Today’s Objectives

To Understand

- Background of ALA Information Systems (IS)
- IT Controls
- Our Methodology
- Cyber Security Threats
Who We Are

- IS Audit Section established in 2001
- To support and assist with Financial Audits
- Created IS “Best Practices”

Enabling Legislation

Audit of data processing operations
- (a) The Division of Legislative Audit may conduct audits of all or any part of automated data processing operations or systems of any entity of the state or political subdivision of the state.

- (b) (1) (A) Data processing charges incurred in the performance of audits or audit-related tasks by the division shall be absorbed by the state agency or political subdivision.

(Ark. Code Ann. § 10-4-424)
Who We Audit

- State Agencies, Boards, and Commissions
- Local Political Sub-Divisions (cities and counties)
- Higher Education (2- and 4-year schools)
- Local Education Agencies (school districts and education cooperatives)
- Prosecuting Attorneys

What We Audit

- Applications
- Networks
- Data Centers
- Operating Systems
- Special Projects
Common IS Audit Issues

- Inadequate logical security
- Poor segregation of duties
- **No business continuity/disaster recovery plan**
- Change management
- **Inadequate data backup**
- Inadequate or no application edit controls
- Inadequate or no network security
- Inadequate policies

Common Responses

- My people aren’t smart enough to remember an 8-character password.
- I have a DRP, but it's in my head.
- It’s all public info and subject to FOI anyway.
- There’s nothing worth stealing.
- My backup is on my hard-drive, and that’s good enough.
- I assure you no disaster will happen here.
- My people know each other’s passwords anyway.
Methodology
IT Controls
Controls over computer-based systems are broken down into two major categories:

- Application controls
- General controls

IT – Application Controls
Controls that pertain to the scope of individual **business processes** or **application systems**

- Data edits
- Separation of business functions
- Balancing of processing totals
- Transaction logging
- Error reporting
IT – General Controls
(a.k.a. Infrastructure Controls)

Apply to all systems components, processes, and data for a given organization or systems environment:

- Information security policy
- Administration, access, and authentication
- Separation of key IT functions
- Management of systems acquisition and implementation
- Change management
- Backup and recovery
- Business continuity

Data Integrity

Transactions should perform upfront validation and editing to ensure the integrity of data before it is entered into a system

GARBAGE IN, GARBAGE OUT
Data Integrity (cont.)

- Prefer test system but often conducted on production
- User confirms test and results
- Examples:
  - Invalid Data Rejected
  - Duplicated Receipts
  - Voids/Deletes

Audit Logging

- **Required** in applications where data can be modified
- Audit log table should have an audit log on itself to record any tampering if no assurance that log cannot be modified
- Useful for finding errors and erroneous transactions
- Can serve as a mitigating control to weak data integrity controls
- Not effective unless regularly reviewed
Access Security

- Should be examined from an overall perspective of how password parameters ensure overall logical security
- Password parameters established by “Best Practices”
- Applies to application and network security

Protect & Use Strong Passwords

https://howsecureismypassword.net
HOW SECURE IS MY PASSWORD?

Enter Password

This site could be stealing your password... it's not, but it easily could be. Be careful where you type your password.

How Secure is My Password?

Password

SHOW SETTINGS

Your password would be cracked almost
Instantly

(Tweet Result)

SHOW DETAILS

COMMON PASSWORD: IN THE TOP 10 MOST USED PASSWORDS

Your password is very commonly used. It would be cracked almost instantly.

CHARACTER VARIETY: JUST LETTERS
Access Rights

- Privileges/permissions granted once the user logs in
- Type of user = level of access, based on user role and job responsibilities
- Ensure the use of unique user IDs that can be traced back to individuals
DATA INTEGRITY

Access Controls – Physical Security

What is Physical Security?

Measures used to protect facilities, resources, or proprietary data stored on physical media

Examples:

- Facility monitoring (surveillance systems, cameras, guards, exterior lighting)
- Access controls to facilities/data center/computers (access cards)
- Alarm systems (fire, burglar, water, humidity, power fluctuations)
- Shredding of sensitive documents
- Proper storage/disposal of hard drives and other electronic storage media
- Secure storage of back-up copies of data and master copies of critical software
Remote Access
Enables users outside a network to have network access and privileges as if they were inside the network

Business Continuity Controls
A comprehensive approach to ensuring normal operations despite interruptions
- Disaster Recovery
- Backup and Recovery
Disaster Recovery

- Documentation of procedures to ensure that the organization continues to operate and can successfully recover computer services in the event of a disaster

- Plans must be comprehensive, up-to-date, and approved by key organizational, management, and executive personnel

- Plans must be tested regularly and results documented
Arkansas Continuity of Operations Program (ACOOP)

 Provides resources for development, maintenance, and testing of Disaster Recovery Plans

  - Methodology
  - Hardware
  - Software
  - Training
  - User assistance

http://www.dis.arkansas.gov
Mena, Arkansas
April 9, 2009  8:00 PM

F3 Tornado – 165 mph winds
3 Dead, 30 Injured
>$25 million in damages

Devastated a 25-block area
Destroyed over 100 homes
Damaged over 600 homes

14½ Miles of Destruction
Backup and Recovery

Management should provide a means to back up relevant data on a regular basis

- Backups could be to media (e.g., tape or external hard drive) or to a remote location via the cloud (i.e., the Internet)
- Backup process must be reliable
- Management should provide a means to ensure that the process is actually recording all data onto the target backup device

Technology Trends

- Electronic Funds Transfers (EFT)
- Remote Deposit Capture (RDC)
- Mobile Trends
- Social Media
Electronic Funds Transfer (EFT)

- A generic term
- Two different methods of transferring funds electronically

Most Common Security Threats in E-commerce Environment

- Malicious code (viruses, worms, Trojans)
- Unwanted programs (spyware, browser parasites)
- Phishing/identity theft
- Hacking and cybervandalism
- Credit card fraud/theft
- Spoofing (pharming)/spam (junk) Web sites
- DoS and DDoS attacks
- Sniffing
- Insider attacks
- Poorly designed server and client software
Types of Breaches

- System Breach
- **Account Takeovers**
- Third Party Payment Processor Breaches
- Mobile Banking Exploitation

Account Takeovers

- Cyber crime is easily committed by exploiting the system users, rather than the systems themselves
- Typically done through the compromise of a legitimate user’s account credentials
**Excerpts from an SLA**

“…Shall indemnify the Financial Institution against any loss, liability, or expense (including attorneys’ fees and expense) resulting from or arising out of any breach….”

“…not to detect error in the transmission or content of any entry….”

“…an entry delivered to the financial institution that purports to have been transmitted or authorized by the company shall be effective even if the entry was not in fact authorized….”

---

**Remote Deposit Capture (RDC)**

Allows a user to
- Scan checks
- Transmit scanned images and/or ACH-data to a bank
RDC Risks

• Redeposit of items/duplicate presentment
• Alteration of deposited items/forged endorsement
• Deposit of counterfeit items
• Poor image quality
• Safety and integrity of deposited items held by customers (i.e., protection of personal information)
• Proper disposal of deposited items by customers
• Data security of and lack of encryption in the RDC system
• Reliability of the RDC vendor

Crusade

To educate public officials on the dangers of technology
Statewide Statistics

- **16 million** denials against 1,900 firewalls every day
- 150 open tickets for infected computers at any given time
- More computers infected with malware in 2014 than in the previous 10 years

HOT!! Key logger/Ransom ware

Definitions

**Cyber security**: Technologies and processes designed to protect computers, networks, and data from unauthorized access, vulnerabilities, and attacks delivered via the Internet by cyber criminals

**Cyber attack**: An attempt to damage, disrupt, or gain unauthorized access to a computer, computer system, data, or electronic communications network

**Cyber crime**: Illegal use of computer technology and the Internet
Top Cyber Security Risks for 2015

1. **Insider Threats** – Employees, Contractors
2. **Ransomware** – Malware that restricts access to the computer system that it infects)
3. **The Internet** – Millions of hackers ready to compromise systems
4. **Cyber-espionage** – Governments
5. **Cyber theft** – Especially financial information
6. **Insecure passwords** – Easy-to-crack

Types of Cyber Attacks

- Malware & Malicious Code (viruses, worms, Trojans) – software intended to damage or disable computers and computer systems
- Botnets – network of private computers infected with malicious software and controlled as a group without the owners' knowledge
- Phishing – e-mail fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients
- Web-based Attacks – means by which malicious code exploits a system's security safeguards
- Denial of Service – attack on a computer system or website aimed at disrupting normal functionality
- Malicious Insiders – malicious threat from within the organization (e.g., employees, former employees, vendors, or business associates)
What Makes Cyber Security So Difficult?

• The Enemy is Everywhere
  ❖ Government Sponsored
  ❖ Terrorists Groups
  ❖ Organized Crime
  ❖ “Hactivists”

• Cyber threat “business-driven”
• Low obstacles
• Convoluted multinational law enforcement
• Plenty security solutions
  (e.g., Firewalls, IDS, IPS)
  ❖ Configured properly?
  ❖ Compatible?
Hiddenwiki.info
Best deep web Tor onion links
List updated May 2015

You will need Tor Browser to visit all the links in this page.
More info and download: TorProject.org

Introduction Points

- TorSearch: Search engine for Tor Hidden Services.
- Dnets: A Hidden Service that searches the clearnet.
- TORCH: Tor Search Engine. Claims to index around 1.1 million pages.
- Grams: Search Darknet Markets and more.

Financial Services

- neobuy: Automatic system to buy Paypal accounts and credit cards instantly in your e-mail. Socks5 included.
- WorldBitcoins: Sell your Bitcoins for Cash (USD), ACH, WU/WMG, UK, PayPal and more.
- LocalBitcoins (clearnet): LocalBitcoins.com: Fastest and easiest way to buy and sell bitcoins
TOR

- Free software for enabling anonymous communication
- Directs Internet traffic through a free, worldwide, volunteer network consisting of more than 6,000 relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis

TOR (cont.)

- Although it may not seem like it, when you browse the Internet you are relaying personal information to Web sites
- Your browser likely provides your IP address and sites you have visited to Web site operators
- To see a demonstration of the kind of information that can be captured about your computer via your browser when you surf the Web, visit http://network-tools.com/analyze/
The Privacy.net Analyzer

This site analyzes your privacy on the Internet and shows some of the information web sites can know about you when you visit. The information can be used to display web content based on things such as country of origin and web browser. Read a description of the text [opens new window]. Your IP address is: 100.00.11.1 from United States (US) in North America (Location comes from a database that lists where the addresses are issued).

Host name: webmail.something.gov (configured by your Internet provider)

Your local IP address from Java called by JavaScript is: 

You have a Do-NOT-TRACK Header Set: DNT=1

Cookie Test Cookies are text files saved by your browser (A cookie can only be read by the web site that originally sent the cookie).

No Cookie from this site is on your system.

Macromedia Flash player is installed and web sites may store files on your computer called "Flash Cookies" or "Local Stored Objects (LSO)" and may not be deleted when regular cookies are cleared.

- Adjust your Flash settings [opens new window].
- Test saving a Flash Cookie [opens new window].

Microsoft Silverlight is installed and web sites may store files on your computer called "Silverlight Cookies" or "Local Stored Objects (LSO)" and may not be deleted when regular cookies are cleared. To adjust settings right-click on the box below to view the Silverlight options. Click here for more information [opens new window].

TOR (cont.)
What’s For Sale

- **Premium Credit Cards for Sale**: (Platinum, Gold, Prestige, Black)
  Name Your Card Type & Country of Preference
  100% Satisfaction Guarantee on Stolen Credit Cards or They Will Be Replaced

- **Hacker Training Tutorials**

- **Counterfeit Credentials for Sale**: New Identities, Passports, Driver’s Licenses and Social Security Cards

- **Malware For Sale**

- **Online Bank Accounts for Sale**
## Markets availability status

<table>
<thead>
<tr>
<th>Market</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agora</td>
<td>66.46%</td>
</tr>
<tr>
<td>Abraxas Market</td>
<td>92.04%</td>
</tr>
<tr>
<td>Dream market</td>
<td>94.51%</td>
</tr>
<tr>
<td>AlphaBay</td>
<td>95%</td>
</tr>
<tr>
<td>Middle Earth Marketplace</td>
<td>80.2%</td>
</tr>
<tr>
<td>Outlaw Market</td>
<td>86.83%</td>
</tr>
<tr>
<td>Mr NiceGuy</td>
<td>81.62%</td>
</tr>
<tr>
<td>TheRealDeal</td>
<td>99.34%</td>
</tr>
<tr>
<td>Silkitie</td>
<td>95.86%</td>
</tr>
<tr>
<td>Crypto Market</td>
<td>91.86%</td>
</tr>
<tr>
<td>T*chka Free Market</td>
<td>80.78%</td>
</tr>
<tr>
<td>Nucleus Market</td>
<td>94.23%</td>
</tr>
<tr>
<td>Ramp (Russian Anonymous Marketplace)</td>
<td>85.74%</td>
</tr>
<tr>
<td>The Majestic Garden</td>
<td>90.67%</td>
</tr>
<tr>
<td>Dark.Net Services</td>
<td>93.51%</td>
</tr>
<tr>
<td>Oxygen</td>
<td>93.1%</td>
</tr>
<tr>
<td>East India Company</td>
<td>93.94%</td>
</tr>
</tbody>
</table>

## Goals of Hacking

- **Curiosity**
- **Stealing services, valuables, or private information**
  - Identity
  - Financial information
  - Computer services (e.g., for spamming)
- **Spying**
- **Disrupting services**
Social Engineering

- Plays upon the weakest point in any computer or information system: a human
- Is a con game – persuading another person to do what you want them to do
- Is based on the premise that, as humans, we want to be helpful
- Look the part (could be technical could be physical) and ask the right questions
Social Engineering Threats

Phishing Email Communications

- Email addresses are harvested
  - Google
  - Social media (e.g., Facebook, LinkedIn, Twitter, Google+, etc.)
  - Data.com
- Hackers develop a social engineering ruse/scam
- Spoof the email into the organization
Cyber Security Threats

- Malware, worms, and Trojan horses
- Botnets and zombies
- Scareware (fake/rogue security software)
- Attack on client-side software
- Ransom attack
- Social network attack
- Web applications
Summary

- Understand that human error is the biggest threat
- Fix vulnerabilities (patches, etc.)
- Create documented policies and procedures
- Implement a computer maintenance program
- Educate officials
- Stay informed of latest and greatest

QUESTIONS?