THE CHAIN:

Don't Be The Weakest Link

The Basics: What and Why

1. The courts capture and store an extremely valuable asset – detailed data about court users and their activities
   - Criminals worldwide trade in personal information not just credit card numbers
2. Courts are recognized as government entities
   - Malicious groups periodically target government servers and websites for disruption

The Vital Role of Awareness

- Nature of threats changes constantly
- People and assets are pretty static
- Perimeter protection only goes so far
- People are the game changers
- Employees are the last line of protection – therefore the target
- "It's an arms race and knowledge translates to deterrence"

Government Entities Mandating Security Awareness Training for Employees

- State of Michigan
- State of AZ (Exec Br.)
- Cook County, IL (CHI)
- State of New Jersey
- City of Los Angeles
- City of Phoenix

FBI lists organized cyber attacks as its top priority for 2014, replacing terrorism

NASCIO lists information security as the top priority of state CIOs for 2014

Electronic Communications Policy

- Focuses on "being a good neighbor"
- Very basic password practices only
- New Employee Orientation focus
- Accompanies computer usage agreement

- NOT cyber security awareness
- NO periodic retraining takes place

- **Who are the Bad Guys?**
- **What are they trying to do?**
- **How are they doing it?**
- **What is the Impact on the State of AZ?**

Who are the bad guys?
What are they trying to do?

- Organized Crime (Cyber Criminals)
  - ID Theft for Profit
  - Exfiltration of Data for Profit
- Political Terrorists (NS)
  - DDOS (distributed denial of service)
  - Install fear, disruption, mistrust for our government, Trade Secrets
- Hacktivists (Groups)
  - DDOS (distributed denial of service)
  - Exfiltration of Data to Post, support a cause, post on Pastebin
- Malicious Insiders
  - Exfiltration of Data to Sell
  - Possible DDOS
- Amateurs (Script Kiddies)
  - Defacement, games and status

Example: Organized Crime (Facts about ID Theft)

- Americans lost $54B in 2011
- Average ID Theft is $5700
- 30M Americans or 1 in 10 are Victims
- On Average $535 to clean up
- Cost to Organization: $100 - $500
- Value of Data
- State of SC

ID Theft in multiple ways

- Phone
- Mail
- Websites
- Credit card sliders
- Social engineering or casual conversation

Example: Political Terrorism (StuxNet)

Why is StuxNet Significant?

- Four Zero Day Attacks
- Windows OS unharmed
- Rootkit
- Target of specific systems, complexity, Natanz Nuclear power
- Theorized to involved other governments
- Potentially Can Be Used Against Anything

Hacktivists

Example: Hacktivists

- Law Enforcement
  - Arizona State Police
  - Utah Chiefs of Police
  - Wisconsin Chiefs of Police
- Stratfor
- Governments
  - DDOS (Distributed Denial of Service) State of MA
  - DDOS (Distributed Denial of Service) State of MN
  - Michigan State Legislature
  - State of Utah

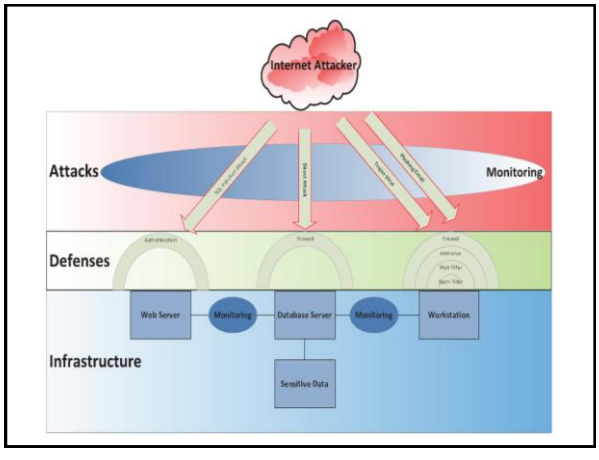
Example: Malicious Insiders (Operation Aurora)

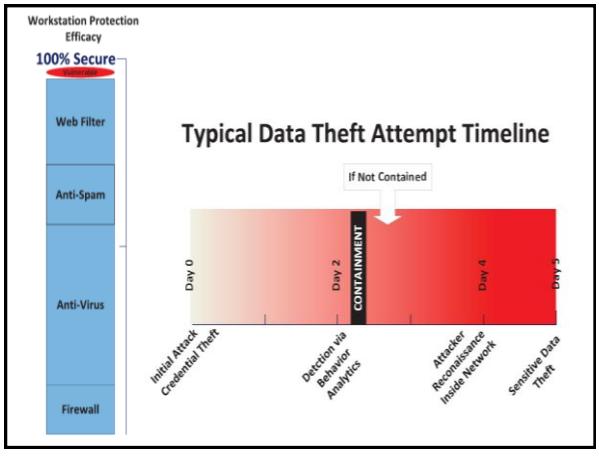
- Google Suffered Cyber Attack
- Chinese insiders spied on others
- Manipulated a vulnerability
- Viewed Email
- Gain access to and potentially modify data at high tech, security and defense contractor companies

Tactics (How are they doing it?)

- Phishing (email reply or clicking on links)
  - Stolen passwords
  - Malware
  - Key loggers
  - Unauthorized Access
- BotNets
  - Denial of Service
  - Distribute Spam
- Infected Websites (ad banners)
  - Install Malware
  - Steal Passwords or other information
- SQL Injection
  - Exfiltration of Data

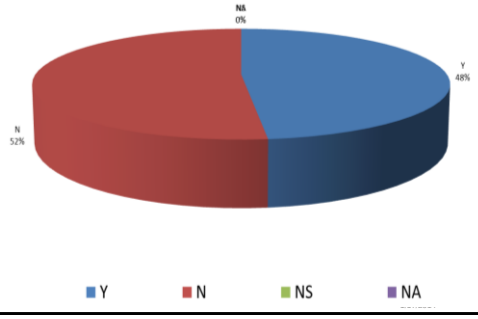
Major Attack/Breach 2011

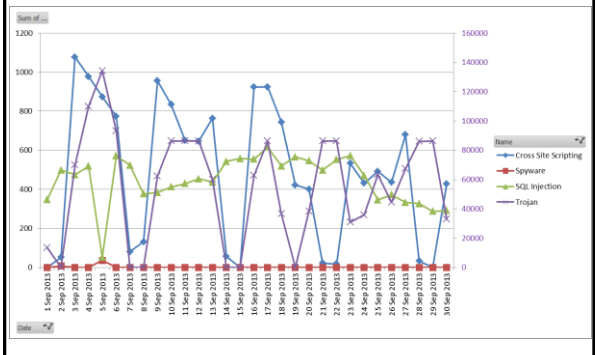


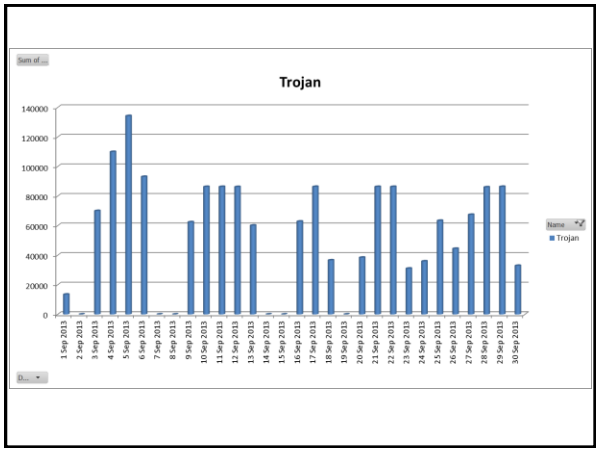


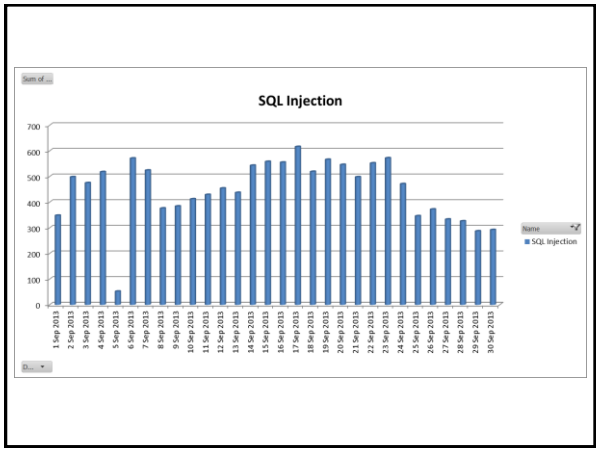
Does this apply to Arizona?

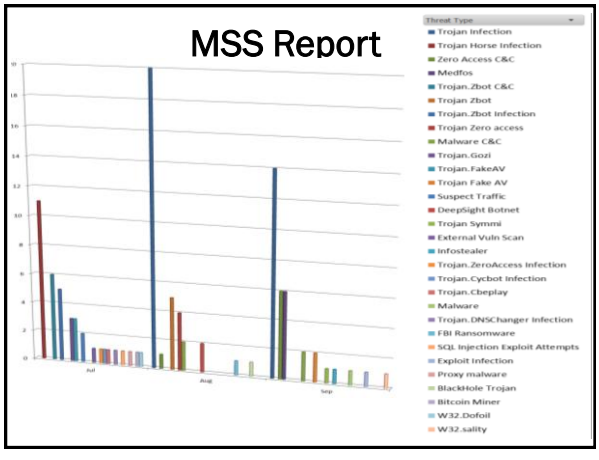
8) Is PII/PHI data available via the internet to authorized and authenticated users? (Y/N)

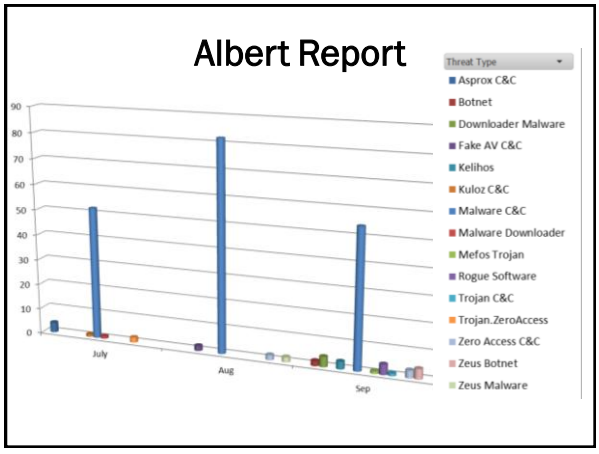


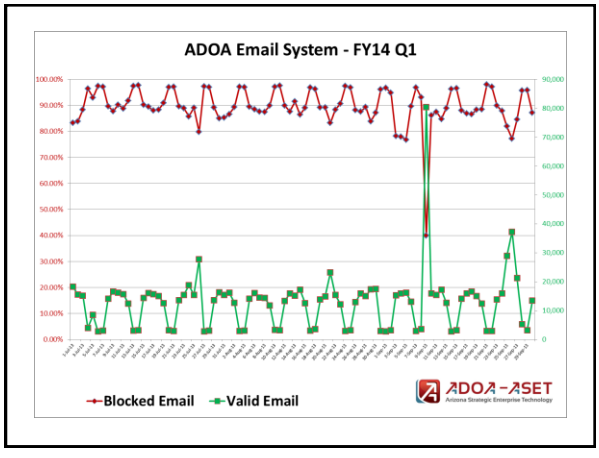


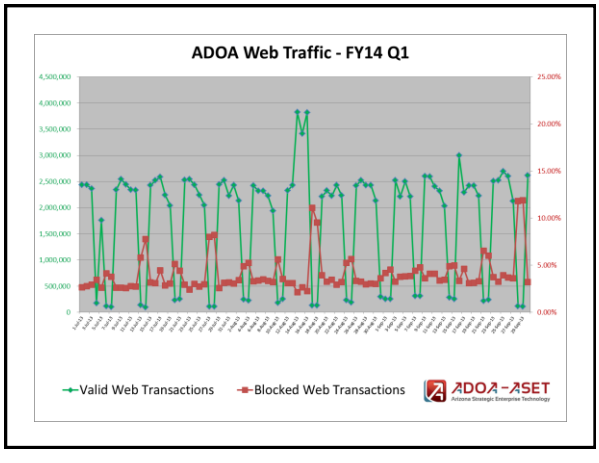

Trojan
Sum of ...
140000
120000
100000
80000
60000
40000
20000
0
Name
Trojan

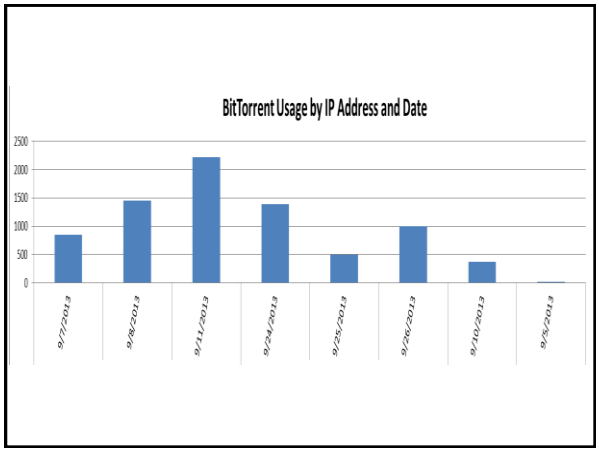

SQL Injection
Sum of ...
700
600
500
400
300
200
100
0
Name
SQL Injection

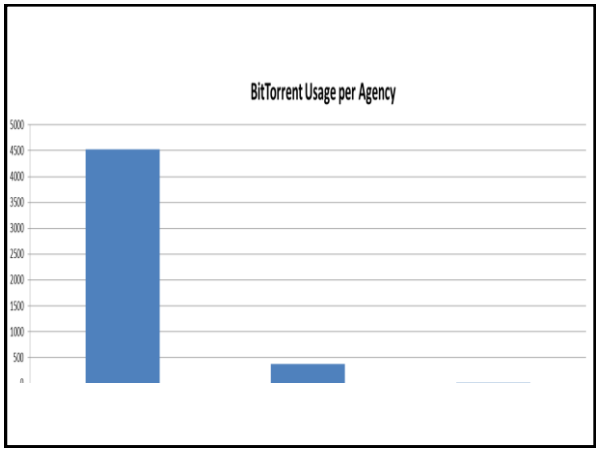

MSS Report
Threat Type
Trojan Infection
Trojan Horse Infection
Zero Access C&C
Medfos
Trojan.Zbot C&C
Trojan Zbot
Trojan.Zbot Infection
Trojan Zero access
Malware C&C
Trojan.Gozi
Trojan.FakeAV
Trojan Fake AV
Suspect Traffic
DeepSight Botnet
Trojan Symmi
External Vuln Scan
Infostealer
Trojan.ZeroAccess Infection
Trojan.Cycbot Infection
Trojan.Cbeplay
Malware
Trojan.DNSChanger Infection
FBI Ransomware
SQL Injection Exploit Attempts
Exploit Infection
Proxy malware
BlackHole Trojan
Bitcoin Miner
W32.Dofoil
W32.sality


Albert Report
Threat Type
Asprox C&C
Botnet
Downloader Malware
Fake AV C&C
Kelihos
Kuloz C&C
Malware C&C
Malware Downloader
Mefos Trojan
Rogue Software
Trojan C&C
Trojan.ZeroAccess
Zero Access C&C
Zeus Botnet
Zeus Malware
90
80
70
60
50
40
30
20
10
0
July
Aug
Sep


ADOA Email System - FY14 Q1
100.00%
90.00%
80.00%
70.00%
60.00%
50.00%
40.00%
30.00%
20.00%
10.00%
0.00%
90,000
80,000
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
Blocked Email
Valid Email
ADOA-ASET
Arizona Strategic Enterprise Technology


ADOA Web Traffic - FY14 Q1
4,500,000
4,000,000
3,500,000
3,000,000
2,500,000
2,000,000
1,500,000
1,000,000
500,000
0
25.00%
20.00%
15.00%
10.00%
5.00%
0.00%
Valid Web Transactions
Blocked Web Transactions
ADOA-ASET
Arizona Strategic Enterprise Technology

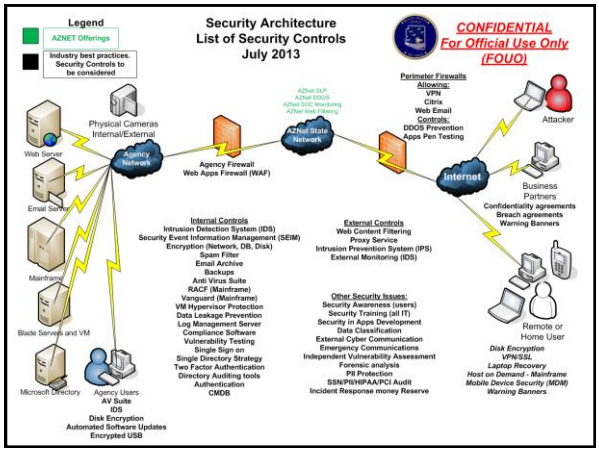




It's All About Awareness

- Surveys
- Report Cards
- Secure coding
- Security Controls Best Practice
- NCSR
- Building a Risk Profile
- Vulnerability Assessments/Penetration Tests

- Asking for Help to Mitigate the Issues



The Internet

The internet puts a wealth of knowledge at your fingertips. It is estimated that close to a billion web pages are added daily. It is also estimated that over 144 billion emails are exchanged per day.

You can make phone calls, send pictures, and share face time with the click of a button. With all this access and ease to world wide information comes responsibility.

The internet is a two way street. You have access to the world and the world has access to you. This is where AJIN and the security mechanisms come into play.

What is AJIN?

(AJIN) or the Arizona Judicial Information Network stretches across all 15 counties in Arizona. It reaches to 181 separate facilities and provides the backbone for our statewide communication network connecting all justice related departments.

Not only does AJIN provide the pathways for our software applications to function, it also creates a secure zone or safe harbor that protects you as you do business functions and access the internet. On the down side, risky behavior by any user at any one of the 181 facilities can potentially affect all other users, since traffic passes very quickly over AJIN.

Security Mechanisms and Controls

AJIN deploys several Proxy systems that filter and scan over 6 million requests to the internet daily. A proxy system is basically a device that intercepts your request to the internet. It then checks the destination to verify it is safe through various controls.

Once the destination is determined safe it assumes your identity and continues the request itself while scanning the traffic to verify it is virus free. It does all of this transparently while keeping you the user safe.

Security Mechanisms and Controls

These same Proxy systems block over 8000 requests daily from users to sites that are either labeled malicious , under a controlled AOC setting, or an infected website trying to send you somewhere that was not your intent.

Security Mechanisms and Controls

The Proxy systems block requested access from within to over 33 countries that typically host malicious websites and /or sponsor outright cyber attacks. We have the capability to control inbound, outbound, or all traffic marked as blocked.

These same countries are scanning our external edge devices (or the firewalls around AJIN), constantly for any possible open doors. They do the scans in little spurts and at all hours of the night to try and remain undetected and unblocked. This gives you an idea of how desperate they are to get to your data.

Security Mechanisms and Controls

AJIN network personnel monitor all traffic inside and outside, 24 X 7, through web proxy appliances and Intrusion Detection Systems.

In the event of a virus outbreak, instructions are sent to automatically block, isolate, and clean the infection on the appliance before it spreads. Should an incident occur we alert all State agencies so they can monitor for it as well.

Security Mechanisms and Controls

The AJIN network team maintains over 40 firewalls throughout the state that are used to allow only designated traffic in and out of AJIN through the security zone.

Without these firewalls in place you could imagine how easy it would be for a compromised computer to infect the entire state.

Security Mechanisms and Controls

AOC contracts with security consultant firms to test our edge devices, like routers and firewalls, to ensure the proper configuration and controls are in place.

When a possible hole in our protection is noted we quickly remove the exposure.

Security Mechanisms and Controls

At times we will even setup what are referred to as "Honey Pots" or systems that have no anti-virus or security on them to capture and locate possible infections so that we can remove them before they spread.

Sometimes, malicious items will slip into the network undetected and wait on a PC or server until some specific event activates them – a classic Trojan Horse. Anti-virus signatures only catch ones that have been activated somewhere and reported.

We want to find and remove harmful code ourselves before it gets activated and spreads – that's a tough job.

On The Watch

You can imagine the time and manpower it takes to keep our network secure in a world that wants to exploit, steal, and manipulate our valuable data. We take security very seriously and so should you as a user on AJIN.

Remember it only takes a single PC to compromise the entire state like what happened back in 2001 when the Code Red II worm was introduced by a compromised computer and spread over the entire state. This infection cost many man hours and travel throughout the state to eliminate it.

PII – Personal Information

- Attracts hackers since it uniquely identifies specific individuals

1. Enter PII only into authorized court systems
2. Use password screensaver with short timer
3. Never put PII on a personal device or store off the network
4. Don't provide it to 3rd parties without contractual arrangement for use and protection

Safety Tip 1

- Never put court data on an external network or device without management authorization to do so.
- AO 2008-68 governs local court communication with affected individuals should a data breach or outright loss occur.
- External devices greatly increase that likelihood.

Safety Tip 2

- Even when PII is not involved, avoid sharing thumb drives from one system to another. Malicious software can easily spread from one computer to another.

Safety Tip 3

- Never open e-mails from someone you do not know. Even when you know the person sending the email, if it looks strange, e-mail them first to ask if they sent it.
- Don't open attachments you aren't expecting!
- Sometimes you will find that someone's e-mail has been compromised somehow and they have no idea the message or attchment was even sent.

Social Engineering

- Simply put, “social engineering” is
  A. The art of human manipulation
  B. Someone masquerading as a person or institution you trust in order to get you to do something they don’t have permission to do
  C. Able to harness any technology to get to you, telephone included
  D. Usually marked by a sense of urgency by the manipulator and facts you are unable to confirm

E-Mail Risk: More Social Engineering

- Basics of Phishing
  - Message contains cues you trust like names of friends or legitimate logos from businesses
  - Often have spelling or grammar mistakes
  - Contains an attachment that is really malicious code and tempts you to open it --OR--
  - Contains links that don’t go where you think they are going
- Bottom Line: These unknowingly install code that compromises your computer and likely spreads to others on AJIN undetected

The Risks of Browsing

- Why is the computer’s browser its most dangerous application?
  A. It allows you to connect to websites you don’t know are malicious and provides a pathway for inserting code into your computer without your knowledge
  B. Its plug-ins can allow other programs direct access to your computer through the web
  C. Browser security settings are typically set low by default

Data Protection

- Security safeguards YOU are personally responsible for using:
  A. A Unique UserID (not shared)
  B. A Locking Screensaver
  C. A Decently Strong Password
  D. Never storing court data on any non-court system

Remember, AO 2008-68 governs data off court network

Creating Stronger Passwords

- How can you make a hard to guess but easy to remember password?

A. Make it a memorable phrase that's the maximum length possible: I love rocky road
B. Or make a longer phrase and use the starting letter of each word in the phrase: One fish two fish red fish blue fish = OFTFRFBF
C. Make some letters upper case: ILoveRockyRoad

Creating Stronger Passwords

- How can you make a hard to guess but easy to remember password?

D. Then substitute at least one number and one special character for letters or at the end
E. !LoveRØckyRØ@d
F. 1F2FrFbF%

Creating Stronger Passwords

- What if you can't remember the password?
  A. Self-resetting using answers to hint questions is becoming the norm
  B. Only select hint questions that are not publicly known
     - Favorite or First Pet Name
     - A Movie Name
     - A Weird Color!

Safety Tip 4

- Never bring your home system to work and plug it into the AJIN network. The system could be compromised and you could quickly compromise the entire network like the scenario mentioned earlier.

Safety Tip 5: Working Remotely

- Activities you perform on the home computer used for VPN access when you telecommute can function as a backdoor to spread infection to the court network and give unauthorized family members access to court resources
- Data and documents you view from your VPN connection for work may remain on your home computer and be accessible to family members

Safety Tip 6: Mobile Devices

- Protect your mobile device:
  A. Require a password/PIN for access
  B. Update to the latest version of the operating system
  C. Only download apps you truly need, some do things other than what they advertise
  D. Don't enable auto connection to Wi-Fi networks
  E. Never jailbreak your smart phone, it compromises device level security controls

Safety Tip 7: Wi-Fi Security

- Recognize risks of using public Wi-Fi
  A. Wi-Fi networks often have no security provisions whatsoever
  B. Unsecured computers can be compromised by attacks over the wireless network without your awareness
  C. All your communications can be eavesdropped on and monitored if not encrypted

Tighten Home Wireless Controls

- If you work from home and use wireless, lock the wireless unit down to the highest security the unit has.
- Do not advertise the wireless SSID in the open
- Do make it a complex name, not the default.
- Lock the unit down by MAC and IP address so that only your device will be granted access.
- Ask the manufacturer to assist you with configuration if you don't understand these.