Emerging Technology Trends and Cyber Security Related Issues

Presented by Andrew Robinson,
Principal Design Architect, Information Systems Architects

Thursday, June 28 2012, vc
Courtyard Marriott, Culver City

Association for Information Technology Professionals (AITP) LA Chapter
Event Registration https://www.acteva.com/go/aitpla

The "Big IT" Emerging Trends

- Big Data/Information
  - "GLOBAL instantaneous realtime"(Business) Intelligence
  - Blurring the inside/outside boundaries:from internal only use/to global availability, personal/public, corporate/public, divisional/corp, project/divisional
  - Map/Geo/Time 2-4d visualization
  - Realtime Social Networking/Collaboration/Classification/Tagging/Rich Media
  - Information Exchange/ Marketplaces/Communities as a basis for economic activity and a means of commerce- collaboration, social networking

The “Big IT” Emerging Trends

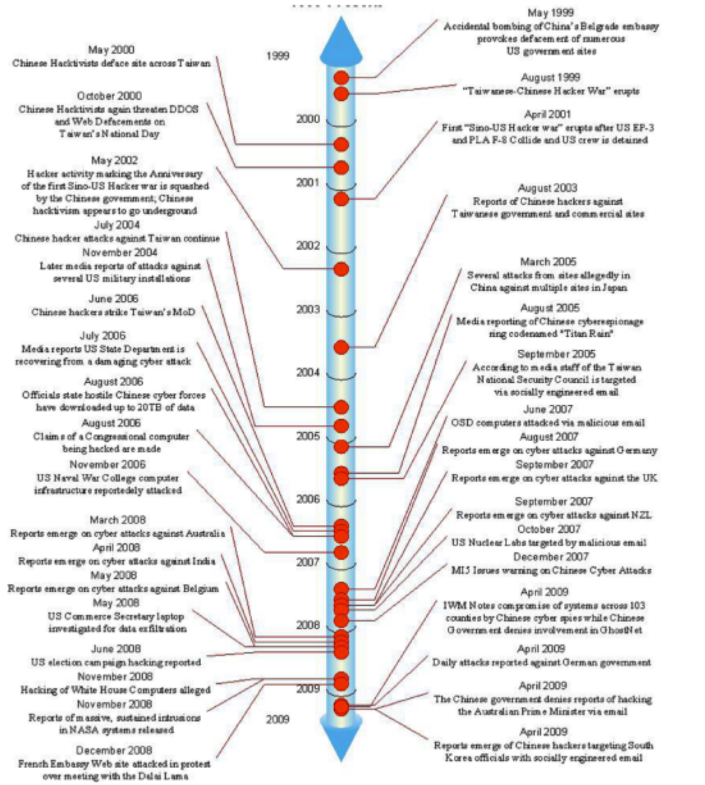
- Big Processing
  - Cloud, SAAS, Grids
- Big Energy
  - Backend Device-- The Data Centre
  - Client Devices -- Little Energy but Lots of them
    - Platforms: Desktop, Notebook, Netbook, SmartPhone, Tablet
  - Renewable onsite/onboard sources for Highest Resilience

Cyber Event History

A Summarized History Beyond Flame and Stuxnet

1. Capability of the PRC to Conduct Cyber Warfare & Computer Network Exploitation (2009), B. Krekel, Northrup Grumman; 9 October 2009
2. Source malware/cybercrime in CSOonline's Malware/Cybercrime section by Taylor Armerding

Timeline of Significant Chinese Related Cyber Events 1999-Present



May 1999
Accidental bombing of China's Belgrade embassy provokes defacement of numerous US government sites

August 1999
"Taiwanese-Chinese Hacker War" erupts

May 2000
Chinese Hacktivists deface site across Taiwan

October 2000
Chinese Hacktivists again threaten DDOS and Web Defacements on Taiwan's National Day

April 2001
First "Sino-US Hacker war" erupts after US EP-3 and PLA F-8 Collide and US crew is detained

May 2002
Hacker activity marking the Anniversary of the first Sino-US Hacker war is squashed by the Chinese government; Chinese hacktivism appears to go underground

August 2003
Reports of Chinese hackers against Taiwanese government and commercial sites

July 2004
Chinese hacker attacks against Taiwan continue

November 2004
Later media reports of attacks against several US military installations

March 2005
Several attacks from sites allegedly in China against multiple sites in Japan

August 2005
Media reporting of Chinese cyberespionage ring codenamed "Titan Rain"

September 2005
According to media staff of the Taiwan National Security Council is targeted via socially engineered email

June 2006
Chinese hackers strike Taiwan's MoD

July 2006
Media reports US State Department is recovering from a damaging cyber attack

August 2006
Officials state hostile Chinese cyber forces have downloaded up to 20TB of data

August 2006
Claims of a Congressional computer being hacked are made

November 2006
US Naval War College computer infrastructure reportedly attacked

June 2007
OSD computers attacked via malicious email

August 2007
Reports emerge on cyber attacks against Germany

September 2007
Reports emerge on cyber attacks against the UK

September 2007
Reports emerge on cyber attacks against NZL

October 2007
US Nuclear Labs targeted by malicious email

December 2007
MI5 Issues warning on Chinese Cyber Attacks

March 2008
Reports emerge on cyber attacks against Australia

April 2008
Reports emerge on cyber attacks against India

May 2008
Reports emerge on cyber attacks against Belgium

May 2008
US Commerce Secretary laptop investigated for data exfiltration

June 2008
US election campaign hacking reported

November 2008
Hacking of White House Computers alleged

November 2008
Reports of massive, sustained intrusions in NASA systems released

December 2008
French Embassy Web site attacked in protest over meeting with the Dalai Lama

April 2009
IWM Notes compromise of systems across 103 counties by Chinese cyber spies while Chinese Government denies involvement in GhostNet

April 2009
Daily attacks reported against German government

April 2009
The Chinese government denies reports of hacking the Australian Prime Minister via email

April 2009
Reports emerge of Chinese hackers targeting South Korea officials with socially engineered email

15 Worst Data Breaches Ever

- 1. Heartland Payment Systems
- Date: March 2008
- Impact: 134 million credit cards exposed through SQL injection to install spyware on Heartland's data systems.
- A federal grand jury indicted Albert Gonzalez and two unnamed Russian accomplices in 2009. Gonzalez, a Cuban-American, was alleged to have masterminded the international operation that stole the credit and debit cards. In March 2010 he was sentenced to 20 years in federal prison. The vulnerability to SQL injection was well understood and security analysts had warned retailers about it for several years. Yet, the continuing vulnerability of many Web-facing applications made SQL injection the most common form of attack against Web sites at the time.

- 2. TJX Companies Inc.
- Date: December 2006
- Impact: 94 million credit cards exposed.
- There are conflicting accounts about how this happened. One supposes that a group of hackers took advantage of a weak data encryption system and stole credit card data during a wireless transfer between two Marshall's stores in Miami, Fla. The other has them breaking into the TJX network through in-store kiosks that allowed people to apply for jobs electronically. According to KNOS Project cofounder and chief architect Kevin McAleavey, this was possible because TJX's network wasn't protected by any firewalls. Albert Gonzalez, hacking legend and ringleader of the Heartland breach, was convicted and sentenced to 40 years in prison, while 11 others were arrested.

- 3. Epsilon
- Date: March 2011
- Impact: Exposed names and e-mails of millions of customers stored in more than 108 retail stores plus several huge financial firms like CitiGroup Inc. and the non-profit educational organization, College Board.
- The source of the breach is still undetermined, but tech experts say it could lead to numerous phishing scams and countless identity theft claims. There are different views on how damaging the Epsilon breach was. Bruce Schneier, chief security technology officer at BT and a prolific author, wrote in a blog post at the time that, "Yes, millions of names and e-mail addresses (and) other customer information might have been stolen. Yes, this personal information could be used to create more personalized and better-targeted phishing attacks. So what? These sorts of breaches happen all the time, and even more personal information is stolen." Still, Kevin McAleavey of the KNOS Project says the breach is being estimated as a $4 billion dollar loss. Since Epsilon has a client list of more than 2,200 global brands and handles more than 40 billion e-mails annually, he says it could be, "the biggest, if not the most expensive, security breach of all-time."

Cyber Risk - Classifying the Hazards

- Man Made - More Likely with impact variance
  - Virus, DOS, DDOS, Information Theft/Tampering
- Natural - Less Likely but catastrophic impact
  - Solar EM Storm damages critical network or power grid infrastructure

Cyber Event Classification

- Process versus Data/Information
- Nuisance Virus to Malware
- Web Click statistics
  - identity location machine IP determination linkage
- Denial of Service (DOS) [web site ransom]
- Distribute Denial of Service (DDOS)
- Advanced Persistent Threats (APT)
  - Information Theft
    - undiscovered, delayed exfiltration discovery, never discovered
  - Information Tampering
- Smart Grid- Critical Infrastructure (CI)
  - SCADA/Embedded Systems
  - Recent reclassification of rogue devices built in ASIAPAC as "Manchurian devices"

The Big BYOD Issues

- Stealing information is big business (Security & Privacy Concerns expressed by most CIO’s and IT Professionals)
  - IP, design, product plans, competitive analysis, test results, marketing lists
- Growing fast, more frequent higher yield events as the cyber attack history slide summarized
- Insiders often knowingly or unknowingly provide help to attackers
  - passive collection of network/server activity and defensive information
- Virtual insiders- those that Bring Your Own Device for others use can unknowingly be of considerable assistance as well
- Cost risk trade-off
  - BYOD is about lowering employee/contractor/stakeholders/partner costs and adding agility to have just the right team participating on projects for the right time

"What BYOD means for your business" Ziff Davis

- BYOD. Bring-your-own-device. Whether you're doing it now or your employees are clamoring for it, your business must face this new reality. The benefits of shifting to this model are great: more productive workers, faster responsiveness to customers, higher employee retention rates with happy employees...even reduced IT costs on operations, hardware and software licensing. That's only half the story. OR
- BYOD also means huge challenges with the management of user-liable devices, exposure of sensitive corporate data stored on devices, leakage of that data through consumer applications and lastly the risk of the introduction of malicious data or software. These challenges can all be answered with the right IT security strategy and tools.

BYOD Recent Survey Facts from 600 IT and Business Leaders

- Everybody is doing it
  - Nearly all respondents (95 percent) said that their companies allow employees to bring their own devices into the office.
- Connected Workers
  - The average number of connected devices in use by a "knowledge worker" is 2.8, according to Cisco
- Plugged In
  - By 2014, Cisco predicts that knowledge workers will have an average of 3.3 devices each by 2014.
- Extremely Positive
  - 76 percent of respondents believe that allowing employees to bring in their own devices can be "extremely positive" for the company at large

BYOD Recent Survey Facts 600 CIO IT Professionals

- IT Support
  - 84 percent of respondents say that their IT departments provide some support for the personal devices that employees bring into the workplace.
- Fully Backed
  - More than one third (36 percent) of respondents say that their IT departments provide full support for the personal devices that employees bring into the office.
- Picky Workers
  - 40 percent of respondents say employees are most concerned about being able to choose the device they want to use at the office

BYOD Recent Survey Facts 600 CIO IT Professionals

- Personal Use
  - Productivity watchdogs beware: The second-biggest reason respondents gave for wanting to bring their own devices into the office is to perform personal activities at work
- Unapproved Apps
  - 69 percent of respondents report that unapproved applications are "much more prevalent" now than they were two years ago.
- Security Privacy
  - The two biggest issues respondents believe they'll face as BYOD increases over time are security and privacy.

Source: Wireless Slideshow- BYOD Finds Fans in IT: By Don Reisinger on 2012-06-05, CIO Insight

HOW CAN THE IT DEPARTMENT MANAGE AND SECURE EMPLOYEE MOBILE DEVICES (BYOD)?

- Management of user-liable devices
- Exposure of sensitive corporate data stored on devices
- Leakage of sensitive corporate data through consumer applications
- Introduction of malicious data or software

Some Smart Phone Statistics

Source: Article "Consumerization of Enterprise Mobility",Trend Micro Enterprise Security July 2011,

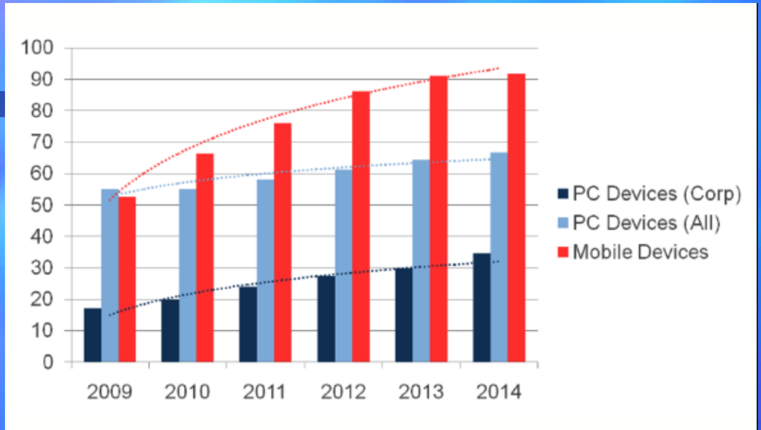


Figure 1: IDC reports Smartphones outsell PCs for the first time in 2010

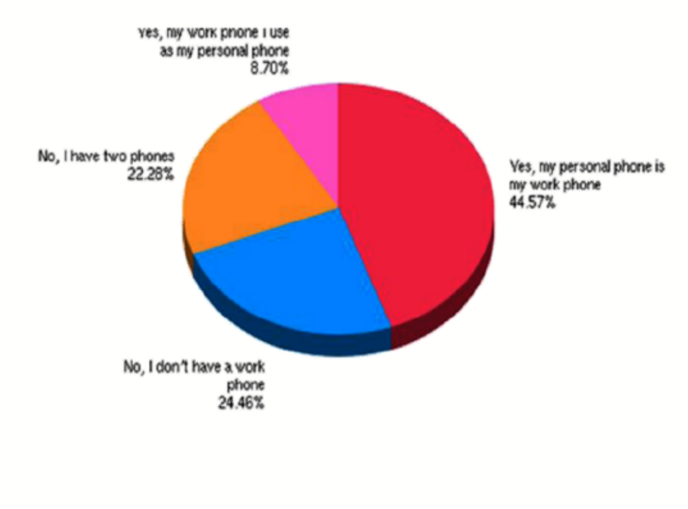
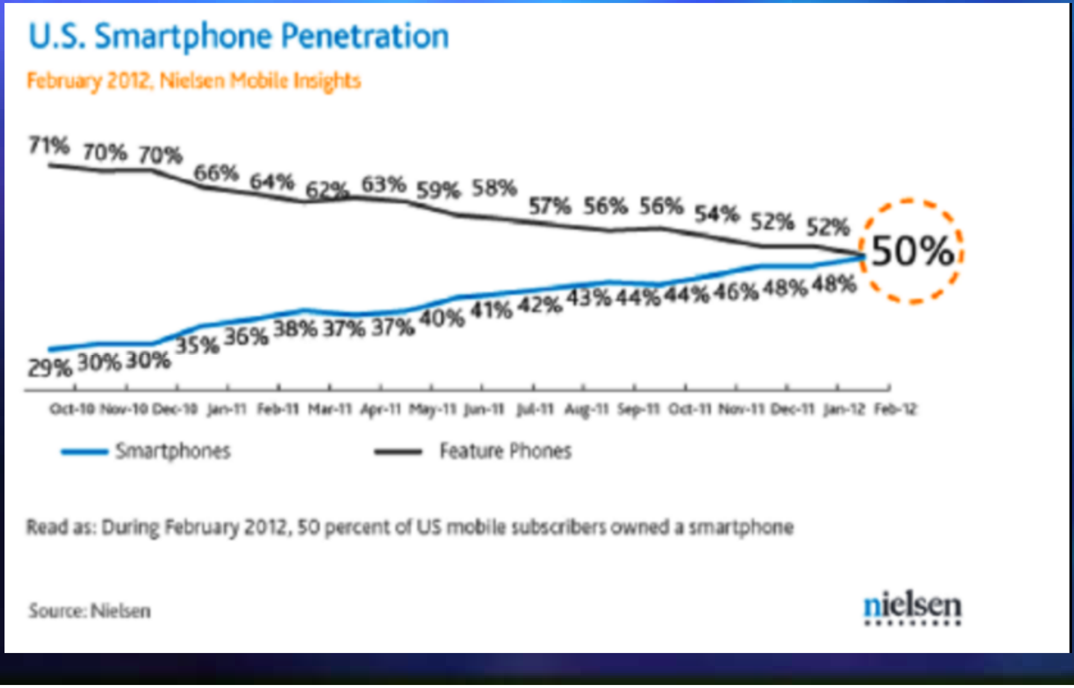


Figure 2: Personal Phone Used for Work Survey



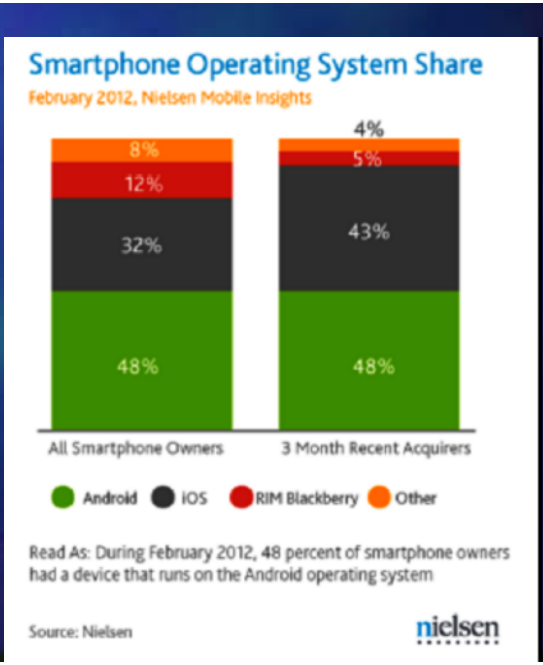
U.S. Smartphone Penetration

February 2012, Nielsen Mobile Insights

Read as: During February 2012, 50 percent of US mobile subscribers owned a smartphone

Source: Nielsen

nielsen



Smartphone Operating System Share

February 2012, Nielsen Mobile Insights

Read As: During February 2012, 48 percent of smartphone owners had a device that runs on the Android operating system

Source: Nielsen

nielsen

A Brief Platform View

Tectonic Market Movement to Smart Phones

3 app/platform types:
Android, iOS, RIM

these often use similar chips and even often share common firmware/driver heritage

A 3% /month market share shift is ongoing
(Source Nielson, Q3 2011)

Now add tablet market data and its even more impressive

Recent Gartner IT research found 86 percent of enterprise respondents are planning to purchase media tablets like an Apple iPad this year

Then there are all those network, smart media access and storage appliances…. Also running ANDROID on a common or at least similar tablet hardware platform

Cyber Attack Information Surface

- Value of information (to whom? Competitor? Marketer/Sales? International Actors? Product Developers/Designers?)
  - now, future (post exploit), ongoing
- Cost or effort/delay to identify and obtain the information
  - defenses/risks/discovery/detection
  - tradecraft/exploit/technology vulnerability revealed
  - undiscovered potential for ongoing information revenue-sustainable revenue
- Value Return

Important Emerging Information Technology Trends- Accelerating BYOD/Consumerization IT/Cloud/Outsourcing

- Wireless Data Transmission (enables virtual access)
  - Super WIFI - 8km 100-300 Mbits
  - Long Term Evolution (LTE)
- Architecture of Resilience for Process, Information and Resources (ie. Trusted Time/Event Seq, Renewable Power and other Resources like Water or raw materials) rules
  - Mission Critical Transactions (Trusted Time Sequencing/Ordering/Priority)
  - High Availability/Redundancy/Reliability:
    - location, location, location
  - At large scale consolidation/concentration -- all your information and processing eggs in one basket leads to
    - partitioning analysis
      - critical facilities
      - critical dependencies (power, networks)
        - standoff services (virtually accessed) in the cloud
    - deeper detailed metric/lifecycle abstractions of GHG, Carbon Footprint, Waste/Recovery)

Important Emerging Information Technology Trends- Accelerating BYOD/Consumerization IT/Cloud/Outsourcing

- Wireless Power Transmission
  - new revenue source
  - customer goes to/past power source
  - lowers/limits distribution network losses/waste

Thank You & Contact Details

- **Andrew Robinson, Principal Design Architect, Information Systems Architects**
  - Email: andrewro@allstream.net
  - Phone: (613) 769-9663 direct

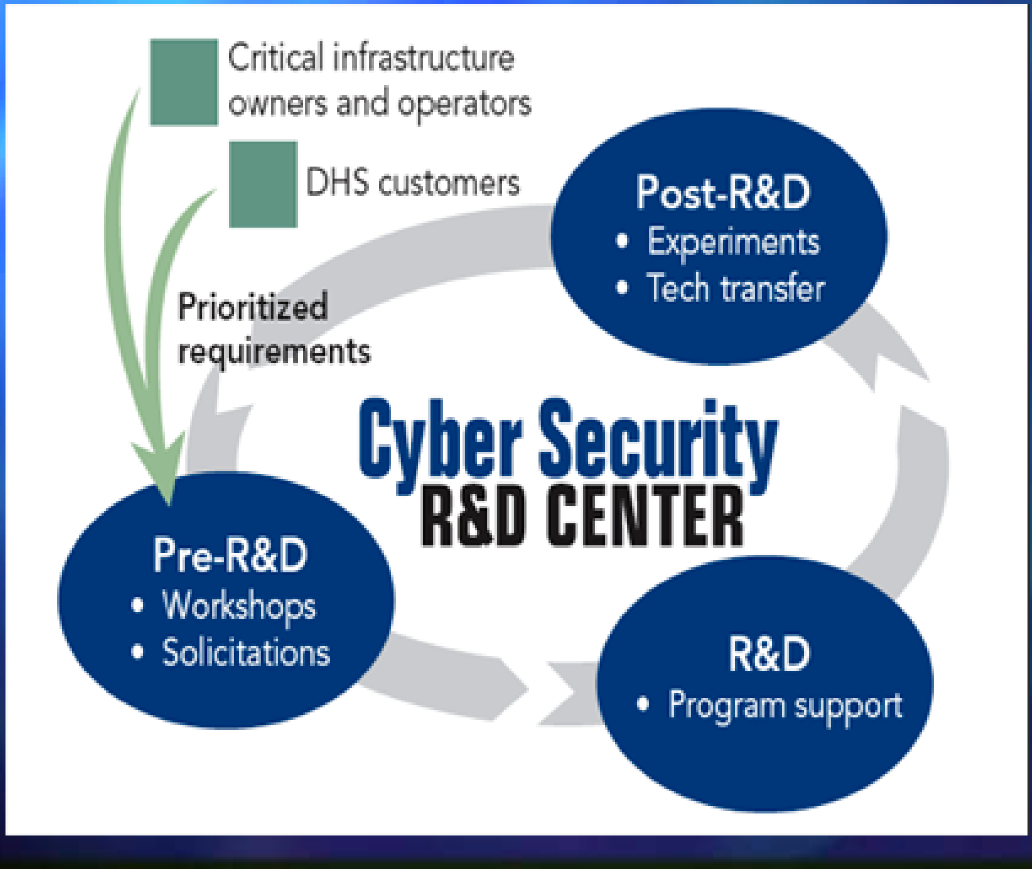
- Some of my ongoing/recent responsibilities:
  - Global Standards Editor, Canadian Vice Chair, International Delegate Working Group (WG) 1, Metric Taxonomy and Maturity Model Standard(s) Development, Joint Technical Committee JTC 1, Standards Committee (SC) 39, "Sustainability for and by IT", Canadian JTC1 2011 Plenary delegate and SC 39 Plenary Delegate
  - Evacuation Planning Tool Productization, Design and Development Lead, New Brunswick Public Safety
  - Design Team Lead, Canadian National - Industry Canada (Canadian FCC equivalent federal department), Wireless Public Alerting Dissemination (WPAD)
  - Cloud SME/Industry (Carriers/Power) Liaison , Public Safety, Centre for Security Science (CSS) Cyber Security Architecture Framework Working Group (AFWG)

- This Deck is posted at
  - http://aitp-la.org/archive.html and http://ppl.ug/Bs3mBmMNoVE/

International Cyber Response

- Components of Emergency Management
  - Public Alerting - US CMAS/IPAWS Canada WPAD
  - Evacuation Planning
  - Command and Control: Military, Government, Critical Infrastructure Facilities
  - Joint Exercises
- "Proactive Defense"-euphemism for "Offense"
  - Evolved from Emergency Management/Disaster Response/Critical Infrastructure Protection
  - Focus on Risk Assessments, Full Spectrum Scenarios, Exercises and Continuous Refinement of Protect Prepare, Respond, Recover Lifecycles
  - Carrier Network Cyber Tool/Monitoring/Operations Investments Key
- International Effort:
  - US Homeland Security Activities "Broad Area Announcements"
  - Sandia (Division of LM) has now started up its own vulnerability lab in addition to other university based cyber labs (ie. DETER)
  - Canadian Public Safety Centre for Security Science (CSS) partnership between Defence Research (DRDC) and Public Safety Canada
  - UK Government 240 million pounds allocated to Cyber Defence- citing 1/3 20000 monthy cyber attacks on govt networks are targeted at obtaining specific information

Broad Area Announcements (BAA) for Project Funding for Advancing Cyber Security Research and Operations from Homeland Security)



Some Recent Media References on BYOD

June 2012

"Bring Your Own Device" BYOD in the June 2012 Media

- Top of Mind CIO/CTP Topic selected articles since June 1 2012
  - Is Obama behind Stuxnet and is BYOD making the IT department redundant?
  - Why IT is Warming to the BYOD trend, CIO Insight, June 6 2012
  - Is BYOD just another chapter that follows on from the paperless office and telecommuting or is there genuine demand for it? Linked in http://lnkd.in/guKJKk

"Bring Your Own Device" BYOD in the June 2012 Media

- BYOD Best Practices and Technical Design Details, CISCO Technical Design Webex, June 20 2012
- BYOD Security Is Top Concern, Baseline Magazine, June 20 2012
- As BYOD Grows, Uncertainty Remains Over How to Implement, June 20 2012
- BYOD Brings Wave of Unknown Security Threats, June 20 2012

“Bring Your Own Device” BYOD in the June 2012 Media

- The New Workforce: Empowered with BYOD and UC
- Microsoft Surface Adds Urgency to Defining BYOD Policies
- Best Practices to prepare your WLAN for BYOD

Panel Discussion Description

- A Panel of Experts shares cutting-edge strategies to manage Cyber security -- for networks, cloud computing, mobile devices

- Today's enterprise security must constantly adapt to new realities -- whether it's rapidly emerging consumer devices/ BYOD, continued cloud adoption, new advanced threats, or compliance. In this environment, we need to know how to:

  - Effectively manage cyber security, mobile security, and cloud security
  - Establish leadership in aligning security to the business
  - Ensure the technology supply chain is secure
  - Address application security threats
  - Effectively communicate security strategy throughout the enterprise

- We have assembled an impressive team of Security Experts/ CSOs to share their views on trends and best practices to ensure enterprise security success.

Panel Members

- AITP-LA has assembled an impressive team of Security Experts/ CSOs to share their views on trends and best practices to ensure enterprise security success. Panelists include:
  - Erik Laykin, Managing Director, Global Electronic Discovery and Investigations--Duff & Phelps, LLC
  - Cheryl Santor, Information Security Manager--Metropolitan Water District of Southern California
  - Andrew Robinson, Principal Design Architect-- Information Systems Architects
  - Stan Stahl, President and Founder—Citadel Information Group

Location

- Courtyard by Marriott--LA Westside
  - 6333 Bristol Parkway
  - Culver City, CA 90230

- Date:
  - Thursday, Jun. 28, 2012
  - 6:00 PM - 9:00 PM

15 Worst Data Breaches Ever

- 1. Heartland Payment Systems
- Date: March 2008
- Impact: 134 million credit cards exposed through SQL injection to install spyware on Heartland's data systems.
- A federal grand jury indicted Albert Gonzalez and two unnamed Russian accomplices in 2009. Gonzalez, a Cuban-American, was alleged to have masterminded the international operation that stole the credit and debit cards. In March 2010 he was sentenced to 20 years in federal prison. The vulnerability to SQL injection was well understood and security analysts had warned retailers about it for several years. Yet, the continuing vulnerability of many Web-facing applications made SQL injection the most common form of attack against Web sites at the time.

- 2. TJX Companies Inc.
- Date: December 2006
- Impact: 94 million credit cards exposed.
- There are conflicting accounts about how this happened. One supposes that a group of hackers took advantage of a weak data encryption system and stole credit card data during a wireless transfer between two Marshall's stores in Miami, Fla. The other has them breaking into the TJX network through in-store kiosks that allowed people to apply for jobs electronically. According to KNOS Project cofounder and chief architect Kevin McAleavey, this was possible because TJX's network wasn't protected by any firewalls. Albert Gonzalez, hacking legend and ringleader of the Heartland breach, was convicted and sentenced to 40 years in prison, while 11 others were arrested.

- 3. Epsilon
- Date: March 2011
- Impact: Exposed names and e-mails of millions of customers stored in more than 108 retail stores plus several huge financial firms like CitiGroup Inc. and the non-profit educational organization, College Board.
- The source of the breach is still undetermined, but tech experts say it could lead to numerous phishing scams and countless identity theft claims. There are different views on how damaging the Epsilon breach was. Bruce Schneier, chief security technology officer at BT and a prolific author, wrote in a blog post at the time that, "Yes, millions of names and e-mail addresses (and) other customer information might have been stolen. Yes, this personal information could be used to create more personalized and better-targeted phishing attacks. So what? These sorts of breaches happen all the time, and even more personal information is stolen." Still, Kevin McAleavey of the KNOS Project says the breach is being estimated as a $4 billion dollar loss. Since Epsilon has a client list of more than 2,200 global brands and handles more than 40 billion e-mails annually, he says it could be, "the biggest, if not the most expensive, security breach of all-time."

15 Worst Data Breaches Ever

- 4. RSA Security
- Date: March 2011
- Impact: Possibly 40 million employee records stolen.
- The impact of the cyber attack that stole information on the company's SecurID authentication tokens is still being debated. The company said two separate hacker groups worked in collaboration with a foreign government to launch a series of spear phishing attacks against RSA employees, posing as people the employees trusted, to penetrate the company's network. EMC reported last July that it had spent at least $66 million on remediation. But according to RSA executives, no customers' networks were breached. John Linkous, vice president, chief security and compliance officer of eIQnetworks, Inc. doesn't buy it. "RSA didn't help the matter by initially being vague about both the attack vector, and (more importantly) the data that was stolen," he says. "It was only a matter of time before subsequent attacks on Lockheed-Martin, L3, and others occurred, all of which are believed to be partially enabled by the RSA breach." Beyond that, Linkous says, is the psychological damage. "The breach of RSA was utterly massive not only from a potential tactical damage perspective, but also in terms of the abject fear that it drove into every CIO who lost the warm-and-fuzzy feeling that the integrity of his or her enterprise authentication model was intact. Among the lessons, he says, are that even good security companies like RSA are not immune to being hacked. Finally, "human beings are, indeed, the weakest link in the chain," Linkous says.

- 5. Stuxnet
- Date: Sometime in 2010, but origins date to 2007
- Impact: Meant to attack Iran's nuclear power program, but will also serve as a template for real-world intrusion and service disruption of power grids, water supplies or public transportation systems.
- The immediate effects of Stuxnet were minimal -- at least in this country -- but eIQnetworks' John Linkous ranks it among the top large-scale breaches because, "it was the first that bridged the virtual and real worlds. When a piece of code can have a tangible effect on a nation, city or person, then we've truly arrived in a strange, new world," he says. Linkous says Stuxnet is proof that nation-states, "are definitely actors -- both attackers and victims -- in the cyberwarfare game." He adds that the more that electro-mechanical industrial and energy systems migrate to larger networks -- particularly the Internet -- "the more we're going to see these real-world intrusions."

15 Worst Data Breaches Ever

- 6. Department of Veterans Affairs
- Date: May 2006
- Impact: An unencrypted national database with names, Social Security numbers, dates of births, and some disability ratings for 26.5 million veterans, active-duty military personnel and spouses was stolen.
- The breach pointed once again to the human element being the weakest link in the security chain. The database was on a laptop and external hard drive that were both stolen in a burglary from a VA analyst's Maryland home. The analyst reported the May 3, 2006 theft to the police immediately, but Veterans Affairs Secretary R. James Nicholson was not told of it until May 16. Nicholson informed the FBI the next day, but the VA issued no public statement until May 22. An unknown person returned the stolen items June 29, 2006. The VA estimated it would cost $100 million to $500 million to prevent and cover possible losses from the theft.

- 7. Sony's PlayStation Network
- Date: April 20, 2011
- Impact: 77 million PlayStation Network accounts hacked; Sony is said to have lost millions while the site was down for a month.
- This is viewed as the worst gaming community data breach of all-time. Of more than 77 million accounts affected, 12 million had unencrypted credit card numbers. According to Sony it still has not found the source of the hack. Whoever they are gained access to full names, passwords, e-mails, home addresses, purchase history, credit card numbers, and PSN/Qriocity logins and passwords. "It's enough to make every good security person wonder, 'If this is what it's like at Sony, what's it like at every other multi-national company that's sitting on millions of user data records?'" says eIQnetworks' John Linkous. He says it should remind those in IT security to identify and apply security controls consistently across their organizations. For customers, "Be careful whom you give your data to. It may not be worth the price to get access to online games or other virtual assets."

15 Worst Data Breaches Ever

- 8. ESTsoft
- Date: July-August 2011
- Impact: The personal information of 35 million South Koreans was exposed after hackers breached the security of a popular software provider.
- It is called South Korea's biggest theft of information in history, affecting a majority of the population. South Korean news outlets reported that attackers with Chinese IP addresses uploaded malware to a server used to update ESTsoft's ALZip compression application. Attackers were able to steal the names, user IDs, hashed passwords, birthdates, genders, telephone numbers, and street and email addresses contained in a database connected to the same network. ESTsoft CEO Kim Jang-joon issued an apology and promised to, "strengthen the security system of our programs."

- 9. Gawker Media
- Date: December 2010
- Impact: Compromised e-mail addresses and passwords of about 1.3 million commenters on popular blogs like Lifehacker, Gizmodo, and Jezebel, plus the theft of the source code for Gawker's custom-built content management system.
- Online forums and blogs are among the most popular targets of hackers. A group calling itself Gnosis claimed responsibility for the attack, saying it had been launched because of Gawker's "outright arrogance" toward the hacker community. "They're rarely secured to the same level as large, commercial websites," says the KNOS Project's Kevin McAleavey, who adds that the main problem was that Gawker stored passwords in a format that was very easy for hackers to understand. "Some users used the same passwords for email and Twitter, and it was only a matter of hours before hackers had hijacked their accounts and begun using them to send spam," says McAleavey.

15 Worst Data Breaches Ever

- 10. Google/other Silicon Valley companies
- Date: Mid-2009
- Impact: Stolen intellectual property
- In an act of industrial espionage, the Chinese government launched a massive and unprecedented attack on Google, Yahoo, and dozens of other Silicon Valley companies. The Chinese hackers exploited a weakness in an old version of Internet Explorer to gain access to Google's internal network. It was first announced that China was trying to gather information on Chinese human rights activists. It's not known exactly what data was stolen from the American companies, but Google admitted that some of its intellectual property had been stolen and that it would soon cease operations in China. For users, the urgent message is that those who haven't recently updated their web browser should do so immediately.

- 11. VeriSign
- Date: Throughout 2010
- Impact: Undisclosed information stolen
- Security experts are unanimous in saying that the most troubling thing about the VeriSign breach, or breaches, in which hackers gained access to privileged systems and information, is the way the company handled it -- poorly. VeriSign never announced the attacks. The incidents did not become public until 2011, through a new SEC-mandated filing. "How many times were they breached?" asks eIQnetworks' John Linkous. "What attack vectors were used? The short answer is: we don't know. And the response to that is simply: we should." "Nearly everyone will be hacked eventually," says Jon Callas, CTO for Entrust, in a post earlier this month on Help Net Security. "The measure of a company is how they respond." VeriSign said no critical systems such as the DNS servers or the certificate servers were compromised, but did say that, "access was gained to information on a small portion of our computers and servers." It has yet to report what the information stolen was and what impact it could have on the company or its customers. Linkous says the company's "failure to disclose until legally required to do so is going to haunt VeriSign for some time."

15 Worst Data Breaches Ever

- 12. CardSystems Solutions
- Date: June 2005
- Impact: 40 million credit card accounts exposed. CSS, one of the top payment processors for Visa, MasterCard, American Express is ultimately forced into acquisition.
- Hackers broke into CardSystems' database using an SQL Trojan attack, which inserted code into the database via the browser page every four days, placing data into a zip file and sending it back through an FTP. Since the company never encrypted users' personal information, hackers gained access to names, accounts numbers, and verification codes to more than 40 million card holders. Visa spokeswoman Rosetta Jones told Wired News at the time that CSS received an audit certification in June 2004 that it was compliant with data storage standards, but an assessment after the breach showed it was not compliant. "Had they been following the rules and requirements, they would not have been compromised," Jones said. The company was acquired by Pay-by-touch at the end of 2005.
- 13. AOL
- Date: August 6, 2006
- Impact: Data on more than 20 million web inquiries, from more than 650,000 users, including shopping and banking data were posted publicly on a web site.
- In January 2007, Business 2.0 Magazine ranked the release of the search data in among the "101 Dumbest Moments in Business." Michael Arrington, a lawyer and founder of the blog site TechCrunch, posted a comment on his blog saying, "The utter stupidity of this is staggering." AOL Research, headed by Dr. Abdur Chowdhury, released a compressed text file on one of its websites containing 20 million search keywords for more than 650,000 users over a three-month period. While it was intended for research purposes, it was mistakenly posted publicly. AOL pulled the file from public access by the next day, but not before it had been mirrored and distributed on the Internet. AOL itself did not identify users, but personally identifiable information was present in many of the queries, and as AOL attributed the queries to particular user accounts, identified numerically, an individual could be identified and matched to their account and search history by such information. The breach led to the resignation of AOL's CTO, Maureen Govern, on Aug. 21, 2006.

15 Worst Data Breaches Ever

- 14. Monster.com
- Date: August 2007
- Impact: Confidential information of 1.3 million job seekers stolen and used in a phishing scam.
- Hackers broke into the U.S. online recruitment site's password-protected resume library using credentials that Monster Worldwide Inc. said were stolen from its clients. Reuters reported that the attack was launched using two servers at a Web-hosting company in Ukraine and a group of personal computers that the hackers controlled after infecting them with a malicious software program. The company said the information stolen was limited to names, addresses, phone numbers and e-mail addresses, and no other details, including bank account numbers, were uploaded. But one problem was that Monster learned of the breach on Aug. 17, but didn't go public with it for five days. Another, reported by Symantec, was that the hackers sent out scam e-mails seeking personal financial data, including bank account numbers. They also asked users to click on links that could infect their PCs with malicious software. Once that information was stolen, hackers e-mailed the victims claiming to have infected their computers with a virus and threatening to delete files unless the victims met payment demands.

- 15. Fidelity National Information Services
- Date: July 2007
- Impact: An employee of FIS subsidiary Certegy Check Services stole 3.2 million customer records including credit card, banking and personal information.
- Network World reported that the theft was discovered in May 2007, and that a database administrator named William Sullivan, said to own a company called S&S Computer Services in Largo, Fla., had been fired. But the theft was not disclosed until July. Sullivan allegedly sold the data for an undisclosed amount to a data broker, who in turn sold it to various marketing firms. A class action lawsuit was filed against FIS and one of its subsidiaries, charging the companies with negligence in connection with the data breach. Sullivan agreed to plead guilty to federal fraud charges and was sentenced to four years and nine months in prison and ordered to pay a $3.2 million fine. On July 7, 2008, a class-action settlement entitled each person whose financial information was stolen to up to $20,000 for unreimbursed identity theft losses.

- Source malware/cybercrime in CSOonline's Malware/Cybercrime section by Taylor Armerding