Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

May 7, 2014

Virginia Information Technologies Agency

ISOAG May 2014 Agenda

I.	Welcome & Opening Remarks	Mike Watson, VITA
II.	Symantec's Internet Security Threat Report	Brian Pallozzi, Symantec
III.	Spreadsheet Security	Ed Miller, VITA
VI.	Upcoming Events	Mike Watson, VITA
VII.	Partnership Update	Bob Baskette, VITA Michael Clark, NG

INTERNET SECURITY THREAT REPORT ⌖ 2014

Brian Pallozzi, CISSP, CCSK

Symantec Presales Engineer

The World's Largest Global Intelligence Network

7 Billion
File, URL & IP Classification

1 Billion+
Devices Protected

2.5 Trillion
Rows of Security Telemetry

550
Threat Researchers

240 Million+
Contributing Users & Sensors

14
Operations & Response Centers

Symantec

ISTR in Context

- Impossible to be 100% secure 100% of the time
- Funding is never enough
- Balance against acceptable business risk
  - Definition of acceptable
    - Unique to every organization
    - Unique to the asset being protected
    - Unique to the threat level of the target
  - Avoid, transfer, reduce/mitigate/control, accept
  - Value of the asset vs. cost of protection
- Attacks are usually not head on
  - Most-valuable assets attacked through lower value targets
  - Don’t forget the human factor

Agenda

1. 2013: The Year of Mega Breach
2. Targeted Attack Campaigns on the Rise
3. Vulnerabilities Continue to Facilitate Attacks
4. The Evolution of Malware
5. Mobile = Danger
6. Future Trend: Internet of Things

Threat Landscape in 2013

Ransomware

Cyberespionage
Privacy
Malicious Insider

Mobile

Internet of Things

Data Breaches

Mega Breaches

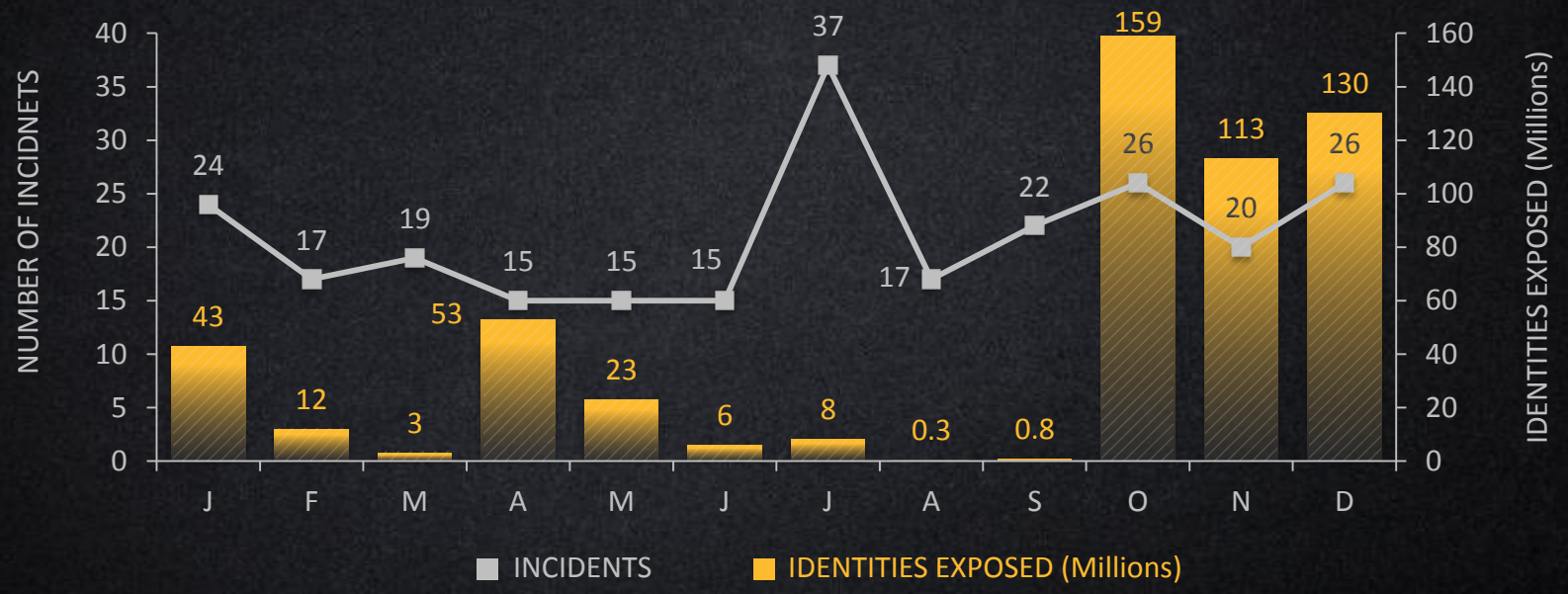
	2011
Breaches	208
Identities Exposed	232M
Breaches >10M	5

2013 was the Year of the **Mega Breach**

Timeline of Mega Breaches

Timeline of Data Breaches, 2013

Source: Symantec



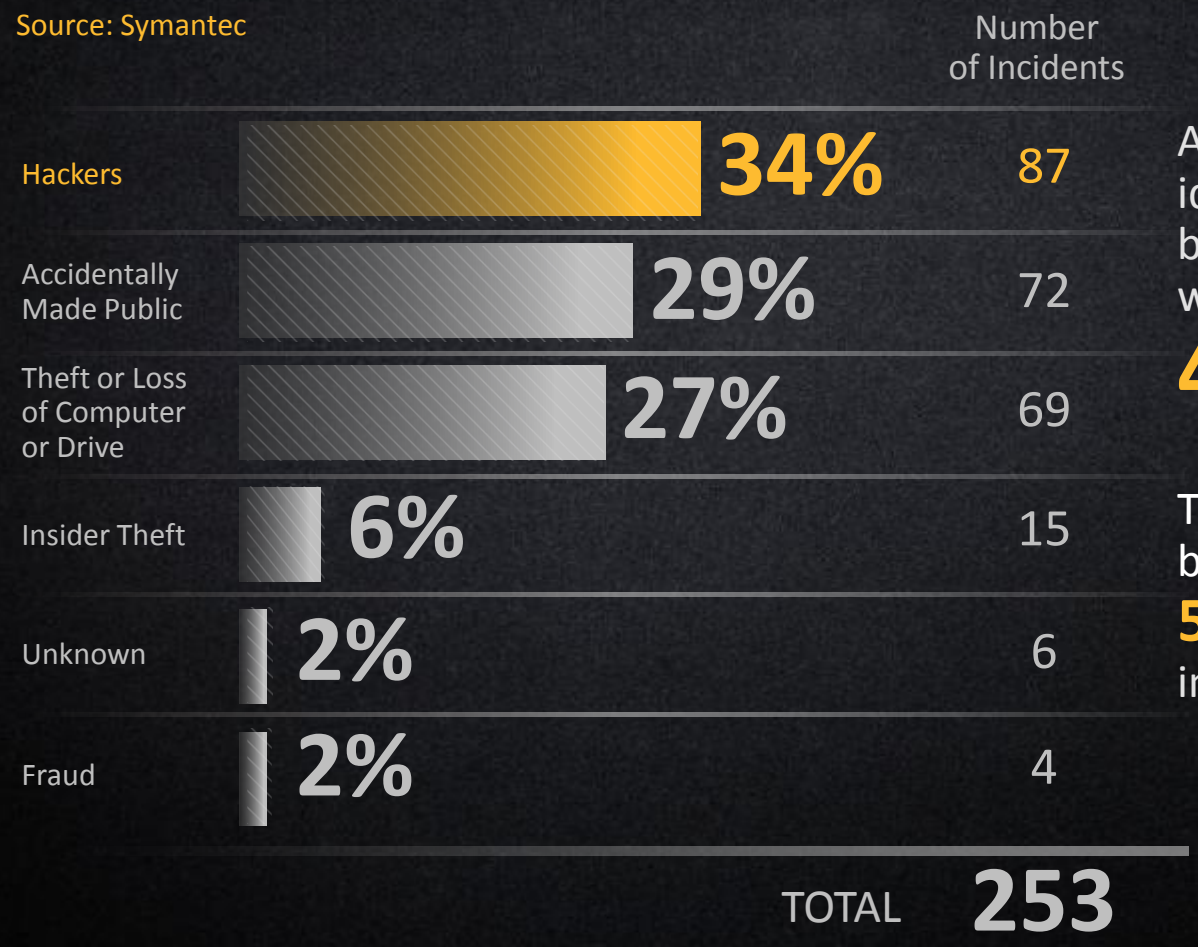
8 of the top 10
breaches were of
more than 10 million identities

Number of identities exposed
were **4 times greater**
than **2012**

Causes of Breaches

Top Causes of Data Breach, 2013

Source: Symantec



Average number of identities exposed per data breach for hacking incidents was approximately

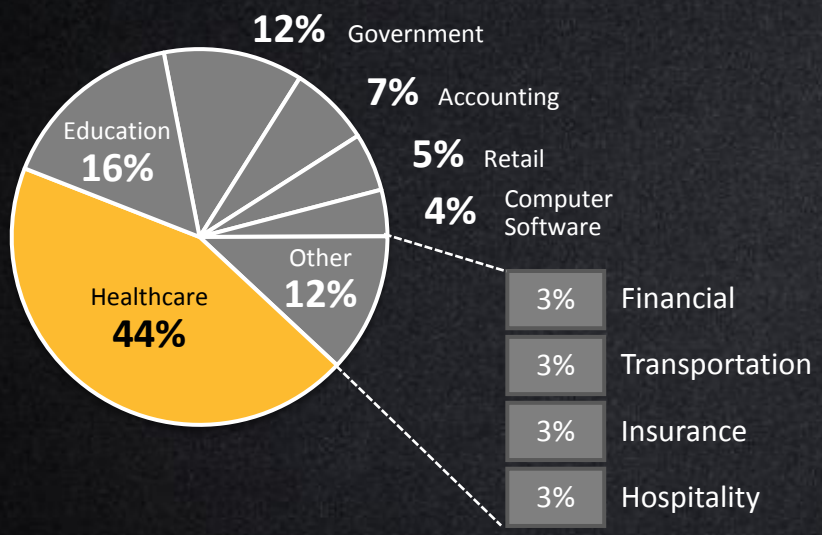
4.7 million

Theft or loss + accidental breaches accounted for **56%** of data breach incidents

Breaches by Sector

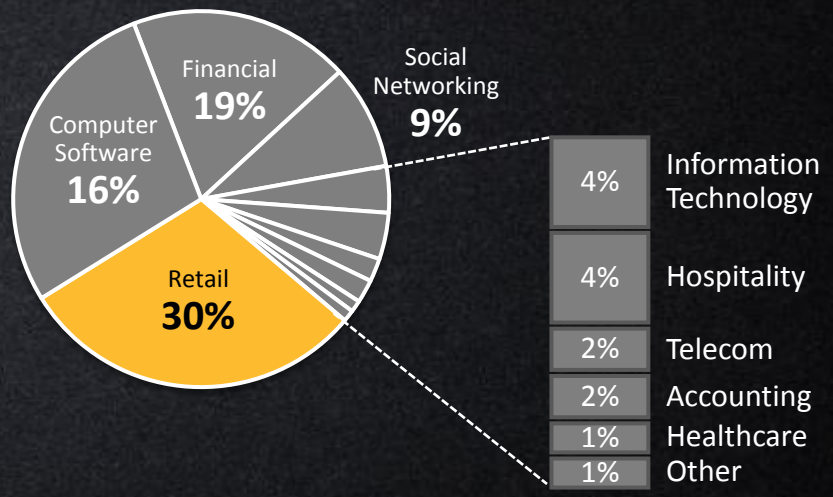
Data Breaches by Sector, 2013

Source: Symantec



Data Breaches by Sector,
Percent of Identities Exposed, 2013

Source: Symantec



Healthcare, education and the public sectors accounted for **58%** of all data breaches

But, **the retail, computer software and financial sectors** accounted for **77%** of all identities exposed in 2013

Breaches: What Was Lost?

01	Real Names
02	Birth Dates
03	Government ID Numbers (Social Security)
04	Home Address
05	Medical Records
06	Phone Numbers
07	Financial Information
08	Email Addresses
09	User Names & Passwords
10	Insurance

Avoiding Data Breaches

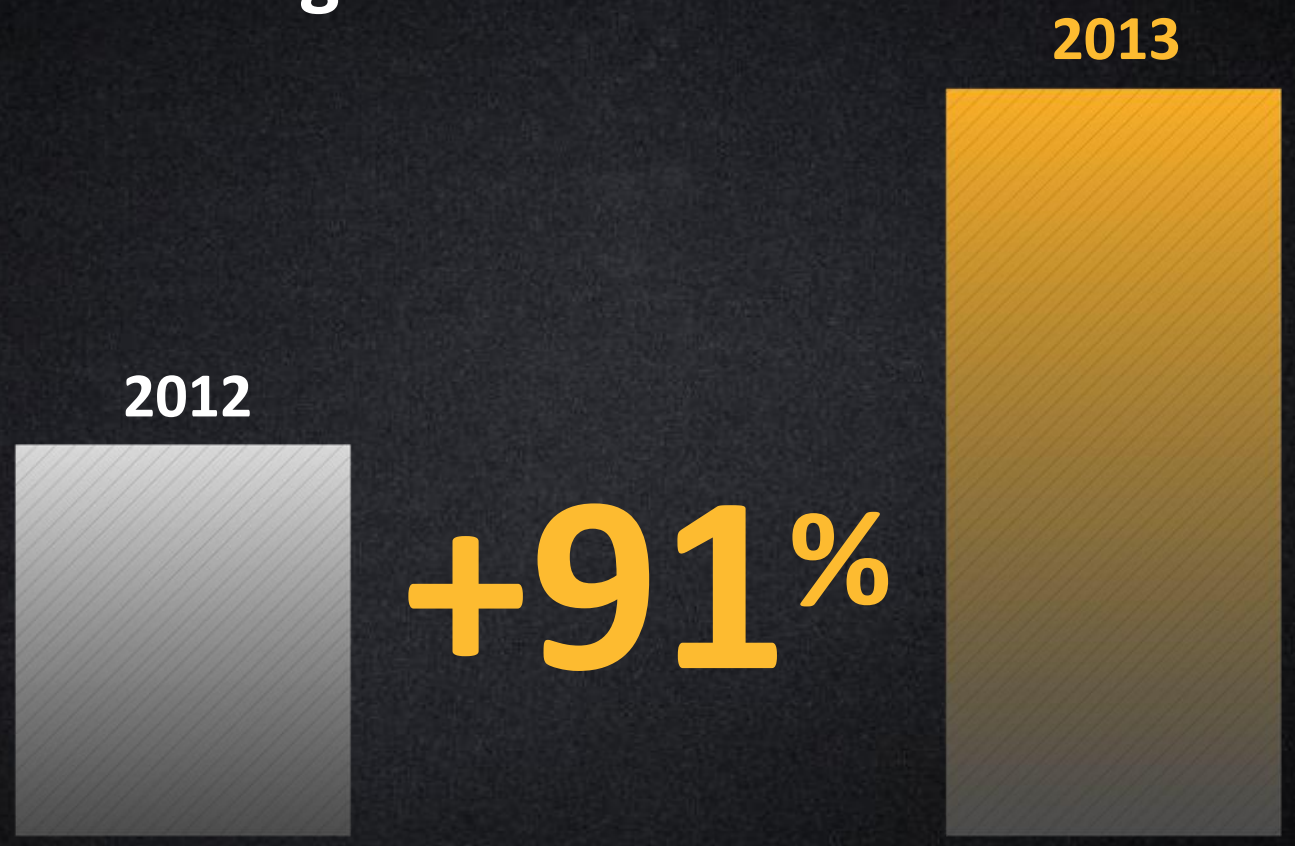
Data Classification	• Determine what sensitive information exists in your organization • Categorize it appropriately and protect it according to its classification level
Data Loss Prevention	• Detect and prevent exfiltration of sensitive information that is targeted by attackers • Enforce rules prohibiting access of confidential data using applications
Host-based Intrusion Detection and Prevention	• Locks down key systems that contain confidential information • Prevents any unauthorized code to run — independent of AV signatures
Email & Web Gateway Security	• Scan & block email with potentially malicious URLs, attachments or content. • Monitor inbound/outbound web traffic and block accordingly
Encryption	• Create and enforce security policy so all confidential information is encrypted
Strong Authentication	• Use two-factor authentication to protect against credential theft

ISTR

INTERNET SECURITY THREAT REPORT ⌖ 2014

Targeted Attacks

Increase in Targeted Attacks

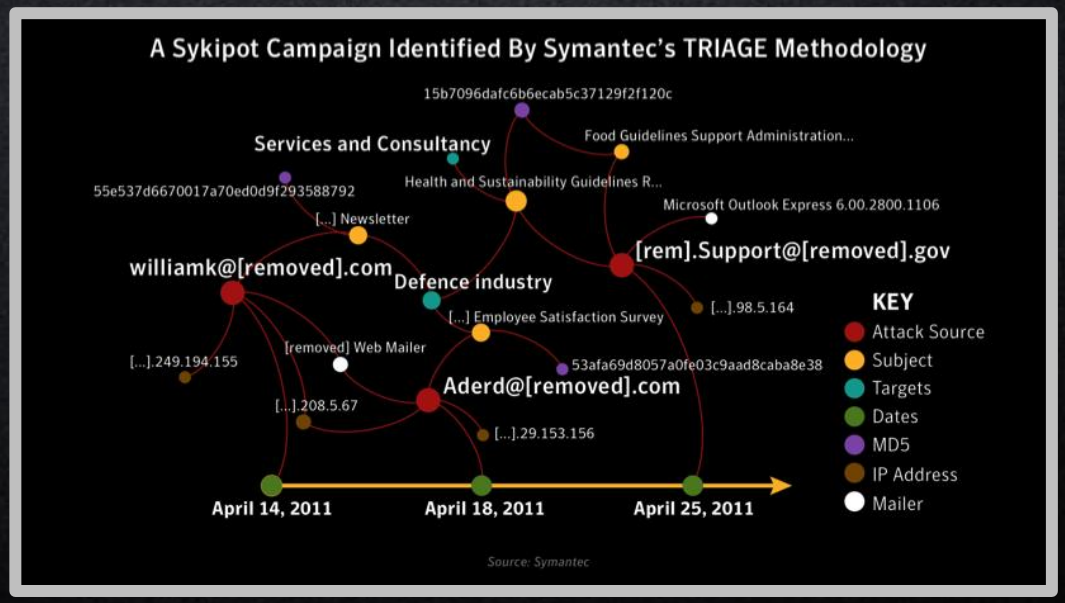


Increase in targeted attack campaigns

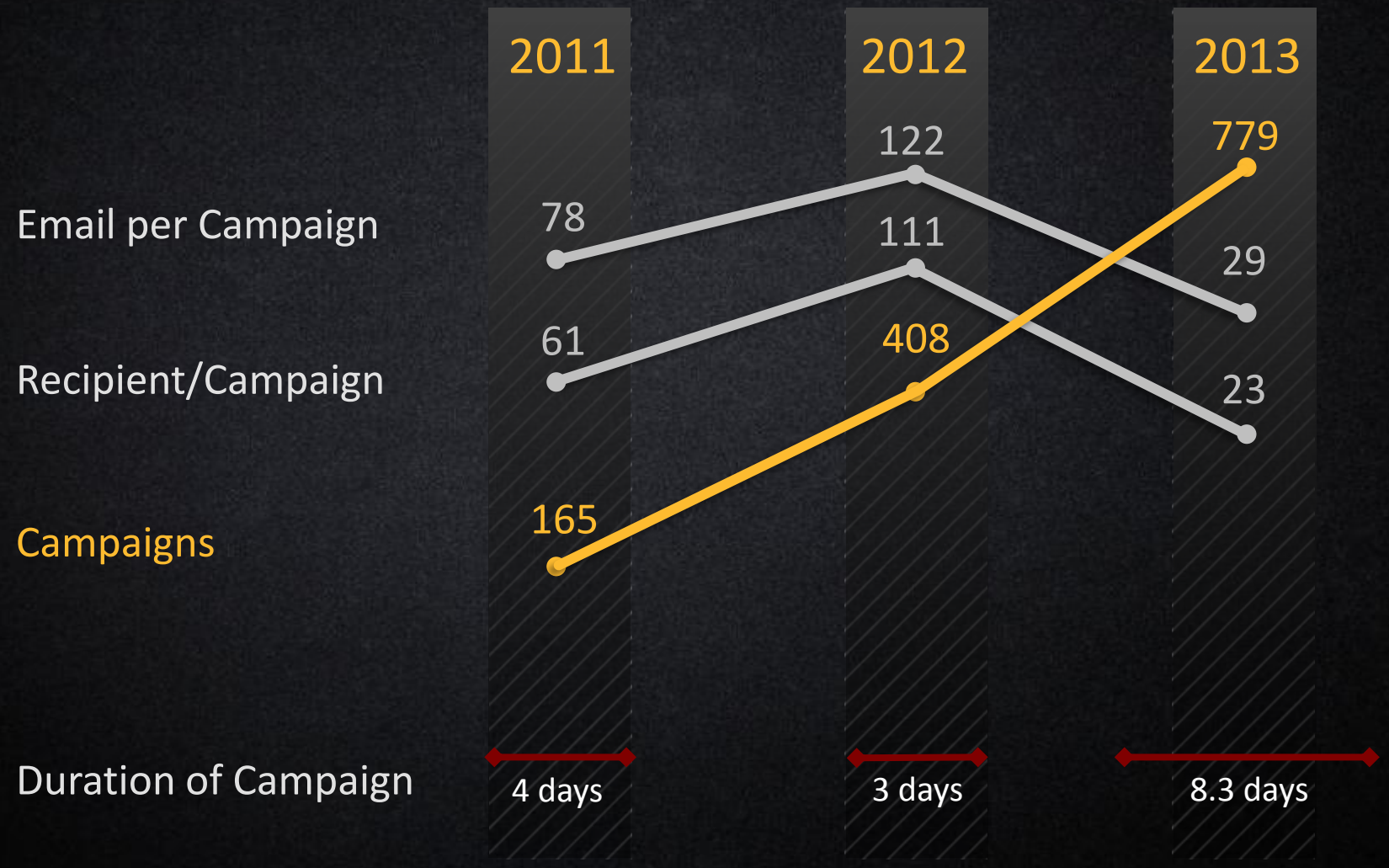
Defining an Attack Campaign

A series of emails that:

- Show clear evidence that subject and target were deliberately selected
- Contain at least 3 or 4 strong correlations to other emails – topic, sender address, source IP address, etc.
- Sent on the same day or across multiple days

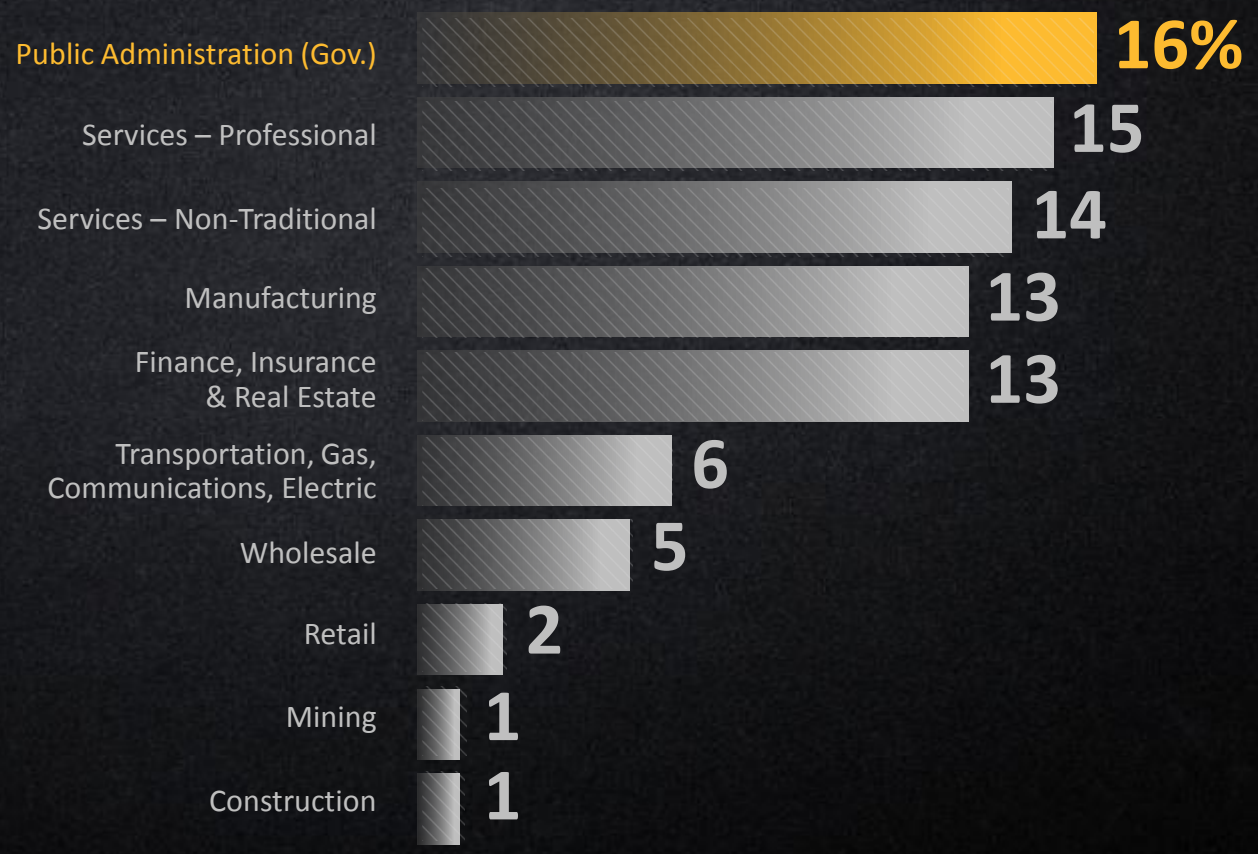


Targeted Attack Campaigns



Targeted Industries

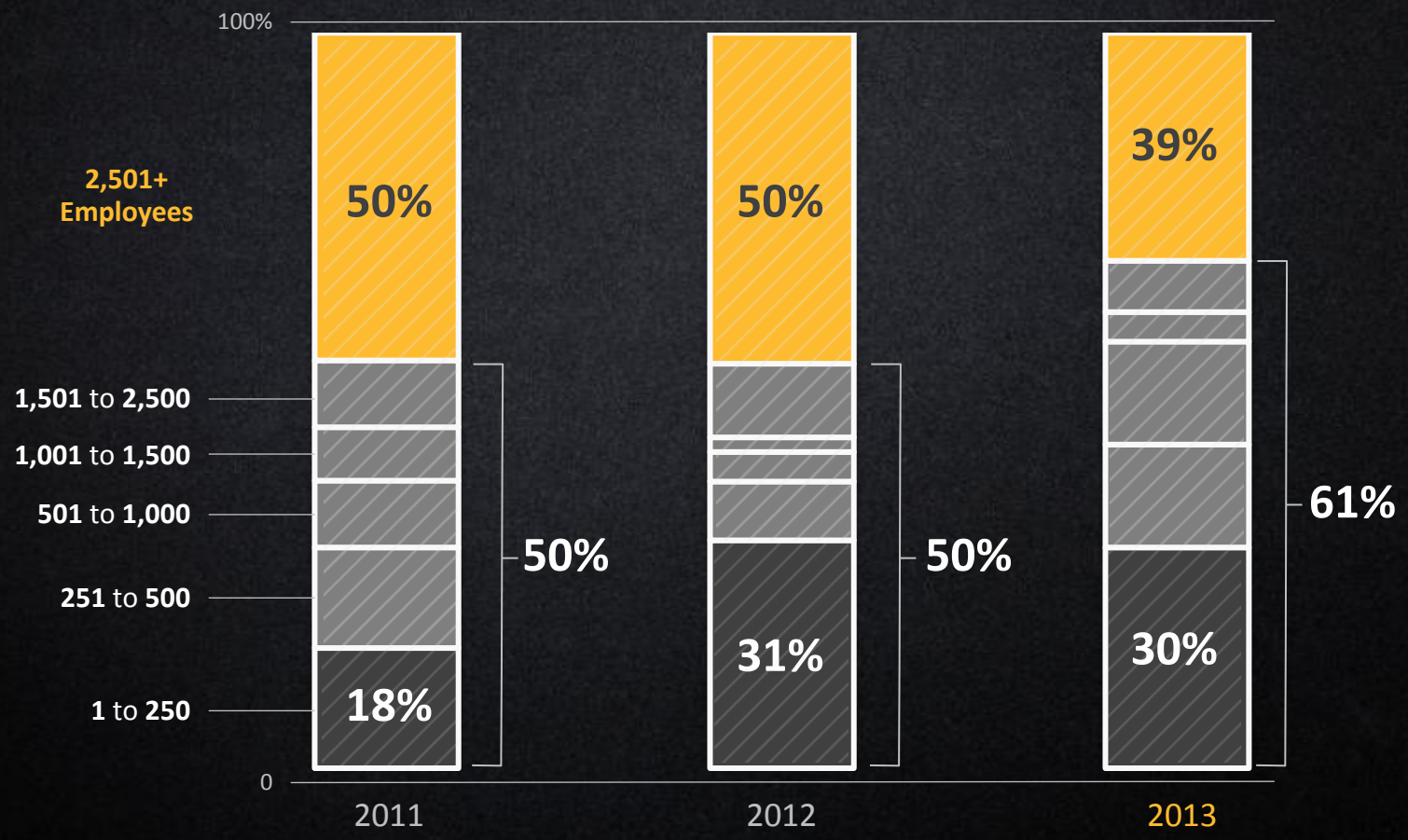
Top 10 Industries Targeted
in Spear-Phishing Attacks, 2013
Source: Symantec



Targeted Organization by Size

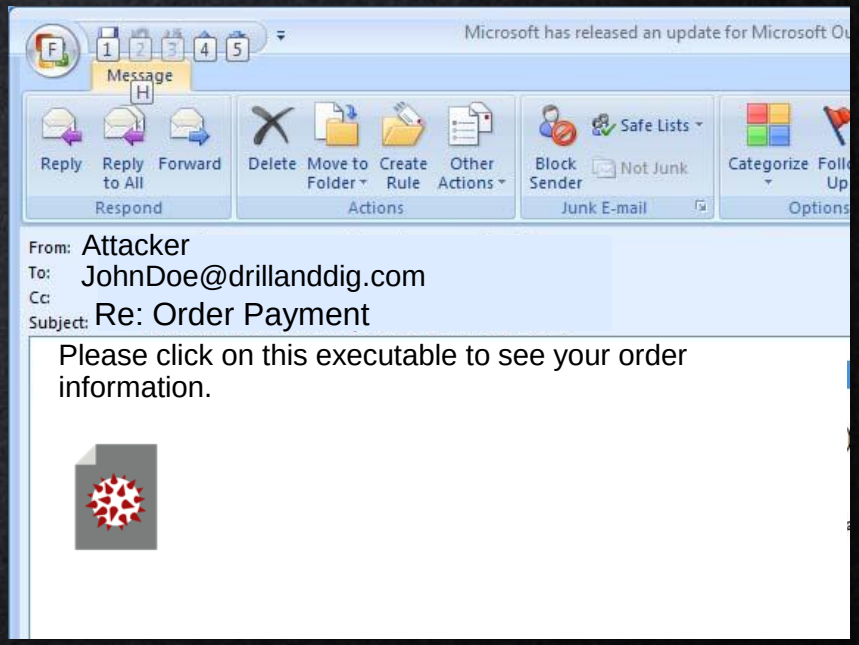
Spear Phishing Attacks by Size of Targeted Organization, 2011 - 2013

Source: Symantec



Most Likely to be Targeted

Executive Assistant at a large mining company



Risk of Being Targeted by Job Role

Risk of Job Role Impact by Targeted Attack
Sent by Spear-Phishing Email
Source: Symantec

Risk	
High	**Personal Assistant (Executive Assistant)**
	Media
Medium	**Senior Management**
	Sales
Low	**C-Level**
	Recruitment
	R&D

Risk of Being Targeted by Industry

Ratio of Organization in an Industry
Impacted by Target Attack
Sent by Spear-Phishing Email
Source: Symantec

Risk		1 in
High	Mining	2.7
	Public Administration (Government)	3.1
	Manufacturing	3.2
Medium	Wholesale	3.4
	Transportation, Communications, Electric, Gas & Sanitary Services	3.9
	Finance, Insurance & Real Estate	4.8
Low	Services – Non-Traditional	6.6
	Construction	11.3
	Agriculture, Forestry & Fishing	12.0

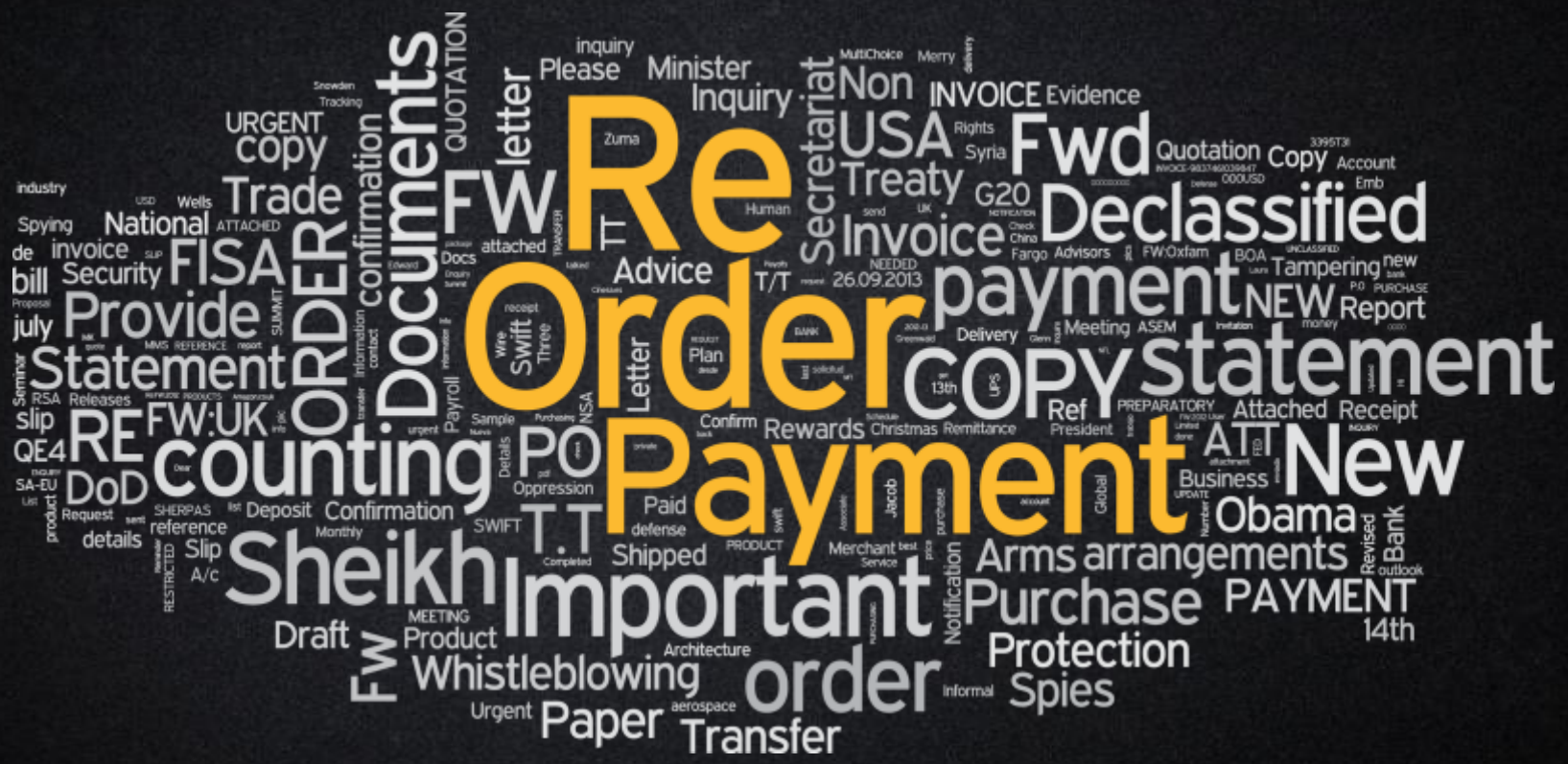
Risk of Being Targeted by Industry Size

Ratio of Organization Targeted by Industry Size
Sent by Spear-Phishing Email

Source: Symantec

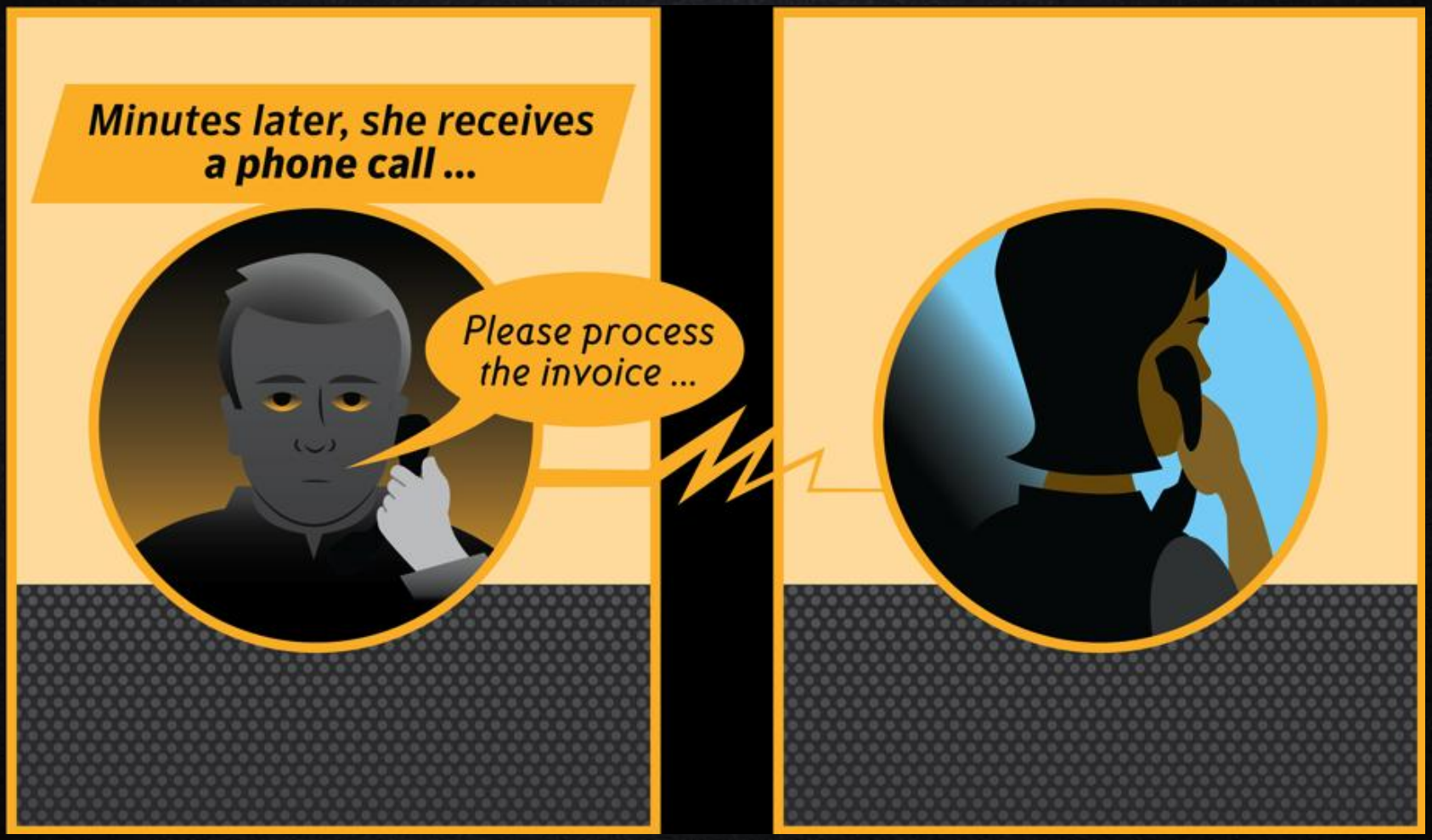
Risk		1 in
High	2,500+	2.3
	1,501-2,500	2.9
	1,001-1,500	2.9
Medium	501-1,000	3.8
	251-500	4.3
	1-250	5.2

Word Cloud: Spear Phishing Attacks

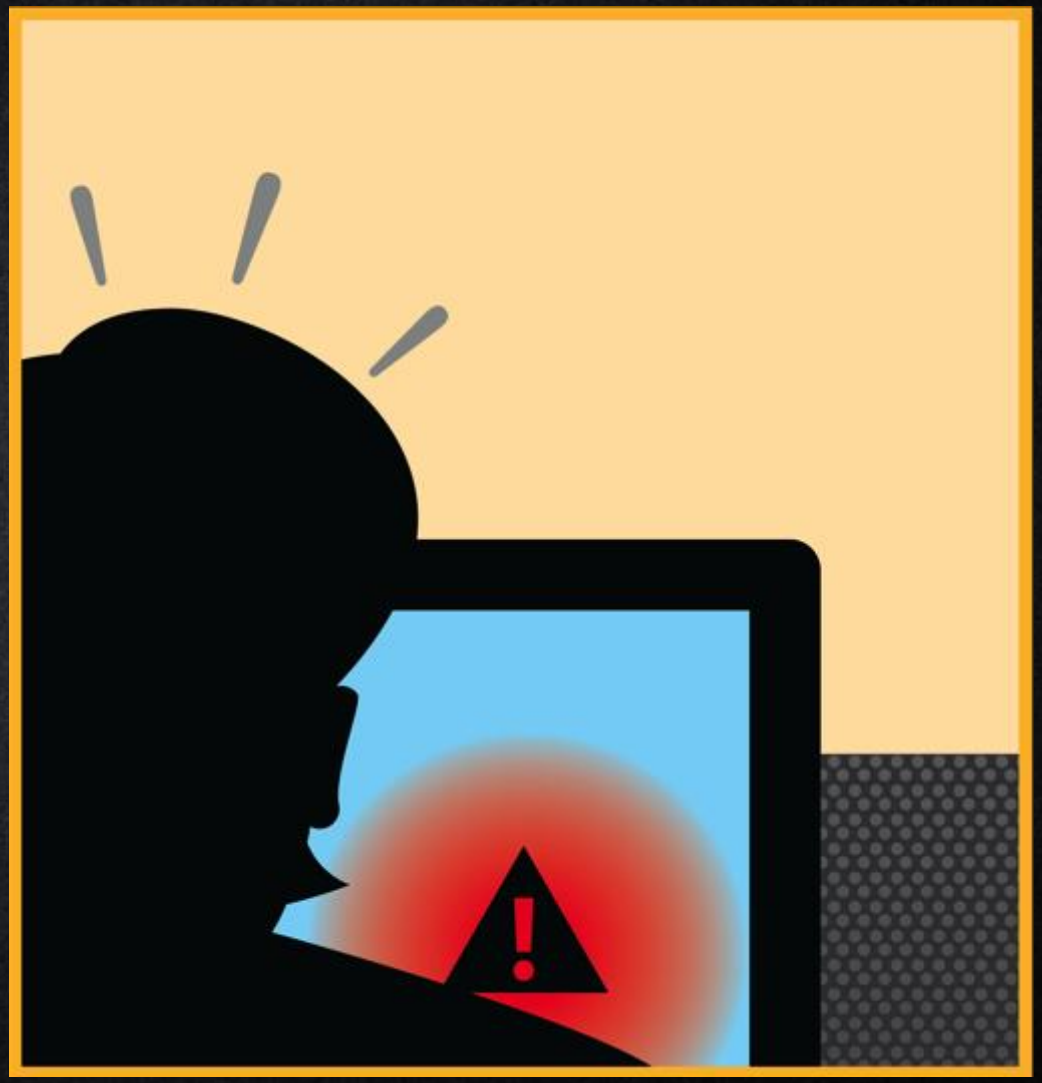

Re
Order
Payment
Important
Sheikh
counting
Documents
Declassified
statement
payment
COPY
New
Fwd
FW
Invoice
Secretariat
USA
Non
INVOICE
Evidence
Please
Minister
Inquiry
inquiry
letter
QUOTATION
confirmation
ORDER
FISA
Provide
Trade
National
Security
invoice
bill
Statement
RE
FW:UK
DoD
PO
T.T
Purchase
Arms
arrangements
PAYMENT
Protection
Spies
order
Whistleblowing
Paper
Transfer
Draft
Product
Urgent
Obama
Treaty
G20
Advice
Tampering
NEW
Report
Receipt
Attached
Rewards
Confirm
Deposit
Confirmation
Shipped
Paid
Notification
Merchant
Business
Bank
14th
Quotation
Copy
Account
Evidence
Rights
Syria
Zuma
Human
attached
Docs
Letter
Swift
Three
Plan
Payroll
Sample
Oppression
Meeting
Delivery
Ref
President
Remittance
Christmas
Merry
MultiChoice
Advisors
Fargo
FW:Oxfam
26.09.2013
T/T
Tracking
Snowden
URGENT
copy
industry
Spying
de
bill
july
slip
QE4
SA-EU
Request
details
reference
Slip
A/c
SHERPAS
SWIFT
MEETING
Architecture
aerospace
informal
Jacob
Global
Revised
outlook
Number
Merchant
Service
Completed
PRODUCT
defense
Monthly
Seminar
RSA
Releases
SUMMIT
REFERENCE
MMS
Proposal
Emb
Check
China
UNCLASSIFIED
PREPARATORY
13th
UPS
Greenwald
Glenn
ASEM
Invitation
money
PURCHASE
P.O
BANK
NSA
Purchasing
urgent
Details
Schedule
Limited
done
attachment
UPDATE
INQUIRY
FED
Amazon.co.uk
Dear
List
product
sent
RESTRICTED
Number
purchase
price
best
Service
Automatic
Purchase
Purchase
Purchase

An employee of a multinational company receives an email referencing an INVOICE ...
Dear Employee,
Please take a moment to open the attached invoice:
Sincerely,
Sender
Invoice

Symantec


Minutes later, she receives a phone call ...
Please process the invoice ...

Click
Invoice



Protection Against Targeted Attacks

Reputational & Behavioral Protection	• Detect and block new and unknown threats based on global reputation and behavior of files
Host-based Intrusion Detection and Prevention	• Locks down key systems that contain confidential information • Prevents any unauthorized code to run — independent of AV signatures
Removable Media Device Control	• Restrict removable devices and functions to prevent malware infection
Email & Web Gateway Security	• Scan & block email with potentially malicious URLs, attachments or content. • Monitor inbound/outbound web traffic and block accordingly
Encryption	• Discover data spills of confidential information that are targeted by attackers • Detect and prevent exfiltration of confidential information that are targeted by attackers
Endpoint & Network Data Correlation	• Create and enforce security policies so all confidential information is encrypted
Network Threat and Vulnerability Monitoring	• Prioritize threat information detected at the network through security intelligence and information coming from endpoint security devices.

ISTR

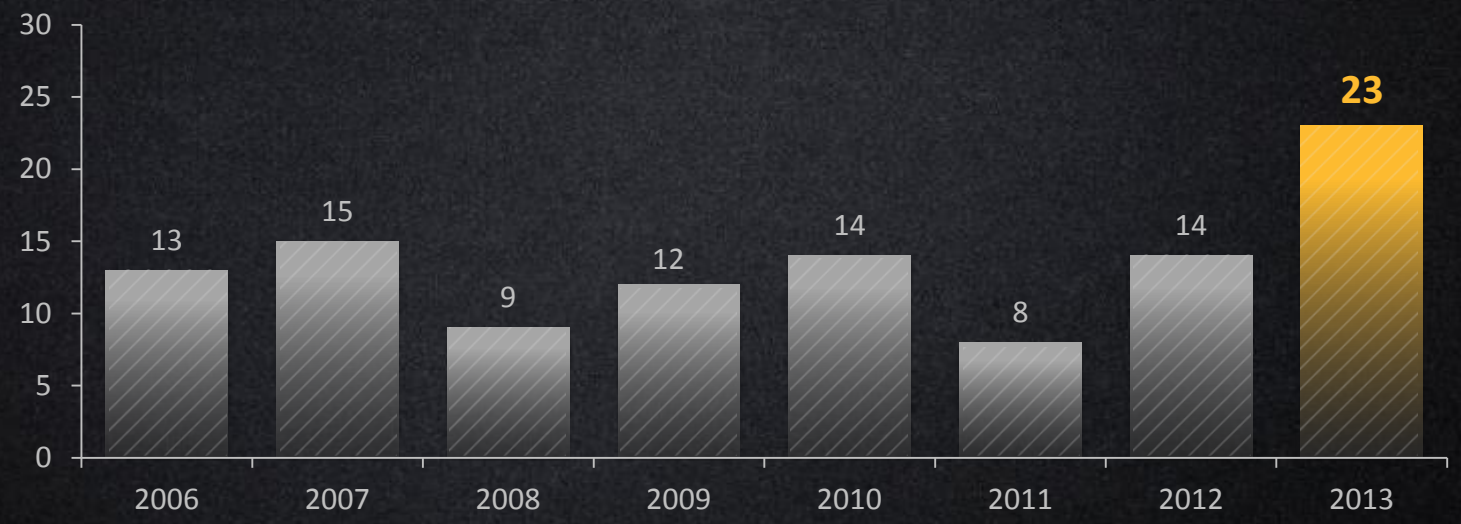
INTERNET SECURITY THREAT REPORT ⌖ 2014

Vulnerabilities

Zero-Day Vulnerabilities

Zero-Day Vulnerabilities, Annual Total, 2006 - 2013

Source: Symantec



23 zero-day vulnerabilities discovered in 2013

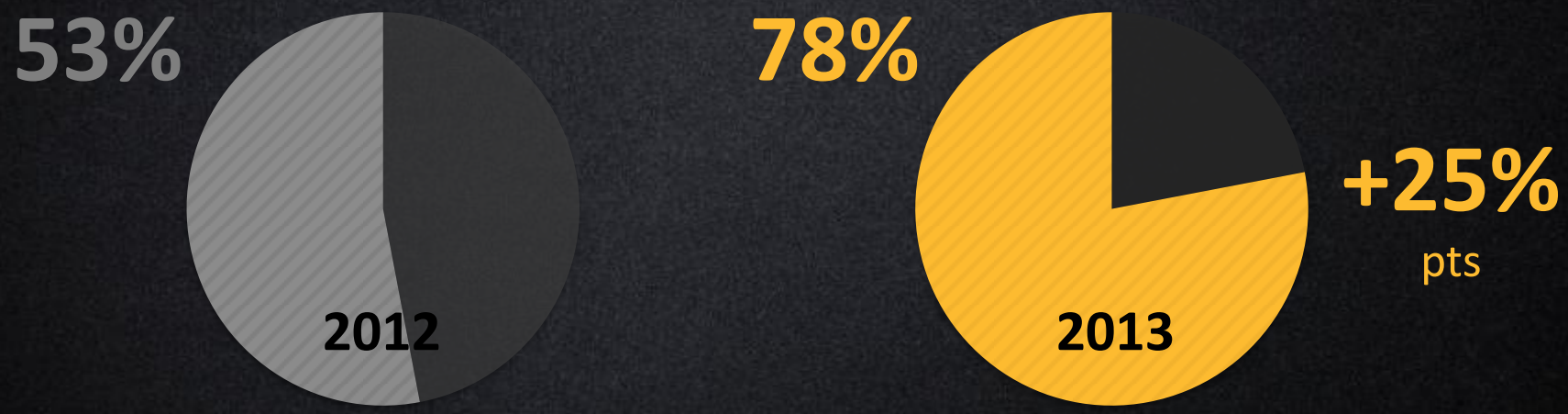
Increase from 14 in 2012

More zero-day vulnerabilities discovered in 2013 than in any year since we started tracking

More zero-days in 2013 than **in past two years combined**

Website Vulnerabilities

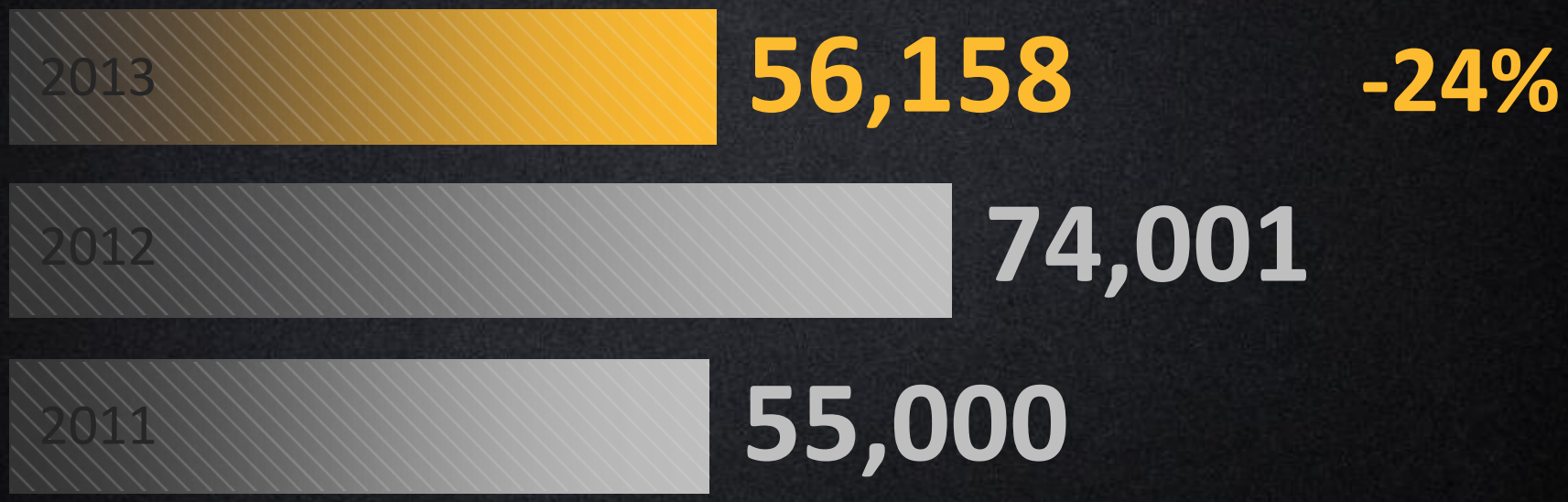
Scanned Websites With Vulnerabilities



1 IN **8** sites had critical unpatched vulnerabilities

Malicious Websites

New Unique Malicious Web Domains



With so many vulnerable websites, cybercriminals don't need to set up own websites to host malware

Web-based Attacks

Web Attacks Blocked Per Day

Web-based attacks continue to grow

Vulnerability Security

Vulnerability Management Program	• Routine, frequent vulnerability assessments and penetrations tests to identify vulnerabilities in applications, systems, and mobile devices • Formal process for addressing identified vulnerabilities
Configuration & Patch Management Program	• Ensure all operating system and application patches are evaluated and deployed in a timely manner • Ensure adherence to formal, secure configuration standards
Application Virtualization	• Leverage application virtualization technologies to reduce risk when legacy web browsers and older versions of 3rd party applications like JAVA or Adobe Reader must be used for compatibility reasons
Reputational & Behavioral Protection	• Detect and block new and unknown threats based on global reputation and behavior of files
Removable Media Device Control	• Restrict removable devices and functions to prevent malware infection

ISTR

INTERNET SECURITY THREAT REPORT 2014

Ransomware

Precursor to Ransomware

FakeAV depended on fear to work

When everyone knows it's fake, there is no fear and the scam fails.

From FakeAV to Ransomware

Cybercriminals moved to **ransomware**

Fear of **arrest**

Simple and (for bad guys) safe method of receiving **"fine"**

At **$100-$400** a victim, it's very profitable

Ransomware

Ransomware exploded globally in **2013**

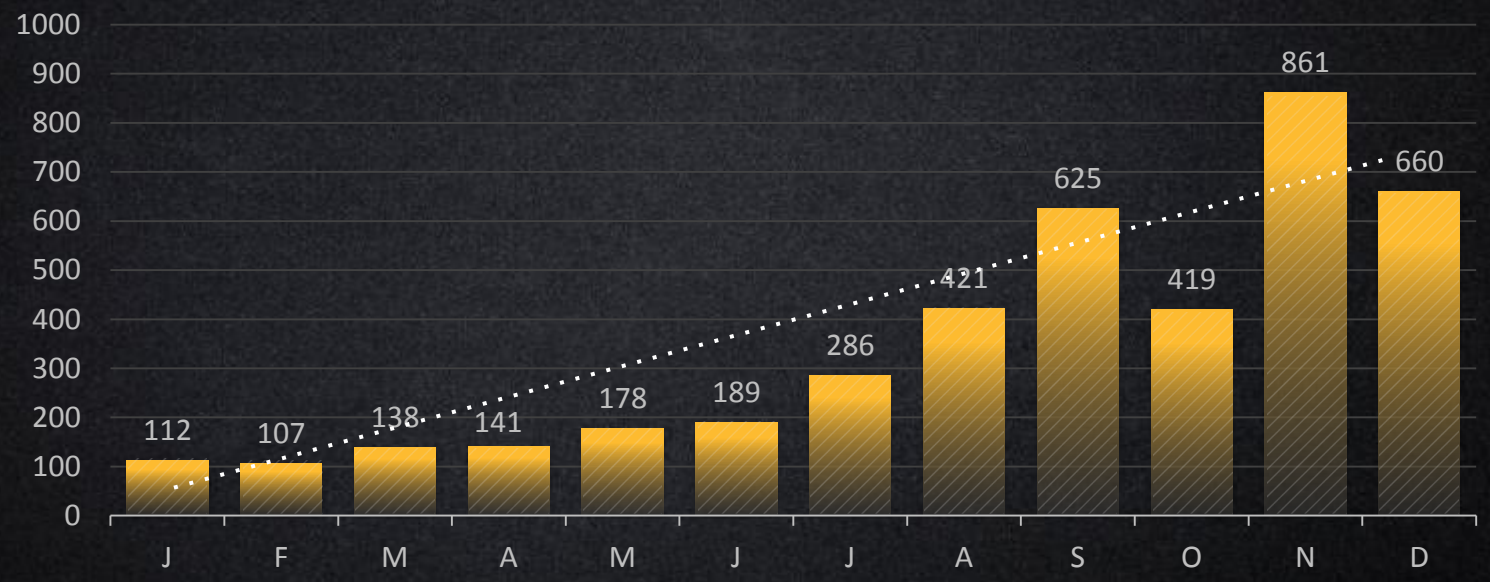
With only **online payment options limiting its reach**

With only **1.5 million** Internet-connected computers, even the **Palestine Territories is a big enough target for criminals**

Ransomware's Growth

Ransomeware Over Time, 2013

Source: Symantec



500% increase in **Ransomware** attacks in **2013**

Ransomware Turns Vicious

When people stop fearing **ransomware?**

Cryptolocker happens!

Cryptolocker most prevalent in threat category called **ransomcrypt**

No pretense of a fine

Must pay to get your **files back**

Ransomcrypt

Cybercriminals use **cryptocurrencies** when doing business with each other

They'd like to make **victims** use them, too

Ransomcrypt: Some Perspective

Number of Attacks Still Small

In December, just **0.2** percent of all **ransomware** was **CryptoLocker**

Threat is Not New

Trojan.Gpcoder (May 2005)
Trojan.Ransomcrypt (June 2009)

What is New?

Online payment methods
Good encryption
Cryptolocker uses RSA 2048 Encryption

Poised for Growth

Defending Against Malware

Reputational & Behavioral Protection	• Detect and block new and unknown threats based on global reputation and behavior of files
Host-based Intrusion Detection and Prevention	• Locks down key systems that contain confidential information • Prevents any unauthorized code to run — independent of AV signatures
Removable Media Device Control	• Restrict removable devices and functions to prevent malware infection
Email & Web Gateway Security	• Scan & block email with potentially malicious URLs, attachments or content. • Monitor inbound/outbound web traffic and block accordingly
Endpoint & Network Data Correlation	• Prioritize threat information detected at the network through security intelligence and information coming from endpoint security devices.
Security Awareness Program	• Ensure employees become the first line of defense against socially engineered attacks, such as phishing, spear phishing, and other types of attacks

ISTR

INTERNET SECURITY THREAT REPORT ⌖ 2014

Mobile = Danger

Symantec

Mobile Threats

Mobile Threats: Malicious Code by Platform, 2013

Source: Symantec

Platform	Number of Threats	Percent of Threats
Android	57	97%
Symbian	1	2%
Windows	1	2%
iOS	0	0%

Android remains the platform of choice for malware authors

Mobile Malware

Android Mobile Malware Families

57

2013

-45%

103

2012

Average Number of Variant Per Family

57

2013

+50%

38

2012

Creation of new mobile malware slowed as malware authors focused on improving existing malware

Average number of variants per family in **2012 was 1:38**

Increased to **1:57 in 2013**

Mobile Users at Risk

38% Of smartphone users have experienced mobile cybercrime in past 12 months

50% Don't use basic precautions such as passwords, security software or back up files for their mobile device

Source: 2013 Norton Report

Mobile Security IQ

	DELETE **SUSPICIOUS EMAILS** FROM PEOPLE THEY DON'T KNOW	HAVE AT LEAST A **BASIC** FREE ANTIVIRUS SOLUTION	AVOID STORING **SENSITIVE FILES** ONLINE
	90%	**72%**	**78%**
	56%	**33%**	**48%**

Source: 2013 Norton Report

Mobile: A Dangerous Mix

1. Prevalence of mobile devices
2. Maturing of mobile malware
3. Mixing of work and personal information on devices
4. User's lack of smart smartphone risk awareness

Mitigating Mobile Attacks

Application Management	• Secure data in corporate applications regardless of device ownership
Device Management	• Remotely wipe devices in case of theft or loss, control password policies • Update devices with applications as needed without physical access
Device Security	• Guard mobile device against malware • Prevent the device from becoming a vulnerability
Identity & Access Control	• Provide strong authentication and authorization for access to enterprise applications and resources • Ensure safe access to enterprise resources from right devices with right postures
Secure File Sharing	• Enable encrypted file sharing to ensure security as users share information

ISTR

INTERNET SECURITY THREAT REPORT ⌖ 2014

Future Trend: Internet of Things

Future Trend: Internet of Things

Confirmed:

Real world attacks against security cameras and baby monitors

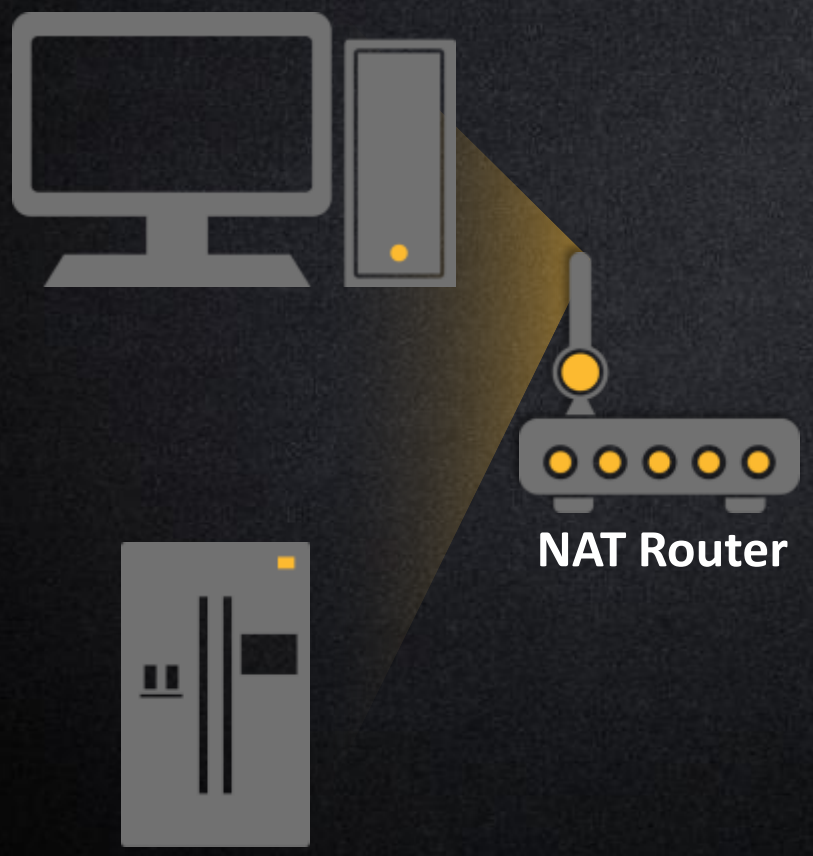
Demonstrated:

Hacking attacks against televisions, cars and medical equipment

Exaggerated:

Reports of refrigerators sending spam messages

Internet of Things: Busting Refrigerator Myth



With NAT router all devices appear to have a **single IP address**

A **Refrigerator and a PC** look like the same IP address

But spam was sent by **W32.Waledac (Kelihos)**

- W32 means a Windows OS

Internet of Things: Real Risks

Biggest Risk? Routers

- **Linux.Darlloz** infects Linux PCs and IoT devices running Linux
- **Linux.Aidra** targets cable and DSL modems

Uses for Infected Routers?

- DDoS attacks
- Browser re-direction
- Even cryptocurriences mining

Reason for Attacks?

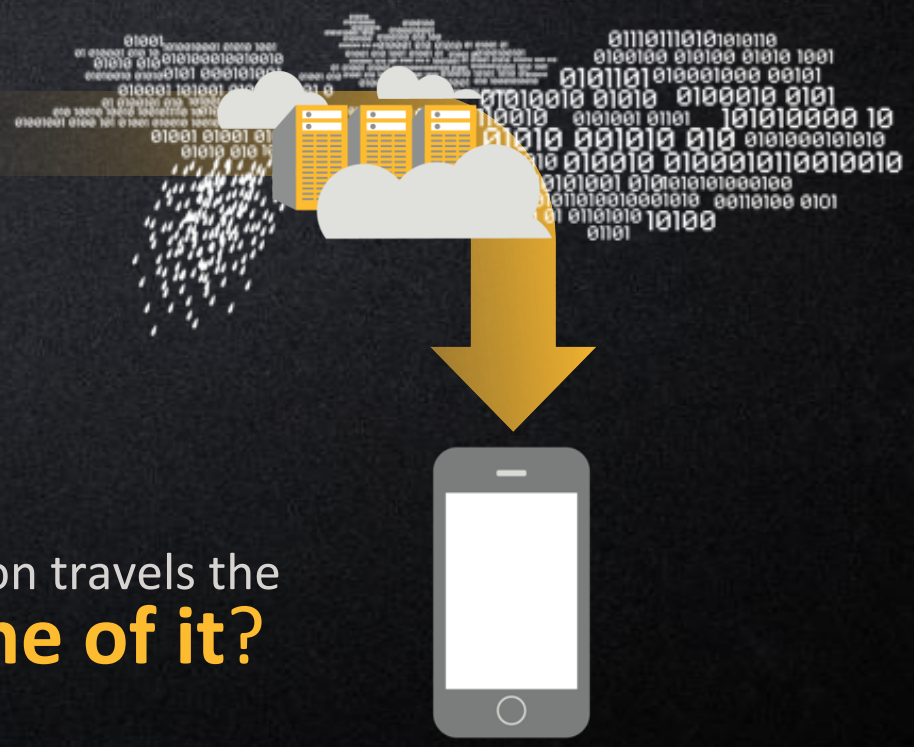
- Unpatched vulnerabilities
- Unchanged default passwords

Internet of Things: What's Next?

Wearable Devices

They will be measuring and transmitting:

- Pulse
- Weight
- Time slept
- Glucose levels
- Blood pressure
- Exposure to sunlight
- Teeth brushing habits
- And more…



As more of our personal information travels the Internet **what will become of it?**

Symantec.

Stay Informed

Download: symantec.com/threatreport

Follow: @threatintel

twitter

Thank you!

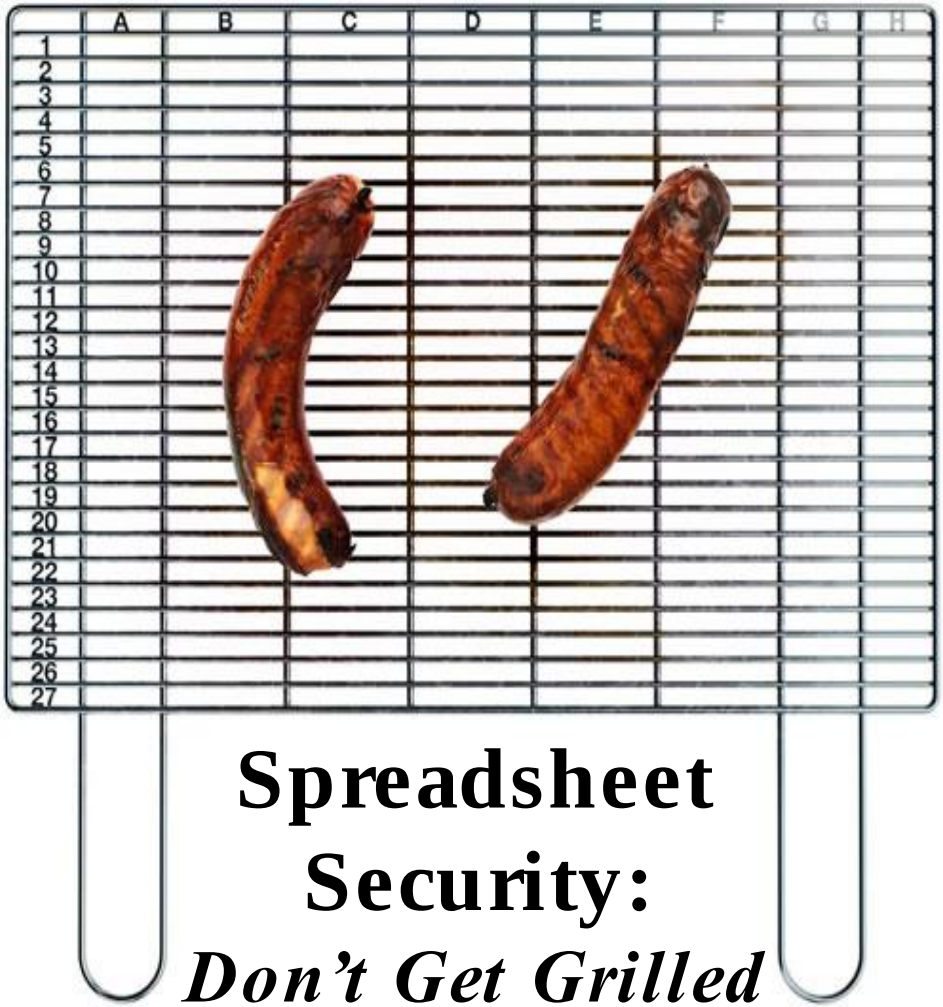
Copyright © 2012 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

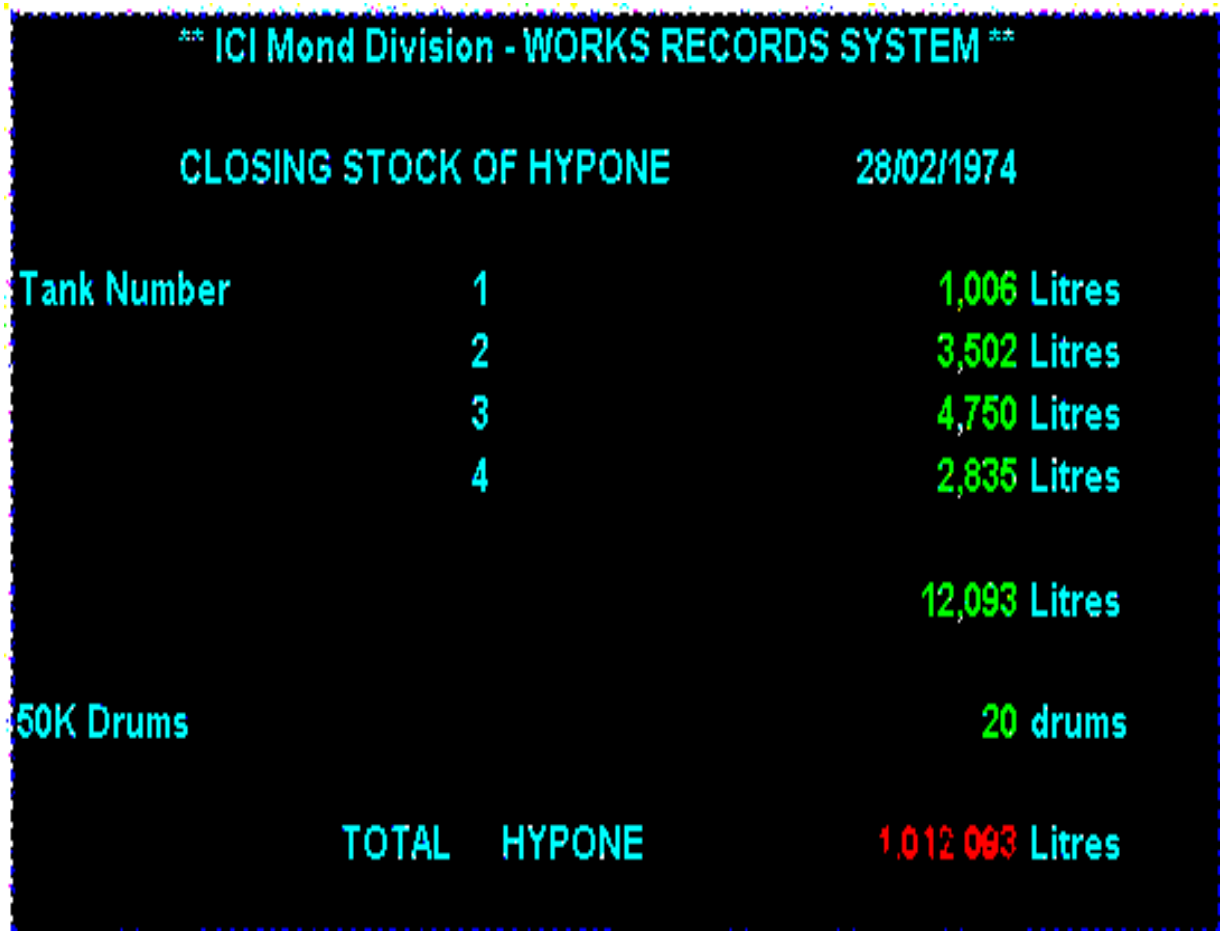
Virginia Information Technologies Agency

Spreadsheet Security

Presented by Ed Miller
ISOAG
May 7, 2014



History of Spreadsheets



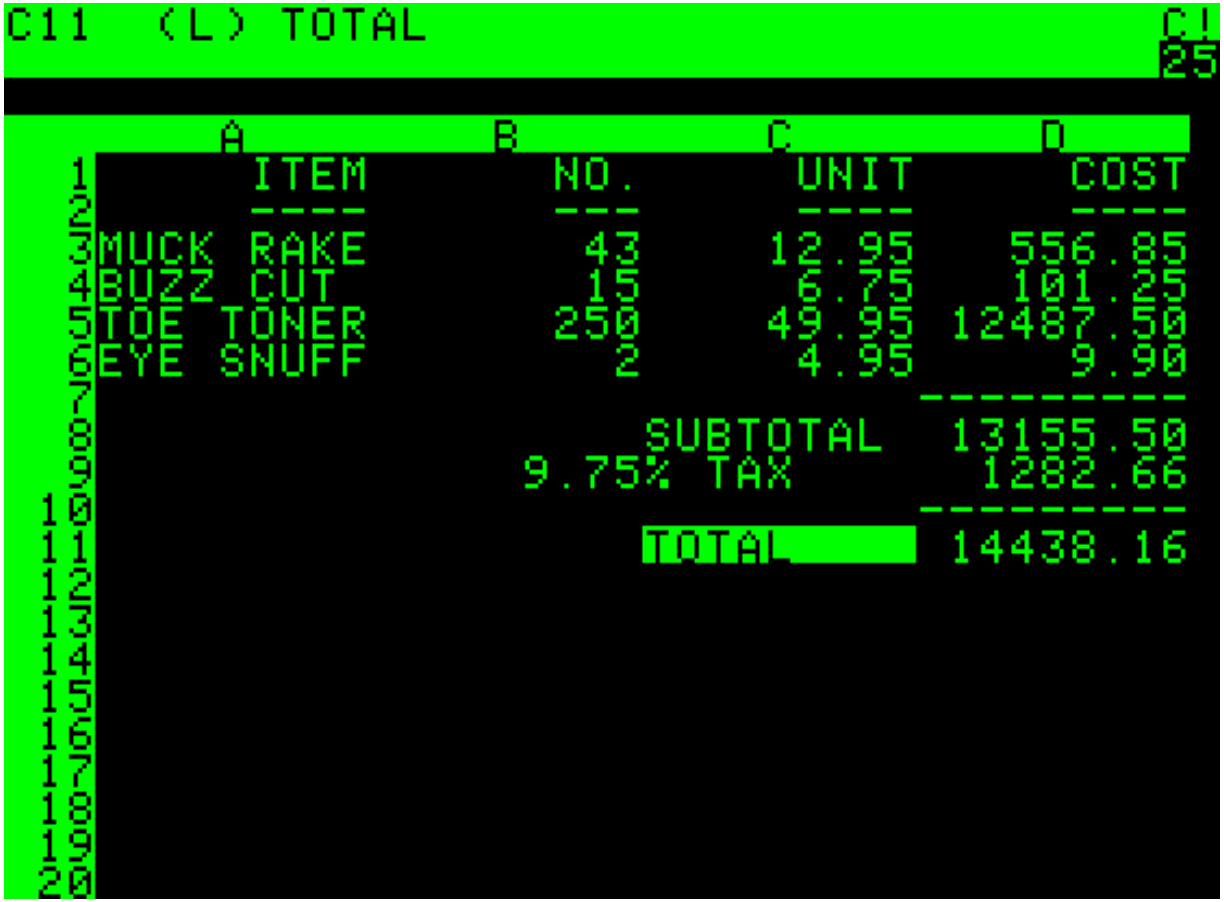
** ICI Mond Division - WORKS RECORDS SYSTEM **

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

Electronic spreadsheets first appeared in the 1960's for mainframe computers.

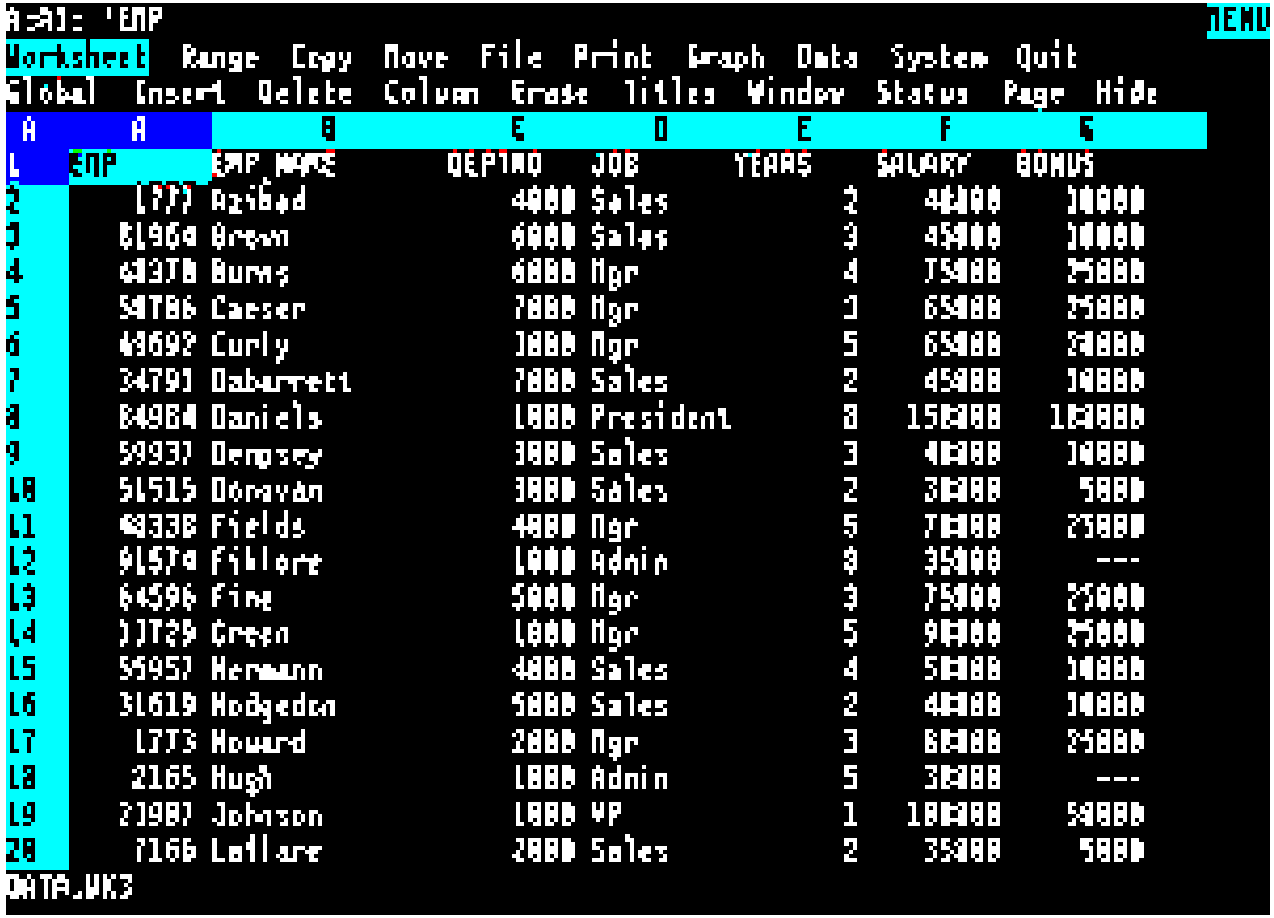
History of Spreadsheets



VisiCalc was the first personal computer spreadsheet.

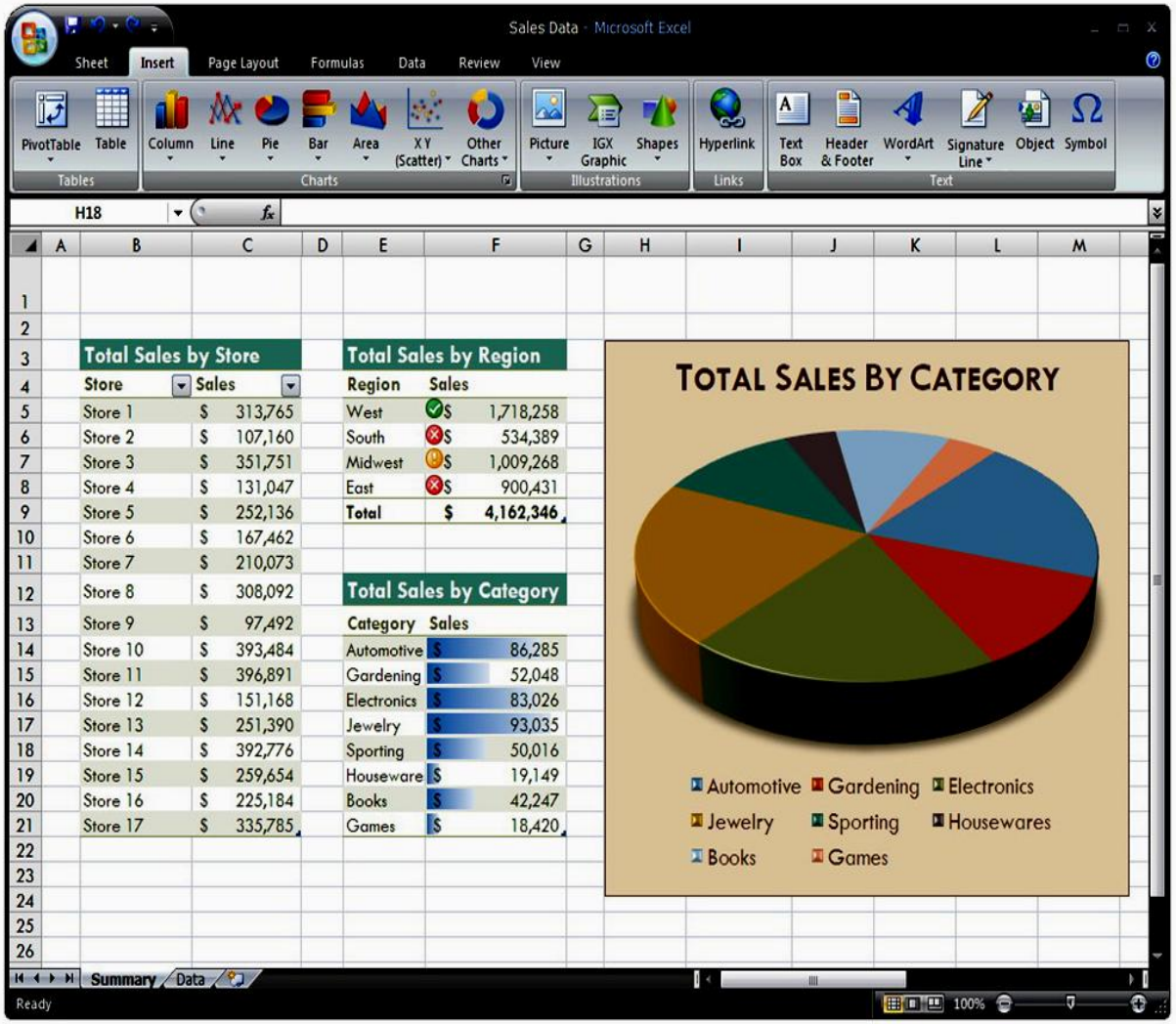
It was invented in 1979 for the Apple II.

History of Spreadsheets



Lotus 123, was first released in 1983.

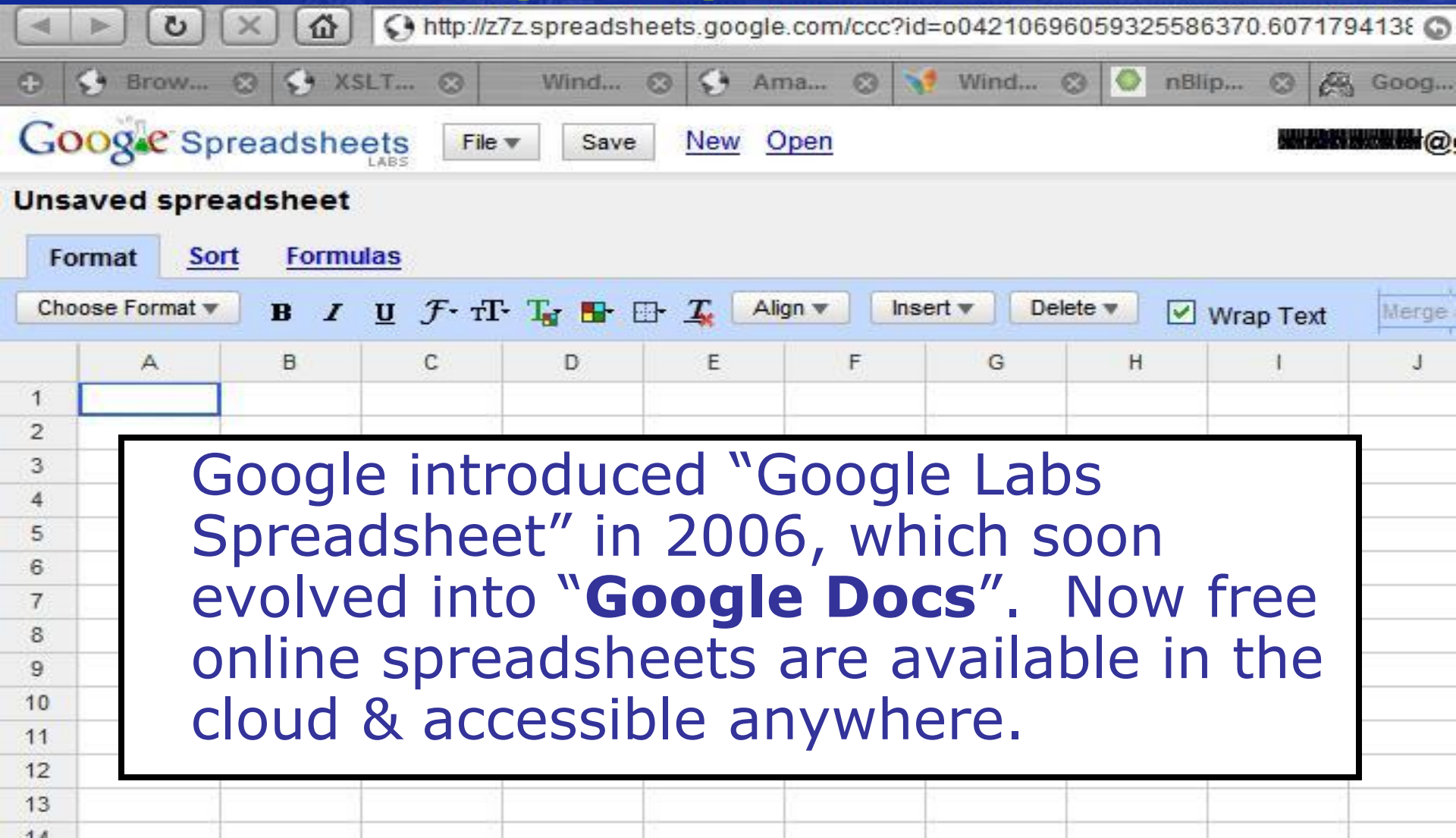
History of Spreadsheets



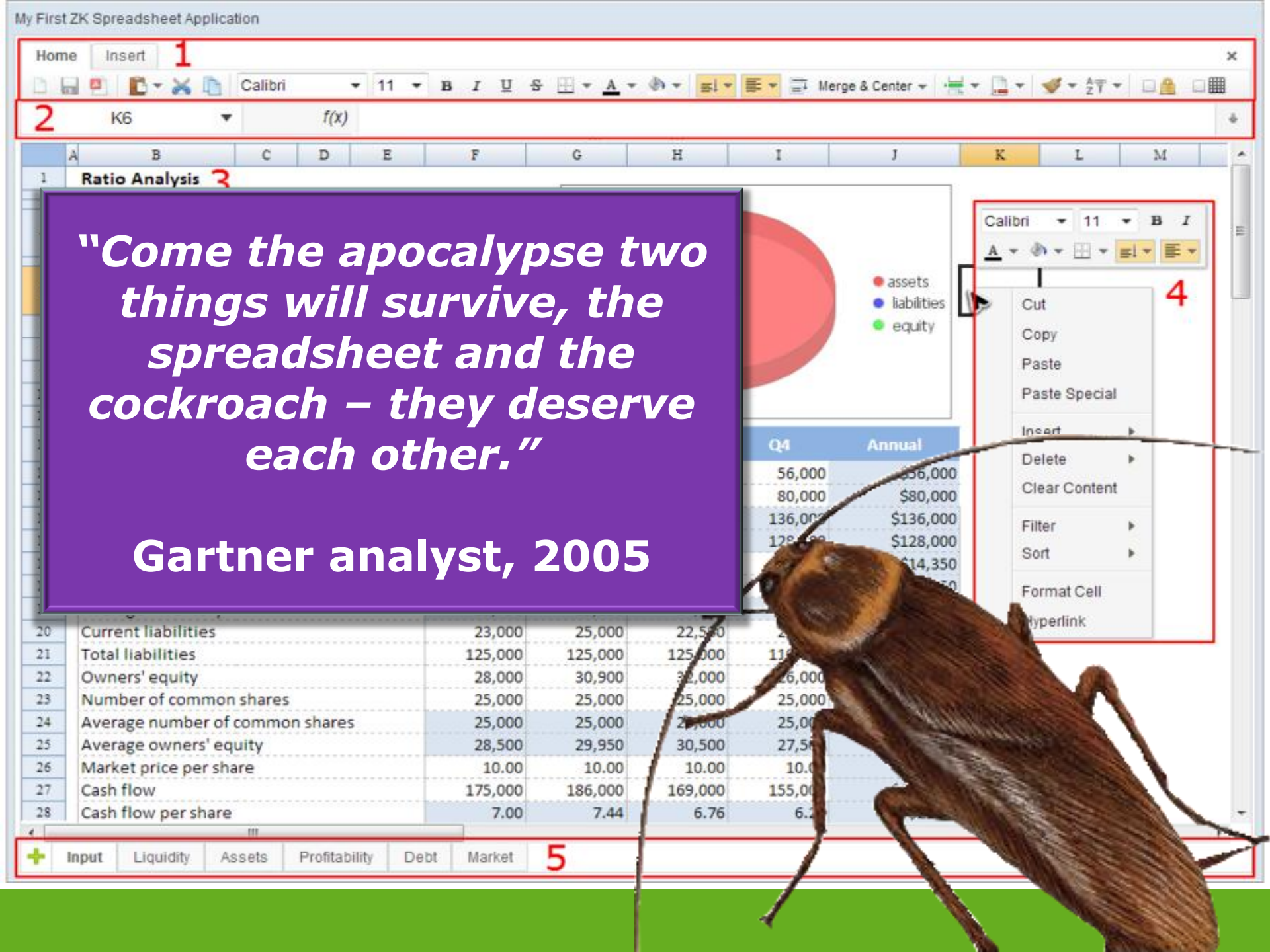
Microsoft Excel was released in 1985 for the Apple Macintosh & in 1987 for MS Windows.

Virginia Information Technologies Agency

History of Spreadsheets



Google introduced "Google Labs Spreadsheet" in 2006, which soon evolved into "**Google Docs**". Now free online spreadsheets are available in the cloud & accessible anywhere.



"Come the apocalypse two things will survive, the spreadsheet and the cockroach – they deserve each other."

Gartner analyst, 2005

End-User-Computing

- Spreadsheets fall into a special category of computer applications referred to as ***"End User Computing"*** or ***EUC***.

- EUC applications are those applications that are:
  - Developed by end users,
  - Maintained by end users, and
  - Utilized by end users.

- They include spreadsheets, MS Access type databases, word processing files, Business Objects, Crystal Reports and others.

Why do we use EUC applications?

- **FAST** – no dependency on programmers or on IT
- **FLEXIBLE** – easily changed to meet new needs
- **EASY TO USE** – in theory, anyone can learn to use EUC apps like Excel
- **LOW COST** – or even free

Problems with End User Computing (EUC)

- Biggest problem with EUC apps, 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: **Untrained users (i.e. non-professional developers)** placing an **undue amount of trust** in the integrity & security of an "application" that has had little to no testing or objective peer review.

Problems with End User Computing (EUC)

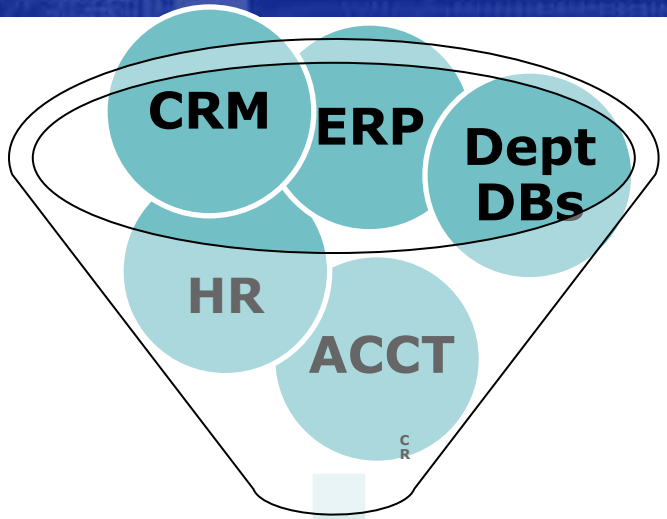
- In addition, end users often implement spreadsheets with ***very few controls***.

- Without controls, it is very difficult to:
  - Prevent errors,
  - Avoid poor decisions,
  - Prevent fraud, and
  - Protect against non-compliance with policies and regulatory mandates

Centralized Data vs. EUC Data

CENTRALIZED DATA

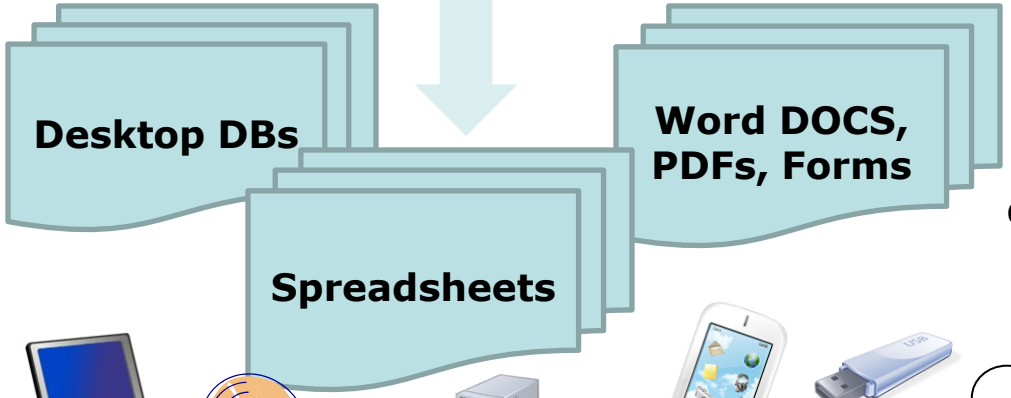
- Visible
- Managed
- Monitored
- Structured Lifecycle



Estimates are that 40 % of centralized data is funneled out & duplicated in EUC spreadsheets, word files, etc.

EUC DATA

- Not very visible
- Not well managed
- Not monitored
- Sketchy Lifecycle



EUC data is often identical to centralized data but the controls are vastly different.

EUC Spreadsheet Risk

Why worry about EUC (spreadsheet) risk?

ERROR

FRAUD

ABUSE

Financial losses

Privacy breaches

Fines & penalties

Legal challenges

Loss of reputation

Spreadsheet Risks

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

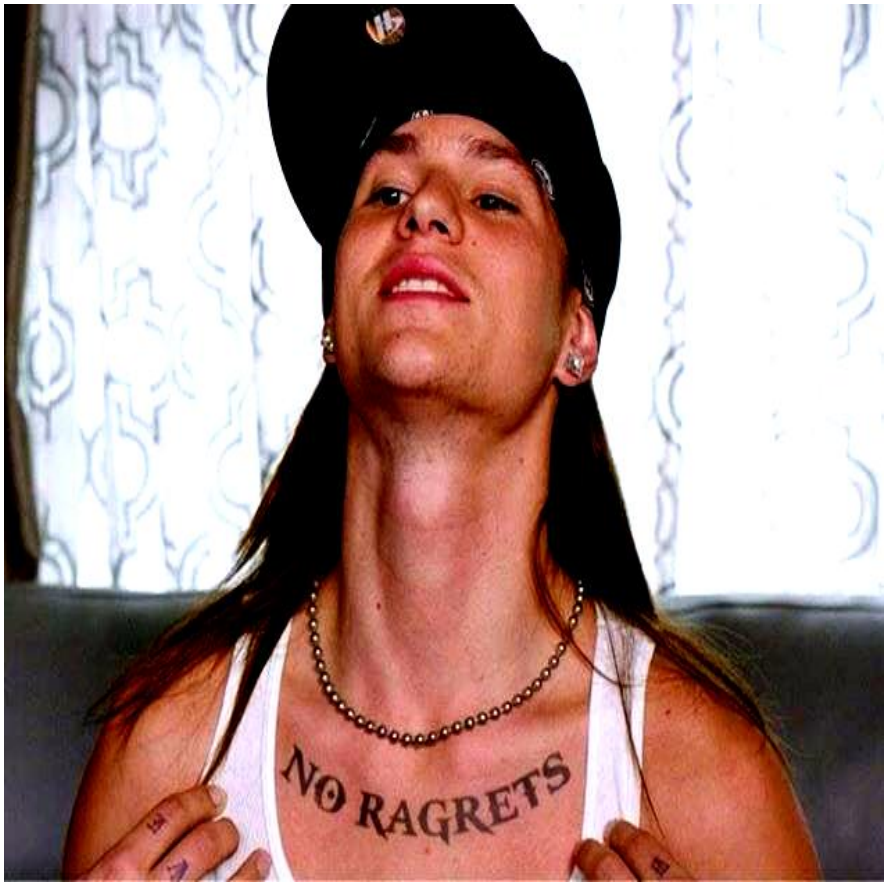
- **Spreadsheets are error-prone**
- **Spreadsheets are not well tested**
- **Errors are difficult to find**

Spreadsheet Risks

- **Users are overconfident of the results**
- **Users interpret information differently**
- **Presentation & reporting is inconsistent or unclear**

Spreadsheet Risks

- **Backup and Archiving are overlooked**
- **Version control is inadequate**
- **Spreadsheets are re-used & re-cycled often resulting in damaged links & invalid formulas**
- **Spreadsheet security & access controls are weak**

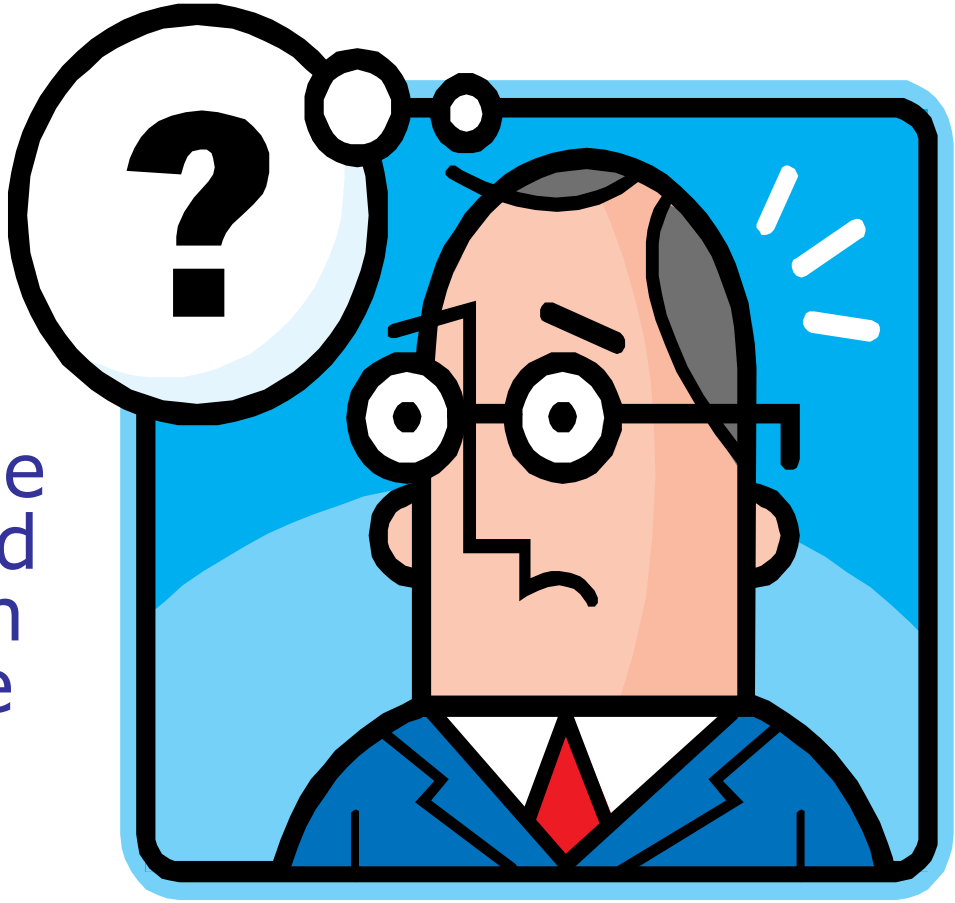


Spreadsheet Risks

- Spreadsheets are easily copied and transported
- Segregation of duties is not implemented
- Training is inadequate
- Spreadsheet preparation guidelines are often non-existent
- Support is inadequate; outside of IT control

Spreadsheet Risks

The 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.

Risk of the Unknown

Risk management is about reducing the impact of the unknowns. It's not about trying to predict all outcomes.

So ask yourself some questions:

- How many spreadsheets exist at your agency?
- Which ones are used in critical business processes?
- Do you know who owns them?
- Do you know where they are?
- Where does the data come from that is fed into it?
- Where does data go to that is extracted from it?

ISO: Information Security Ostrich

Virginia Information Technologies Agency

Spreadsheet Errors

Let's talk about errors

Errors are a big 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

Common Spreadsheet Errors

Logic errors

- Incorrect formulas or omitted factors in formulas
- Incorrect sorting, calculations, order of calculations or other programmable elements

Common Spreadsheet Errors

Interface errors

- Download errors (incomplete, out-of-date, out-of-range, etc.)
- Faulty import/export of data
- Improperly linked spreadsheets

Common Spreadsheet Errors

Other errors

- Erroneous cell ranges
- Version control errors
- Formatting & column width errors
- Errors in interpretation

Common Spreadsheet Errors

Compromised Data

Spreadsheets are very easy to duplicate & transport, resulting in compromise due to lost/stolen USB drives, laptops, smartphones & CD's or from unauthorized email attachments or file & cloud copies.

We all make mistakes.

Here's a spreadsheet where a patient's weight, height and other factors are used to determine the proper drug dosage.

Patient Name:

Data Entry Box

Calculations

Weight Kilograms -	0.0
Height Centimeters -	0.00
BSA Square Meter -	0.000

CELL E19

Medications

Pre-operative

			mg
Atropine	IM	0.02 mg/kg	0.10
Atropine	IV	0.01 mg/kg	0.10
Cimetidine	PO/Slow IV	7.5 mg/kg	0.0
Clonidine	PO	4 mcg/kg	0.000
Glycopyrrolate	IV/IM	0.01 mg/kg	0.00
Ketamine Stun	IM	5 mg/kg	0.0
Metoclopramide	IV	0.1 mg/kg	0.0
Midazolam	IV	0.05 mg/kg	0.00
Midazolam	PO	0.5 mg/kg	0.0
Midazolam	IM	0.08 mg/kg	0.00
Midazolam	Nasal	0.3 mg/kg	0.0
Morphine	IM	0.1 mg/kg	0.0
Ranitidine	IV *(up to 50 mg)*	1 mg/kg	0.0

Errors Occur Easily!

Look at this formula for calculating a dose of Atropine contained on the previous spreadsheet:

=IF(E19*0.02>0.6,0.6,IF(E19*0.02<0.1,0.1,E19*0.02))

- E19 is "Weight Kilograms" & the only variable, while the other numbers (0.02, 0.1, etc) are embedded constants used for calculating drug dosage
- The formula is somewhat hard to follow & is without any documentation
- There is no data validation on this spreadsheet so a data entry error for someone's weight (E19) could mean that the wrong dose is calculated
- An inadvertent, incorrect or unauthorized change in any of part of this formula could do the same thing! What's the chain of custody?
- Incidentally, medication errors cause 7,000 deaths per year in the U.S.

(Analysis by Grenville J. Croll & Raymond J. Butler (2006))

It's the 77,000. In column B, there is a space after the comma.

This causes Excel to interpret it as text & gives it a value of 0 when used in a formula.

This type of problem is common with imported data.

		B	C	D	E
		Amounts		**Amounts**	
		200,000		200,000	
		20,000		20,000	
		400,000		400,000	
		77, 000		77,000	
		564,000		564,000	
8		55,000		55,000	
9		66,000		66,000	
10	**TOTAL:**	**1,305,000**		**1,382,000**	
11	**FORMULA:**	**=SUM(B3:B9)**		**=SUM(D3:D9)**	
12					

Spreadsheet Errors

- Question: What percentage of spreadsheets contain significant errors?

a) 0 – 20 %
b) 21 – 40 %
c) 41 – 60 %
d) 61 – 80%
e) 81 – 100 %

Auditor, Researcher, or Consultant	Year	% of SS Sample w/ errors	Comments
Hicks	1995	100 %	An erro
Coopers & Lybrand	1997	91 %	91 % we financial reportin
KPMG	1998	91 %	91 % co king
Lukasic	1998	100 %	Sample 16%
Butler	2000	86 %	86% co ayments.
Clermont, Hanin & Mittermieir	2002	100 %	Spreads had significa
Panko / U. of Hawaii	2003	100 %	5 % of t
Panko / U. of Hawaii	2004	100 %	5 % of t
Lawrence & Lee	2004	100%	Only th dited & *all 30* had errors.
Dartmouth College	2009	94%	An audit of 50 spreadsheets, found only 3 *without* a significant error
Collectively		**96 %**	

It's not a matter of IF a spreadsheet contains errors.

It's a matter of HOW MANY and HOW SIGNIFICANT.

Spreadsheet Fraud

What are the FRAUD vulnerabilities of SS?

Presentation Fraud

Excel spreadsheets can easily be setup to "present" numbers differently than the ones that are actually there.

Common fraud examples are hidden rows or columns, custom cell formatting or setting the font color to be the same as background.

Presentation Fraud

Numbers can be formatted to hide or obfuscate the true number

Actual	**Formatted**	
-56790	56790	formatted to display -negative as positive
-56790	$ 56,790.00	formatted to display -negative as positive with $ signs
-56790	$ 711	formatted to display a fixed positive number instead -negative num
-56790		formatted to hide value using format strings
-56790		formatted to hide value using white font color
-56790		formattted so font size is nearly invisible
-340740	-340740	SUM
∑(A4:A9)	∑(B4:B9)	

What are the fraud vulnerabilities of SS?

Data Fraud

- The perpetrator simply changes numbers or sources of data and relies on the difficulty and infrequency of independent checks to avoid detection.

What are the fraud vulnerabilities of SS?

Function Fraud

- This type of fraud disguising its actions by using some of the more complex features and functions of Excel, such as Visual Basic and macros.

- These features are often difficult for an average or casual user of the spreadsheet to understand and detect.

Examples of frauds

WYSIWYG: What You So Intensely Wish You'd Got

Real Life Spreadsheet Frauds

A securities trader for AllFirst Bank (Allied Irish Bank) falsely linked commission spreadsheets, pilfering relatively unnoticeable amounts at a time, but eventually perpetuating a fraud totaling over **$690 million dollars**. *(2001)*

Société Générale, a French banking & financial services firm, was defrauded of over €7 **billion** euro by a junior account rep who allegedly orchestrated a series of bogus transactions using embedded Visual Basic *(May 2008)*.

The CFO of Proquest used "hidden" rows & columns so that false account entries didn't show up when they were printed in hard-copy & also covered up false information by rendering it invisible by using "white font" *(cfo.com July 2008)*

Examples of errors

"Excel NEVER cras "

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 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. However, the USPS disbursed over $2.3 million to the clerks because of an error in an Excel spreadsheet, an overpayment of $1.7 million. (*March 2010 Inspector General Audit Report*)

Real Life Spreadsheet Errors

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

Examples of data breaches

"Hit any user to continue"

Real Life Spreadsheet Data Breaches

An employee at the Georgia Department of Labor mistakenly e-mailed a spreadsheet to over 1,000 people that contained the PII of people that had filed for unemployment . *(eSecurity Planet, 9/13/2013)*

Employees of the Oregon Health & Science University used Google cloud services, without authorization, to maintain a spreadsheet of patient data. OHSU did not have a contractual agreement with Google to use or store OHSU patient health information & had to notify >3,000 patients that their protected health information was compromised . *(Healthcare IT News, 7/29/2013)*

Real Life Spreadsheet Data Breaches

An employee of the South Carolina Department of Health emailed a spreadsheet attachment with the PII of 228,435 Medicaid beneficiaries to his private email account.
(Midland Crimestoppers, 4/19/2012).

SPAM YANKEES! The New York Yankees baseball organization accidentally emailed a spreadsheet to its vendors that contained PII for more than 20,000 season ticket holder accounts. *(Deadspin, 4/27/2011).*

It can happen here!

"There are two ways to develop error-free spreadsheets.

Only the third one works."

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 due a formula error that miscalculated the amount of sales.

(Richmond Times-Dispatch August 8, 2004)

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. A reduction to food tax revenue was accidentally *added* instead of *subtracted*.

(*JLARC Report 338/Aug 2006)*

It can happen here!

A natural gas subsidiary of energy conglomerate Dominion Resources used the same computer file name for each week's storage balance spreadsheet & accidentally sent the wrong week's spreadsheet to Dominion.

The misinformation led Dominion to increase natural gas prices. A class-action lawsuit estimated that Dominion wrongly hiked consumer prices by as much as $200 million.
(The Daily Press, 6/17/2005)

Audit Findings

Audit [au·dit] *noun*: Annual event where CPAs come in and officially point out mathematical errors in your spreadsheets.

Auditor of Public Accounts

Dept of Corrections (2007)	…no security … to restrict … access, either within Excel or the network. ... users can enter, change, delete data & formulas in any or all of the spreadsheets with no trail…
VCU (2008)	The Office of Financial Aid did not accurately calculate … refund(s).… Financial Aid staff used a spreadsheet to compute the refunds; however, incorrect formulas led to incorrect calculations.

Review of Cost Allocation, Billing, and Collections for VITA (2008)	**VITA used a number of spreadsheets to calculate & create rate structures… This was a time-consuming and labor-intensive process …. In general, we found that VITA did not fully document, support, and explain these spreadsheets.** **In addition, only one individual within the agency had the …knowledge to explain the … calculations.** **Management did not appear to adequately review these spreadsheets, …, which resulted in the lack of documentation & a calculation error totaling $1.9 million.**

Auditor of Public Accounts

Agencies of Secretary of Finance (2012)	The level & volume of financial activity …. has grown over the years, & the use of Excel spreadsheets to track & record critical information is inefficient, requires excess effort, & is prone to errors due to the complexity of the data and reporting requirements.
COV Single Audit Report - Virginia Employment Commission (2013)	Finding: … an understatement of approximately $1.5 million in accounts receivable for employer taxes due to a formula error in the spreadsheet.

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 own the risk.

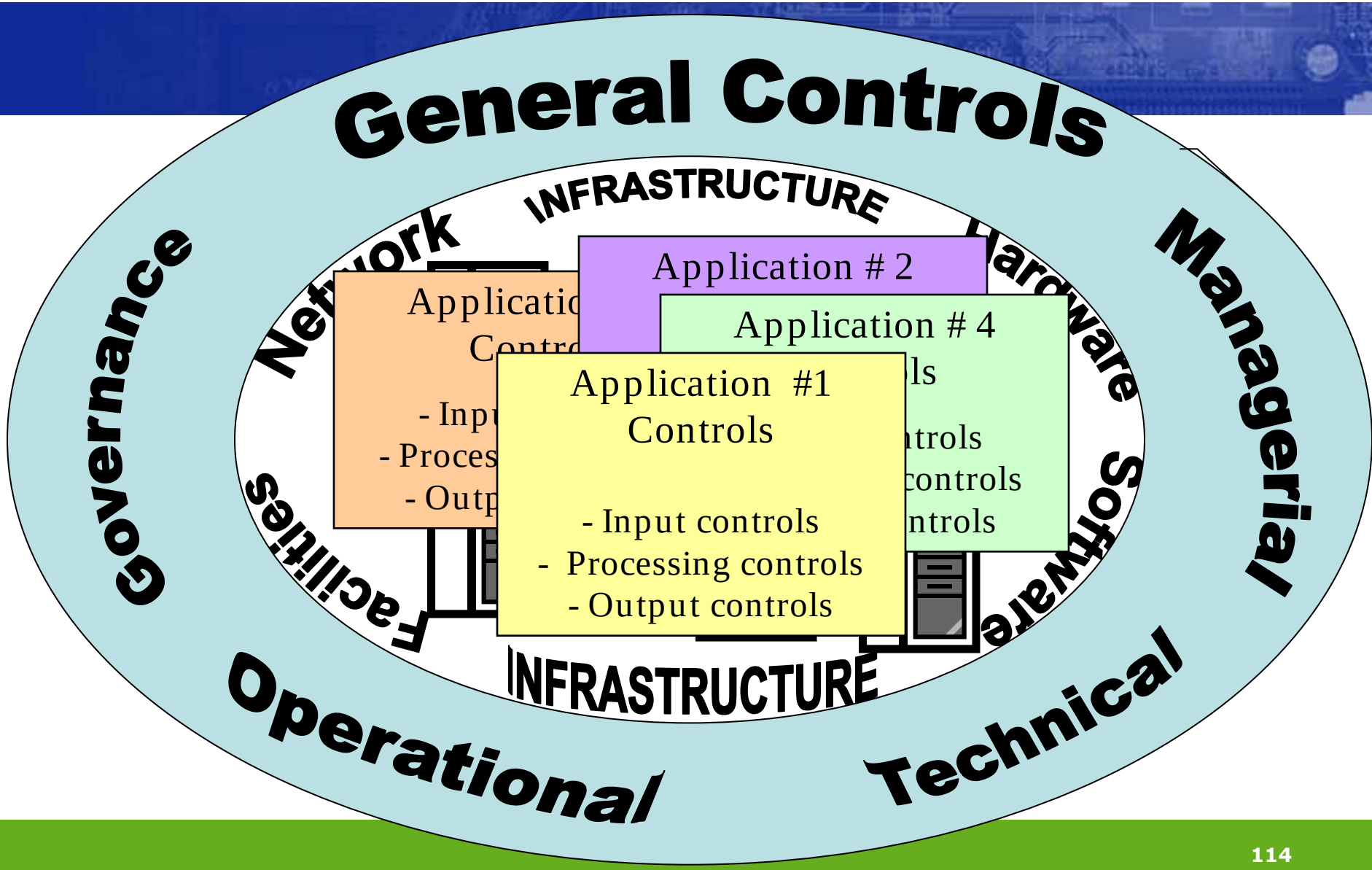
However, business owners often do not understand or even bother to implement the very few programmable application level controls that are available in a spreadsheet.

Who owns Spreadsheet Risk?

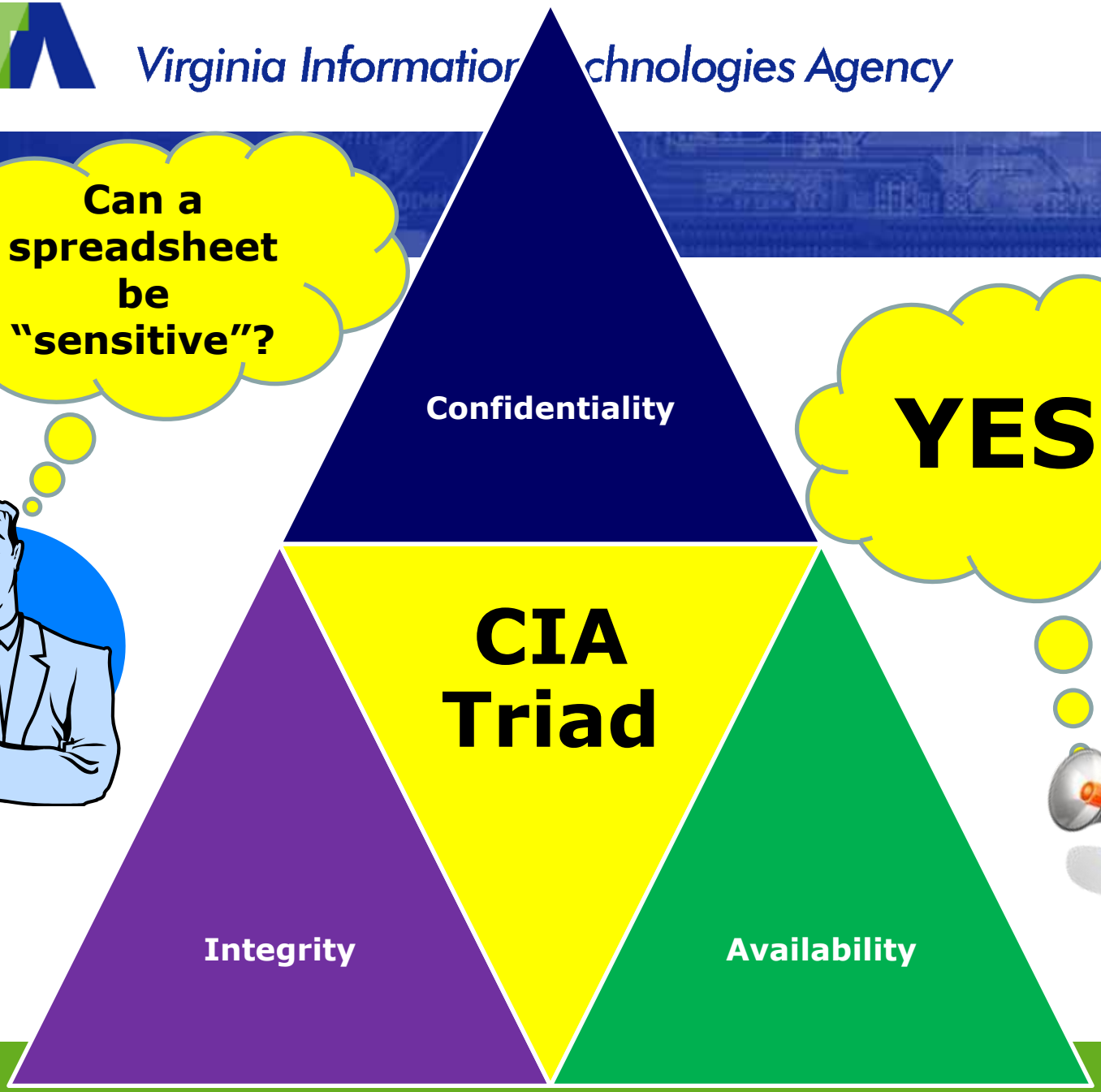
As a result, spreadsheet security is largely reliant on "general" or "common" IT controls, i.e. the controls & security provided by general support servers & services.

General control support servers & services are 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
INFRASTRUCTURE
Network
Hardware
Software
Facilities
INFRASTRUCTURE
Governance
Managerial
Operational
Technical
Application # 2
Application # 4
Application #1
Controls
- Input controls
- Processing controls
- Output controls

Can a spreadsheet be "sensitive"?

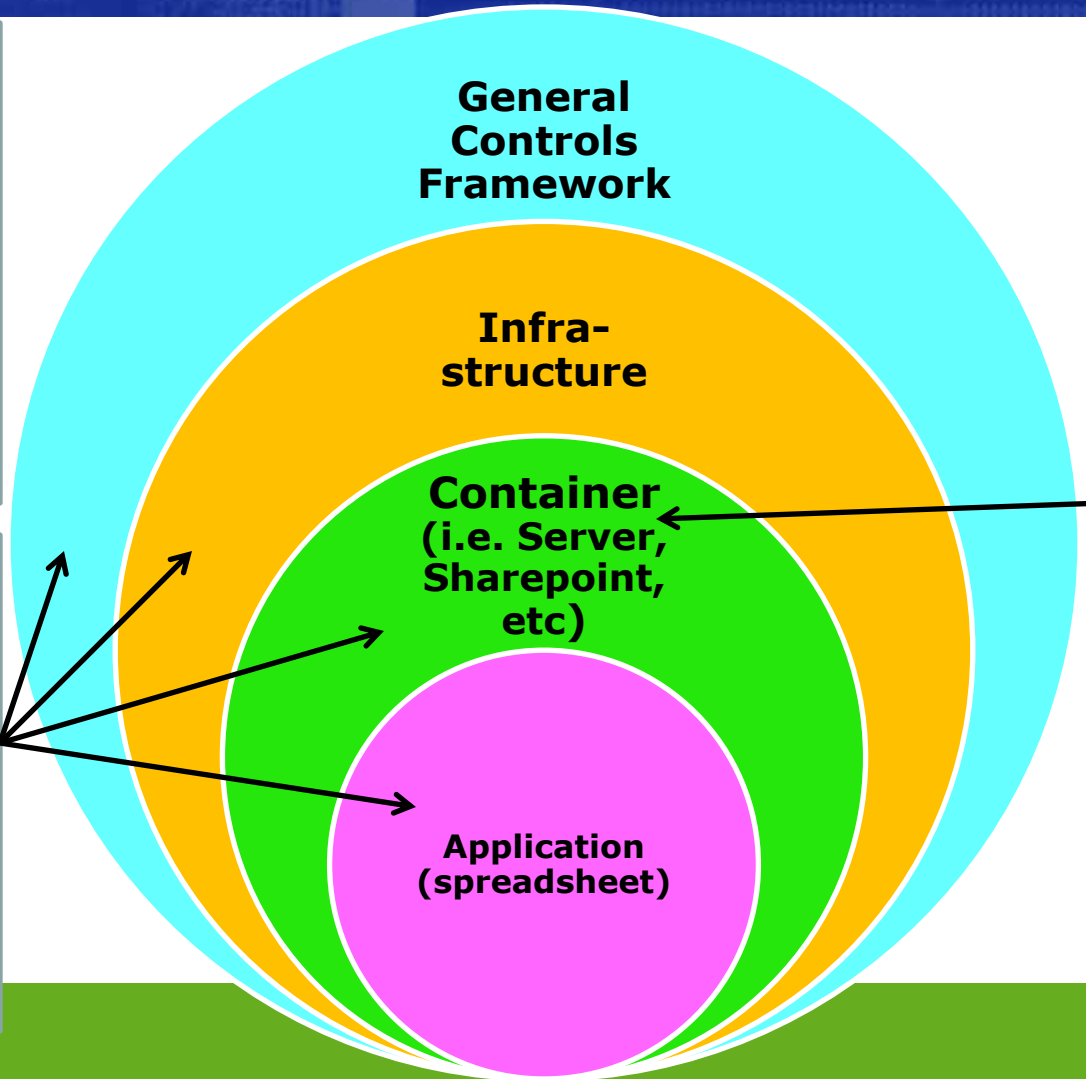


YES!

Can a spreadsheet be a sensitive *SYSTEM*?

A spreadsheet is a form of IT system & all business-critical IT systems must have adequate controls.

A Sensitive Spreadsheet, the same as any sensitive application, is protected at a number of levels.



In the case of a sensitive spreadsheet, the specific container where the spreadsheet resides is the sensitive system.

Spreadsheet Best Practices

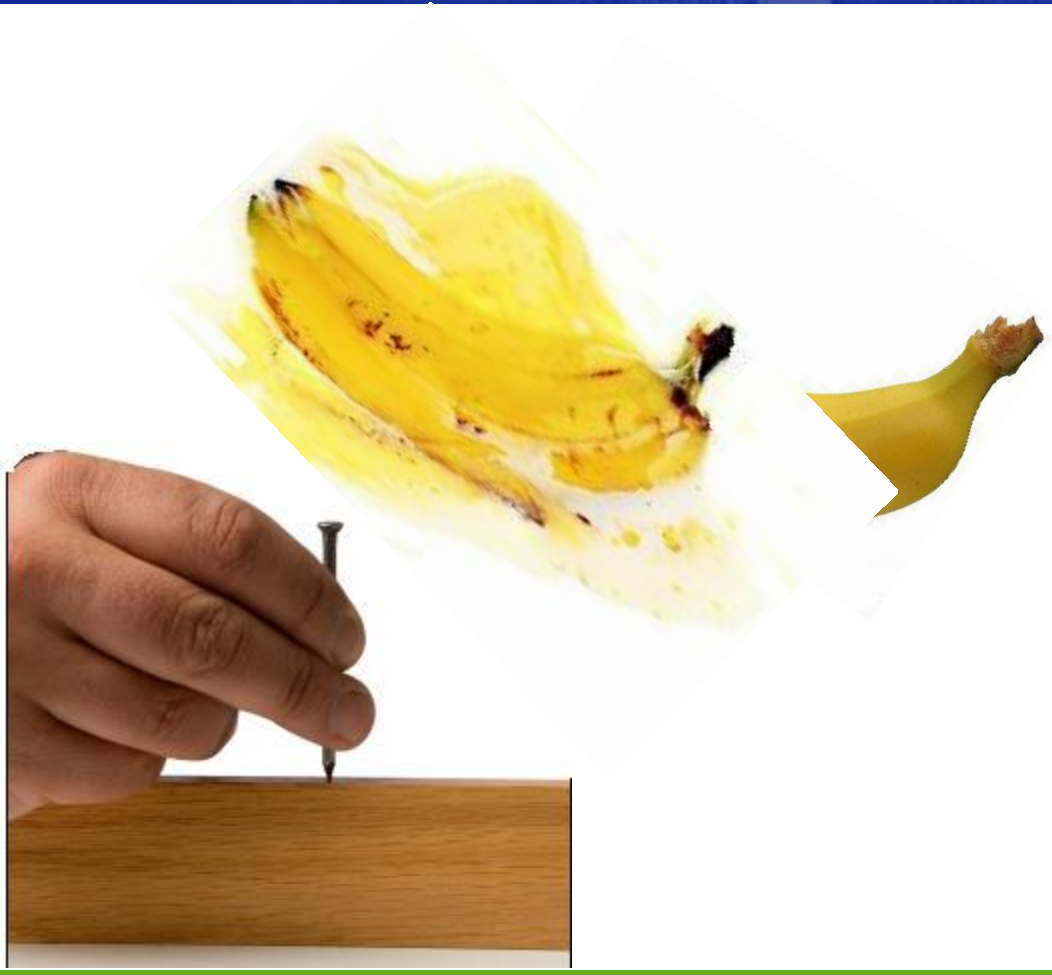
PRICEWATERHOUSECOOPERS

- 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

High Risk Spreadsheets



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

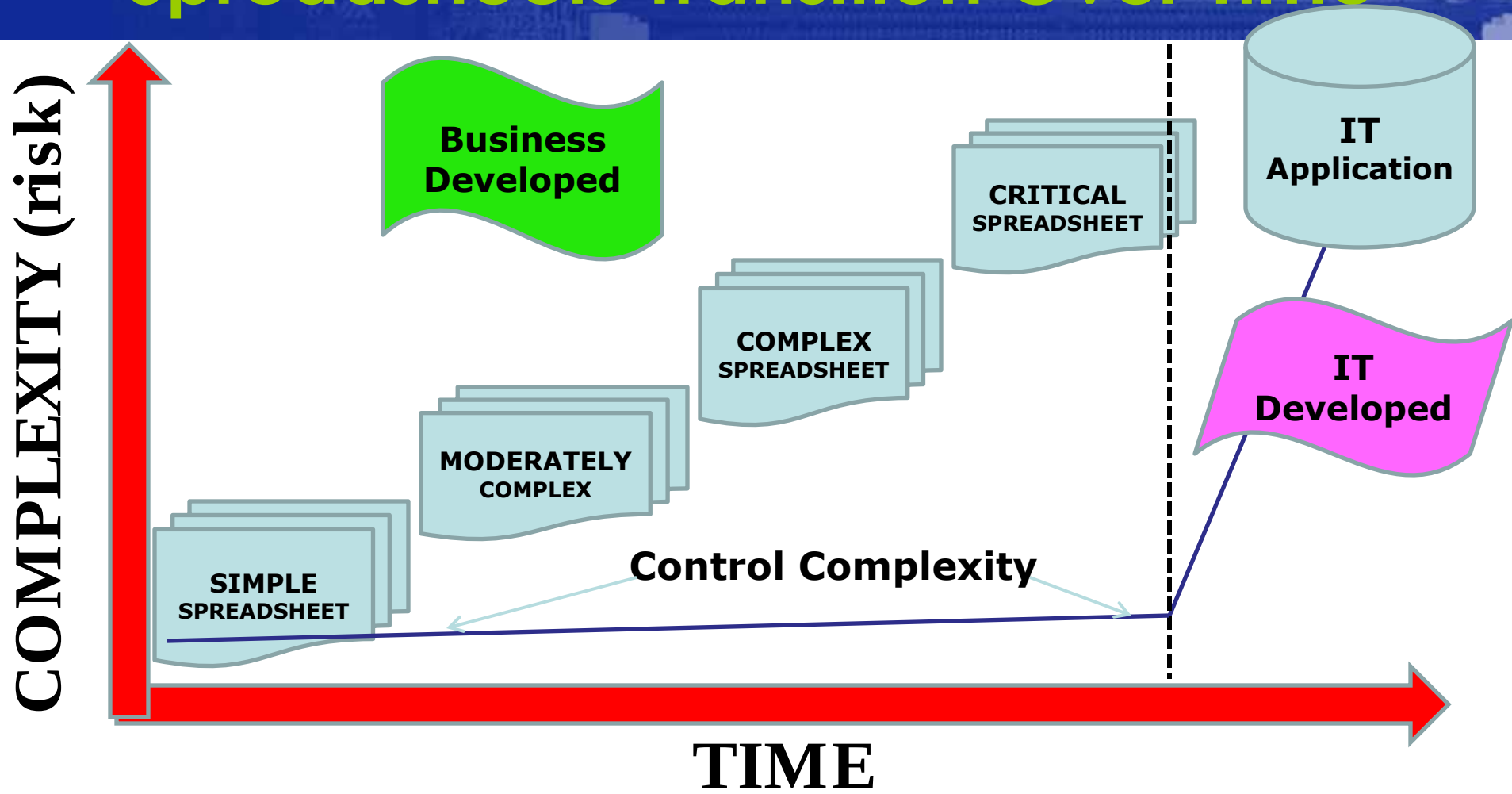
It's just not the right tool for the job!

Do spreadsheets ever get too complex?

"We have a clear corporate policy. Spreadsheets must not be used for business critical applications. That means they just don't tell us."

Investment bank CIO, 2008

Spreadsheets Transition Over Time



Determining Spreadsheet Risks

Likelihood (i.e. Complexity)

The more complex or complicated a spreadsheet is, the higher the **likelihood** of errors or issues and the greater the need for controls.

Impact (i.e. Use)

What the spreadsheet is used for is a good indicator of the **impact** the spreadsheet may have on agency risk. The closer a spreadsheet is to decision making, financial data or PII, the higher the risk and need for controls.

Attributes of Complex Spreadsheets

Evaluate how "complex" or complicated is the spreadsheet to determine the "likelihood" that the spreadsheet has an error.

LOW: SS's with ***limited*** complexity are usually relatively small in size & have few formulas or calculations.

MODERATE: ***Moderately*** complex SS's perform moderately complicated 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 is often large in size, has multiple users & may have frequent changes & updates.

Virginia Information Technologies Agency

Attributes of Spreadsheet Impact

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.

LOW IMPACT=OPERATIONAL /ADMINISTRATIVE: *Errors would have no real long-term impact.* SS's used to track, monitor or log data to support operational & admin processes. May also include "ad hoc", transitional, or temporary spreadsheets.

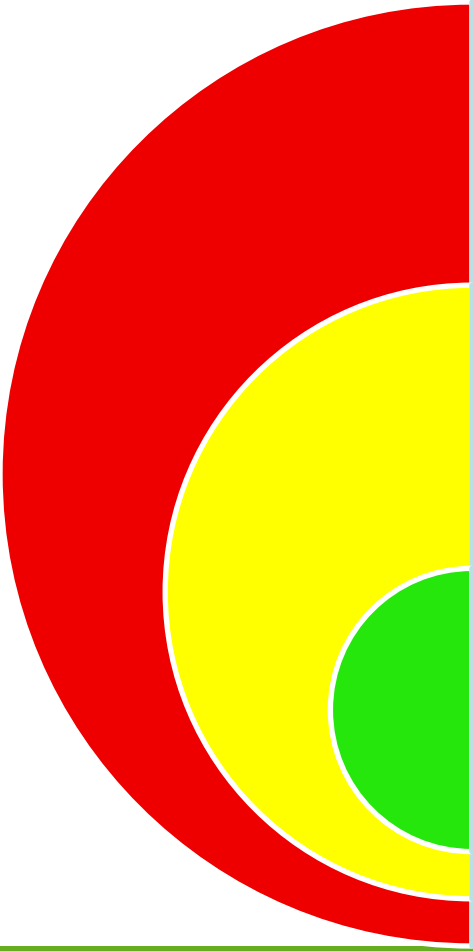
MODERATE IMPACT=ANALYTICAL: *An error or delay could result in a material impact or a materially incorrect decision.* SS's used to support analytical & management decision making.

HIGH IMPACT=FINANCIAL/COMPLIANCE/PII/PHI : *An error or delay could result in a highly significant loss, a critical mistake or embarrassment to the agency.* 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), customer records, etc. or contain sensitive or personally identifiable information (PII) like SSN's.

Determining Spreadsheet Controls

	COMPLEXITY: LIKELIHOOD		
USE: IMPACT (type of spreadsheet)	**LOW Complexity**	**MODERATE Complexity**	**HIGH Complexity**
Financial/PII/PHI (High Impact)			**Implement complex controls**
Analytical (Moderate Impact)		**Implement moderate controls**	
Operational/Administrative (Low Impact)	**Implement simple controls or accept risk**		

Controls for Spreadsheets



High Risk: Complex Controls	•Logic Inspection •Security & Data Integrity •Input Validation •Peer Review •Analytics (automated tools)
Moderate Risk: Moderate Controls	•Segregation of Duties •Change Control •Archives (Retention) •Standards & Guidelines
Low Risk: Simple Controls	•Access Control •Version Control •Backups •Documentation •Training

What do spreadsheet controls look like?

Control	Control Description
Segregation of Duties	Define user roles, authorities, and responsibilities for issues such as ownership, review, & usage. Include this information on the spreadsheet.
Documentation	Include documentation for important spreadsheets that briefly explains the purpose the spreadsheet, the procedures, key functions, key formulas, & usage instructions.
Change Control	Monitor, review, approve, test & track all changes made to a spreadsheet such as adding new formulas, columns, rows, format, or design enhancements. Consider Test vs. Production versions or spreadsheets.
Version Control	Use a naming convention when saving spreadsheets to ensure that only current & approved versions of spreadsheets are being used. Include name and path on the spreadsheet.

What do spreadsheet controls look like?

Control	Control Description
Access Control	Store spreadsheets on a secured server & in subfolders that are restricted to authorized employees. Use file level security and put passwords on sensitive spreadsheets.
Security & Data Integrity	Lock & protect all key cells that calculate, summarize or contain a formula that should not change. Ensure that data is secure by protecting cells, tabs, workbooks, formulas and restricted data.
Logic Inspection / Peer Review	Use peer review to inspect the logic in critical spreadsheets. This review should be conducted by someone independent, i.e. someone other than the user or developer of the spreadsheet.
Standards & Guidelines	Develop agency standards for spreadsheets to assure consistency in presentation, usage, and development.

What do spreadsheet controls look like?

Control	Control Description
Archive (Retention)	Maintain historical files of spreadsheets that are no longer in use in a segregated drive and lock them as "read only."
Backup	Implement a process to back up spreadsheets so that complete and accurate information is routinely and safely stored in case its needed.
Input Control	Ensure the accuracy & completeness of all inputted data. This may include cross-reference to other systems; reconciliation back to source documents; hash totals etc. This also includes the use of look-up tables, drop-down boxes, and colors & borders to identify areas for data input.

What do spreadsheet controls look like?

Control	Control Description
Analytics (Automated tools)	Use automated tools if you have a number of high risk spreadsheets & also the budget to get the tools. They will automatically scan & inventory your network for spreadsheets. Some analytic tools will review & perform diagnostics to determine formula logic errors or if inadvertent or fraudulent data manipulation has occurred.
Tokenization & Data Loss Prevention Tools (DLP)	Tokenization replaces things like SSNs, credit card numbers or bank account data with randomly generated characters called tokens. If tokenization is used in the centralized DBs, exported tokenized data will be useless if breached later in a spreadsheet. Many data breaches occur when sensitive spreadsheets are attached to email. DLP can monitor & prevent it.

link

Virginia Information Technologies Agency

Inventory & Risk Ranking Tool for Your Spreadsheets

Inventory & risk rank your spreadsheets!

Know *WHAT* it is, *WHERE* it is and *WHO* owns it.

Then determine if its:

Critical!

Merely important or significant

Don't really need to be worry about it

Business Owner to complete

General Information Relating to Each Spreadsheet or Small Database within the				Impact Consideration								Spreadsh
Insert Spreadsheet or Small Database Name	Insert Brief Description of Purpose of Spreadsheet or Small Database	Insert Location Saved	Primary User (Owner)	What is the materiality of this Spreadsheet or Small Database? (Select from drop down box)	Materiality Risk Level			Purpose of the Spreadsheet or Small Database (Select from drop down box)	Purpose Risk Level			Impact Risk Score
					Risk Level				Risk Level			
					Low	*Moderate*	*High*		*Low*	*Moderate*	*High*	
Example: Monthly Bank Reconciliation.xls	*To reconcile Wachovia bank account 12345-67 to the G/L account 100012*	*Finance Divisions's shared drive (server1\Finance\Share)*	*Michael Lewis*	Critical			1.5	Financial/Compliance/PII			1.5	3
Example: QualityControl.xls	*To track agency services & inquiries*	*Citizen Division's shared drive (server3/citdiv/)*	*John Johnson*	Material		1		Analy		1		2
				Immaterial	0.5					1		1.5
				Immaterial	0.5			al		1		1.5
				Immaterial				Analytical		1		1.5
				Immaterial				Analytical		1		1.5
				Immaterial				Analytical		1		1.5
				Im				Analytical		1		1.5
					0.5			Analytical		1		1.5
					0.5			Analytical		1		1.5
				al	0.5			Analytical				
				Immaterial	0.5			Analytical				
				Immaterial	0.5			Analytical				
				Immaterial	0.5			Analytical				
				Immaterial	0.5			Analytical				
				Immaterial	0.5			Analytical				
				Immaterial	0.5			Analytical				
				Immaterial	0.5			Analytical				
				Immaterial	0.5			Analytical				

www.irec.executiveboard.com

link

Business Owner to complete

General Information Relating to Each Spreadsheet or Small Database within the												Spreadsh
				Impact Consideration								
Insert Spreadsheet or Small Database Name	Insert Brief Description of Purpose of Spreadsheet or Small Database	Insert Location Saved	Primary User (Owner)	What is the materiality of this Spreadsheet or Small Database? (Select from drop down box)	Materiality Risk Level			Purpose of the Spreadsheet or Small Database (Select from drop down box)	Purpose Risk Level			Impact Risk Score
					Risk Level				Risk Level			
					Low	*Moderate*	*High*		*Low*	*Moderate*	*High*	
Example: Monthly Bank Reconciliation.xls	*To reconcile Wachovia bank account 12345-67 to the G/L account 100012*	*Finance Divisions's shared drive (server1\Finance\Share)*	*Michael Lewis*	Critical			1.5	Financial/Compliance/ PII			1.5	3
Example: QualityControl.xls	*To track agency services & inquiries*	*Citizen Division's shared drive (server3/citdiv/)*	*John Johnson*	Material		1		Analytical		1		2
				Immaterial	0.5			Analytical		1		1.5
				Immaterial	0.5			Analytical		1		1.5
				Immaterial	0.5			Analytical		1		1.5
				Immaterial	0.5			Analytical		1		1.5
				Immaterial	0.5			Analytical		1		1.5
				Immaterial	0.5			Analytical		1		1.5
				Immaterial	0.5			Analytical		1		1.5
				Immaterial	0.5			Analytical		1		1.5
				Immaterial	0.5			Analytical				
				Immaterial	0.5			Analytical				
				Immaterial	0.5			Analytical				
				Immaterial	0.5			Analytical				link
				Immaterial	0.5			Analytical				

Virginia Information Technologies Agency

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

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

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**
   (start with a self assessment by spreadsheet owners)
4. **Identify gaps**
   (what controls do we need & what do we have)
5. **Remediate!**
   (implement needed controls)

Presentation Summary

You never finish a spreadsheet.

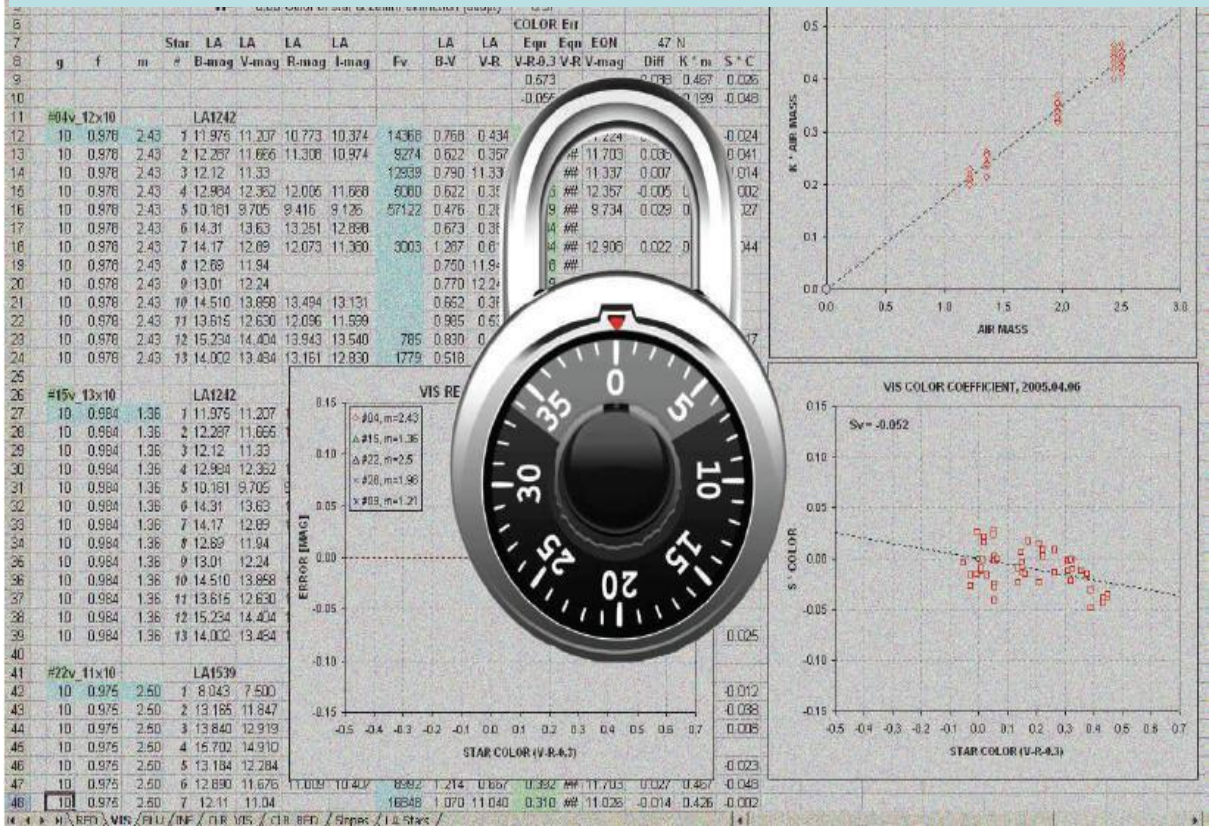
You just stop working on it.

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@vita.virginia.gov
or call:
804-416-6027

Thank you! Any Questions?



Upcoming Events

Future ISOAG

June 4 **1:00 – 4:00 pm @ CESC**

Keynote: **Tom Tollerton &**

Ben Sady

Dixon Hughes Goodman LLP

Topic: **NIST Cyber Security Framework**

ISOAG meets the 1st Wednesday of each month in 2014

IS Orientation

When: Thursday, June 5, 2014

Time: 1:00 pm to 3:30 pm

Where: CESC , Room 1211

Register here:

http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10

Next IS Orientation will be held on Sept 4, 2014

Submit Events

- If your group or organization is promoting a security related event and would like to have it communicated to the Information Security Officer community:

  Please submit all upcoming events to: **CommonwealthSecurity@VITA.Virginia.Gov**

ISOAG-Partnership Update

IT Infrastructure Partnership Team
Bob Baskette

7 May, 2014

ADJOURN

THANK YOU FOR ATTENDING

Picture courtesy of www.v3.co.uk