Emerging Trends Affecting Cyber Security

Dr. Denise Chatam Walker

CSO, Chief Emergency Management Officer

Lone Star College System

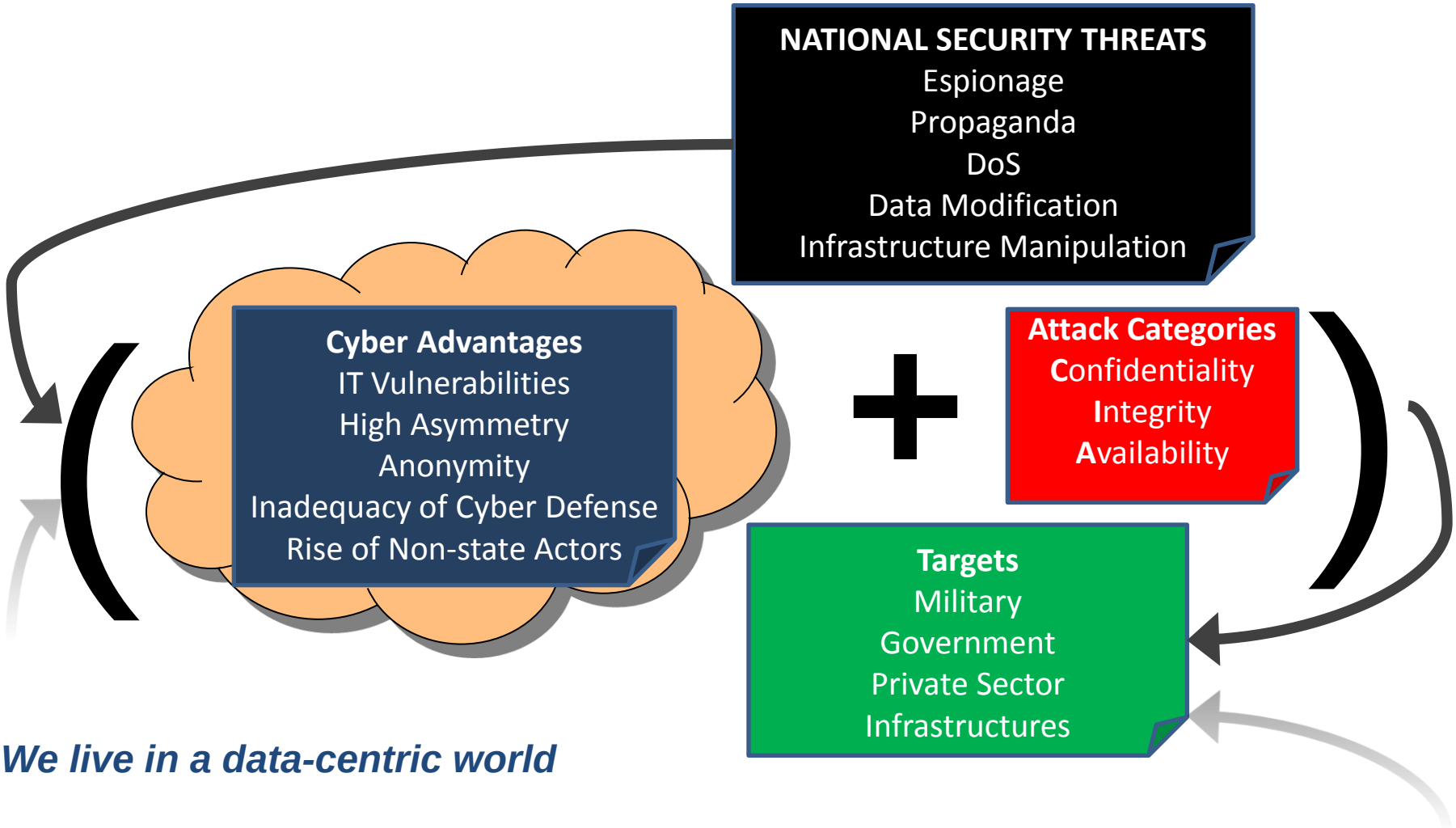
16 May, 2012

2012 Tech Trends

- BYOD…media tablets
- Social networking for business
- Biometric authentication
- Cloud going mainstream
- Virtualized enterprise
- Electronic wallets
- Geo-locations
- Gamification
- Apps available in App Stores
- Big data

Cyber Defense Arena

Successful attacking is about information gathering and reconnaissance



We live in a data-centric world

Greatest Concerns in 2012

- Remote employees
- BYOD
- Cloud computing…major provider suffers significant breach
- Removable media
- 3rd party apps…proliferation of new apps
- Data categorization challenges…data loss prevention (DLP)
- Risks coming from anywhere
- Identity theft
- New cyber legislation, security, and compliance
- DR/BCP planning
- Consumerization of IT
- Mobile Device Management (MDM)
- Gen Y

Security Trends

- **Attack Source - 2/3 from malnets**
  - Preventing attacks by isolating the source rather than defending perimeters
- **Using social media to deliver payloads**
  - Users more trusting of content
  - Increased number of social networks
- **High-profile attacks on mobile computing devices rising**
  - Apple iPhone and iPad (closed) tends to be more secure than networks accessed by Google Android (open) devices
  - Increasing number of devices
  - A new opportunity for hackers

Security Trends

- **Top economic crimes**
  - corporate fraud
  - distributing viruses
  - illegally accessing data
  - stealing personal corporate fraud
- **Cybercriminal activity**
- **Attacks on emerging technologies**

State of Cyber Defense

- **Less than half of U.S. organizations have adequate technology to secure their cloud computing infrastructures.**

- **Executives, IT security, and compliance disagree on:**
  - Cloud is as secure as on-premise data centers
  - Who is responsible for cloud data security
  - What security measures to use

- **Ownership of cloud security is dispersed**

- **Executives review cyber-risks**
  - 36% at least once a year
  - 15% never do.

Threats on the Rise

- **Scareware**
  - LizaMoon SQL Injection (buy AV)
- **iFrame injections**
  - Advertising/redirection to malicious websites
- **JavaScript malware**
  - Bypass security measures to run embedded code
- **Blackhole exploit kit**
  - Uses unpatched exploits to hack computers
- **WordPress injection attacks**
  - malicious code at start/end of blog that blocks access

Cybercriminals

- **Many actors…Motivation varies**
  - Shift to organized groups attacking for profit or retaliation
  - Motivation drives the technique used
  - Types of actors: Hactivist, cyber crime, nation states, terrorism
- **Organized criminals use advanced malware for attacks**
- **Advanced Persistent Threats (APTs) affecting SMBs and consumers**
- **Recent Attacks**
  - RSA's SecureID incident – Employee opens attached Excel doc in email
  - Stuxnet's successor - Duqu discovery
    - Stuxnet infected SCADA equipment changing results
  - Hacktivists/Script-kiddies target machines
  - Anonymous, LulzSe

Cybercriminals

- **Create and disseminate malware**
  - Underground “pay-per-install” industry
    - Hackers charge to access malware
  - More than 50 “families” of malware
    - Data-stealing Trojan horses
    - Spam bots
    - DoS bots
    - Fake AV
  - Malware “repacked” every 11 days, on average, to avoid AV detection
  - Freeware, toolkit, hackers available underground

Attacks by the Numbers

- **Malicious Attacks Blocked by one vendor**
  - 2011: 5.5 billion
  - 2010: 3 billion (HP, 2012)
- **Vulnerabilities Identified Decline**
  - 21% decline between 2010 and 2011
- **Targeted Attacks Aim at Business**
  - 50% -- Enterprises (2,500+ employees)
  - 32% -- Midmarket companies (250 to 2,500 employees)
  - 18% -- Small Businesses (under 250 employees)
    - Don't think they're a target
    - Not taking action to protect themselves.

Vulnerable Users

- **Vulnerable Users are Beachhead for Server Attack**
  - **Attacks shifting to Users**
    - Servers behind firewalls -- direct server attacks are rare
    - Compromised users are beachheads to attack servers
    - Example user-based attacks -- Spear-phishing
      …RSA breach compromised its SecureID system
  - **Why current technologies fail**
    - Attacks are sophisticated and targeted
      - Botnets, malicious active content, XSS, Anonymizers, etc.
    - Desktop/gateway AV – signature technology for the known
    - Employee awareness

New Vulnerabilities

- **New Vulnerabilities**
  - Exploits have gone elsewhere
    - Custom-built Web apps
  - New techniques allow attackers to exploit old vulnerabilities to launch new attacks
    - Blackhole exploit injected into USPS website
  - Vulnerability severity is increasing (17% in 5 years)
    - High security vulnerabilities causing remote code execution
  - Browser/browser plug-ins with highest number of vulnerabilities disclosed
    - Leaders: ShockWave and Java
  - Software may be more secure, the apps running on top of them are introducing vulnerabilities

Browser

- **Browser market share**
  - IE remains the most popular enterprise browser -->50% overall traffic
    - 4% - IE 9 (latest stable release)
    - 30% - IE 8 (most dominate browser)
    - 18% - IE 7
    - 3% - IE 6 (over a decade old – support ends 2014).
- **Browser plugins**
  - Outdated browser plugins - a significant threat
    - Adobe Reader, Adobe Shockwave, MS Outlook, Java, Adobe Flash, MS Silverlight, QuickTime, Windows Media Player, and RealPlayer
      - MS updates at the OS level; Adobe does not
  - Browser exploit kits tend to target Java, Adobe Reader and Adobe Flash

Web Apps

- **Web Attacks Increasing**
  - 2009: 250,000 attacks
  - 2010: 480,000 attacks
  - 2011: 500,000 attacks(HP, 2012)
- **Commercial Web Apps…the new frontier**
  - 24% - attacks had a high severity rating
  - 36% - of all vulnerabilities came thru these apps
  - 4 of the 6 most popular Open Source Vulnerability Database (OSVDB) vulnerabilities are exploitable via the web
  - Vulnerabilities increase with customization and add-ons
- **HTML5 trends**
  - Fuels growth of next gen web app attacks
  - Developers not using secure coding practices

Web Apps

Coding mistakes in web apps leading to vulnerabilities

- Can be difficult to detect
- Can result in loss of compliance, data sharing, or fuel other attacks
- 93% Apps vulnerable to information leakage and improper error handling
- 86% contained injections flaws letting hackers take control over internal databases on a Web site.
- SQL injection vulnerabilities attacked 3x over other XSS
- 54% contained XSS flaws - Cross-Site Scripting Attacks
  - 2011: 10 million attacks
  - 2010: 25 million attacks
- 50%+ of web sites expose server type/software version from the header information

Advanced Persistent Threats (APTs)

- **Adversaries take advantage of IT complexity**
- **Defenses:**
  - Layering
  - Defense-in-depth
  - Use IDS, IPS, Monitoring, Assessments
  - Change control
  - Communicate

Spread of 3rd Party Apps

- **Proliferation of vulnerable 3rd-party apps**
- **Patch management using Windows Server Update Services (WSUS) is useless…**
  - 95% of organizations have installed social media apps
  - 78% of Web 2.0 app support file transfer
  - 66% apps have known vulnerabilities
  - 28% propagate malware
- **Proliferate mobile malware**
  - Google Marketplace/Apple's App Store more vulnerable than Blackberry
    - Mobile malware largely targets Android OS
  - *Trending:* Mobile devices getting anti-theft protection

Search Engines

- **Search engines becoming a leading attack vector**
  - Malware distributors inject code in legitimate and fake websites to lure people to download malware.

- **Black path search engine optimization**
  - Poison search results
    - Points to one malicious page forcing it to surge towards the top in the search engine results
  - Looks at the user agent to determine if you fall within desired target area
    - Browser version

Botnets

- **Botnets - a universal threat**
  - Spread attacks
  - Collect hosts to be sold
  - Active families: Zeus, Asprox, Spyeye, Gumblar, Powerbot
  - Increased presence and growing
    - 75% of all new malware strains were Trojan apps
      - Silently infects PCs so that act like botnets then phoning home to attackers with stolen information
- **Botnet-related ecosystems**
  - Offer “malware infection as a service”
  - Leased hourly or daily for attacks/scams.

Mobile

- **Mobile browsers traffic**
  - 50%+ Apple IoS (growing)
  - 35-40% Android (declining)
  - 13-15% Blackberry (declining)
  - Lost devices - major security challenge
- **Mobile employees, smart devices and removable media**
  - Access networks
  - Transmit/store data
- **42%**
  - Employees use their personal mobile devices at work
  - Enterprises unable to secure these devices.

Mobile

- **Mobile Risk**
  - 95% have company's data on mobile devices
  - 40% of organizations with mobile devices containing corporate data have no plans to address this vulnerability.
- **IT landscapes becoming more dispersed**
- **Mobile app security still in its infancy**
- **Mobile app are different yet the same**
- **Number of attack types conducted against mobile apps are increasing**
- **No platform is safe**
- **Webkits opens the doors for hackers**

Spyware

- **Geo-location – a potential privacy violation**
  - Knows where you live, where you are
  - Tracks personal habits
  - Employer use increasing
  - Malware leveraged to customize attacks
    - Money making potential

Sports & Gambling

- **Sports & Gambling**
  - Sporting events (i.e., March Madness, Super Bowl, NBA selection process, NFL division championships)
    - Sports and gambling parallel in peaks and valleys
      - Significant bandwidth consumed as employees monitored events
  - Gambling goes hand-in-hand with major sporting events
  - Increasing number of employees gambling during normal work hours on company computing systems
    - Employee compromise possible

Social Media

- **96% Gen Y on it**
- **93% of online users use it**
- **20% of 2011 marriages started online**
- **Facebook**
  - 2nd only to email
  - 3rd largest, if a country
    - (China, India, ***Facebook***, US, Indonesia, ***Twitter***)
- **Twitter**
  - 6th largest, if a country
  - 3 Yrs. = 1 billion tweets
- **Hitting social networks by fooling users**
  - **Cybercriminals**: Send email redirecting to fake website
  - **Motivators:** financial, proprietary data, competitive advantage, revenge

Social Networking

- **Social Networking**
  - **5% - Web app traffic -** total traffic w/in an organization
    - Facebook, Gmail, YouTube, Twitter, MSN Messenger, Hotmail, Yahoo mail
  - **Facebook** enterprise traffic is declining
    - Policy blocks
    - Facebook implement new security measures
      - WebSense for URL scanning
  - **Twitter** transactions increasing slightly
    - Quick check and leave
    - Valued as a business tool

Policies/Blocks Increasing

- **Blocks**
  - Total social networking blocks
  - Post/write to social networking sites
  - Time of date, you can read but not write, rate limiting, etc.
  - Streaming media
  - Instant messaging (IM)
  - Webmail
  - Quota
  - Botnet
  - Proxy/Anonymizers
- **Policies**
  - IM
  - Malware
  - Webmail
  - Streaming media
  - File type
  - Risk score setting
  - XSS/cookie theft
  - Spyware/Adware
  - Protocols

BYOD

- **Gen Y likes**
- **BYOD and IT self-service - increased data loss**
- **Shifting device ownership to employees risks:**
  - Security breaches
    - Theft, negligence, device sharing, BYO-virus
    - Clean your own infections
    - Launch own network services (consumerization of IT)
  - Lost productivity due to device failures
  - Corporate network congestion

BYOD…Coping Strategies

- **Requires a formal BYOD plan**
  - Only a few have or have started a plan
- **Segregated networks are highly recommend**
    - Production, Guest, BYOD
    - A secure wireless network with coverage and capacity
    - Network must handle the load
- **Device aware infrastructure**
  - The ability to detect what devices are on/attempting to get on the network
- **Access controls**
  - Deny and why
- **Ability to disassociate devices from the network when required**
- **Self service portal**
  - Password resets, app provisioning, FAQs

Disaster Recovery

- **Organizations DR Plans**
  - 95% have a Plan
  - 44% have a remote, cloud-based Plan
- **DR Planning is important but doesn't get the attention it deserves**
  - When your systems are in DR they are in risk
  - Old DR paradigm
    - Production apps – email, sales, accounting, marketing/design, LOB apps, payroll, VoIP
- **Resilience is the new DR**
  - High availability - next generation for infrastructure
  - High available IT infrastructure changing DR planning
    - Apps still run from another location uninterrupted, i.e., email

In the Cloud…

- **Safety of Cloud Infrastructure**
  - 33+% think cloud infrastructure environments, i.e., IaaS are as secure as on-premise data centers
  - 34-52% have sufficient policies and procedures for cloud infrastructure.
- **Responsibility for defining security requirements …**
  - 21% compliance officers
  - 22% business unit leaders
- **Lacking technologies**
  - 35% have adequate technologies to secure their IaaS environments
- **Auditing**
  - 59% of internal audit reviews don't include feedback on security in the cloud infrastructure environment

Cloud Defenses

- **Defenses organizations Have:**
  - 88% - firewalls to protect sensitive or confidential information
  - 85% - antivirus/antimalware software in place
  - 50%- identity and access management
  - 31% - major cloud providers use encryption to protect data from insider threats.
    - **If data is encrypted,** 69% place non-regulated customer data in the cloud
      - Email address lists, purchase history, shipping information.
    - **If data is not encrypted**, 52% still place this data in the cloud.

Encryption concerns

- View by end users: "over-kill“, not welcomed
- Expensive and intrusive: Encrypting all production data without looking at the value
- Causes degradation in performance
- Data loss if encryption keys are lost or employees refuse to provide passwords
- Another password prompt for information access
- Management of encryption systems - certificates, keys, passwords, additional storage requirements
- IS/IT personnel must work closely
- Finding the right balance among locking data down, discomfort, and acceptable risk.

DIY

- **Web exploit toolkits, purchased and traded online, let hackers access enterprise IT systems to steal mission-critical data.**
  - 80%+ attacks successfully infected systems.
- **Blackhole: Pre-packaged Attacks**
  - Vulnerabilities
  - Exploit delivery
    - compromise through SQL, injection, XSS, etc.
    - Spam campaigns – send malicious email
  - Anti-detection
  - Compromise hosts
- **Malicious attacks skyrockets as hackers explore new targets**
  - Increased use of toolkits

DIY

- **Reconnaissance**
  - Use poor coding practices to detect web server info
  - Social engineering
- **Obfuscation**
  - The deliberate act of making code difficult to understand
  - Used to evade security devices
    - JavaScript
    - Exploit (driven by exploits in the wild)
    - PDFs

APPROACHES

A New Way of Thinking

- **Current State**
  - Old paradigm - target threats, block the threat
  - Common approach - stacks of AV layers searching for inbound attacks
  - No silver bullet or single solution
  - Threats evolve yet remain cyclical
    - High tech, low tech, no tech
  - Threat-centric
  - Core configuration and vulnerability exposure of the endpoint overlooked or low priority.

Current to Desired State…

Traditional

- **Blacklisting as the core**
  - Zero Day
  - 3rd Party App Risks
  - Malware-as-a-Service
  - Consumerization of IT

Layered, Defense-in-Depth

- **Guard data and endpoints**
- **Use a layered approach**
  - Lvl 1: Patch/Configuration Management
  - Lvl 2: Application Control
  - Lvl 3: Device Control
  - Lvl 4: AV/AntiMalware, Firewalls, etc.
- **Forensics analysis**
- **Digital rights management**
- **Security policy management**
- **Protect intellectual property**
- **Enforcement policies**
- **Training/employee awareness**

A New Way of Thinking

- **Layer 1: Patch and configuration management**
  - Can eliminate much of the attackable "surface area" of your endpoints (OS, 3rd Party vulnerabilities)
- **Layer 2: Application whitelisting**
  - Prevents unknown/unwanted software and malware executing on endpoints and servers.
- **Layer 3: Data encryption**
  - Protects data that traverses/resides on your servers, networks and endpoints.
- **Layer 4: Device control (DMZ, IDS/IPS, Firewalls, Log Mgmt., Lifecycle development), AV, Training, DLP, Policies, etc.**
  - Enables central management
  - Enforce security policies
  - Prevent data loss and theft
  - Thwart malware intrusion.

Trusting apps - Risk-based

- **Automate monitoring**
- **Remember many internet apps are not trustworthy**
- **Many legitimate apps for PCs, fewer for mobile**
- **Android apps subject to modification in the open**
  - **Buyer Beware:** downloads from app store may not be what you think
  - **Discipline Required:** Mobile apps on a corporate network a vector for cyber attacks
- **Connect all business and organizational processes to security requirements**

Summary

- Create a formal BYOD policy (compliance)
- Audit wireless network and identity services
- Create a DR/BCP Plan with resiliency in mind
- Use a layered, defense-in-depth approach
- Conduct a risk assessment of your environment
- Manage changes to your environment

Thank you!

Dr. Denise Chatam Walker

Chief Emergency Management Officer
Lone Star College System
Houston, TX
281.290.3680
Denise.c.walker@lonestar.edu

Resources:

*"**Cybercrime: Secure IT or Lose IT** (2008) and "**Mass Notification and Crisis Communications: Planning, Preparedness, & Systems**",* Dr. Denise Chatam Walker, (2011)

References

Geers, Kenneth. Cyberspace and the Changing Nature of Warfare, NATO Open, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2011
Evault, 10 Steps to Safeguard Small Business Data, 2012
Emerging Threats - How Quickly They Emerge, and How Much of a Threat Will They Really Be?
Symantec, Internet Security Threat Report, 2011
Washington State Dept. of Labor & Industries, Underground Economy Benchmark Report, 2011 Report to the Legislature, Nov. 2011
McAfee/SAIC, Underground Economies, 2012
MainNerve, Inc., The Internet Underground Economy, March 2012
Latisys, Is Your Organization Ready for the Cloud?, May 2012
Araujo, Charles. Managing Across the Cloud Ecosystem: Risks & Opportunities, April, 2012
HP, On Failure in Managed Enterpriese Networks, (HPL-2012-101), May 2012
HP, HP Labs 2011 Annual Research Report, February 2012
Ponemon Institute, Increasing Encryption Deployments ... The Response to Compliance Regulations & Cyber Attacks, April 2012
Ponemon Institute, Unleash the Power of Web 2.0, September 2012
Evault, The Essentials Series: Strategies for Cloud Storage, Data Protection, & Disaster Recovery, 2012
HP, Top Security Threats & Trends: 2011 Cyber Risk Report, 2012
Three Technology Challenges of 2012: Mobile Device Management, DR and Security, 2012
Schoenfeld, Steve. Blue Coat, 2012 Security Trends & Technology, 2012
Grossman, Jeremiah, The Top Five Myths of Website Security, Whitehat Security, 2011
Charney, Scott. Trustworthy Computing Next, Microsoft Corp., February 2012
Brandon, John. 10 Predictions for What the CIO Role Will Look Like in 2020, www.cio.com, May 3, 2012
Cloud Security Alliance. State of the Web 2012. May 2012