begin to remove SSNs from DoD ID cards

Removal will Occur in Three Phases

Changes to cards will be made upon ID card renewal.

Phase One: Remove Dependent SSNs
To begin by end of calendar year 2008

Phase Two: Remove all printed SSNs*
To begin by end of calendar year 2009

Phase Three: Remove SSNs embedded in barcodes
To begin during calendar year 2012



To ensure the safety of Service members and their families' Identity Information

In response to an increasing awareness of the growing need to protect the safety of Service members and their families' identity information, DoD will begin to remove Social Security Numbers (SSNs) from DoD ID cards.

**Geneva Conventions ID cards will retain the last four digits of the SSN.*

SSN Removal

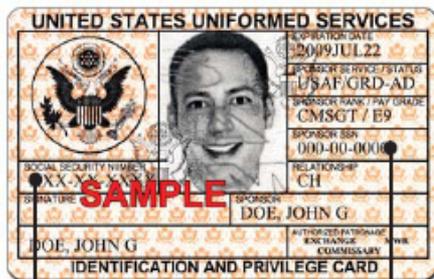
SSN Removal

PHASE I

Remove Dependent SSN

TESLIN CARD FAMILY

(Dependent ID Card)



DD Form 1173

Dependent SSN will be replaced with XXX-XX-XXXX

Sponsor SSN will remain visible



DD Form 1173-1

PHASE II

Remove All Printed SSNs

TESLIN CARD FAMILY

(All ID Cards)

Sponsor SSN will be replaced with XXX-XX-XXXX



Cardholder SSN will be replaced with XXX-XX-XXXX



GENEVA CONVENTIONS CARD FAMILY



SSN will be truncated to only show the last four digits of the cardholder's SSN

PHASE III

Remove SSNs Embedded in Barcodes

TESLIN CARD FAMILY

(All ID Cards)



SSN will be removed from barcodes

CAC CARD FAMILY

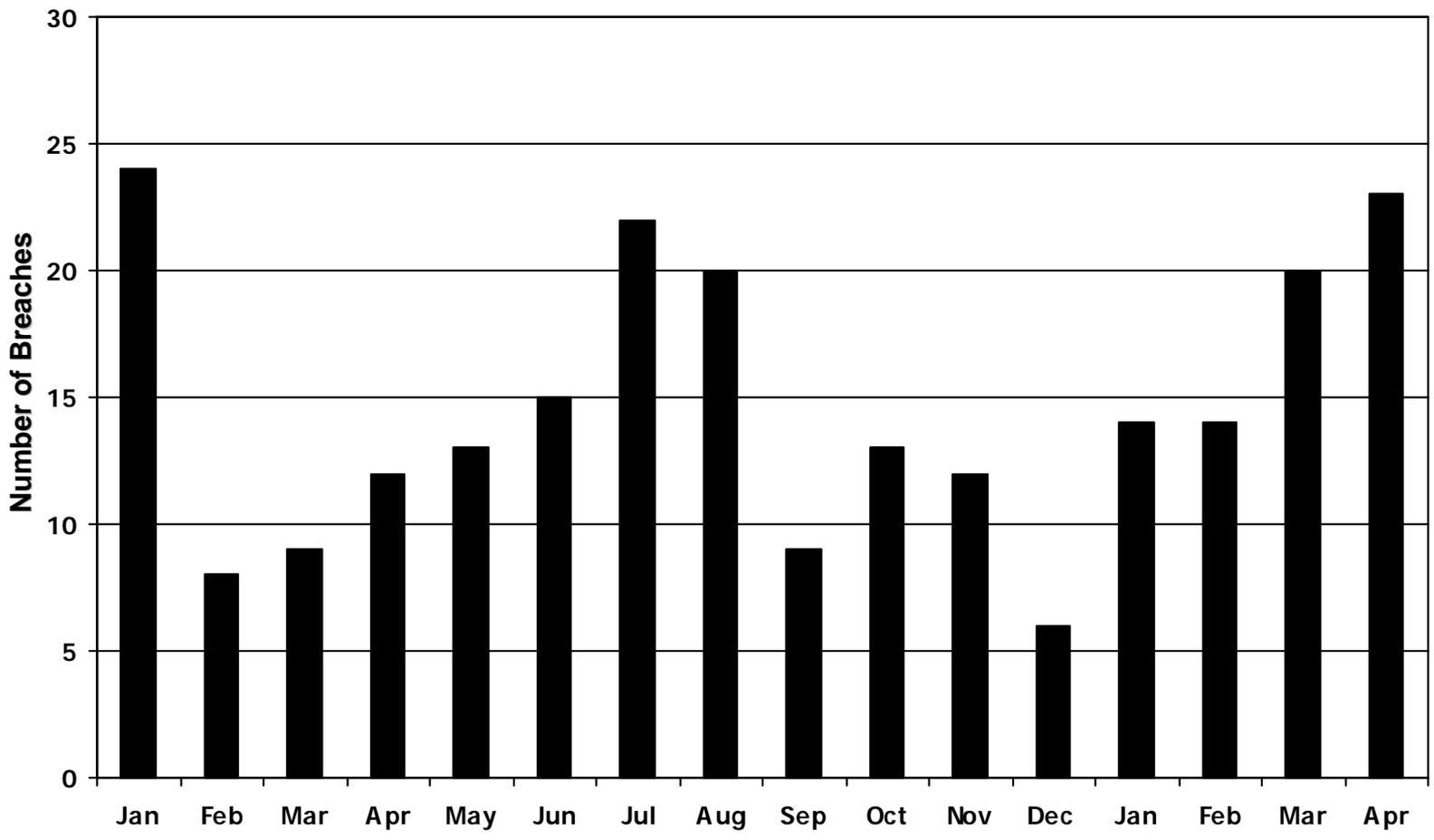


SSN will be removed from barcodes



DON PII High Risk Breach Statistics

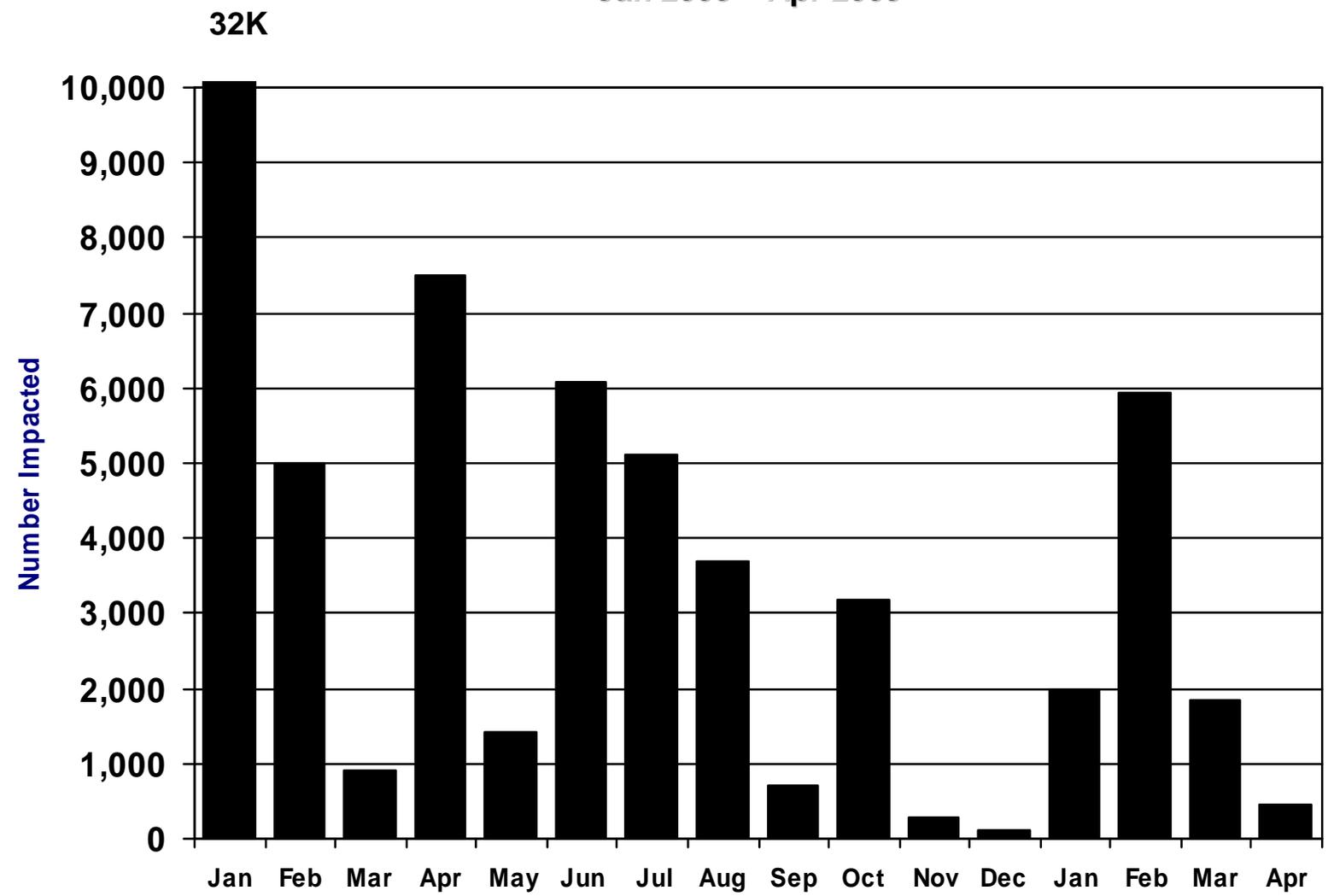
Jan 2008 – Apr 2009





DON PII High Risk Breach Statistics

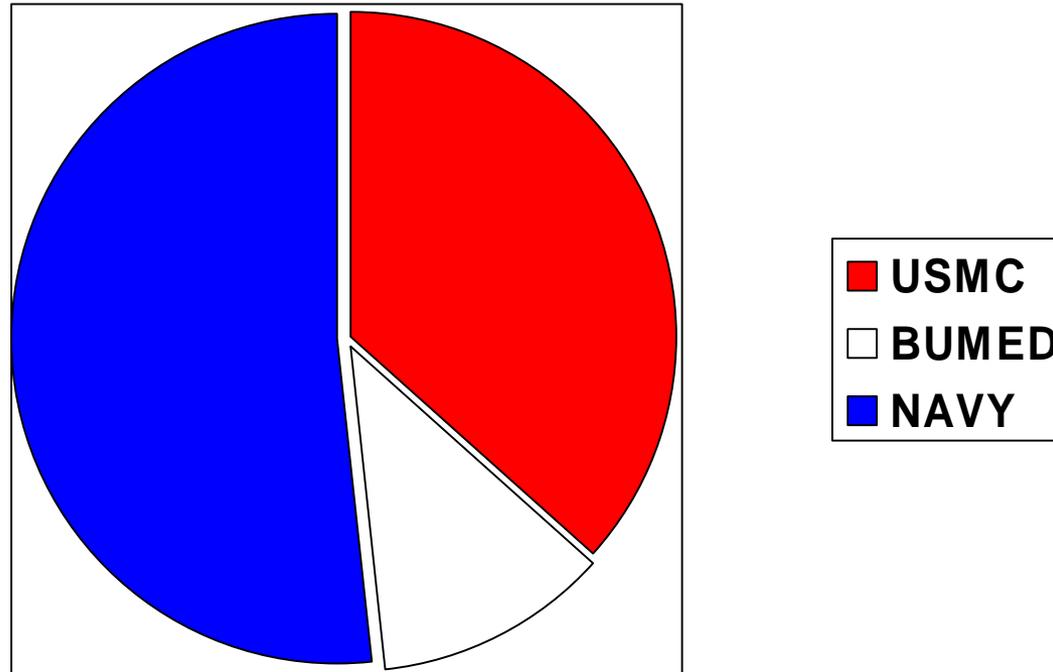
Jan 2008 – Apr 2009





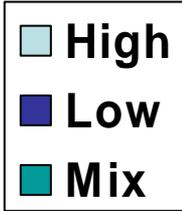
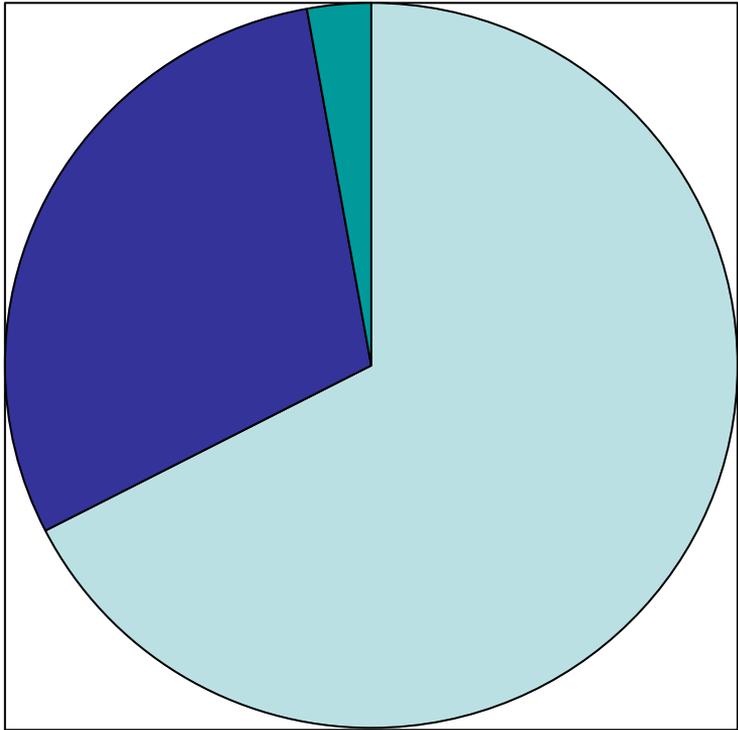
DON Breaches By Activity

May 08 – Jan 09





Level Of RISK

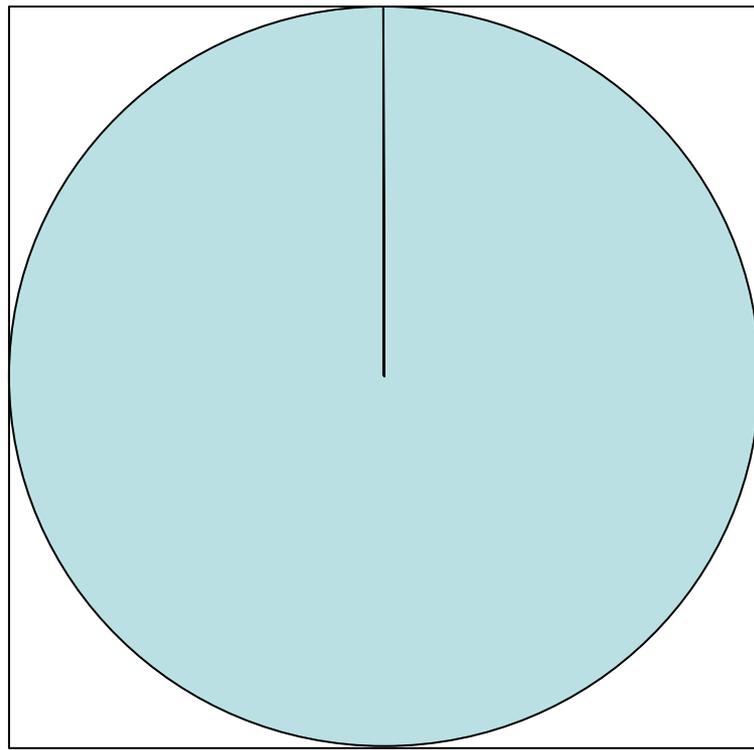


60 % of high risk breaches become low risk when Data at Rest solution is fully implemented.



Who Controls The PII Data?

May 08 – Jan 09

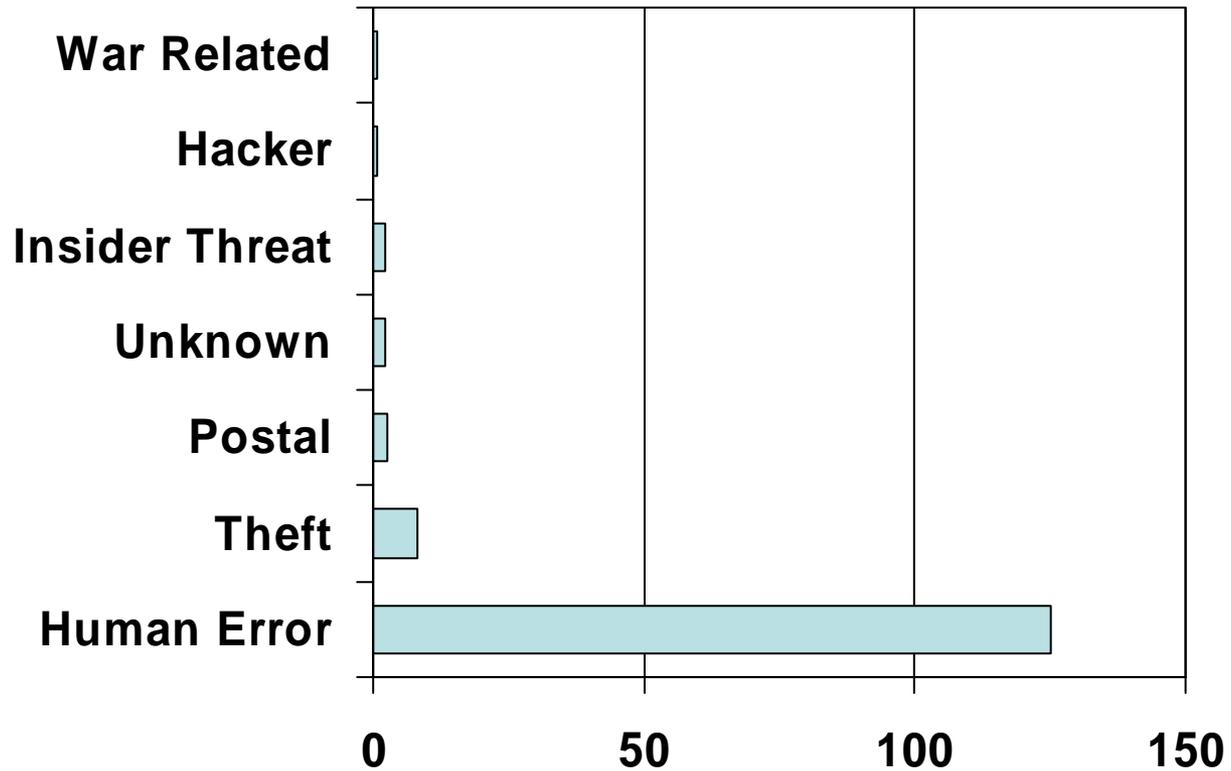


- Government Controlled
- Contractor Controlled



DON "High Risk" Breach Causes

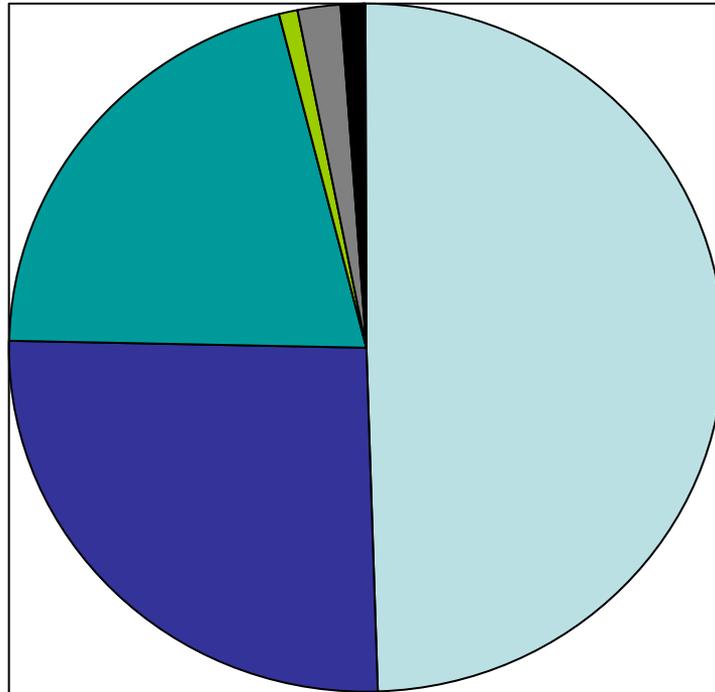
May 08 – Jan 09





Personnel Affected By Breach

May 08 – Jan 09

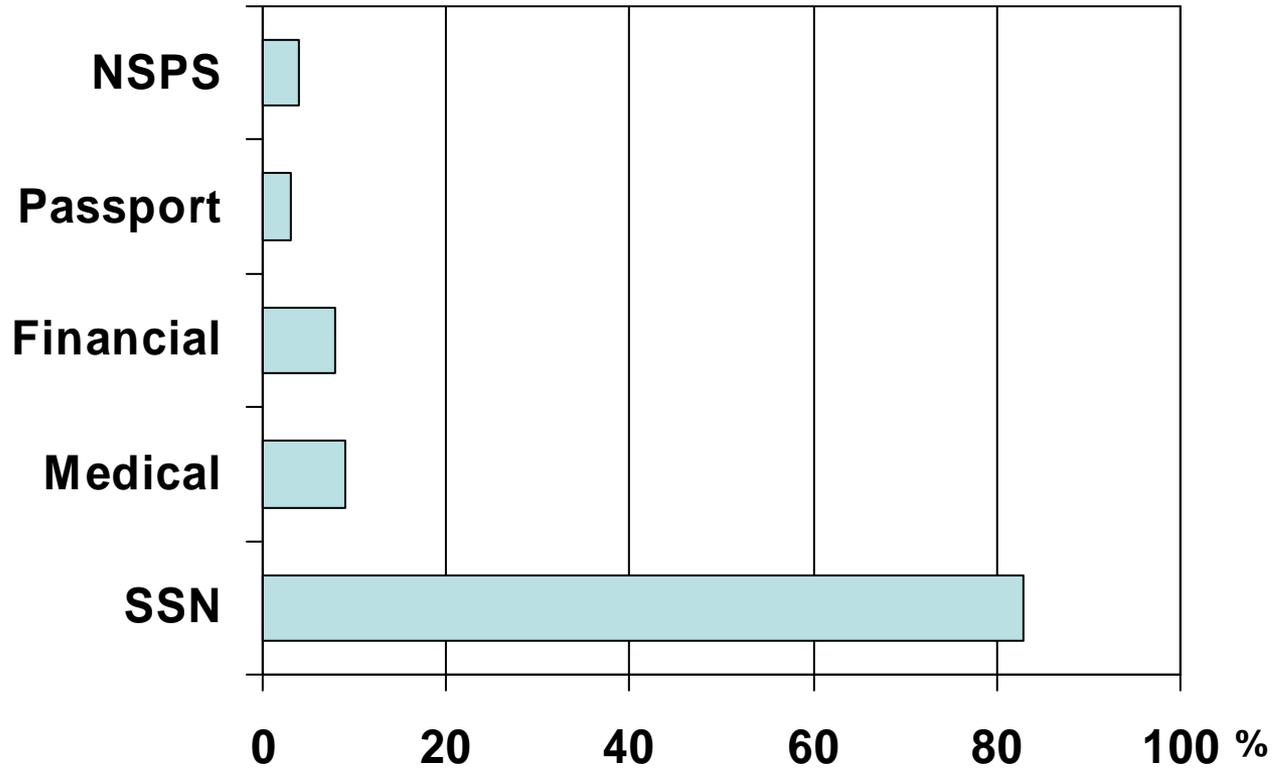


- Military
- Government Civilian
- Civilian (public/dependent)
- Military Retiree
- Contractor
- NAF



Type Of PII Lost, Stolen or Compromised

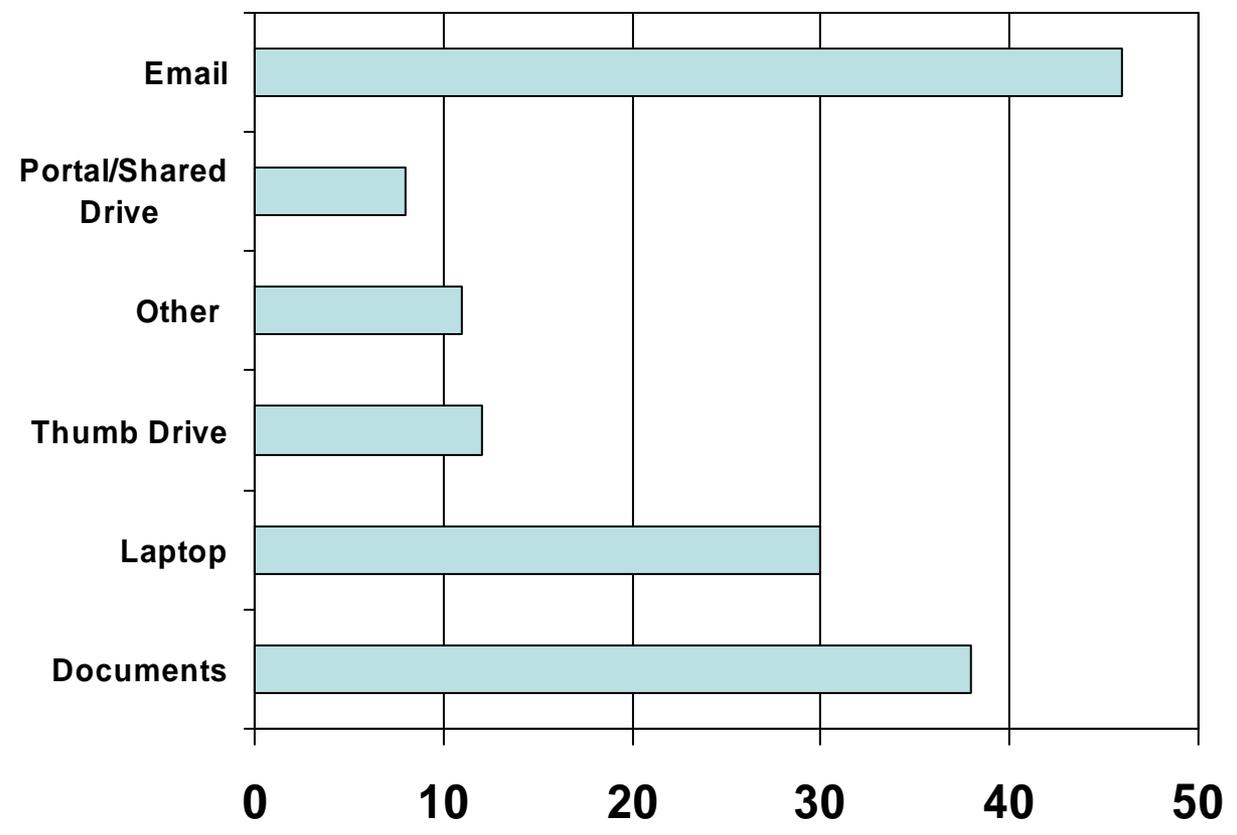
May 08 – Jan 09





Type Media For DON Breaches

May 08 – Jan 09





DON CIO Web Site and Important Privacy Links

- DON privacy topics, products & resources: doncio.navy.mil
- DON Privacy Act and SORNs: privacy.navy.mil
- DoD SSN reduction initiative: dmdc.osd.mil/smartcard
- DoD PIA and privacy guidance: defenselink.mil/privacy
- Cell phone data eraser website: recellular.com
- Computer security: onguardonline.gov
- Cyber security awareness: staysafeonline.org
- Spyware removal: unwantedlinks.com
- Report ID theft and info: ftc.gov/idtheft
- Credit report request: annualcreditreport.com
- Virus and malicious code protection:
itfgno.mil/antivirus/home_use.htm#3 (.mil address only)



Back Up Material



Identity Theft Trends and INFO

- FTC reports 8M+ of U.S. adult population has experienced ID theft in '07, expect to see that grow; cost passed to businesses & consumer
- In '05 1.8M cases new account fraud; 6.5M cases existing account fraud
- Crimes are still **more often offline than online** but thieves becoming more organized and sophisticated
- Risk is greatest when information was stolen by someone targeting the data e.g. hacker, burglar. Insider threat is growing
- 1/2 of known ID thieves were known by victim**; 1/4 were dishonest employees
- Social Security numbers are "the most valuable commodity for an identity thief."** Can obtain from public records or buy on internet.-
- Phishing attacks aimed at ID theft affect all of us
 - Banks, Pay Pal, bogus job offers
- Health ID theft/insurance fraud, a significant and growing concern
- ID theft for children and people who are deceased, a growing trend
- FYI, by law, consumer credit card liability is \$ 50.00; Debit card is \$50.00 if reported within 48 hrs; \$500.00 if reported w/in 60 days; after 60 days may lose all \$'s in account plus overdraft amount!



What Are the Fixes To Reduce ID Theft?

The beneficial uses of SSNs and high risk PII must be weighed carefully against the harms from would-be ID thieves; needs a comprehensive, multi faceted approach.

Reduce the supply of SSNs and “high risk” PII available to thieves

- Remove SSNs from all public records
- Remove the SSN from DoD and DON forms, when possible
- Reduce the display, storage and transmission of SSNs and PII
- Improve data security
- Create strict laws that make the sale of SSNs a crime

Reduce the demand for SSNs by minimizing their value to ID thieves.

- Require/encourage adoption of more effective authentication procedures by financial institutions
- Aggressively prosecute ID thieves



PII Breach Consequences

Responsible command bears cost

- Locating the affected/finding addresses
- Mailing and postage
- Credit protection monitoring ?
- Toll free hotline
- Sanitizing servers

Bad press

Loss of confidence and trust by public and DON personnel in the safeguarding of privacy information

Contractor, Government Civilian & Military consequences for mishandling. See table on DON CIO web site.

Penalties under the Privacy Act



Recent Breaches

- Heartland Payment Systems, which processes payroll and credit card payments for more than 250,000 businesses, announced that consumer credit card data (# unknown) may have been exposed. Law suits filed. Jan 09
- A Sydney man whose Facebook profile was hacked said his Facebook friends were being asked to wire money to the hacker, who led them to believe their friend had been robbed at gunpoint in London and needed money to return home. Jan 09
- An email with 2 un-encrypted attachments was sent to over 700 NSPS employees. The attachments could be manipulated to find underlying performance data. Jan 09
- A man found confidential U.S. military files on an MP3 player he purchased at an Oklahoma thrift shop. The player contained 60 files with the names and personal details of U.S. soldiers, including those who served in Afghanistan and Iraq. Jan 09
- Personal information of job seekers was stolen from Monster.com's database. The company is encouraging users to change their passwords after thieves stole names, birth dates, e-mail addresses, ethnicities and other personal information. USAJobs.com, which is hosted by Monster.com, was also affected. The company is warning users to watch out for phishing schemes. Jan 09
- Former Navy Yeoman sentenced to 15 years in ID theft of \$2M involving 100 Navy reservists.
- Former IT sub contractor w/NMCI access sentenced to 6 years in federal prison for attempting to sell 17,000 PII records to a foreign government.