

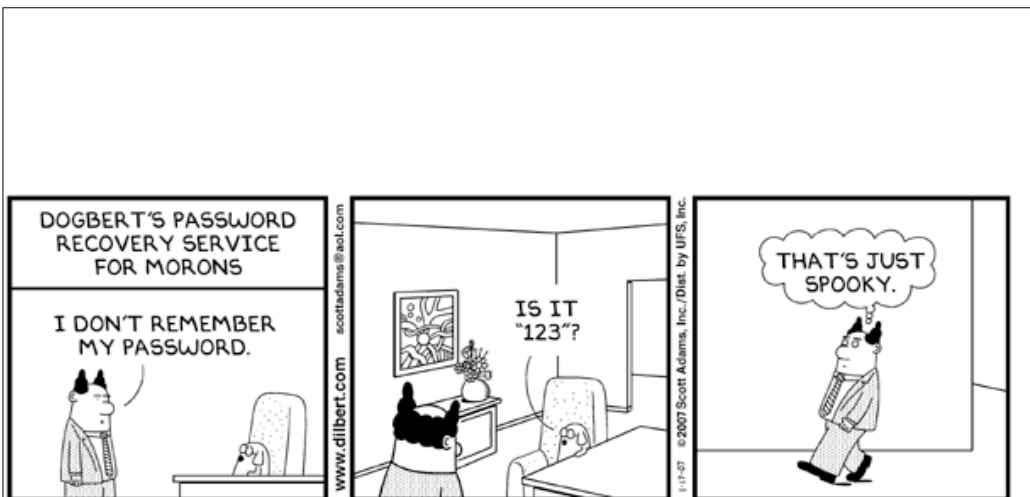
# CSO Conference – New Orleans 2007

## Modernization Security Initiatives

Matthew McCormack, CISSP

Acting Director

MITS IT Security Engineering

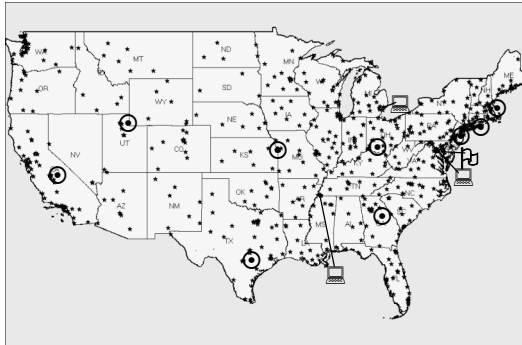


© Scott Adams, Inc./Dist. by UFS, Inc.



► **IRS Deals With The Same Issues As Any Fortune 500 Company**

- Implementation Of An Effective Security Program Is Challenged By The Complex And Geographically Dispersed Infrastructure
- Partnering With Trusted Third Parties Will Expand This Challenge Even More



► **Dispersed Infrastructure**

- 3 Geographical Areas
- 13 Territories
- 3 Computer Centers
- 9 Computer Campuses
- 450+ Field Offices
- Over 300 IT Applications
- 80,000+ Workstations (Increasing During Key Periods)
- 100,000+ FTEs

IRS National Foot Print

▣ Headquarters

⊙ Campuses

▣ Computing Centers

★ Field Office



## Considerations Which Drive Our Security Effort

► **IRS Is A Service Agency**

- Our Performance And Our Approaches Must Demonstrate This
- Taxpayer Perception Is Tremendously Important

► **Our Program Must Satisfy Legal Standards And Guidelines**

- Life Cycle Security Engineering
- Certification And Accreditation Program
- Security Controls Refinement
- Government Regulations & Guidance

► **Third Parties Are Now Part Of The Agency Model Of Trust**

- The Business Relationship We Share Is Now Part Of The Agency Identity
- Lines Are Blurring In The Cyber World

► **A Single Failure Equals A Massive Loss Of Confidence**

- Will Manifest In A Swift Undoing Of Credibility
- Failure Will Impact **Both Sides** Of Our Relationship



## Awareness of Continuous External Threats

### ▶ Hackers And Criminals Are Elevating Their Efforts And Increasing Their Sophistication Due To Tougher Security Practices

- Phishing For Identity Information
- Networks Are Far More Complex Than Previously / Harder To Secure
- Bogus Web Pages From Redirected Sessions
- Spyware

### ▶ System Patching

- Stay Current With Known Threats
- Intelligent Scanning Can ID Transmissions That Look To Be Exploiting Vulnerabilities

### ▶ Secure Transmissions

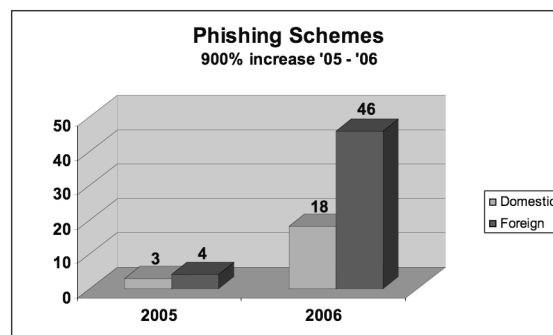
- Encryption
- VPN
- Hashing



### ▶ 900% Increase From 2005 – 2006

### ▶ 70% Hosted In Foreign Nations

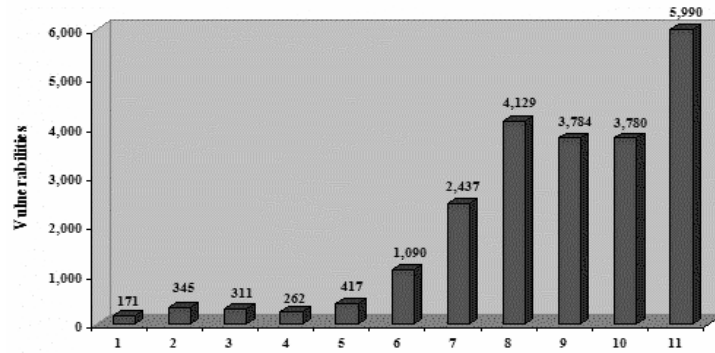
## IT Security Reality: Phishing Metrics



## IT Security Reality: Vulnerabilities

- ▶ Paradigm Shift Yields An Increased Focus On Client-side And Web-based Application Attacks Vs. Server-side
- ▶ Attackers No Longer Need To Penetrate Enterprise Security
  - Entice End-users To Come And Get The Hack

New CERT Security Vulnerabilities Reported by Year



## Modernization Security Initiatives

- ▶ XML Threat Mitigation
- ▶ Two Factor Authentication
- ▶ Full Disk Encryption
- ▶ Enterprise Data Encryption



## Xml Threat Mitigation

### ▶ Use Of XML Documents In Tax Related Matters Is Increasing

- Driven By In Part By Business Suitability
- Standard Messaging Format For All Transactions
- XML Provides For Enhancement Of Operations And Services

### ▶ Presence Of XML Raises Security Concerns

- Malicious Code
- SQL Injection
- Malformed Schema

### ▶ Introduced Solutions Shouldn't Damage Existing Security Practice

### ▶ Use Of XML Tied To Growing Business Functionality Needs

- Security Engineering Must Be **Adaptable**



## Xml Threat Mitigation

### ▶ IRS Evaluated Several Commercial XML Gateways

- Speed
- Functionality
- Operating System
- Cost

### ▶ Issues We Faced

- Little Configuration Guidance
- Few Other Agencies Using them
- Lack of Enterprise Metrics



## Xml Threat Mitigation

### ► Deployment

- MeF First To Implement The XML Gateways
- Deemed Highly Successful
- Increased Functions Of The Gateways To Include Virus Scanning And SSL Termination Points
- Last Year Also Deployed On EMS
- IRS Currently Evaluating Deployment To The CCG's



## Enterprise Tape Encryption

- *Per OMB 06-16: Agencies Must Encrypt All Data On Mobile Computers/Devices Which Carry Agency Data Unless The Data Is Determined To Be Non-sensitive, In Writing, By Your Deputy Secretary Or An Individual He/She May Designate In Writing;*
- IRS Ships Over 4000 Tapes A Month To Various 3<sup>rd</sup> Parties
- IRS Tape Storage Libraries Contain Hundreds Of Thousands Of Tapes
- VPN Options Are Not Always Feasible For Very Large File Transfers



## Enterprise Tape Encryption

### IRS Evaluated 3 Methods Of Addressing Our Encryption Mandate

#### ▶ Software-based Solutions

- Generally Less Expensive
- Require Additional Processing Power
- Could Impact Processing Throughput

#### ▶ Tape Drive-based Solutions

- Very Expensive
- Proprietary In Nature Making Data Exchange More Difficult
- Reliable
- No Additional Personnel Costs
- No Processing Throughput Concerns

#### ▶ Appliance-based Solutions

- Moderately Expensive
- Open Tape Drives Allow Easier Data Exchange On Any Platform
- Offers Inexpensive Software Clients For Third Party Exchanges
- Require Additional Support Personnel



## Two Factor Authentication

▶ *Per OMB 06-16: The Service Must Allow Remote Access Only With Two-factor Authentication Where One Of The Factors Is Provided By A Device Separate From The Computer Gaining Access;*

▶ *Additional Mitigation For Man-in-the-middle Attacks And Replay Attacks*

▶ *IRS Evaluated 2 Methods To Accomplish This Task Each With It's Own Challenges*

- *Electronic Token Based*
- *Matrix (Bingo) Card*



## Two Factor Authentication

### ▶ Electronic Token Based Authentication

- Required Significant Infrastructure To Be Built (Time And Money)
- Physical Cost Per Token
- Complexity Of Future Upgrades

### ▶ Matrix (Bingo Cards) Authentication

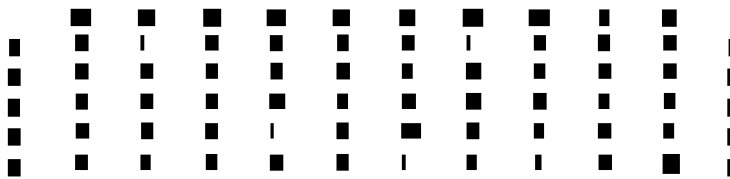
- Fewer Characters Requested For Authentication
- Shoulder Surfing
- Ease Of Destruction (Washing Machine)
- Distribution Challenges

### ▶ Selected Bingo Cards Due To Ease Of Infrastructure Modification And Overall Cost To Provision 30,000 Laptops (Cheaper By Roughly A Factor Of 4)



## Two Factor Authentication

### *Bingo Card Example*



## Two Factor Authentication

### *Bingo Card Authentication Example*



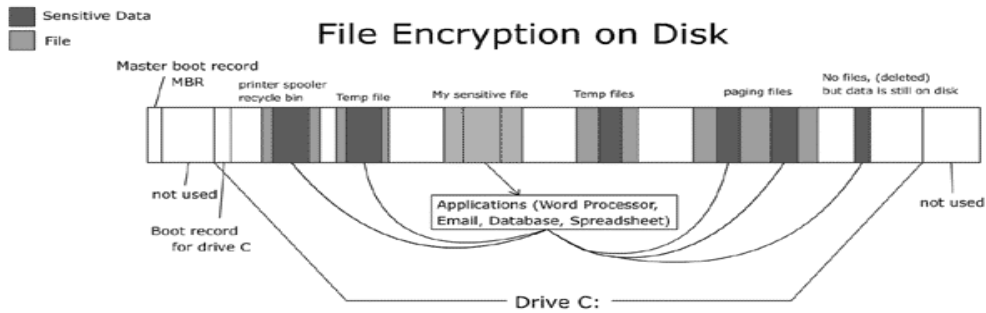
## Full Disk Encryption

- ▶ *Per OMB 06-16: Agencies Must Encrypt All Data On Mobile Computers/Devices Which Carry Agency Data Unless The Data Is Determined To Be Non-sensitive, In Writing, By Your Deputy Secretary Or An Individual He/She May Designate In Writing;*
- ▶ Veteran's Administration.....
- ▶ The U.S. Federal Bureau Of Investigation (FBI) Estimates 50% Of Network Penetration Is Due To Data Derived From Stolen Laptops
- ▶ Meta Group Estimates That Organizations Typically Lose Between 5% And 8% Of Their Laptops Per Year
- ▶ The 2003 CSI/FBI Survey Estimates That The Average Cost Of Data From A Lost Laptop Is \$47,000 – One Company Estimated The Loss Of A Single Laptop Cost A Staggering \$2,000,000.
- ▶ ...And Yet, Recent Global Studies Show That Less Than 20% Of Laptops Have Full-disk Encryption



## Full Disk Encryption

*What Is Encrypted Using Standard OS Encryption Such As EFS.....*

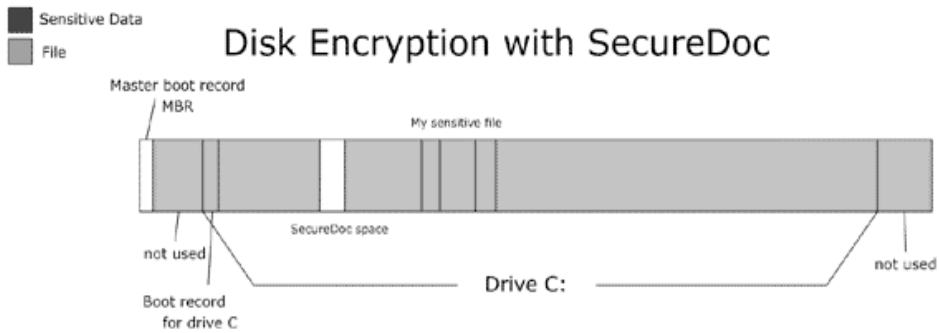


Basic File Encryption Leaves Significant Portions Of The Drive/Data Unencrypted And Therefore Vulnerable.



## Full Disk Encryption

*What Is Encrypted Using Full Disk Encryption.....*



Full Disk Encryption Encrypts The Entire Disk Including The Unused Space Before The Partition C And After It. Encrypting Only The C Drive May Leave Attacker Some Code In These Spaces.



## Full Disk Encryption

- ▶ IRS Successfully Deployed Full Disk Encryption To Over 30,000 Laptops During A Rollout Period Of Roughly 1 Month After Infrastructure Build Out.
- ▶ Any Stolen Laptop Will Be Virtually Useless To The Thief
- ▶ There Is No Unencrypted Sensitive Data On Any IRS Laptops With Full Disk Encryption Deployed



Internal  
Revenue  
Service

## Summary

- ▶ The IRS Is Trying To Stay Ahead Of The Curve With Continuous Security Initiatives
- ▶ There Is No End State To Security
- ▶ As Technology Changes, So Do We.....



Internal  
Revenue  
Service

**Opinions & Comments**

**Matthew McCormack, CISSP**  
**[matthew.l.mccormack@irs.gov](mailto:matthew.l.mccormack@irs.gov)**  
**(202)283-2843**

