MACPA
CPE Mega Conference

Defending Against Cyber Threats:

Understanding Vulnerabilities & Implememting Best Practices

October 24, 2013

Claudia Rast, JD

BUTZEL LONG
ATTORNEYS AND COUNSELORS

Cybersecurity Basics

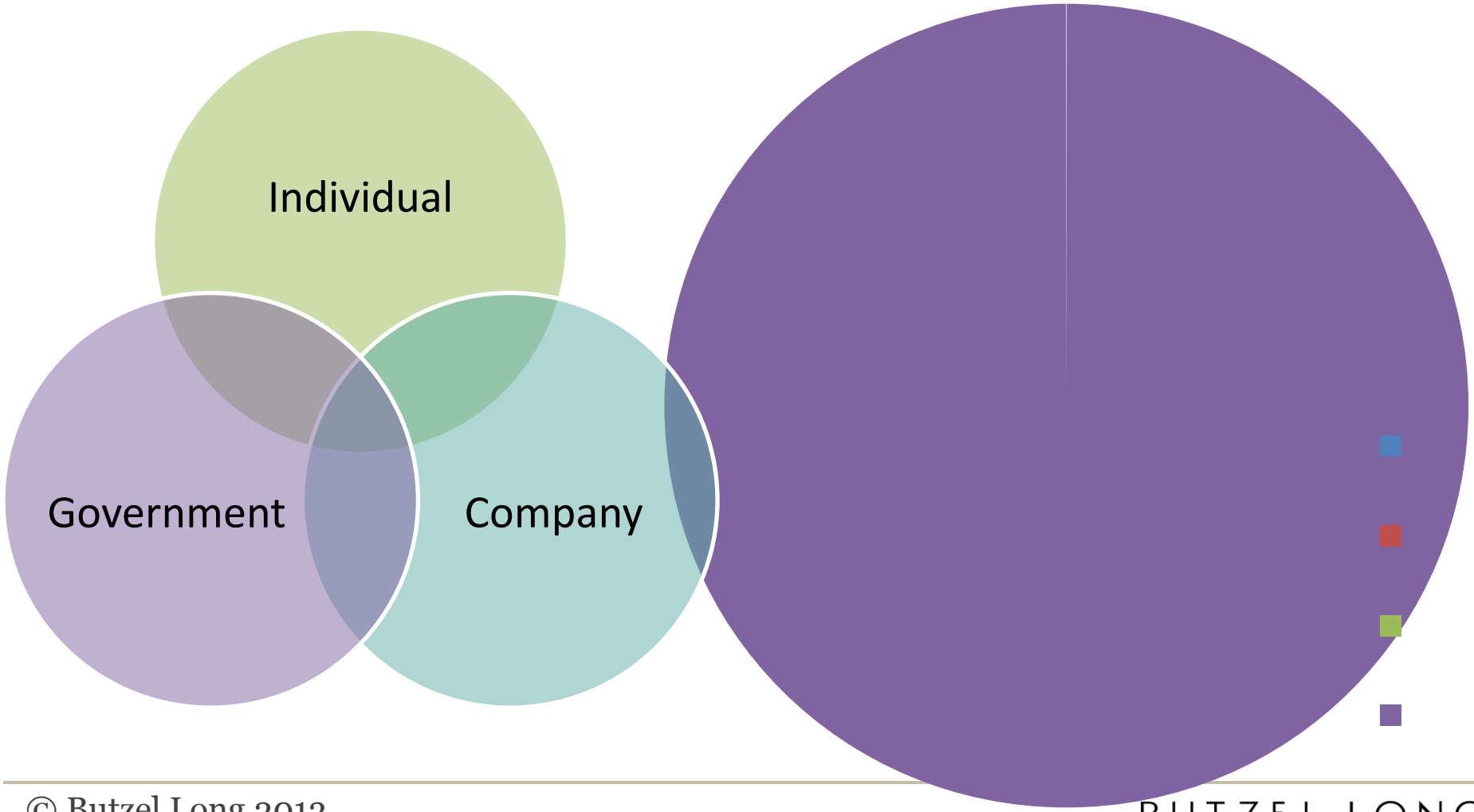
- What Are the Threats?
- Who Are the Threat Agents?
- Who Are they After?
- What Do they Want?
- What Are their Methods?
- Deconstructing a Cyber Attack
- What Are the Results of such Attacks?
- Tools, Tips & Best Practices

The Elements

- Privacy
  - Name, address, SS#, CC#, PII, PHI, ePHI
  - Anonymous aggregated data? (Acxiom, etc.)
  - Google Now
  - Predictive Apps are 80% accurate
- Security
  - Person
  - Place

The Disappearance of Privacy

Private/Public Data

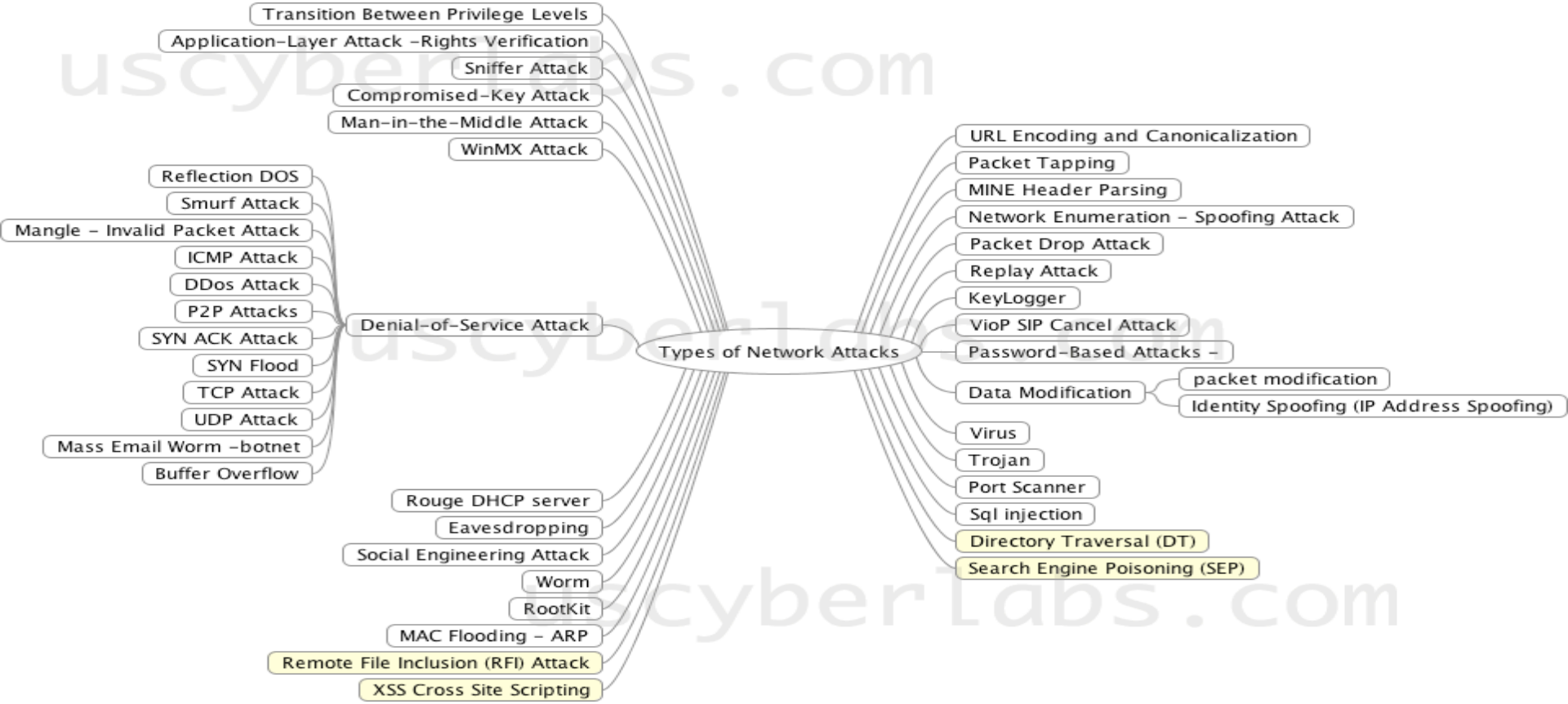


Breach & Theft

- Unknowing/Ignorant/Careless
- Grossly Negligent
- Intentional/Willful
- Malicious/Terrorist
- State-Sponsored

What Are the Threats?

From USCyberlabs.com



Who Are the Threat Agents?

- Corporations
- Cybercriminals
- Insiders/Employees (Ed Snowden)
- Hacktivists (Anonymous; WikiLeaks)
- Nation-States (China; Russia)
- Terrorists (Iran; Syria)

CERT Insider Threat Profile

- >30% of Insider Saboteurs had prior arrest history (2011 study showed 30% of U.S. adults arrested by age 23)
- Behavior Issues: bragging about the damage they could do if they wanted (trigger: passed over for promotion)
- Using Company resources for side business or talk re competing business
- Coercing coworkers to get credentials
- Warning: >70% IP theft occurs w/in 30 days of announcing departure
- >50% Insider Saboteurs were former employee with access via "backdoors" or credentials that were never disabled

from Carnegie Mellon's Common Sense Guide to Mitigation Insider Threats, 4th Ed. Dec. 2012

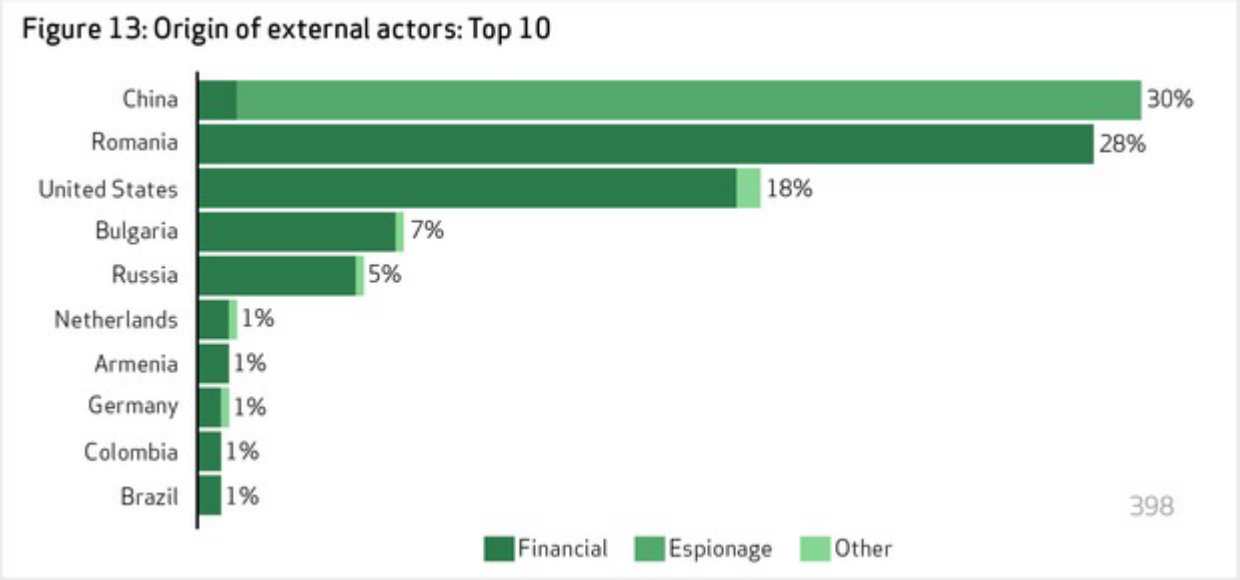
CERT: Insider Threat Findings

- Criminals who executed a "low and slow" approach accomplished more damage and escaped detection for longer
- Insiders' means were not very technically sophisticated
- Fraud by managers differs substantially from fraud by non-managers by damage and duration
- Most cases do not involve collusion
- Most incidents were detected through an audit, customer complaints, or co-worker suspicions
- Personally identifiable information (PII) is a prominent target of those committing fraud

from Carnegie Mellon's Common Sense Guide to Mitigation Insider Threats, 4th Ed. Dec. 2012

Nation-State Threat Agents

From Verizon 2013 Data Breach Investigations Report:



*Who Are They After?**

- Manufacturing
- Finance and Insurance
- Information and Communication
- Health and Social Services
- Retail and Wholesale

from IBM Security Services Cyber Security Intelligence Index, June 2013

What Do They Want?

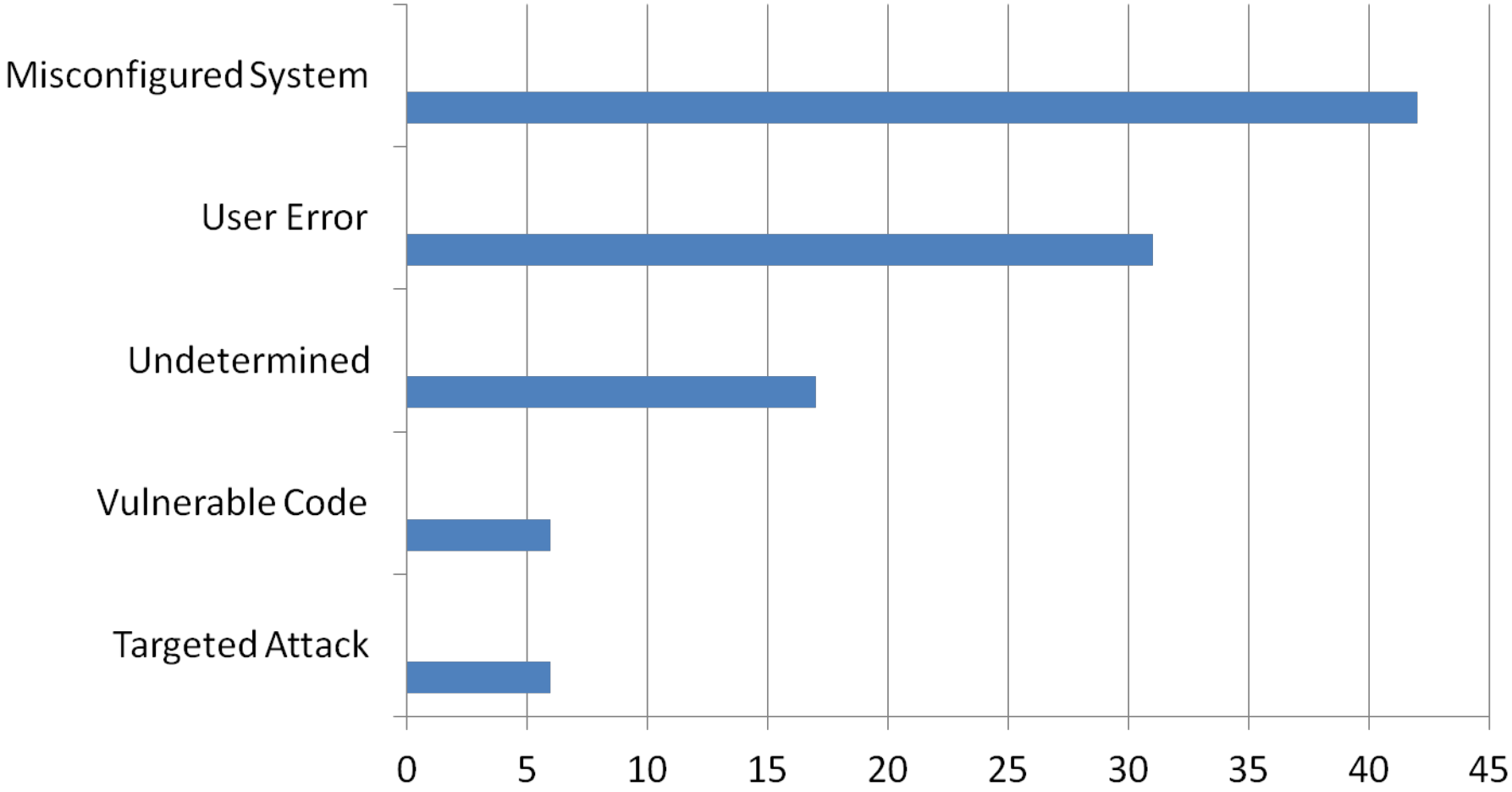
- Money
- Information
- Mayhem

*What Type of Information Do They Want?**

- New Energy Sources
- Energy Conservation
- Bio-Tech (including pharma and nano)
- New Materials & Minerals (e.g., rare earth)
- Information Technology
- Hi-End Equipment Manufacturing ("know-how, not necessarily “processes”)
- Clean Energy Vehicles

From China’s Five-Year Plan released March 2011

What Are Their Methods?



*Top Domestic Threats 2012-13**

from IBM Security Services Cyber Security Intelligence Index, June 2013

- Code Injection 35%
- Sustained Probe/Scan 28%
- Unauthorized Access 13%
- Suspicious Activity 12%
- Access or Credentials Abuse 10%
- DDoS Attacks 2%

Top 10 Threat Methods in Europe 2012

(ENISA) European Network and Information Security Agency

1. Drive-by Exploits
2. Worms/Trojans
3. Code Injection
4. Exploit Kits
5. Botnets
6. DDoS Attacks
7. (Spear)Phishing
8. Data Breaches
9. Rogueware /Scareware
10. SPAM

Deconstructing a Cyber Attack…

Spearphishing ***(social tactics: 4x increase from 2011 to 2012)***

This is an email sent to Mandiant Employees

Date: Wed, 18 Apr 2012 06:31:41 -0700

From: Kevin Mandia <kevin.mandia@rocketmail.com>

Subject: Internal Discussion on the Press Release

Hello,

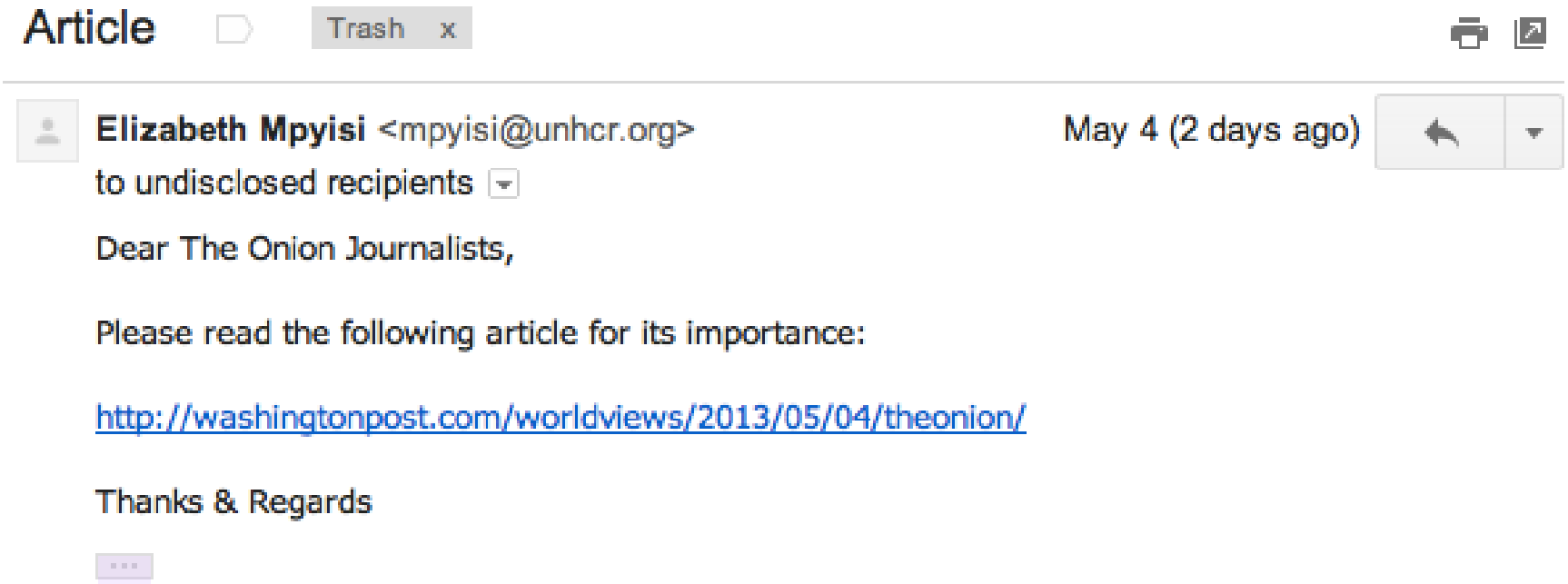
Shall we schedule a time to meet next week? We need to finalize the press release.

Details click here.

Kevin Mandia

Spearphishing @ The Onion

- The Syrian Electric Army sent phishing emails beginning May 3, 2013:


Article

Trash x

Elizabeth Mpyisi <mpyisi@unhcr.org> May 4 (2 days ago)

to undisclosed recipients

Dear The Onion Journalists,

Please read the following article for its importance:

http://washingtonpost.com/worldviews/2013/05/04/theonion/

Thanks & Regards

Once "In," What Can They Do?

- Create/modify/delete/execute programs
- Upload/download files
- Create/delete/directories
- List/start/stop processes
- Modify system registry
- Take screenshots of user's desktop
- Capture keystrokes
- Capture mouse movements
- Start interactive command shell
- Create a remote desktop interface
- Harvest passwords
- Enumerate users
- Enumerate other systems on the network
- Set system to "sleep" (go inactive)
- Log off the current user
- Shut down the system

How Do They Get In?

- Poor Access Controls
- Improper/Weak Authentication
- Insufficiently Protected Credentials
- Poor Patch Management; Weak Testing
- No Defined Security Perimeter; Lack of Network Segmentation
- Improper Device Configuration; Poor Monitoring
- Lack of Security Audits, Logging Practices
- Weak Enforcement of Remote Login Policies

Sources & Targets: It's Us.

Source

- Mobile Computing *(controlling BYOD)*
- Social Media *(online & customer service)*
- Big Data

Target

- Critical Infrastructures *(electric, oil, gas, water, traffic, ports, chemical)*
- Trust Infrastructures *(finance, insurance, accounting, legal)*
- The Cloud *(who owns, who controls, where located)*

Example of Cyber Risks to Industry

- Access to Power: Electric Grid
- Access to Water: Potable & Operations
- SCADA Controls
- EMS/HVAC
- Communications
- Loss of IP, Trade Secrets
- Worse Case: Loss of ALL Data—Aramco, August 2012 (30,000 computers wiped)

What Results from Cyber Attacks?

- 2007: Oak Ridge National Lab hacked via email w/attachment; unknown outsiders get access to databases
- 2008: CIA reports hackers disrupt, or threaten to disrupt 4 foreign cities
- 2009: US UAV's hacked by Iraqi insurgents using $24.99 software; can "see" what UAVs see
- 2011: FBI identifies 20 incidents where online banking credentials of small-med. US biz compromised; $20M in fraudulent attempts→ $11M in real losses
- 2011: US Chamber of Commerce network penetrated for >1yr by PLA with full access to member communications & trade policy positions

What Results? (cont.)

- 2012: APT1 Intrusion of Telvent/Schneider
  - Company controls > ½ oil/gas pipelines in North and Latin America
  - Firewall breached and SCADA files stolen
- 2012: Tridium NiagraAX EMS Software
  - NJ manufacturing company's weak credentials storage exploited
  - State gov't bldg EMS exploited by weak authentication
- 2012: Cyber-attack "Red October" since 2007, using vulnerabilities in Word & Excel; gathered info from embassies, research firms, military, energy, nuclear & other critical infrastructures; full extent & dmg unknown
- 2012: US ICS-CERT reports 2 power plants suffer critical malware infections from USB drives

What Results? (cont.)

- 2013: DOE hacked, 14 servers & 20 workstations compromised; sophistication indicates foreign gov't
- 2013: Watering Hole Attacks; Visitors Spread Poison Ivy
  - Council of Foreign Relations
  - Department of Labor
  - Capstone Turbine Corporation
- 2013: Syrian Electric Army → BBC, CBS, AP Wire, The Onion
- 2013: Mopar & other auto suppliers hacked in North America & Europe
- 2013: US reports electric grid under near constant attack from multiple actors

Current Federal Activities

- Executive Order 13636: Improving Critical Infrastructure Cybersecurity -- released on February 12, 2013
  - Relies on public-private collaboration
  - Enhance information sharing, develops a cybersecurity framework, and creates a voluntary cybersecurity program
  - Requires the Department of Homeland Security to identify the "critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national Security"
- H.R. 624: Cyber Intelligence Sharing and Protection Act (CISPA) Sponsor: Rep. Mike Rogers [MI-8]
- S. 21: Cybersecurity and American Cyber Competitiveness Act of 2013 Sponsor: Sen. John D. Rockefeller [WV]

Cyber Insurance is Available, But

- A May 2013 DHS Roundtable identified five uninsurable risks:
  - Catastrophic Risks where federal gov't should be responsible (e.g., cyber Pearl Harbor, 9/11)
  - Operational Mistakes (e.g., true negligence)
  - Reputational damage
  - Industrial espionage
  - Data as an asset (e.g., IP, trade secret)

Breach Costs & Risk Protection

- Verizon's 2013 Data Breach Investigation Report documented 1.1Billion compromised records between 2003 and 2012
- Average cost per compromised record in 2012: $188 (down from $210 in 2010)
- Average cost per data breach incident to a company: $5.4M (down from $7.2M in 2010)
- Building the Effective Cyber Risk Culture (DHS May 2013)
  - engaged executive leadership
  - targeted cyber risk management and awareness
  - cost-effective technology investments tailored to organizational needs
  - relevant cyber risk information sharing

Best Practices for Management

- Perform Risk Assessment (Physical Plant, Information Systems & Workforce)
- Segregate & Secure High Risk Information, Operations & Workers
- Implement Company-wide Training (onging)
- Incorporate Security By Design (i.e., from the beginning)
- Enable Network Security Monitoring & Review of Log Files
- Demand Compliance from Contractors & Suppliers
- Conduct Table-Top Drills
- Have Experts at the Ready If/When an Attack Occurs

Best Practices for Social Media Staff

- Password / Access/ Control
  - Most Common Passwords: "password" and "123456" and any four-digit number beginning with "1" (most born in 20th Century)
- Centralize Social Media Channels
  - Consolidate accounts to publish from one secure interface
- Control Those with Access to Media
  - Not the place for interns, entry-level staff
- Train Those with Access to Media
  - Social Media is a $1.3 Trillion Market

Hire Qualified IT Professionals

- Don't allow staff with no IT expertise to hire IT professionals
- Establish formal job descriptions that detail the responsibilities, educational and professional requirements, and organizational reporting for key privacy management positions
- Implement hiring practices that include comprehensive screening of credentials, **background checks**, and reference checking
- Develop training programs related to privacy and security matters
- Conduct regular performance appraisals on these key personnel

Best Practices for IT Department

- Eliminate Unnecessary Data
- Conduct Ongoing & Active Risk Analysis
- Collect, Analyze & Share Incident Data
- Collect, Analyze & Share Tactical Threat Intelligence, Especially Indicators of Compromise
- Focus on Better & Faster Detection
- Establish Metrics: "Number of Compromised Systems" & "Mean Time To Detection" in Networks; Use Metrics to Drive Security
- Evaluate Threat Landscape to Prioritize Treatment Strategy (It's not a "One-Size Fits All" World)
- Track Workforce: Who's Who, What they Do & When they Go

Opportunities for the Audit Profession

- Privacy Audits
  - Gramm Leach Bliley
  - HIPAA/HITECH
- Security Audits
  - HIPAA/HITECH
- Payment Card Industry (PCI) Audits
- Cybersecurity Audits
  - Vulnerability, Intrusion & Penetration Testing

QUESTIONS