VA Data Breach Follow-Up

Adair Martinez, Deputy Assistant Secretary
for Information Protection and Risk Management
Department of Veterans Affairs

Incidents In The News - VA Is Not Alone

"Data breaches probed at New Jersey Blue Cross, Georgetown – Stolen laptop had personal data on 300,000…swiped disk had data on 38,000

- ComputerWorld, Jan. 30, 2008

Incident Response In The Department Of Veterans Affairs

- VA has unique factors that impact the number and severity of security and privacy incidents
- Size of the organization
  - Over 235,000 federal employees
  - Over 100,000 students and contractors
  - Over 1,300 facilities including Medical Centers, Benefits Regional Offices, National Cemeteries, Outpatient Clinics, Vet Centers, Data Centers, and Consolidate Mail Outpatient Pharmacies
- VA's major healthcare IT application – VA's Computerized Patient Record System (CPRS) – award winning electronic medical record system – holds tremendous amounts of medical data

Incident Response

- Where we have been
- Where we are now
- Trends and metrics
- Where we are going
- Tools of the trade
- Lessons learned

Incident Response
Where We Have Been - The Laptop

- May 3, 2006
- VA focused efforts on encrypting all data taken off site and tightening policy to address this
- Laptop and hard drive were found

Incident Response
Where We Have Been - Unisys

- August 3, 2006
- VA's attention drawn to our contractor's level of security controls
- Desktop pc was recovered

Incident Response
Where We Have Been - Birmingham

- January 22, 2007
- Research data security becomes a focus within VA
- Hard drive has not been found

Incident Response
Where We Have Been – PL 109-461

- Veterans Benefits, Healthcare and Information Technology Act of 2006
- VA is the only agency with its own law governing information security and privacy breaches
- It defines how we report to Congress

Title IX: Information Security Matters - Department of Veterans Affairs Information Security Enhancement Act of 2006 - (Sec. 902) Directs the Secretary to establish and maintain a VA-wide information security program (program) to provide for the development and maintenance of cost-effective security controls needed to protect VA information, in any media or format, and VA information systems. Outlines program elements and requirements, including compliance with information security requirements promulgated by the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB). Outlines program responsibilities of the Secretary, the Assistant Secretary for Information and Technology, the Associate Deputy Assistant Secretary for Cyber and Information Security, and other VA officials. Requires the program to: (1) ensure that information security protections are commensurate with the risk and potential harm from unauthorized access, use, disclosure, disruption, modification, or destruction; and (2) include a plan and milestones of actions being taken to correct any security compliance failure or policy violation.

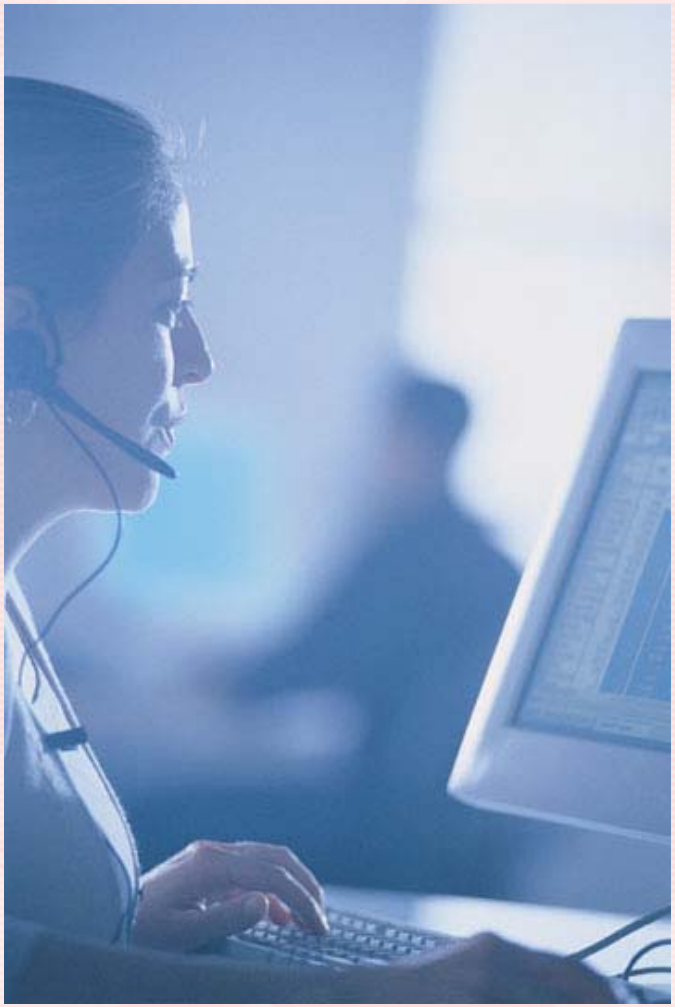
Directs the Secretary to ensure that, in the event of a data breach with respect to sensitive personal information (SPI) maintained by the VA, a non-VA entity or the VA's Office of Inspector General conducts an independent risk analysis of potential misuse of SPI involved in the breach. Requires the Secretary, if a potential misuse is determined, to provide to affected individuals credit protection services, fraud alerts, and credit monitoring through credit reporting agencies. Requires a report from the Secretary to the veterans' committees after each SPI data breach.

Provides confidentiality requirements for VA contractors who perform any function that requires access to SPI.

Requires: (1) quarterly reports from the Secretary to the veterans' committees on any SPI data breaches; and (2) immediate notification of such committees in the event of a significant SPI data breach.

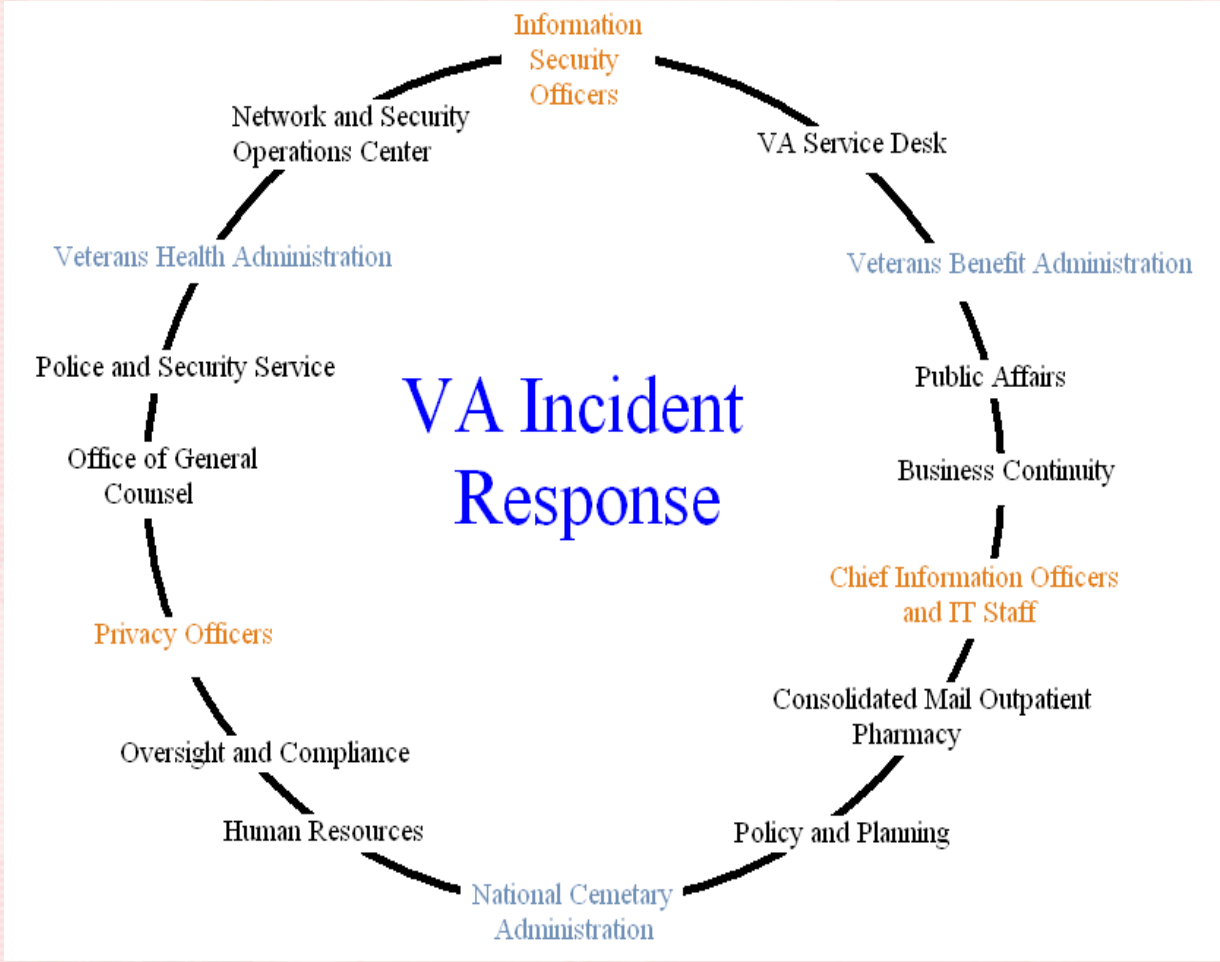
Incident Response
Where We Are Now – Reporting Incidents

- Trained ISO's and PO's in the field are the first responders
- All security incidents are reported up through the VA-NSOC
- VA-NSOC and the Incident Resolution Team work together to investigate and bring closure to incidents



Incident Response – Where We Are Now

- Incident Resolution Core Team (IRCT)
- Incident Resolution Team (IRT)

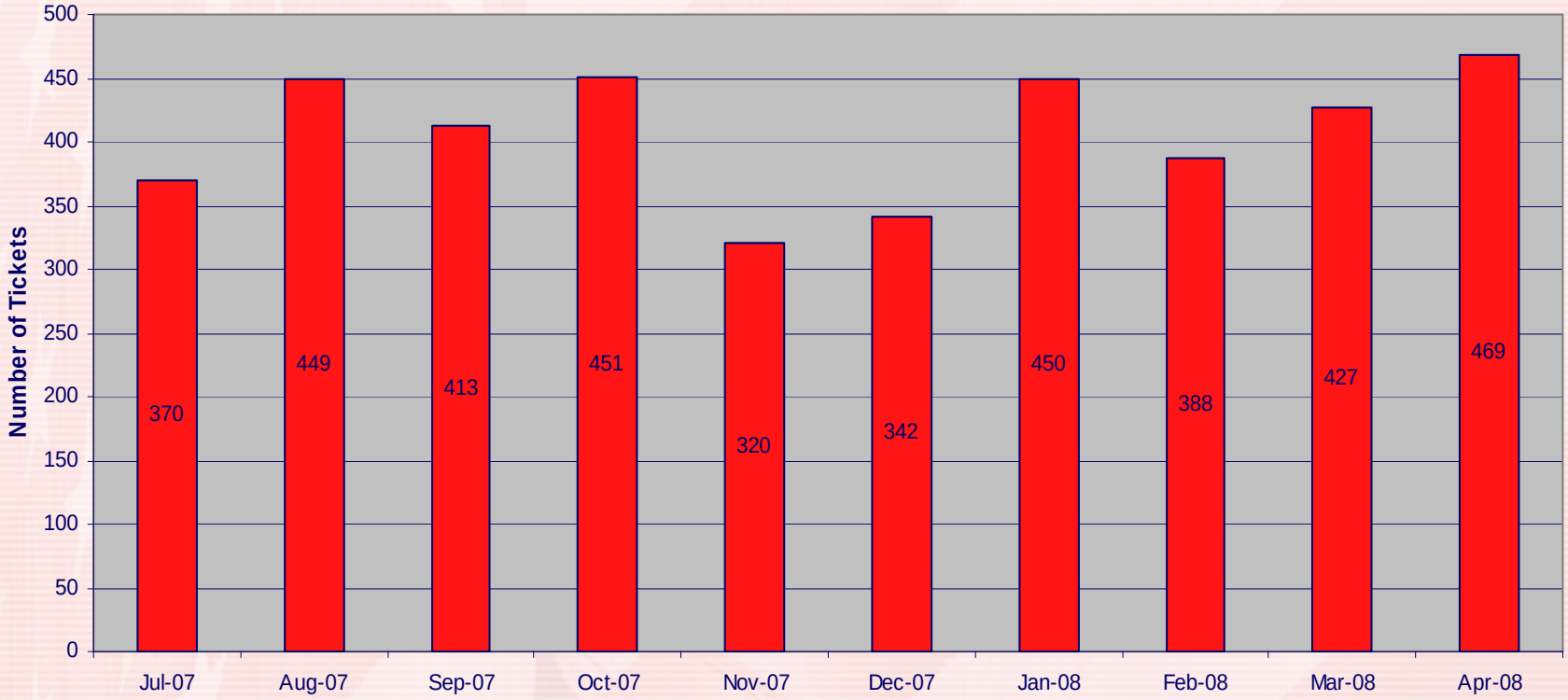


Incident Response
Where We Are Now

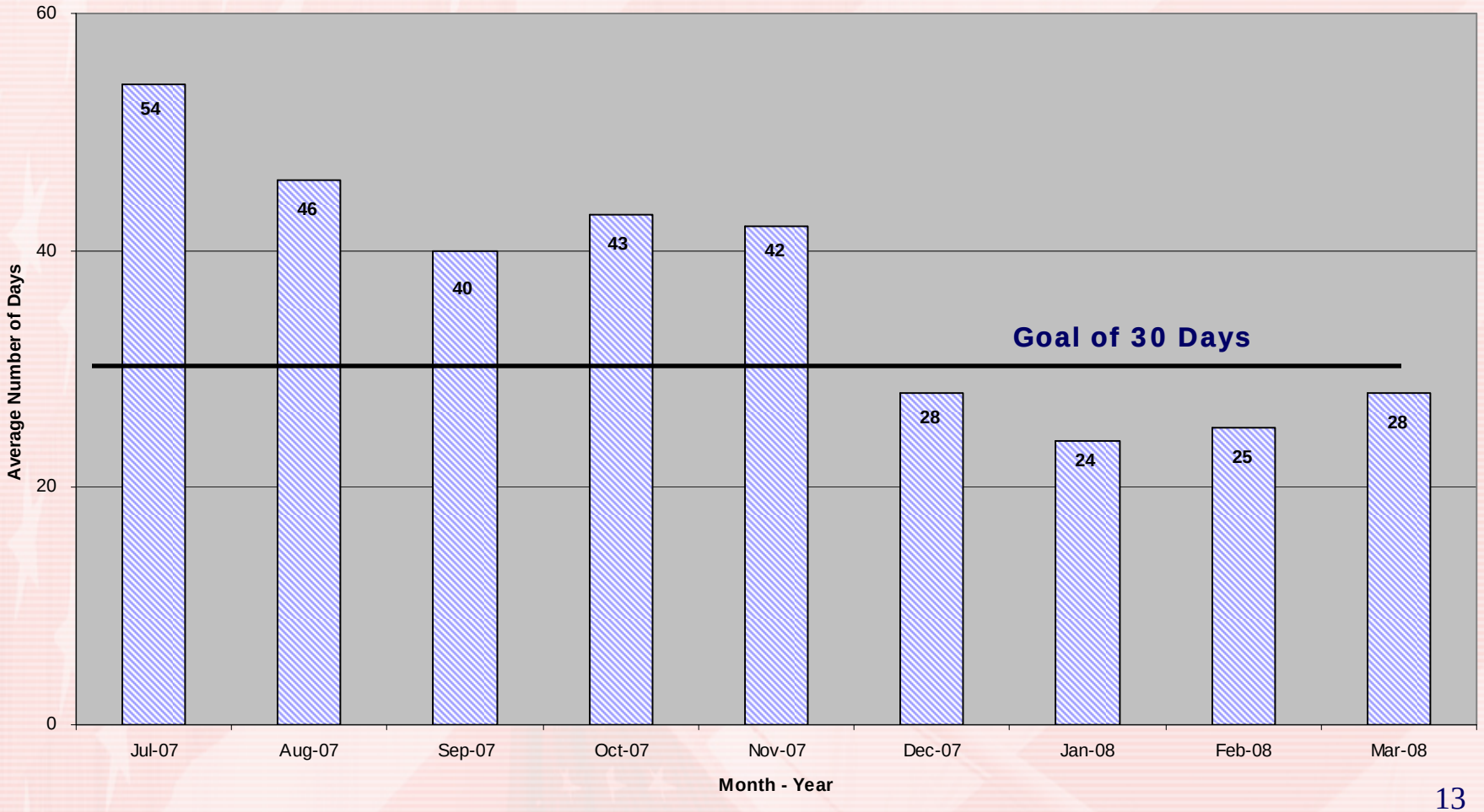
- OI&T Information Protection

  Daily Brief
- Weekly Summary of Major Incidents
- Quarterly Reports to Congress

VA Information Security Incidents



Average Number of Days from a Data Breach to Mailing of Notification Letters - As of 05/29/08



Education – The Key To Culture Change In The Information Protection Community

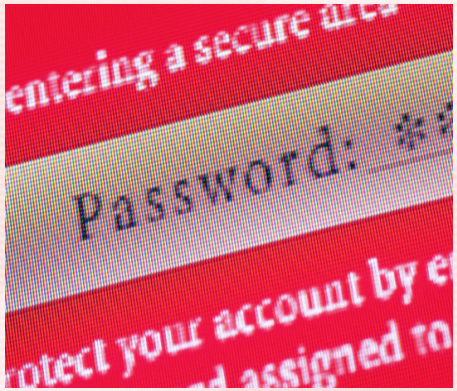
- Role-based training
- InfoSec conference
- ISO Intern program
- CISSP certification program
- Annual Cyber Security Awareness training
- Instructor led and computer based training
- The VA Cyber Security Practitioner program

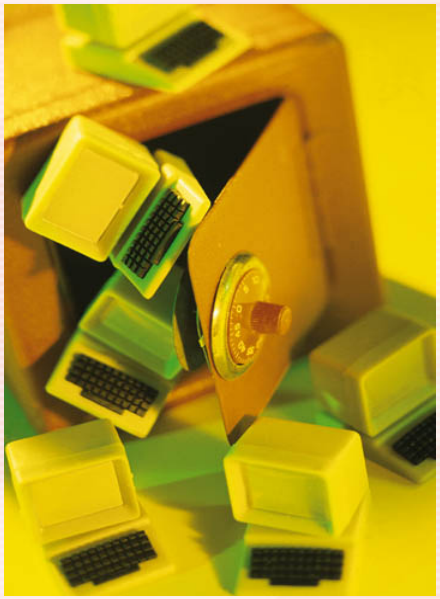
Incident Response
Where We Are Going

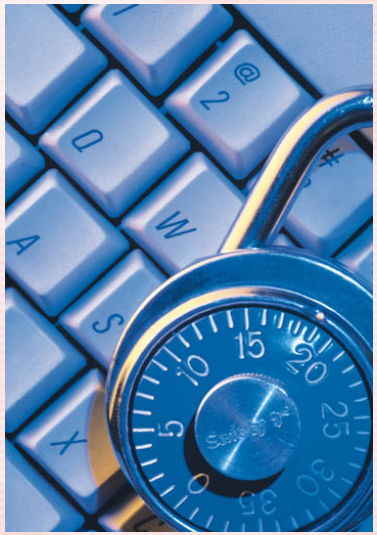
- Handbook 6500.2 – Management of Security and Privacy Incidents
  - Addresses roles and responsibilities of the NSOC, IRCT, ISOs, POs and CIOs in the incident response process
  - Implements the policies regarding Incident Response set forth in Directive and Handbook 6500
  - Is in accordance with NIST Special Publication 800-61

Handbook 6500.2 – Covering The Four Phases Of An Incident

1. Preparation
2. Detection, Reporting, and Analysis
3. Containment, Eradication and Recovery
4. Post–Incident Activity







Handbook 6500.2 – The Primary Goals Of Managing Data Breaches

- Providing prompt and accurate notification and remediation to those whose PII or PHI have been compromised
- Ensuring continued public trust in VA as the guardian of PII and PHI

Handbook 6500.2 – Establishing Processes For Managing Data Breach Incidents

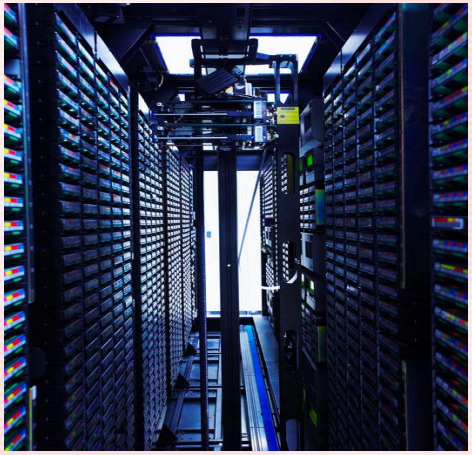
- Assessing risk
- Establishing a central management focal point
- Implementing appropriate policies and procedures
- Promoting awareness
- Monitoring and evaluating policy and control effectiveness

Handbook 6500.2
Appendix G: Letter Templates

- HIPAA Notification Letter
- Next-of-Kin Notification Letter
- General Notification Letter
- Credit Protection Letter
- All Clear Notification Letter

Incident Response
Where We Are Going

- VIRTS – VA Incident Response Tracking System
- Continually improving the incident resolution process
- Continually improving the incident risk assessment tool



The Tools Of The Trade

- Credit Protection Services
- Data Breach Analysis
- Independent Risk Analysis

Incident Response – Lessons Learned

- It will happen to you
- Be prepared
- Have contracts in place
- Promote a culture of awareness and reporting
- Education of all staff is key
- An ounce of prevention is worth a pound of cure

Questions