# Implementing an Effective Information Security Program in Your Agency

Presented by:
Steve Aronson, Aronson Insurance
Ted Joyce, N B Independent Brokerage
Jeff Yates, Agents Council for Technology



## Our Presenters

**Jeff Yates**

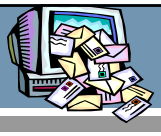
Agents Council for Technology

IIABA

Alexandria, VA

Jeff.yates@iiaba.net

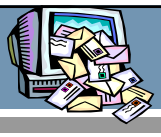
## First, a Little Housekeeping



- Please enter your questions in the Question & Answer box
- You will receive a  follow up email—feel free to email me
- A recording will be available at www.iiaba.net/act at the "Security & Privacy" quick link, along with more tools & articles



## Our Presenters



**Steve Aronson**

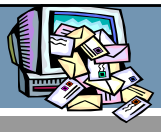
Aronson Insurance, Needham, MA

50/50 Personal & Commercial
3 offices, 20 employees

AMS 360 user
AUGIE Leader

Chair, ACT Agency Security
Best Practices Work Group

## Our Presenters



**Ted Joyce**

N B Independent Brokerage

Chicago, Illinois

Multiple Offices

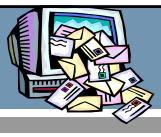
P&C—100% commercial

Nexsure Agency Management System

AUGIE Leader

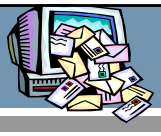


## Focus of Webinar



- Protection of client & employee private personal information (PI) in your agency's custody
- Not only data-- all information whether electronic, paper, or voice
- The information may be in your system, in your files, on your desk, on PCs, mobile devices, home computers, back ups, thumb drives
- It may be in email, info entered on your website, or info sent to you using social media
- It may be in the possession of third party contractors

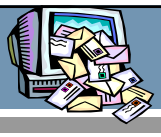
## Why is this important?



- Law requires it:
  - Gramm Leach Bliley
  - State privacy, consumer protection and data breach notification laws
- Agents have been audited & fined
- Severe harm to client trust and business reputation if clients' data is breached
- Some cost to implement these safeguards, but bigger cost if there is a breach of client or employee PI



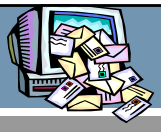
## Key First Steps



- Understand applicable laws & regulations
- Appoint Information Security Coordinator & involve your employees
- Develop your written information security plan
- Determine all of the PI you use & keep and every place where it might be found whether paper or electronic
- Decide who needs to see what & then restrict authorization

Take advantage of the ACT prototype plan–
www.iiaba.net/act

## What is Private Personal Information (PI)?



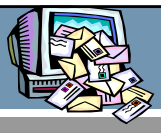
Some examples (which differ in various federal and state laws):

First name and last name, or first initial and last name, **and** any one or more of the following:

- Social Security number
- driver's license number, passport number, or state-issued identification number
- financial account number, or credit or debit card number, access code, personal identification number or password
- protected health information
- policy number

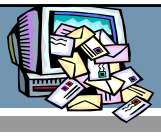


## Steps to take with employees



- Train them!
  - When hired
  - At least annually
- Regular audits for compliance
- Keep written records of training & audits
- Cut off terminated employees immediately from any access
- Remind staff about safe surfing regularly
- Monitor your employee's adherence to the plan as well as the system for any unusual patterns (Discuss with your IT professional)

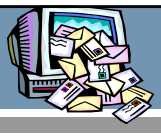
## Internal Physical Risks to Manage



- Your Office
  - locks on doors & windows
  - central station burglar alarm
- Escort visitors
- Lock file cabinets & desks
- No documents with PI left on desks. Or password information
- Must shred all PI documents & wipe all data off computers & other devices

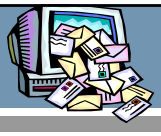


## Network Protection



- Use a network professional
- Firewall: commercial grade hardware best
- Virus & malware protection on servers, desktops portable devices and home computers
- Keep all hardware & software versions up-to-date; automatic updates best

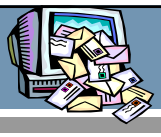
## Computer Protection



- Servers
  - strong passwords; changed regularly; locked down tight
- Desktop PCs
  - strong passwords (AsjRkx7#) & regularly changed
- Staff can't share ID's and passwords
- No storage of PI on desktops, laptops or mobile devices
- Use screen saver with password protection every 15-30 minutes

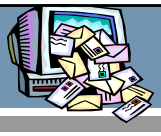


## Major External Risks



- Encrypt backups, thumb drives & PCs; password protect all mobile devices
- Keep PI off laptops, mobile devices & home computers
- Do not leave portable devices in your car - EVER
- Download software that will wipe data from mobile devices if lost
- Use Real Time tool to manage carrier passwords

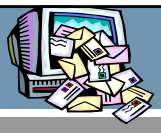
## Additional External Risks



- Connect to office through SSL / VPN connection
- Use non-default password on all WiFi connections from within the agency office as well as laptops
- Before discarding: destroy data on PCs, copiers, fax & scanners & other portable computers & devices
- Obtain written commitment from third party contractors to protect your data



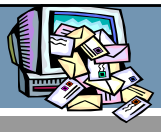
## Secure Email



- Email is like an open postcard
- PI often contained on CL applications
- TLS or “Transport Layer Security” industry recommended solution
  - Needs to be turned on & “key” obtained from trusted certificate authority
  - Partner with carriers and large clients
- Proprietary secure email solutions
- Real Time is secure

See “Security & Privacy” page at www.iiaba.net/act for TLS info

## Other Internet exposures



- Do not ask for PI or ids & passwords on online quote forms without initiating a SSL connection (https)
- Social Media: keep PI off this channel; when discussion moves to specific client situations, take it to regular agency channels
- Do not use the same passwords on your social media sites as you use for your other business sites

See ACT's "Don't Get Caught in the Web" & "Agency E&O Considerations when using Social Media"

www.iiaba.net/act on "Security & Privacy" page



## Questions