Silent Attack:
The Importance of Cyber Security
Owen Zorge
State of Arizona
State Compliance and Privacy Officer
Equifax Breach

- 145.5 Million consumers affected
- $200 - $300 Million cost estimate after insurance
- Total $4 Billion company value loss
- Preventable
  - Apache Struts patch available 2 months prior to breach.
  - Encryption of sensitive data
    - Personally Identifiable Information
    - Protected Health Information
• 13 Russian nationals indicted in Mueller investigation on charges related to meddling in US elections

• UK and US blame Russia for 'malicious' NotPetya cyber-attack

• Cyberattack Caused Olympic Opening Ceremony Disruption

• FBI and Homeland Security launch probe as foreign cyber attackers target U.S. water supply
Why Cyber?

- “There is no such thing as a cyber emergency, there are only emergencies caused by many things. In order to declare a state of emergency you need to have kinetic affects, threats to health and public safety”

- Many things can cause an emergency: nature, man made, cyber, accident, malfunction

- Major General Michael McGuire TAG State of Arizona
Cyber Disruption and Physical Effects

Electrical Grid

Oil and Gas Pipelines

Economy

Water infrastructure
Cyber Disruption and Physical Effects

Transportation

Wildfires

Weather

Mass Notification
What did go Wrong?
History of cyber and physical

- DHS Generator
- Natanz nuclear power - Iran
- North Carolina
- Ukraine power grid
- Internet of Things (IoT) attack
- Dallas sirens
- WannaCry ransomware
- Notpetya ransomware Maersk

Sept 2007
Nov 2007
Jan 2014
Dec 2015
Oct 2016
April 2017
May 2017
June 2017
Who and How

Who

• Hacktivists
  – Anonymous, WikiLeaks
• Insiders
  – Snowden
• Criminals
  – Individuals, gangs, groups
• Terrorist
  – ISIL, al-Qaeda
• Nations
  – US, China, Russia, Israel, Iran

How

• Structured Query Language (SQL) injection
• BotNet
• Phishing
• Social Media
Why is there concern?

### Why - Attacks
- **Cyber Investigations**: 15/Day
- **Trojan Attempts**: 3000/Day
- **SQL Injection**: 50/Day
- **SPAM**: 100K/Day
- **Web Activity**: 8.3M/Month

### Why - Cost
- **2017 - 1579 breaches** (+45% over 2016)
- **178,955,069 Records** (+389% over 2016)
- **157,953,329 SSNs** (+702% over 2016)
- **14,207,346 Payment Cards** (+90% - over 2016)
- **@$225 = $40,264,890,525** cost to organizations
Problem Statement

- Gaps in security in every Agency
- Inefficiencies in Security in the form of duplication in every agency
- Increased risk in agency scorecards
- Lack of economies of scale with enterprise purchasing
- Lack of knowledgeable cyber resources in all agencies

<table>
<thead>
<tr>
<th>State</th>
<th>Number of Records</th>
<th>Type of Incident</th>
<th>Loss Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Montana</td>
<td>1.3M</td>
<td>Incident</td>
<td>$250K</td>
</tr>
<tr>
<td>Utah</td>
<td>280K</td>
<td>Data Breach</td>
<td>$3.2M</td>
</tr>
<tr>
<td>South Carolina</td>
<td>3.2M</td>
<td>Data Breach</td>
<td>$27M</td>
</tr>
</tbody>
</table>

Arizona
- Attacked by ransomware and encrypting files
- Suffering credential compromise and fraud losses
- Downloading Trojan to compromise identity, gain access to applications, and put into question the integrity of data
Layered Security

Protect – National Cyber Security Framework

Identify
- Asset Management
- Business Environment
- Governance
- Risk Assessment

Protect
- Access Control
- Awareness Training
- Data Security
- Information Protection
- Maintenance
- Protective Technology

Respond
- Response Planning
- Communication
- Analysis
- Mitigation
- Improvements

Recover
- Recovery Planning
- Improvements
- Communication

Remediate – Critical Security Controls

20) Penetration Tests and Red Team Exercises
19) Incident Response and Management
18) Application Software Security
17) Security Skills Assessment and Appropriate Training to Fill Gaps
16) Account Monitoring and Control
15) Wireless Access Control
14) Controlled Access Based on the Need to Know
13) Data Protection
12) Boundary Defense
11) Secure Configurations for Network Devices
10) Data Recovery Capability
09) Limitation and Control of Network Ports
08) Malware Defenses
07) Email and Web Browser Protections
06) Maintenance, Monitoring and Analysis of Audit Logs
05) Controlled Use of Administrative Privileges
04) Continuous Vulnerability Assessment and Remediation
03) Secure Configurations for Hardware and Software
02) Inventory of Authorized and Unauthorized Software
01) Inventory of Authorized and Unauthorized Devices
00) Penetration Tests and Red Team Exercises

16 Enterprise Security Controls

Discovery Phase
Education- ISO, CIO, Dir
Scheduling
Implementation

16 Security controls to Enterprise

CSC13 – Data Loss Prevention
CSC12 – Distributed Denial of Service
CSC4 – Application Penetration Testing
CSC4 Vulnerability Assessments
CSC6 – Security Information Event Management
CSC4 – Vulnerability Management Tool
CSC5, CSC14, CSC16 – Directory Audit Tool
CSC17, CSC20 – Security Awareness

CSC7 – Spam Filter
CSC12, CSC18 – Web Application Firewall
CSC7 – Web Content Filtering
CSC8 – Advanced Endpoint Protection
CSC6 – File Integrity Management
CSC6 – Security Monitoring
CSC3, CSC11 – Server Hardening
CSC14 – Multi Factor Authentication
Vendor Day

RiskSense

Cloudflare

SAC - The Security Awareness Company

Gemalto

Forcepoint

Dell

Cylance

Secureworks

Arizona Department of Administration
Goal Council Project

Enterprise Security

Reduce risk to State of Arizona
Build efficiencies and economies of scale
Save money
Goals

• Statewide score of 700 by December 31, 2017
  – Accomplished with a Statewide score of 739
• All agencies to attain a score of 700 or greater by March 31, 2018
• September 2017

• February 2018
Cloud Baseline Security Controls

• Based on NIST 800-53 Rev 4 controls
  – 16 State of Arizona Statewide IT Security Policies
• Used to evaluate Infrastructure as a Service and Platform as a Service
• Three levels of control review:
  • AZ Mandatory Control Baseline: 35 Controls
    • For RFP and other processes to assess multiple vendors
    • For public facing data and websites
  • NIST Low Control Baseline: 125 Controls
    • For Data Classification Category: Public
  • NIST Medium Control Baseline: 325 Controls
    • For Data Classification Category: Confidential
**Arizona Security Operations Center (AZ-SOC)**

- Daily monitoring of multiple systems
  - Multi State Information Sharing and Analysis Center (MS-ISAC)
  - Security Information and Event Management (SIEM)
  - Intrusion Detection Systems
  - Next Gen Firewalls
  - Arizona Cyber Threat Response Alliance (ACTRA)

- Daily AZ-SOC Alerts
  - Agencies alerted to threats
  - Required to acknowledge and respond to alerts
  - Required to investigate, remediate and report back to AZ-SOC
Cyber Disruption

• Include Whole Community in ongoing cyber discussion
  – Federal, National Guard, state, county, local, tribal, private sector
  – Exercise capabilities across Whole Community to identify gaps

• Continue to enhance and educate on the importance of timely information sharing.

• All hazards response to cyber incidents
Preparedness - Partnerships

- Arizona National Guard
  - Network Assessments and Cyber Response
- US Department of Homeland Security
  - Protective Security Advisors
  - Cyber Security Advisors
- FBI Infragard
- Arizona Cyber Threat Response Alliance (ACTRA)
  - Organization of public and private companies
  - Real time & Actionable Threat Information
  - Arizona Cyber Warfare Range
- Arizona Counter Terrorism Information Center (ACTIC)
- Multi State – Information Sharing and Analysis Center (MS-ISAC)
Cyber Exercises & Workshops

- National Cyber Security Awareness Month: October
  - Regional workshops and exercises
- State Cyber Tabletop Exercises
- US Department of Homeland Security Cyber Guard Prelude
  - May 2015, 2016, 2017
- US Cyber Command Cyber Guard
  - June 2015, 2016, 2017
- National Guard Cyber Shield
Incident Response and SEOC

- Incident Starts Locally
- National Incident Management System (NIMS)
- Incident Command System (ICS)
- County, Tribal and State Emergency Operations Centers
- State Emergency Response and Recovery Plan (SERRP)
  - 15 Emergency Support Functions (ESF)
  - 7 Support Annexes
  - 6 Incident Annexes, Cyber Incident Annex
  - Primary and Support Agencies for Each Function and Annex
Cyber Annex Overview

• Primary Agency
  – Arizona Department of Administration, Arizona Strategic Enterprise Technology

• Support Agencies
  – State
  – Federal
  – Military
  – Private
## Arizona Cyber Annex Overview

<table>
<thead>
<tr>
<th></th>
<th>System Fault (1)</th>
<th>Accident (2)</th>
<th>Disaster (3)</th>
<th>Crime (4)</th>
<th>Terrorism (5)</th>
<th>Act of War (5)</th>
<th>Key:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scope</strong></td>
<td>Statewide</td>
<td>Statewide</td>
<td>Regional</td>
<td>National</td>
<td>Global</td>
<td></td>
<td></td>
</tr>
<tr>
<td>End User (Client)</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>R = Responsible</td>
</tr>
<tr>
<td>Service Provider</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A = Assist</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>Federal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>US-DHS</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td></td>
<td>C = Coordinating</td>
</tr>
<tr>
<td>US-DOJ/FBI</td>
<td>S</td>
<td>P</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td></td>
<td>P = Primary</td>
</tr>
<tr>
<td>US-SS</td>
<td>S</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td></td>
<td>S = Supporting</td>
</tr>
<tr>
<td>DoD</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>P</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>State</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AZ-DEMA</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AZ-DOA/ASET</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACTIC</td>
<td>S</td>
<td>S</td>
<td>P</td>
<td>S</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AZ-DPS</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AZ-DOHS</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AZ-AGA</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AZ-GOV</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS-ISAC</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Law Enforcement</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIO/CISO</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. End User (Client) - Network and Computer owners and users
2. Service Provider - Entities providing information technology interconnection and internet service
3. Manufacturer - Hardware and software manufacturers
4. FBI and USSS share jurisdiction for most cyber crimes
Cyber Disruption Resources

• Emergency Management Assistance Compact (EMAC)
• National Guard Cyber Protection Teams (CPT)
  – Nationwide assigned to National Guard, Army, Air Force, and other branches of DoD
• National Guard Defensive Cyber Operations – Element/Team (DCO-E/T)
Federal Cyber Resources

• US Department of Homeland Security
  – Stop. Think. Connect.
    • www.dhs.gov/stopthinkconnect
    • October is National Cyber Security Awareness Month
      – Weekly Themes
    • Toolkits: Students, Parents and Educators, Professionals, Older Americans, Government, Industry, Small Business, Law Enforcement
  – US Computer Emergency Readiness Team (US-CERT)
    • www.us-cert.gov
    • Strives for safer, stronger Internet for all Americans by responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners.
  – Ready.Gov
    • Planning Ahead for Disasters
Federal Cyber Resources – Best Practices

• National Institute of Standards and Technology (NIST)
  – www.nist.gov
  – NIST Cybersecurity Framework
    • www.nist.gov/cyberframework
    • Identify, Protect, Detect, Respond, Recover
    • NIST Special Publications (SP)
      – 800-53 Rev 4, Security and Privacy Controls
National Cyber Resources

• Information Sharing and Analysis Centers (ISAC)
  – National Council of ISACs
    • [www.nationalisacs.org](http://www.nationalisacs.org)
  – Sector-based ISACs that collaborate with each other across private and public sector critical infrastructure.
Information Privacy

• Health Insurance Portability and Accountability Act (HIPAA)
  – www.hhs.gov/hipaa/index.html
  – Do you process any Protected Health Information (PHI)?

• Payment Card Industry Data Security Standard (PCI DSS)
  – www.pcisecuritystandards.org
  – Do you process or store any Payment Card information?

• Personally Identifiable Information (PII)
  – NIST SP 800-122
    • www.nist.gov/publications/guide-protecting-confidentiality-personally-identifiable-informationpii
  – Do you process or store SSNs, Date of Birth, etc.?
Local Cyber Resources

- **Arizona Infragard**
  - [http://azinfragard.org](http://azinfragard.org)
  - Mission: to help protect Arizona’s infrastructure by supporting the priorities of the FBI; to cultivate partnerships with public and private sectors through bi-directional sharing of actionable information, training and educational events.

- **Arizona Cyber Threat Response Alliance (ACTRA)**
  - [http://azinfragard.org/?page_id=8](http://azinfragard.org/?page_id=8)
  - Mission: The hub for collaborative cyber information sharing in a neutral environment of trust where partners from industry, academia, law enforcement, and intelligence come together...

- **Arizona Counter Terrorism Information Center (ACTIC)**
  - [www.azactic.gov](http://www.azactic.gov), 1-877-2-SAVE-AZ
  - The ACTIC is a joint effort between the Arizona Department of Public Safety, Arizona Department of Homeland Security, Federal Bureau of Investigation, and other participating agencies... providing both intelligence, investigative and technical support to state, local, tribal and federal law enforcement agencies as well as other agencies critical to Arizona and the country’s homeland security efforts.
Top Cyber Safety Tips

• Use Strong Passwords or Multi Factor Authentication
  – Passphrases, at least 14 characters
  – Different for each website
• Anti Virus and Advanced Endpoint Protection
• Click Carefully!
• Security Awareness Training
• Only install necessary software on systems
  – Patch all software and hardware regularly
  – Test all patches
• Internet of Things
  – Set to auto update and/or update regularly
• Only use supported hardware and software
• Know your data, know your risks
• Use Secure WiFi
  – Be careful of public WiFi
Questions

Owen Zorge
State Compliance and Privacy Officer

Arizona Department of Administration (ADOA)
Arizona Strategic Enterprise Technology (ASET)
Office: (602) 542-0742
Cell: (602) 620-2932
owen.zorge@azdoa.gov
aset.az.gov