



Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

February 5, 2014



ISOAG February 2014 Agenda

- | | |
|---|---|
| I. Welcome & Opening Remarks | Bob Baskette, VITA |
| II. Are You the Next Hack? | Karen McDowell, UVA |
| III. Archer | Ed Miller, VITA |
| IV. 2013 Penetration Test | Bob Baskette, VITA |
| V. Upcoming Events | Bob Baskette, VITA |
| VI. Partnership Update | Bob Baskette, VITA
Michael Clark, NG |



Karen McDowell, Ph.D., GCIH
Information Security, Policy, and Records Office - ISPRO
University of Virginia

ARE YOU THE NEXT HACK?

Target Breach: Any Lessons Learned?



Neiman Marcus Breach

- 1.1 million credit and debit cards involved
- Possibly same Eastern European or Russian group that hacked Target
- Both companies experienced prior, smaller scale breaches



BlackPOS - Possibly

- Hackers had persistent access (APT?)
- Control server within Target's internal network for some months
- Not sophisticated



Best1_user and BackupU\$r

Anyone know these credentials?



Europay, Mastercard and Visa

- EMV: European Chip and PIN cards – chip embedded payment cards
- US uses Magnetic-striped payment cards, chip and signature



Anatomy of a Hack

- Step 1: Do Reconnaissance
- Step 2: Attract the Victim
- Step 3: Gain Control
- Step 4: Exfiltrate Data and conscript computers



Overall: Cloak Source

- Hackers routinely penetrate major universities, routing attacks through them.
- Millions of attacks weekly, as many as 100,000 a day from China (Wisconsin)
- Decentralized universities are porous and create perfect proxies.
- University employees are prime targets

**Universities Face a Rising Barrage of Cyberattacks, New York Times 7/17/2013*

Antivirus is Only a Speed Bump



- Attacks routinely bypass antivirus
- Viruses are moving targets in arms race
- Zero-day attacks

APT and Spear Phishing

- RSA Hack, Pentagon, Lockheed Martin, Oak Ridge Labs, New York Times, Northrup Grumman, Capital One, Chase, Zappos, College Board, etc.



The New York Times



Store

Mac

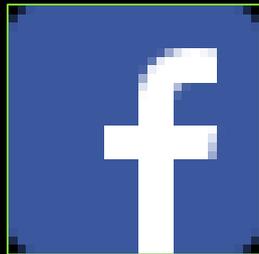
iPod

iPhone

iPad

iTunes

Support



REUTERS

EDITION: U.S.



Adobe



Microsoft

Google

THE WALL STREET JOURNAL.

Deceit by Any Name

- Phishing
- QRishing
- Smishing
- Spear phishing
- USBishing
- Vishing

A Cautionary Tale



Robin Sage

- 25-year old female
- Naval Network Warfare Command
- Cyber threat analyst
- Internship at the NSA
- Educated at MIT
- New Hampshire prep school
- Ten years work experience

Moral of the Robin Sage Story

- Just because it's on social media doesn't mean it's true.
- Limit the amount of personal information you post online.
- Remember, what goes on the Internet, stays on the Internet.
- Nobody loves you on the Internet.



Login to Social Media Accounts



Only by typing in the URL –

Do not respond to social media email requests



1-877-929-7168 has invited you to join
Twitter!

Accept invitation

Twitter helps you stay connected with
what's happening right now and with
the people and organizations you care
about.

Social Media Basic Protection

- Limit amount of PI you share on any social media account
- Don't respond to email requests to do anything on social media.
- Instead login to the account and see what's going on...may be a scam.

- Logout of any VPN session before you login to any social media site.
- Never accept a request by email or text to connect on social media.
- Never accept a download/plugin from any social media site.

Using Social Media While at Work

Even If Legit, Verify!

Subject: Karen, you have notifications pending

facebook

Hi Karen,

Here's some activity you may have missed on Facebook.

 8 notifications



Someone, someone, someone and someone have posted statuses, photos and more on Facebook.

You have missed some popular stories:

 someone commented on someone's photo.

 Someone commented on someone's status.

Verify Sponsored Ads, Any Ads

Ads related to **phones** ⓘ

[Sprint® Online Offer - sprint.com](#)

www.sprint.com/ ▼

Switch Today and Save \$100 on Select Android **Phones**. Learn More.

[Samsung Galaxy Note 3](#)

[Easy Pay Installment Plan](#)

[Shop Sprint Phones](#)

[Sprint Corporate Discount](#)

[T-Mobile® Phones on Sale](#)

www.t-mobile.com/Phone-Sale ▼

Our most popular **phones** are on sale for a limited time only. Order now.

[U.S. Cellular® Wireless - uscellular.com](#)

www.uscellular.com/Phones ▼

Get a New **Phone** Faster Without Signing a New Contract! Visit Now.

Stay Away from ASK.COM!!

- Installs one or more toolbars, masquerading as Search bars
- Loads the Registry with all kinds of ugly stuff
- Hijacks your home page
- Slows your computer to a crawl
- Stay away from ooVoo, Ask.com in Sponsored Links, Codecs, etc.



ORACLE

We recommend installing the **FREE** Browser Add-on from Ask



Get the best of the Web delivered to you!

Receive Facebook status updates directly in your browser, listen to thousands of top radio stations, and get easy access to search, YouTube videos, local weather, and news. Supports Internet Explorer and Mozilla Firefox.

Install the Ask Toolbar and make Ask my default search provider

By installing this application and associated updater, you agree to the [Terms and Conditions](#) and [Privacy Policy](#). You can easily remove this application at any time.

Cancel

Next >

Beware Sponsored Ads in Browsers

Ads ⓘ

[iPhone 4 Instructions](#)

www.ask.com/iPhone+4+Instructions

View **iPhone 4** Instructions.

Get Answers Now on Ask.com!

Think Twice Before Accepting Bundled Software



Step: 1 of 3

Adobe Flash Player



Version 11.9.900.152

[System requirements](#)

Your system:

Windows, English

[Are you an IT manager or OEM?](#)

Optional offer:

- Yes, install free **McAfee Security Scan Plus** to check the status of my PC security.

 **McAfee** Security Scan Plus

[Learn more](#)

Terms & conditions:

By clicking the "Update now" button, you acknowledge that you have read and agree to the [Adobe Software Licensing Agreement](#) and the [McAfee Security Scan Plus License Agreement](#).

Note: Your antivirus software must allow you to install software.

Update now

Total size: 17.3 MB

Do I Need This Download?

- Treat any "Please update me" message as a notification that it's time to do a manual update – type "adobe.com" in the browser's address bar
- Difficult to do this with Java updates



Especially in social media, including YouTube

- **Never** accept a download from YouTube.
- If you think you need the software, type in the URL yourself and verify.



Ransomware *CryptoLocker* [.zip]

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally view this.

Encryption was produced using a **unique** public key [RSA-2048](#) generated for this computer. To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files.

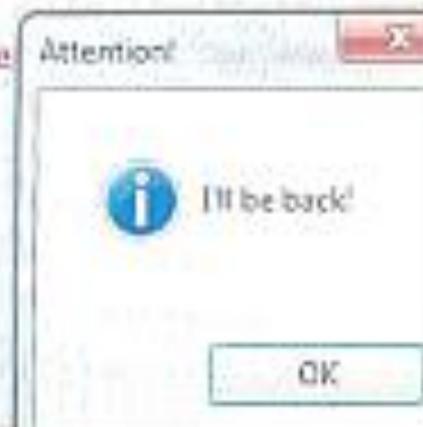
To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR / similar amount** in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will result in the **destruction of the private key by server**.

Private key will be destroyed on
10/7/2013
2:08 PM

Time left
71 : 50 : 49



Four Hallmarks of Phishing

- Asks you to take action
- Timing
- Unsolicited
- Urgent



They are hiring grammarians, so don't bet on bad grammar.



Security Issue

For your protection, we have locked your online banking access.

To regain access, click : [Sign On to WellsFargo Online](#) and proceed with the verification process.

Goes to:

<http://rumihotel.com/rumivr/rumidata/rumi1/1/3/index.html>

Wells Fargo safeguards your account when there is a possibility that someone other than you is attempting to sign on.

Target Email to Customers

- Three phishing indicators
 - Unknown address
 - Generic greeting
 - Prompting action to click on an ID theft insurance link
- Two other major errors
 - “Don't click links within emails you don't recognize.”
 - “..ask for a call-back number”

Intended Consequences

- Hackers spear phish using stolen credentials, widen their net
- Devastating consequences if same or similar password used on all sites
- Worst case scenario to use the same password for different accounts



Spear Phishing at UVa

We have noticed that some of our EMPLOYEE ACCOUNT have been compromised. You are to [CLICK HERE](#) and verify your account so that we can effectively thwart the damage done by phishing on our network..

Goes to: `hxxp://admin-now-forward.info/employee-self-service/email-healthcare.html`

Regards,

Systems Security Department

Fed Ex

Order: KGH-6753-59378246

**Order Date: Thursday, 24
January 2013, 10:24 AM**

Dear Customer,

Your parcel has arrived at the post office at January 29. Our courier was unable to deliver the parcel to you.

To receive your parcel, please, go to the nearest office and show this receipt.

**GET & PRINT
RECEIPT**

Best Regards, The FedEx Team.

----- Original Message -----

Subject: Special Order Delivery Problem

From: "Walmart Delivery Agent" <southfla@hospitalitystaff.com>

Date: Sun, December 29, 2013 5:55 pm

To:

Walmart

Save money. Live better.

Sir/Madam,

Your order WM-001193908

delivery has failed because the address was not specified correctly.

You are advised to fill this form and send it back to us.

If your reply is not received within one week, you will be paid your money back but 17% will be deducted since your order was booked for Christmas holidays.

2013 Wal-Mart Stores, Inc.

Dear Faculty Staff & Employee Email Subscribers

Welcome to 2014 Academic Session

Your Email Account have been put on-hold by our server, you can no longer send or receive emails, to

avoid this kindly click on the link [UPGRADE](#) to submit

your old account for New to enable you to send and receive emails

Goes to: <http://itshelpdeskupgraderoutine.bravesites.com>

Thank You

ITS Service Provider Team

Google Docs Phishing

Dear Customer,

As part of our year 2013 Email Security Upgrade, Admin Helpdesk Support require you to immediately update your account information by following the reference link below to prevent your Email address not to be de-activated on our Email service database.

CLICK the secured link Below****

<https://docs.google.com/a/blumail.org/spreadsheet/viewform?formkey>

Failure to confirm and verify your email account on our database as instructed, Your e-mail account will be blocked in 24 hours.

Thank you for your cooperation.

©2013 Email System Admin.

Eubank

Funeral Home &
Cremation Services

For this unprecedented event, we offer our deepest prayers of condolence and invite to you to be present at the celebration of your friends life service on Sunday, January 26, 2014 that will take place at Eubank Funeral Home at 11:00 a.m.

Please find invitation and more detailed information about the farewell ceremony [here](#) .

Goes to - <http://thevaldmans.com/box/w4wx5ye.../funeralinvitation>

Best wishes and prayers,

Funeral home receptionist,
Ryan Jensen

Dear Mailbox User,

Please be informed that your Email account on file has been listed for suspension and will be disabled shortly if not Activated Now. Errors were discovered in your account. For security reasons, you are required to secure and [please click here](#) to Upgrade your mailbox and its quota size.

<http://admin-mail-upgrade-portal.jigsy.com/portal>

ITS help desk

ADMIN TEAM

© 1995 - 2014 Outlook Communications

Phind the phish



Dear Account User:

Your account has been violated by a third party. Unauthorized usage and access of your account from a different location you haven't used before. You are to verify your account with 24 hour. Failure to verify your account within this period, your account will be deactivated and suspended.

TO VERIFY YOUR ACCOUNT CLICK ON VERIFICATION PORTAL: [CLICK HERE](#)

Goes to: <http://webmailhelpdeskwebs.com>

SERVICE DESK - IT HELP DESK

©COPYRIGHT 2014 WEB-TEAM. ALL RIGHT RESERVED.

Hand Crafted Spear Phishing

ACH Processing Service

SUCCESS Notification

We have successfully processed ACH file 'ACH2013-02-20-2.txt' (id '894.799') submitted by user 'blc6v' on '2013-02-20 18:57:28.6'.

FILE SUMMARY:

Item count: **346**

Total debits: **\$619,335.87**

Total credits: **\$619,335.87**

For more details [click here](#)

Hackers Exploit Our Trust



QRishing

- Link Shorteners: bitly.com, tinyURL
 - <http://1.usa.gov/1aCGgb5>
- QR Codes



<http://bit.ly/173aD6i> add +



Do more with your links. [Learn More](#)

Join now. It's free!

[Sign in](#)

Feds shut down Silk Road, arrest alleged admin Dread Pirate Roberts | Ars Technica

<http://arstechnica.com/tech-policy/2013/10/feds-shut-down-silk-road-arrest-alleged-admin-dread-pirate-roberts/>



Global bitly link
first created on Oct 02, 2013.



2,742

total clicks

bit.ly/173aD6i

Copy



Traffic to this link peaked at **2,335** clicks on **Wed Oct 02 2013**.

Clicks

Link Shorteners

- Bit.ly <http://bit.ly/173aD6i> add +
- TinyURL > Enable Preview
- goo.gl > previews in Google
- t.co > previews in Twitter/tweets

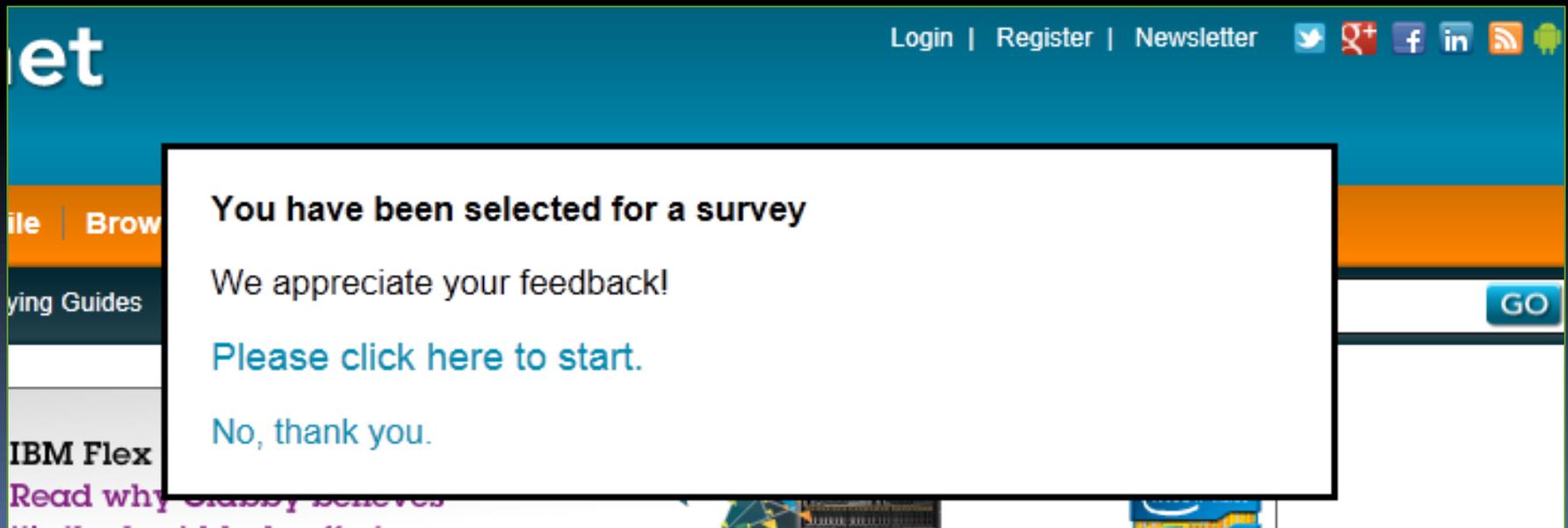
Smishing



**GATEWAY BANK
ALERT: Your card
starting with 4138*
has been
DEACTIVATED .
Please contact us
at 804-414-7700.**

VISHING by Land or Cell

- Your account needs updating...
- Register for free prizes!
- Your credit card has been deactivated...
- Surveys



The screenshot shows a website interface with a teal header. The word "et" is visible on the left. In the top right, there are links for "Login | Register | Newsletter" and social media icons for Twitter, Google+, Facebook, LinkedIn, RSS, and Android. A white pop-up box with a black border is centered on the page, containing the following text:

You have been selected for a survey

We appreciate your feedback!

[Please click here to start.](#)

[No, thank you.](#)

Below the pop-up, a search bar with a "GO" button is visible. The background shows a navigation menu with "file | Brow" and "ying Guides", and a section for "IBM Flex" with a link to "Read why Glassy believes".

Vishing: Tech Support Scams

Hello, we are calling from Windows and your computer looks like it is infected. Our Microsoft Certified Technician can fix it for you.

Social Engineering by USB!

- Credit union hired a penetration tester to seed 20 USB sticks with a Trojan and scatter them in the parking lot before work.
- 15 credit union employees plugged into the network with these sticks
- Moral of the story?

Money Mules



Hello,

Please email me if you can spare few hours a week and you need an extra income.

All that you do is based online. You set your own schedule. The job includes mostly survey completing and data entry. No experience required.

Best regards,
Sarah Jones

Cover Your Webcam – Sticky?

- Wide variety of webcams, IP surveillance cameras and baby monitors made by China camera giant contain software bug





Are Smart Phones Secure?

- Easily lost or stolen
- Maintain Situational Awareness
- Consider Defense-in-Depth



Defense-in-Depth for Phones

- Turn on GPS, Geotagging, Bluetooth and NFC, only when necessary
- Verify SMS/text messages independently to avoid *smishing*
- Take initiative to update system and application software
- Know "Remote wipe" option
- Enable "Ask to join networks" function on iPhone

Android, iPhone, Blackberry

- Passcode

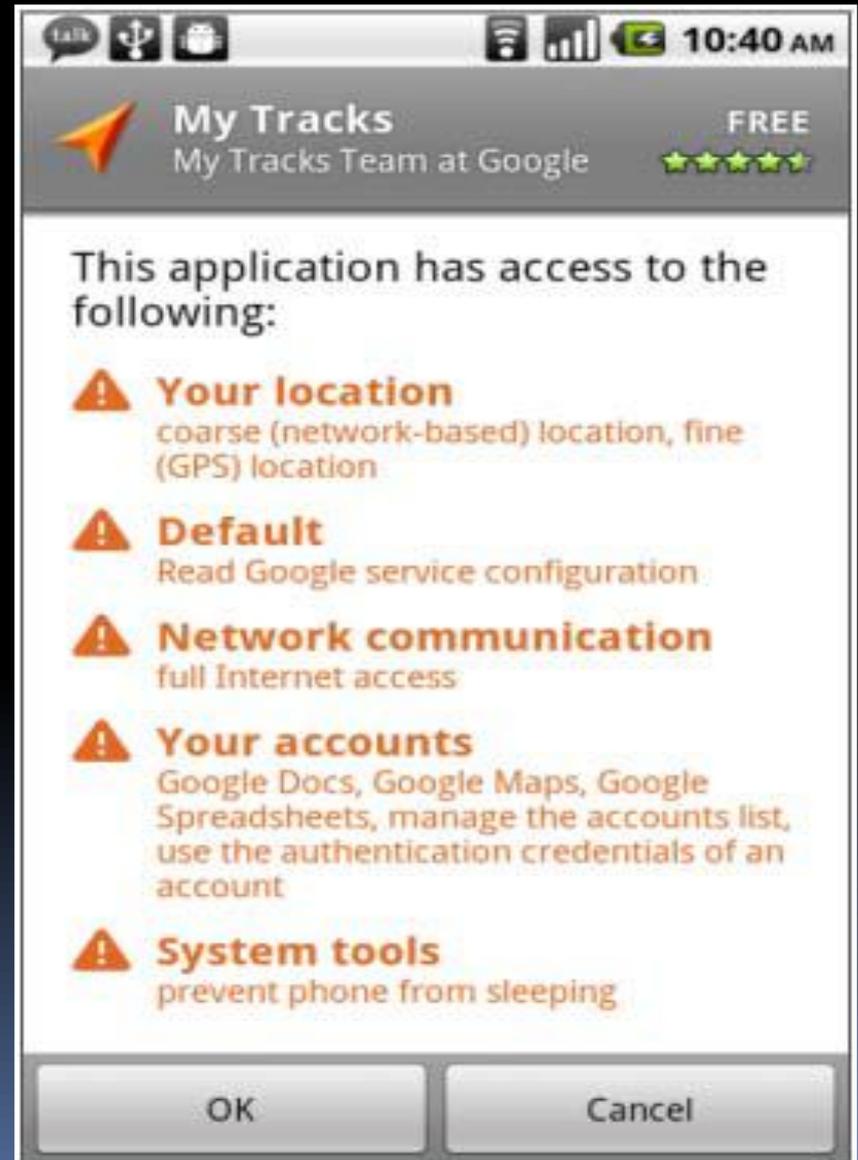
- Enable at least 4 digits but this also depends upon IT policies
- Exceeding the number of allowed password attempts deletes all data

- Auto-Lock

- Locks the screen after a pre-set time period of non-use (consider 30 minutes or less)
- Passcode-lock enhances auto-lock

Are Market Place Downloads Safe?

- Do not click “Install” before you review.
- Do you want this app to have so much access to your information?
- Think before you app!



Best, Free Protection

- Lookout Mobile Security
 - <https://www.lookout.com/>
- Verizon Mobile Security
 - <http://www.verizon.com>
- Vipre Mobile Security
 - <http://www.vipremobile.com/>

Gmail "2-step" verification



Accounts

Account

Password management

Change password

Account recovery options

Security

Products

Data liberation

2-step verification ?

Status: ON

Edit

Authorizing applications
and sites ?

Edit

Password Guesser

out.12920:join: Oct 21 14:36:33 Gussed akovacs (/usr1/bin/badpasswd in
maxwell.passwd) [**morrison**] .AB8KhkzFZkCc

out.12920:join: Oct 21 14:36:33 Gussed dsummers (/usr1/bin/badpasswd in
maxwell.passwd) [**w0mbat**] /P8idUdpMO/6Q

out.12920:join: Oct 21 14:36:33 Gussed crockett (/usr1/bin/badpasswd in
maxwell.passwd) [**bxxxsxxx**] 2ULXddBrRGI.I

out.12920:join: Oct 21 14:36:33 Gussed jlucas (/usr1/bin/badpasswd in
maxwell.passwd) [**stealth**] 6KIlfIIF00qP6

out.12920:join: Oct 21 14:36:33 Gussed cminton (/usr1/bin/badpasswd in
maxwell.passwd) [**Faustus**] 6hiuZITiFmIX.

Automated Password Cracking

Password Managers

- Stand-alone
 - 1Password (~\$50/yr)
 - Dashlane (free & premium 19.95/yr)
 - KeyPass (open source & free)
 - LastPass (free & premium ~\$12/yr)
 - PasswordSafe (open source & free)
- Built into the browser
 - I don't trust them, though they claim to encrypt passwords

Google Yourself Once a Month



Google - images: <your name>

Wireless Network Tips

- Use WPA2 encryption on router
- Change the default SSID *and* the default login and password
- Create strong passwords for all devices including printers
- Install an alternate DNS provider, like OpenDNS, or Norton DNS

Public Hotspot Wireless Insecurity



Do not use your login credentials to access email, banking or any sensitive data in public hotspots.

International Travel

- Before you go...Acquire a temporary device & email account, prepaid, throwaway phone. Strong passwords
- While you're there...assume anything you do will be intercepted. Keep devices with you at all times.
- When you return...Discontinue use of device. Reformat, reinstall, dispose, change passwords
- Read *Traveling Light in a Time of Digital Thievery* NYT 2/10/2012

Speedtest.net



Test your speed.
Then try again with a fast, free web browser.

Download Google Chrome

BEGIN TEST

Slow speeds?

Make your PC faster by fixing system issues



137.54.3.87
University of Virginia

★★★★★ Rate Your ISP

5,296,718,685

START
SCAN

Update Software

- File Hippo

<http://www.filehippo.com/updatechecker/>

- Apple Mac Updates

- Microsoft Updates

- Qualys <https://browsercheck.qualys.com/>

- Secunia Personal Software Inspector

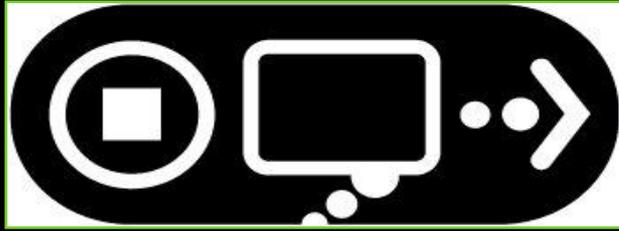
http://secunia.com/vulnerability_scanning/personal/

Top Seven Human Risks

- Phishing
- Poor password security
- Failing to patch or update devices
- Insecure use of mobile media
- Sharing too much on social media
- Not realizing you are a target
- Accidentally disclosing or losing data

Top Risks in 2014

- Targeted phishing aka spear phishing continues to become more sophisticated
- Confidential data or PII in the cloud or in transmission lost or stolen
- Malware on mobile devices
- International travel with data assets
- Retail and data broker breaches



stopthinkconnect.org

You would be surprised
how easy it is to hack
your computer...

STOP.THINK.CONNECT



Introduction to ARCHER

Ed Miller

edward.miller@vita.virginia.gov

804-416-6027



What is Archer?

- Archer is the Commonwealth repository of IT Security Information.
- We are using Archer to collect and analyze:
 - IT security audit information
 - Business impact analysis information
 - Risk assessments
 - Security incidents
- Archer is the source of calculations for “Data Points”



Data Points

Plan on seeing a “data points” email, on or around February 11th.

Please review it carefully. We want to get this as “final” as possible in the next few weeks.



Accessing Archer

- All primary ISOs have been setup as users in Archer. For now, each agency can have up to 2 ISO users setup.
- If you're a primary ISO and find that you don't have, but need access to Archer, please send an email to commonwealthsecurity@vita.virginia.gov. If you're a primary ISO and want a backup ISO to have access, also send an email.

Accessing Archer

- To access Archer, you need VPN access with 2 factor authentication





Accessing Archer

- Login to VPN
- Open your browser to this address:

<https://itgrcs.vita.virginia.gov>

Single sign-on

NOTE: you could run in to some version issues with IE that inhibit your login. Let me know, I've got some work arounds.



Archer

- Archer consists of a number of database tables. These are the main ones:
- Agency
- Application
- IT Security Audits
- Business Processes
- Incidents



Agency Table

- The Agency table contains demographic information about your agency.
- It is also the place where data points and other metrics are accumulated and summarized.



Agency: Virginia Information Technologies Agency

New Copy Save Apply Edit Delete Recalculate Export Print Em

First Published: 8/6/2013 8:43 AM Last Updated: 12/23/2013 8:40 PM

► About

▼ General Information

Agency Name:	Virginia Information Technologies Agency	Agency Acronym:	VITA
Web Site:	http://www.vita.virginia.gov	Partnership Full Service Customer:	Yes
Agency Number:	136	Number of Employees:	
Agency Secretariat:	Technology	Government Branch:	Executive Branch
Annual Report Governance (subject to):	Yes		
Description:			



▼ Agency Scorecard Data

ISO Certification Status:		Previous Year ISO Certification Status:	
3 Year Audit Obligation:	7 %	3 Year Audit Obligation - Previous Year:	7 %
Current Year Percentage of Audits Received:	0 %	Previous Year Percentage of Audits Received:	0 %
Current Year Percentage of Quarterly Updates Received:	0 %	Previous Year Percentage of Quarterly Updates Received:	100 %
Audit Plan Status:		Audit Plan Status - Previous Year:	
Business Impact Analysis Status:		Business Impact Analysis Status - Previous Year:	
3 Year Risk Assessment Obligation:	33 %	3 Year Risk Assessment Obligation - Previous Year:	33 %
Current Year Percentage of Risk Assessment Received:		Previous Year Percentage of Risk Assessments Received:	



▼ IT Security Audits (Agency)

Audit Plan ID	3 Year Period End	3 Year Period Start Date	Date Audit Plan Expires	Number of Audits Past Due	Percentage of Audits Complete
AP-212160	2014	1/1/2012	7/17/2013	10	11 %
AP-221052	2016	1/1/2014	12/5/2014	3	0 %

▼ Infrastructure Metrics

Total Applications:	101	Total Processes:	117
Total Sensitive Systems:	15	Total Critical Business Processes:	20
Total Information Assets:	0	Total Devices:	0
Total Products & Services:	0	Total Facilities:	0

▼ Agency Headquarters Information

Address:	11751 Meadowville Lane	Google Map:	Google Map
City:	Chester	State:	
Zip Code:	23836		



Application Table

- The Application table contains information about all of your agency's applications.
- If your agency is subject to using CETR (Commonwealth Enterprise Technologies Repository), we routinely import this data from CETR into Archer. Otherwise, analysts at VITA enter your applications based on the audit plan you submitted.



Application Table

- In addition to maintaining (duplicating) the information in CETR, we are also tracking some additional information:
- Date of next audit / Date of last audit
- RPO / RTO that you reported
- The business processes that are dependent on the application
- Risk criticality of the application as to C-I-A
- Links to any audit findings related to the application



▼ General Information

Agency:	<u>Virginia Information Technologies Agency</u>	Agency Number:	136
Application Name:	Peoplesoft EPM Planning & Budgeting	Application ID:	APPID-205860
		Application Type:	
Last Updated:	12/18/2013 12:45 PM	IT Security Audits (IT Systems Scheduled to Audit):	<u>SA-212176</u> <u>SA-221122</u>
Description:	VITA's Internal Budget and Enterprise Planning Module System		
Recovery Time Objective (RTO):		Recovery Point Objective (RPO):	
Customer Impacting:	Yes	Customer Impacting Information:	
Sensitive System:	Yes		



▼ Application Risk Information

Inherent Risk:		Residual Risk:	
Confidentiality:		Integrity:	
Availability:		Criticality Rating:	
High Risk Vulnerabilities:	0	Risk Rating:	Not Rated
Last Agency IT Risk Assessment:	12/1/2011	Last IT Security Audit:	
Next Agency IT Risk Assessment:		Next Scheduled IT Security Audit:	

▼ Business Risk Information

Highest Business Function Confidentiality Risk:	High	Highest Business Function Integrity Risk:	Moderate
Highest Business Function Availability Risk:	Low	Count of Critical Business Functions:	1



Application Information

Parent Application

Personnel

▼ CETR

Application Identifier:	136AP0015	Application Acronym:	Budget/EPM
Application ID CETR:	1388	Application Category:	Agency
Status:	In production - with frequent business changes	Status Reason:	
Year Placed in Service:	2006	Year Last Major Update/Upgrade:	2007
Primary Business Application Domain:	Planning and Budgeting	Web Category:	Neither
Annual Cost to Support:	\$10,000-\$100,000	Subject to IT Audit:	No
Hosted by:	VITA	Hosted by (additional info):	
Deployment type:	Distributed servers	Deployment type (add'l info):	
Client type:	Thin Client - browser only	General Public:	No
Sensitive as to Confidentiality:	No	Confidential Data Description:	



IT Security Audit Table

- The data in this section tracks:
- Audit Plans: scheduled audit dates
- IT Security Audits: electronic copies of audit reports
- Findings (applied to the application associated with the finding and related IT security control)
- Corrective Action Plans & Quarterly Updates



IT Security Audits: AP-212160



New Copy Save Apply Edit Delete

Recalculate Export Print Em

General Information

Agency:	<u>Virginia Information Technologies Agency</u>	Audit Plan ID:	AP-212160
Date Audit Plan Submitted:	7/17/2012	Date Audit Plan Approved:	11/19/2013
3 Year Period Start Date:	1/1/2012	Date Audit Plan Expires:	7/17/2013
Number of Audits Past Due:	10	CSRM Approval:	Approved
3 Year Period End:	2014		
Audits Completed in Year One:	0 %	Audits Completed in Year Three:	0 %
Audits Completed in Year Two:	0 %	Percentage of Audits Complete:	11 %

Audit Plan Attachment

Name	Size	Type	Upload Date
FY13 - FY15 VITA IT Security Audit Plan.docx	22345	.docx	11/19/2013 3:28:42 PM



▼ Scheduled IT Security Audits

Scheduled Audit Tracking ID	IT Systems Scheduled to Audit	Scheduled Audit Description	Scheduled Audit Completion	Actual Audit Completion	All Audits Complete	CSRM Review Status
SA-212161	VITA Architecture Review	VAR	12/31/2009	10/1/2009	Yes	Approved
SA-212162	Computer Services Chargeback System	Computer Services Billing System	12/31/2013		No	Approved
SA-212163	Vendor Invoice Payment & Reconciliation	VIPER System	12/31/2013		No	Approved
SA-212164	Telecommunications Inventory Billing System (TIBS)	TEAM Telco Billing Systems	12/31/2013		No	Approved
SA-212165	Consolidated Personnel Information Repository (CPIR)	Consolidated Personnel Information Repository (CPIR)	12/31/2012		No	Approved
SA-212166	Personnel Action Application (PAA)	HR Admin – PAA	12/31/2012		No	Approved
SA-212167	People System	People System	12/31/2012		No	Approved
SA-212168	Peoplesoft Financials		6/30/2014		No	Approved
SA-212169	Comprehensive Billing - MBA - Direct Bill	Comprehensive Billing System	12/31/2013		No	Approved
SA-212170	Peoplesoft Financials		7/31/2012		No	Approved
SA-212171	VITA Application Security	VITA Application Security	12/31/2014		No	Approved



▼ Findings (IT Security Audit Findings)

Finding ID	Agency	Finding	Affected Applications	Status
FND-124	Virginia Information Technologies Agency	Improve the VAR System Access Policy to include noted processes & documentation or obtain an approved exception to the VITA Logical System Access Control Policy & Procedure	VITA Architecture Review	Open
FND-125	Virginia Information Technologies Agency	We have encrypted all attachments within the VAR application as an additional mitigation approach. We have also added the VAR replacement as part of an effort to have an overall solution for sensitive document management to the agency work plan.	VITA Architecture Review	Open
FND-126	Virginia Information Technologies Agency	We have encrypted all attachments within the VAR application as an additional mitigation approach. We have also added the VAR replacement as part of an effort to have an overall solution for sensitive document management to the agency work plan.	VITA Architecture Review	Closed
FND-127	Virginia Information Technologies Agency	We have encrypted all attachments within the VAR application as an additional mitigation approach. We have also added the VAR replacement as part of an effort to have an overall solution for sensitive document management to the agency work plan.	VITA Architecture Review	Open
FND-128	Virginia Information Technologies Agency	We have encrypted all attachments within the VAR application as an additional mitigation approach. We have also added the VAR replacement as part of an effort to have an overall solution for sensitive document management to the agency work plan.	VITA Architecture Review	Open



Business Processes

- Business processes identified from your agency's BIA
- Name and description of the process
- Identification of Mission Essential Functions
- BIA attributes for impact to confidentiality, safety, finance, legal/regulatory, customer services, etc.
- RTO of the process
- The applications that support this process



Business Processes: Payroll processing- Pan Flu



New
 Copy
 Save
 Apply
 Edit
 Delete

◀ Record 30 of 46 ▶

Recalculate
 Export
 Print
 Er

First Published: 9/1/2013 1:50 PM Last Updated: 9/10/2013 4:18 PM

▶ About

▼ General Information

Agency:	Virginia Information Technologies Agency	Process ID:	BPID-212123
Process Name:	Payroll processing- Pan Flu	Status:	Active
Risk Rating:		Compliance Rating:	Not Rated
First Published:	9/1/2013 1:50 PM	Last Updated:	9/10/2013 4:18 PM
Business Purpose:	To process payroll in an emergency situation should the office facilities not be available		
Description:			



Details

Business Impact Analysis

Mappings

▼ Personnel

Business Process Owner: Michael Watson

Agency Business Process Owner: Barbara Orr

▼ Business Process Attributes

Availability: Low

Confidentiality: High

Integrity: Low

Business Process Customer:

Mission Essential Function: No

Criticality Rating: 



Business Processes: Payroll processing- Pan Flu



New
 Copy
 Save
 Apply
 Edit
 Delete

Record 30 of 46

Recalculate
 Export
 Print
 Er

[Details](#) |
 [Business Impact Analysis](#) |
 [Mappings](#)

Business Impact Analysis

Operational Impact Description:			
Impact to Confidentiality:		Impact to Finances:	Not Rated
Impact to Customer Service:		Impact to Life:	Not Rated
Impact to Safety:	Not Rated	Regulatory Impact:	
Legal Impact:		Peak Period:	
Day 1:		Day 2:	
Day 3:		Day 4:	
Day 5:		Day 6:	
Week 1:		Week 2:	
Week 3:		Week 4:	
Manually Performed:	No	MTD:	



Details Business Impact Analysis **Mappings**

▼ Applications

Application ID	Application Name ▲	Agency	Criticality Rating
APPID-205857	<u>PAM Time and Leave Reporting</u>	<u>Virginia Information Technologies Agency</u>	🟡



Incidents

- IT security incidents are documented
- VCCC ticket number
- Incident Priority
- Description of the incident
- Assignment and resolution of the incident



▼ Event Information

Incident ID:	INC-40	Affected Agency:	<u>Virginia Information Technologies Agency</u>
Incident Summary:	VITA Web38 Un-Authorized Access	Status:	Closed
Date/Time Occurred:	5/25/2013 7:35 AM	Priority:	
Date/Time Reported:	5/25/2013 7:35 AM	Source:	
Date/Time Closed:	12/18/2013 12:00 AM	Priority Level:	Priority 2 (P2)
Days Open:	206	Intellitactics Ticket:	20130525113307700
VCCC Ticket Number:		Incident Category:	IT Malware
Incident Details:	VITA server Web38 was attacked, and accessed by an un-authorized person. Logs have been collected, along with forensic images of the servers hard drive. These are still being analyzed.		
Incident Access History:	View Access History	Related Incidents:	



Dashboards

- When you access Archer, the information in these main tables, plus others, will be summarized in a Dashboard.
- You can click and drill down through the dashboards on any hyperlinked area.

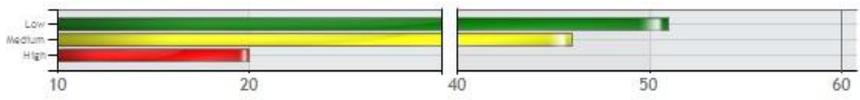


Dashboard: Agency Executive Dashboard

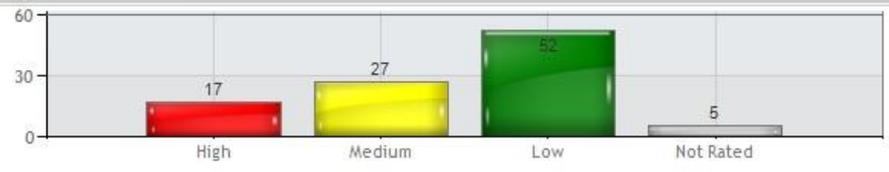
Welcome, Joe User

Agency Business Processes

Processes by Criticality Rating



Agency Applications



Agency Findings

Findings by Status



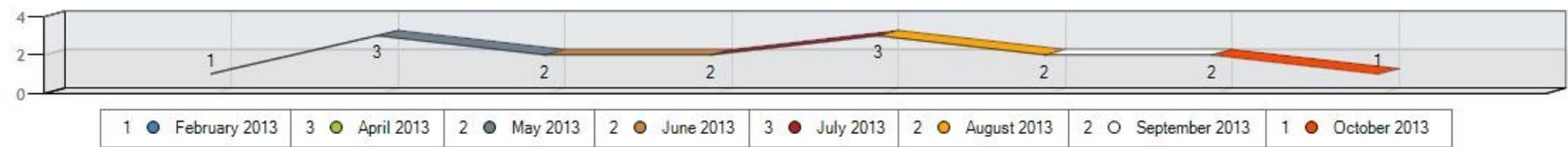
Agency Infrastructure Information

COV Asset Distribution

Agency Name ▲	Total Applications	Total Sensitive Systems	Total Processes	Total Critical Business Processes
Virginia Information Technologies Agency	101	15	117	20

Agency Incident Summary

Incidents Reported by Month





Agency Executive Dashboard

- **Agency Business Process**
 - Processes by Criticality Rating
 - Processes by Application
 - COV: Agency Application by Business Process
- **Agency Applications**
 - Processes by Criticality Rating
 - Processes by Application
 - COV: Agency Application by Business Process
- **Agency Findings**
 - Findings by Status
 - COV: Overdue Findings
- **Agency Infrastructure Information**
 - COV: Asset Distribution
 - Agency Datapoints
 - COV: Sensitive Systems Missing a Security Audit
 - COV: Systems with Sensitive Data
- **Agency Incident Summary**
 - Incidents Reported by Month
 - Most Recently Reported Incidents
 - Incidents Reported by Quarter
 - Open Incidents by Priority
 - Incidents by Status
 - Incidents Reported by Month and Priority



Agency Datapoints

Agency Name ▲	ISO Certification Status	Audit Plan Status	Audit Plan Status - Previous Year	Current Year Percentage of Audits Received	Previous Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	Previous Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	3 Year Audit Obligation - Previous Year	Business Impact Analysis Status	Business Impact Analysis Status - Previous Year	3 Year Risk Assessment Obligation	3 Year Risk Assessment Obligation - Previous Year
Virginia	●	●	●	0 %	0 %	0 %	100 %	7 %	7 %	●		33 %	33 %

ISO Certification Details

Name (Full)	Agency ▲	ISO Certification Status	ISO Designation Date	ISO Designation Expiration Date	Certifications are in Good Standing and CPEs are Complete	Date ISO Academy Classes Completed	ISO Third Party Certifications
Michael Watson	Virginia Information Technologies Agency	●	7/15/2013	7/15/2015	Yes	7/1/2013	Certified Information Systems Auditor (CISA)

Actionable Finding Information

COV: Overdue Findings

Finding ID ▲	Agency	Affected Applications	Name	Status	Criticality
FND-127	Virginia Information Technologies Agency	VITA Architecture Review	Define & document VAR encryption practices including noted areas	Open	●
FND-128	Virginia Information Technologies Agency	VITA Architecture Review	Define & document VAR encryption practices including noted	Open	●

Actionable IT Security Audit Information

COV: Scheduled IT Security Audit Issues

Audit Plan ID ▲ 2	Agency ▲ 1	Date Audit Plan Submitted	Date Audit Plan Expires	Number of Audits Past Due
AP-212160	Virginia Information Technologies Agency	7/17/2012	7/17/2013	10
AP-221052	Virginia Information Technologies Agency	12/5/2013	12/5/2014	3

Page 1 of 1 (2 records)

Actionable Application Information

COV: Applications Not Associated With Business Proce

Actionable Business Process Information

COV: Actionable Business Processes



Agency Actionable Dashboard

- **Actionable Finding Information**
 - Overdue Findings
 - Scheduled Finding Completion Dates
- **Actionable IT Security Audit Information**
 - Scheduled IT Security Audit Issues
 - Sensitive Systems Missing IT Security Audits
 - Upcoming Scheduled IT Security Audits
- **Actionable Application Information**
 - Applications not Associated with Business Processes
 - Critical Systems that are Not Sensitive
- **Actionable Business Processes**
 - Actionable Business Processes
 - Processes by Criticality Rating
 - Applications not Associated with Business Processes
- **Actionable IT Risk Assessments**
 - Sensitive Systems Missing IT Risk Assessments
 - Agency Application IT Risk Assessment Status



Dashboards

- Green is Good. Red is not so Good.
- BUT, these are mostly measurements of very high-level compliance issues in a few limited areas.
- Being “compliant” or “green”, does not mean your agency is secure. They are simply indicators at a particular point in time.



Dashboards

- “Compliant” organizations are not necessarily “secure”.
- However, organizations with excellent “security” are almost always “compliant”.
- Compliance is a stepping stone to being secure.
- And keep in mind, we are only measuring compliance in a limited (although important) area.

Live Archer Demo



Questions





Upcoming Events





Future ISOAG

March 5 1:00 – 4:00 pm @ CESC

Keynote: “Mobile Device Security”

with Jack Mannino

And

“SOA Security” with James Watwood

ISOAG meets the 1st Wednesday of each month in 2014



IS Orientation

When: Thursday, March 6, 2014
Time: 9:00 am to 11:00 am
Where: CESC , Room 1211

Register here:

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

Next IS Orientation will be held on Jun 5, 2014



VA TECH Hosting SANS IT Audit Class

- What:** **AUD507**
Auditing Networks, Perimeters & Systems
- When:** **March 10-15, 2014**
- Where:** **2150 Torgersen Hall, VA Tech,**
Blacksburg
- Cost:** **\$1350/class only, \$1949/Class& GIAC Exam**

Register here: <http://www.cpe.vt.edu/isect>



VEMA 2014 Symposium Pre-Conference

- What:** Social Media in Emergency Mgmt & Disaster Response
- When:** March 18, 2014, 9am – 5pm
- Where:** Hampton Roads Convention Center, Hampton
- Cost:** \$0

Course is listed in the Knowledge Center as

[VDEM - V460: Social Media in Emergency Management and Disaster Response \(VEMA Symposium\) - Hampton](#)

(If you are unable to locate this course in your agency KC, contact your KC Administrator and ask them to load it in the KC)



Save The Date

IT Security Conference

"Information Security Enabling the Business"

The 2014 Commonwealth of Virginia Information Security Conference will be held at the Crowne Plaza Hotel in Richmond, Virginia on April 3-4, 2014. This year's theme "Information Security Enabling the Business" will focus on the significant value information security can contribute to the mission and goals of an organization. Emphasis will be given to the balance of security risks and business needs, effective security metrics, regulatory compliance, information security governance, major business trends with security implications and other issues.

This opportunity to hear presentations and share ideas with fellow managers, auditors and technical professionals around this theme should not be missed !!!!



Keynote Speakers

IT Security Conference

"Information Security Enabling the Business"

**Dr. Ron Ross - National Institute of Standards and
Technology**

**Dr. Ross will speak on TACIT Security - "Institutionalizing
Cyber Protection for Critical Assets"**



Keynote Speakers

IT Security Conference

"Information Security Enabling the Business"

Justin Somaini – Chief Trust Officer at Box

Mr. Somaini will discuss - "The need for Security Transformation"



Conference Topics

IT Security Conference

"Information Security Enabling the Business"

Telecommuting

Social Networking

Wireless Policy and Compliance

Enterprise Governance and IT Architecture

Balancing Security/Risk Management

Note: Topics are subject to change prior to conference



Conference Topics

IT Security Conference

"Information Security Enabling the Business"

Dealing with Big Data

APA Vision

Security Awareness

How to Deal with Auditors (and ISO's)

Security Metrics

BIA/DR – Lessons Learned and how to Pitch

Note: Topics are subject to change prior to conference



Vendor Attendees

IT Security Conference

"Information Security Enabling the Business"

Verizon
IBM
Impact Makers
AT&T
Gartner
North Highland

ePlus Technology
Syrinx Technologies
Accuvant
Symantec
Oracle
FishNet Security



Registration

IT Security Conference

"Information Security Enabling the Business"

Registration fee: \$125.00

The conference website is currently being updated and we will notify you when the site will be available for registration.



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*

5 February, 2014



NORTHROP GRUMMAN



ADJOURN

THANK YOU FOR ATTENDING

