act.
AGENTS COUNCIL FOR TECHNOLOGY

ACT Security Issues – 'Pocket Guide' Topics & Resources

1) **Mitigation of Cyber Risk –** There are a number of significant risks to an agency that can be devastating; flood, fire, earthquake, loss of principal, data breach, cyberattack, etc. Primary need is for adequate planning.
Resources: III - Small Biz & Disaster Recovery Planning Small Biz Data Breach Protection
SBA - Disaster Planning SBA - Disaster Recovery SBA - Planning Template & Guide
FCC - CyberPlanner WSJ: Hackers Shift Attacks to Small Firms ACT: IA Guide to Systems Security

2) **Agency Passwords -** Know the resources, implement a strategy.
Resource(s): http://www.signononce.org/ http://www.roboform.com/ https://lastpass.com/

3) **Data Breach Laws –** Understand your state(s) laws, requirements, prevention.
Resource(s): Mintz-Levin DataLossDB.org FTC Data Security Tips
https://www.pcisecuritystandards.org/ ACT Article August 2013 Omnibus Rule

4) **Document Retention -** Federal legislation, state laws on proper document retention & destruction.
Resource(s): http://www.hhs.gov/ocr/privacy/ Gramm-Leach-Bliley Act FTC Privacy & Data Security

5) **Encrypting Databases -** Compliance with State Privacy and PII regulations, adhering to the strictest state in client database.
Resource(s): Mintz-Levin Symantec PGP BitLocker

6) **IP Phone System Security –** Know the overall security of your data infrastructure - Unencrypted VoIP traffic can easily be captured through packet analyzers.
Resource(s): VoIP Phone Security Issues http://www.sans.org

7) **Real Time Monitoring of Agency Equipment for Data Breach -** Understand the content of data flowing in and out of your network. Monitor via of Data Loss Prevention (DLP) solutions.
Resource(s): http://www.sans.org

8) **Paper versus Paperless –** Critical planning for agency & staff to ensure move to away from paper is successful. Data hosting, education on security vulnerabilities and precautions.
Resource(s): ACT: Planning for Paperless ACT: Turning Off Paper ACT: Creating a Security policy
IIABA Agency Best Practices Program

9) **Protecting Confidential Information –** PHI & PII; Agents must be aware of the state and federal laws. Conducting a risk analysis, complete compliance gap assessments. Develop, train and monitor policies.
Resource(s): HIPAA Omnibus Rule Impact PCI Compliance Guide HIPAA Security Rule Toolkit
Gramm-Leach-Bliley ACT HIPAA/HITECH Breach Notification Rule FTC ID Theft & Deterrence Act

10) **Remote Access of Agency Systems -** Remote access requires awareness to mitigate risks. Use strong authentication, Intrusion Detection/ Prevention System (IDS, IPS), VPNs for secure remote transmission.
Resource(s) (i.e., links to resources): Best Remote PC Access SW 2015 Citrix Server

11) **Using ASP Systems for Security -** ASP systems keep data from agency management and other systems always accessible, data backed up, & automatically updated. Be aware of price points, keep antivirus in mind.
Resource(s): LockMedia - About ASPs Cisco - Evaluating ASPs Anderson - Choosing an AMS
Top Anti-Virus SW

Ver: May 06, 2015

12) Mobile Devices – In using mobile devices to conduct business, you are exposing your company to additional security threats. Info on encryption, secure wireless connections, other device security.

Resource(s): Managing Security Risks of Portable Devices "BYOD" Opportunities & Risks Keeping Agency Data Secure Understanding Mobile Apps Lookout Mobile Security

13) Education/Training – A critical piece of a security policy should be ongoing education & training outlining everyone's roles and responsibilities in safeguarding company assets and client information.

Resource(s): HIPAA Security Awareness Training Security Must Be A Top Agency Priority

14) Document Destruction – Paper & files that can be located on LANs, cloud drives, local hard drives, mobile devices and USB/external drives. Know Federal & State Law requirements, develop/follow a process.

Resource(s): FTC - Disposing of Consumer Report Information ShredOne Security Topics Blog

15) Electronic Communication - Know and understand the federal & state laws regarding electronic communication. Utilize a Best Practices approach and ACORD standards with electronic communication.

Resource(s): eSign in Global and National Commerce Act Locke-Lord; Guidelines for eSign, eDelivery BP Guide to Agency Business Processes & Info Mgmt ACT eSign Series ACORD Standards - Activity Notifications Uniform Electronic Transactions Act