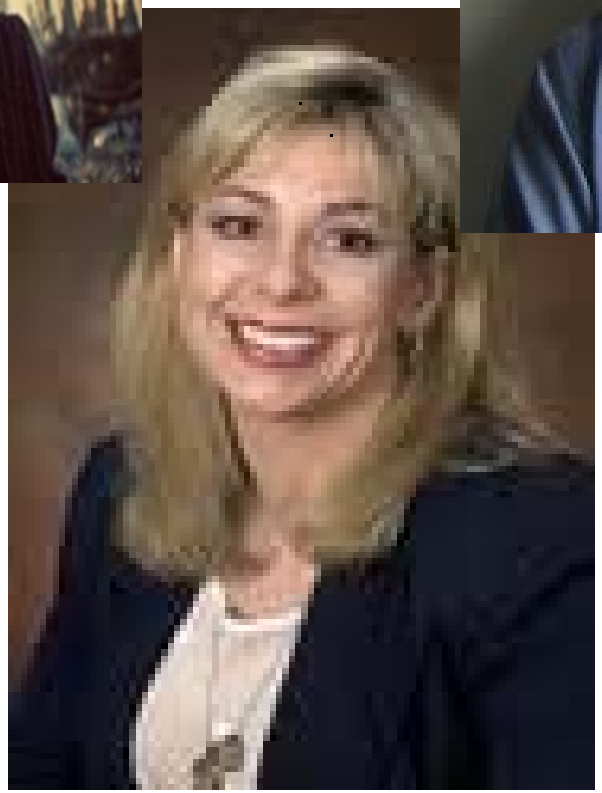
"Black Hat Webcast Series”

“Digital Forensics, What Is The Meaning Of This?”

Wednesday, September 28, 2011

Taylor Banks

Dov Yoran



Pamela Fusco

- Principal, Booz Allen
- CSO Digex, CISO Merck, EVP Citi
- Industry expert, 25 year seasoned global

Cyberologist; Founding member

CSA & CISO Exec Forum

- Certified/accredited CISSP, CISM,

CCSK, CHS III, NSA (IAM), NCS Adjunct Faculty, UAT Honorary Doctorate of Science in Technology

- Delegate, Policing Cyberspace, Chinese Prosecutors Society, Presidential Commission CCIP, US Navy veteran & Cryptologist, Pamela has been bestowed with numerous honors and awards including a Presidential Citation.

Dov Yoran

- CEO ThreatGRID, Co-founder,

MetroSITE Group

- Riptech, Inc.,
- Founding member of the CSA
- Board of Directors NY Metro

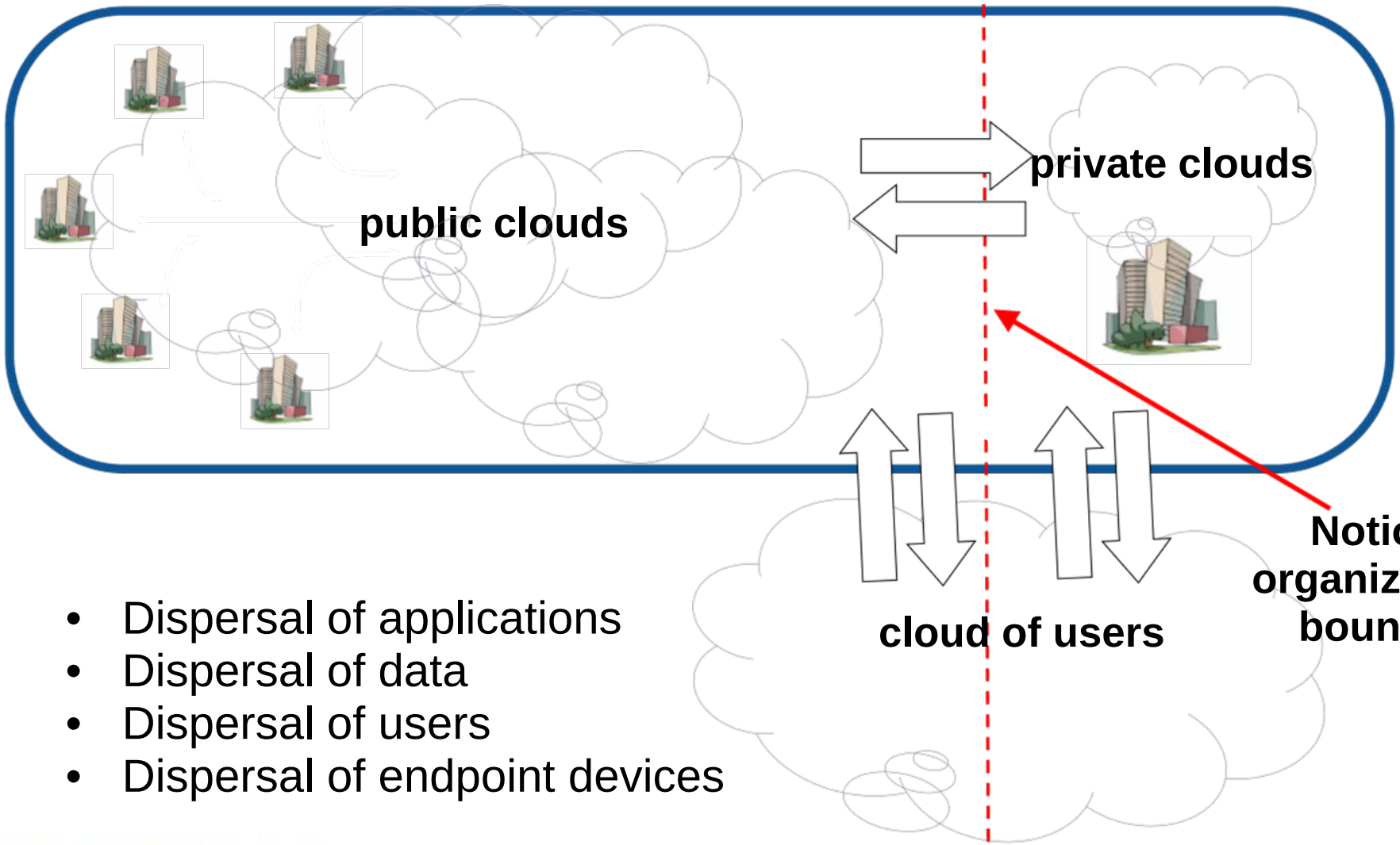
ISSA and NY Metro CSA chapters and a frequent speaker at industry conferences

- Masters, Science in Engineering Management, concentration in InfoSec Management from George Washington University and is a cum laude graduate with a Bachelor of Science in Chemistry from Tufts University

Taylor Banks

- Founder CogniSec
- 14 years InfoSec and privacy
- Facilitator and seasoned instructor for engineers, architects, managers/executives. DOD, FBI and the NSA.
- Since 2007, Taylor has focused on the security in and of virtual infrastructure.
- Since 1999, Mr. Banks has written and delivered courseware for, and earned certifications from organizations including CheckPoint, Nokia, VeriSign, ISC2, (IBM) ISS, NAI, ISECOM, Caymas Systems, InfoWeapons and VMware.

2011-2014: the Hybrid Enterprise



- Dispersal of applications
- Dispersal of data
- Dispersal of users
- Dispersal of endpoint devices

Cloud Forcing Key Issues

- Critical mass of separation between data owners and data processors
- Anonymity of geography of data centers & devices
- Anonymity of provider
- Transient provider relationships
- Physical controls must be replaced by virtual controls
- Identity management has a key role to play
- Cloud WILL drive change in the security status quo
- Reset button for security ecosystem

Key Cloud Security Problems of Today

CSA Top Threats Research

- Trust: Lack of Provider transparency, impacts Governance, Risk Management, Compliance
- Data: Leakage, Loss or Storage in unfriendly geography
- Insecure Cloud software
- Malicious use of Cloud services
- Account/Service Hijacking
- Malicious Insiders
- Cloud-specific attacks

Key Problems of Tomorrow

- Globally incompatible legislation and policy
- Non-standard Private & Public clouds
- Lack of continuous Risk Mgt & Compliance monitoring
- Incomplete Identity Mgt implementations
- Haphazard response to security incidents

Personal Data Closets in the Cloud

- Involves the sharing or storage by users of their own information on remote servers owned/operated by others and accessed through the www or other connections
- Any information stored locally on a PC can be stored in a cloud
  - email, word docs, spreadsheets, videos/pics, health records, tax and/or other financial information
  - (SMB) business plans, PPT, accounting, advertising campaigns, sales numbers, appointment calendars, contact info etc.

Intra and Extra Data Exchange

- Inter exchange: an individual, a business, a government agency, or other entity sharing information
  - The entire contents of a user's storage device may be stored with a single cloud provider or with many

SOCIAL NETWORKING

"Facebook Pwn"

- Java-based tool is described by those who developed it as a "Facebook profile dumper"
- Sends friend requests to a list of Facebook profiles, and polls for the acceptance notification
  - Victim accepts the invitation
  - “tool” dumps **all** their information, pictures and friend list to a local folder

Hacking Insulin Pumps
BlackHat 2011

- Exceptional risks: Program a remote control to command pumps to dispense the incorrect dosage of insulin
- Devices could be fixed sooner with a "patch," and current Medtronic pumps are left with outdated software code that can be exploited
- Ignored in repeated attempts to alert the company to the defects

Digital Forensics and Investigations Panelist Discussion

Can you provide details about recent malicious and hostile activities and techniques?

Has anyone conducted a digital investigation? Conducted one in the cloud?

Digital Forensics and Investigations Panelist Discussion

Can you share your insights and expertise about automated malware processing and defensive practices which support forensic analysis, investigations and **identify root cause?**

Steps involved in an IR, Forensics – what should you do in general (cloud or not)

Digital Forensics and Investigations Panelist Discussion

Purposeful identification and guidance, what is most meaningful with regards to the collection, retention, disclosure and evidence gathering when tracking the hacker?

Digital Forensics and Investigations Panelist Discussion

Targeted attack vectors and perpetrators

Who are the main targets?

Who are the attackers?

Where are they hiding?

Who actually owns the data from a legal perspective? Provider, Enterprise, etc.?

Summary
Panelists insights for the future

Top items investigators should be considered with?

Forensics? Can it be complete?

Is it Viable for prosecution?

Darn logs, everywhere, are they purposeful? If yes which logs.

Always Use Protection

Thank You !