ACT Security Issues – Summary Guide; Topics & Resources

July, 2015

Topic: Mitigation of Cyber Risk

Critical Risk: There are a number of significant risks to an agency that can be devastating including flood, fire, earthquake, loss of principal, data breach, cyberattack, etc. Importantly, the Wall Street Journal reported in 2011 that the percentage of cyberattacks on businesses of less than 100 employees increased from 27% to 63% between 2009 and 2010, and then rose another 64% from 2013-2014. The agency must acknowledge these risks and be prepared to face each to avoid a disaster.

Overview of Possible Solutions: The primary requirement is planning - An agency must develop a written plan to address each risk. For a natural disaster, work with your agency management system provider on how to access data if your local office is destroyed (an ASP is a solid choice here). Find a secondary site from which to work. Arrange for your staff to work remotely. Find alternate power sources: i.e., generators. You can also contract with disaster relief providers. Security risks require even more extensive planning for communications to customers, reputation protection, legal advice, etc. Not only do you need a plan in the event of attack, you must have in place a written security procedure plan for the agency to prove you have done your best to protect your customer's data. Written – and consistently updated - plans in the agency are critical for mitigation of risk.

Resources:
Symantec Data Breach Risk Calculator
Ins Info Institute - Developing a Small Business Disaster Recovery Plan
US Small Business Administration - Advance Disaster Planning
US Small Business Administration - Disaster Recovery Planning
Small Business Disaster Recovery Planning Template and Guide
Business News Daily - Mitigating Data Breach Damage
FCC - Small Business Cyber Planner 2.0
Wall Street Journal: Hackers Shift Attacks to Small Firms
ACT: Independent Agent's Guide to Systems Security

Topic: Agency Passwords

Critical Risk (to industry): Sloppy password management makes protecting private client information extremely difficult. Writing down user ID and passwords or putting them in an unsecured electronic document does not provide adequate security.

Overview of Possible Solutions(s): There are three parts to effective password management for your organization. **1)** Use the password management capability built into your agency management system – including Single Sign-On, **2)** should make sure you use ID Federation with your insurance companies as soon as it becomes available, **3)** use a third-party enterprise Single Sign-On (SSO) solution for all other passwords.

Resource(s):
ID Federation: http://idfederation.org/ * or * http://www.signononce.org/
RoboForm password manager LastPass password manager

Topic: **Real Time Monitoring of Agency Equipment for Data Breach**

Critical Risk (to industry): Understanding the content of data which flows in and out of an organizations network is critical. Monitoring through the use of Data Loss Prevention (DLP) solutions has become increasingly popular to protect sensitive data and provide insight into the use of content within an organization.

Overview of Possible Solutions(s): Data Loss Prevention solutions range from simple desktop based clients to extensive inline network based appliances designed to analyze traffic for sensitive data such as credit card and social security numbers. In recent years, SAAS or cloud based DLP solutions have become another option for organizations looking to utilize a 3rd party or service provider to perform this function. Visit the resource center at SANS.org for more information on the types of DLP solutions available for the one that best fits your organization's needs.

Resource(s):
SANS - Data Loss Prevention Hardware and Education
Symantec - Data Loss Prevention products

Topic: **Using ASP Systems for Security**

Critical Risk (to industry): ASP (Application Service Provider) or web-based systems keep data from agency management and other systems always accessible, data backed up with multiple redundant copies, and automatically updated with all software upgrades as they occur. In comparison, LAN-, desktop-based, and even Thin Client systems can more easily be compromised due to damage, require agency staff time to back-up and upgrade, and are not as mobile-accessible.

Overview of Possible Solutions(s): Almost all major industry software vendors offer ASP versions, and many offer only ASP. Whether you are using a management system, comparative rater, or CRM, check with your vendor on availability and pricing. Note: ASP systems tend to have higher price points than desktop, as the vendor incurs cost for data hosting, management, access, software updates, and other security. Also keep in mind anti-virus and other protection software still needs to be in place.

Resource(s):
Lockmedia - ASP Background
CISCO - Evaluating ASPs
Anderson - Choosing an AMS
Top Anti-Virus SW

Topic: **Data Breach Laws**

Critical Risk (to industry): Independent Agents possess in their files data that if breached could cause great harm to the affected individuals and agencies. It is critical that the agency understand the data breach laws of their home state as well as any other state where they do business. At present the formal data breach laws have only been created at the state level. Attempts at a federal data breach law has failed for the last 6 years but we expect to see something again this year.

It is imperative that agencies understand these laws and begin the quest to prevent a breach before it happens and happen it will. This pocket guide is the first of many steps to bring you information to assist in this endeavor.

Each of 47 states and 3 US Territories have identified what specifically constitutes a Data Breach. Understanding these laws should trigger a reaction to an event within their agency/brokerage. The agency/brokerage must have a clear understanding of the reporting requirements, as well as potential fines and penalties to the agency.

Overview of Possible Solutions(s): Currently two solid resources: **Mintz-Levin** shows by state, the definition of breach, covered entities, notice procedures, and penalties. **DataLossDB** is a reporting database for all industries of the types of reported data breaches, including fines in some cases. It is also incumbent upon the agency/brokerage to understand where the Federal Trade Commission (FTC) stands on protecting personal information. In addition, if applicable, the Payment Card Industry (PCI) has its own set of compliance responsibilities. For those agencies that write group health insurance you are also required to meet the standards of the HIPAA HITECH breach rules.

Resource(s):

Mintz-Levin - State Data Security Breach Notification Laws
DataLossDB.org - Stats and Incidents on Security Breaches *(requires free sign-up)*
FTC - Data Security Guidance
PCI - Security Standards Council
ACT Article August 2013 HIPAA Omnibus Rule

Topic: Mobile Devices

Critical Risk (to industry):
If you are using mobile devices to conduct any type of business, you are exposing your company to additional security threats that can expose and compromise your business network and data. One of the biggest challenges can be data loss or breaches caused by lost or stolen mobile devices. Another threat targeting mobile devices is the introduction of attacks and malware.

Overview of Possible Solutions(s):
There should be an approval process for any mobile devices used to conduct business that is signed, reviewed and outlines the following:

1. All devices must be password protected
2. Use secure wireless connections when transmitting business information – No free services from coffee shops or airports
3. Reporting process for lost or stolen equipment (immediate located or wiped)
4. All devices are securely wiped prior to disposal or trade in
5. Encrypted drives and SD cards
6. Use security on all mobile devices, keep software updated, use only trusted apps.
7. Apply business workflows and procedures to mobile use (proper client file documentation in the agency management system)
8. Apply business email policies and best practices to mobile device as you would in your office.

Resource(s):
Managing the Security Risks of Portable Devices
"Bring Your Own Device" Opportunities & Risks

Keeping Agency Data Secure
OnGuardOnline.gov - Understanding Mobile Apps
Lookout Mobile Security

Topic: **Education & Training**

Critical Risk (to industry):
As employees in insurance agencies and brokerages, access to vast amounts of private information is made available to us and can be susceptible to theft. One of the most important pieces of a security policy should be ongoing education & training outlining everyone's roles and responsibilities in safeguarding company assets and client information.

There should be written security policies and breach notification procedures. These documents need to be reviewed in detail with all new employees and periodically with all employees so that security and data safeguarding are a part of any insurance agency's culture.

Overview of Possible Solutions(s):
A yearly review of the entire security policy as well as the breach notification procedures, awareness of threats and all privacy responsibilities should be undertaken by every organization. Particular aspects of a security policy, real world breach examples or current "lessons learned" can be reviewed on a monthly or quarterly basis to keep security and information safeguarding in everyone's minds and show managements support and expectations to policy adherence.

A training calendar should be established for each of the following: IT; security compliance officer; executive management, supervisors, mobile employees and all employees.
Responsibilities and knowledge of security policies and privacy statements

Resource(s):
HIPAA Security Awareness Training
ACT Article - Security Must Be a Top Agency Priority

Topic: **Electronic Communication**

Critical Risk (to industry):
As Electronic communication increases because of consumer demand, there are key areas that the independent agency must address, and areas for improved efficiency and security that should be addressed. The e-sign and UETA Laws create obligations on the part of both carriers and agencies regarding proper record-keeping of consumer consent.

Overview of Possible Solutions(s):
Know and understand the federal and your state laws regarding electronic communication. Utilize a Best Practices approach and ACORD standards with electronic communication. Start with a single business process and product line and create a process map for the ideal workflow and security in each area. Sensitive personal information should not be sent via email, whether in the email text or as an attachment. Instead, emails should be sent with links to a secure site. Utilize the ACORD XML activity notification from carrier to agency with .pdf attachment of policy information for the best workflow.

Resource(s):

Electronic Signatures in Global and National Commerce Act
Locke-Lord - Guidelines for e-Signature and e-Delivery in the Insurance Business
ACT/IIABA - Best Practices Guide to Agency Business Processes & Information Management
Agents Council for Technology: ACT eSignature - Carriers ACT eSignature – Vendors ACT eSignature - Agents
ACORD XML Activity Notification, contact info: standards@ACORD.org
Uniform Electronic Transactions Act (UETA)
National Council of State Legislators - UETA Transactions *(requires account creation)*
ACT/IIABA eDelivery Consent Form *(coming end of July 2015)*

Topic: Document Retention

Critical Risk (to industry): The longer an organization keeps client information the more documents can be lost in the event of a data breach. Information should be kept for only as long as legally required and as the agency requires.

Overview of Possible Solution(s): Federal legislation, state laws, and certain state departments of insurance have requirements for a proper document retention policy as well as requirements for proper disposal of private client information. The organization should create a document retention policy which all agency systems can fully support, and all staff must comply.

Resource(s):
HHS.gov - HIPAA Background, Guidance
Gramm-Leach-Bliley Act (GLBA)
Federal Trade Commission - Privacy & Data Security Update

Topic: Paper versus Paperless

Critical Risk (to industry): Critical decisions are necessary when an agency moves from paper to paperless environment. To name a few; Data storage – local v. cloud, , consistent workflows and continuity, staff training and requirements, retention of documents-histories, access to documents via the carrier websites and user access based on need.

Overview of Possible Solution(s): Agency must prepare correctly by analyzing current workflows and amending them according to new requirements for paperless process. Train and monitor staff for adherence and continuity, with a good communication plan. Agencies must decide on where to host data (locally on server or store data in the cloud) and must educate themselves on the security vulnerabilities and precautions needed for each. Also each choice has a different financial impact and either choice may not be financially feasible for an agency. Agency must adhere to state and federal retention guidelines for documents when moving from paper to paperless. Paper copy of documents may no longer be necessary when agencies have access to client documents on the carrier website.

Resource(s):
ACT articles: Phase 1 - Improving Agency Workflows by Going Paperless
Phase 2 - Turning Off Paper in Agencies
ACT article: Creating an Agency Information Security Plan
Third party vendors providing paperless environment capability such as DocStar.
Also, refer to IIABA Agency Best Practices program.

Topic: **Protecting Confidential Information**

Critical Risk (to industry): The risk to agencies within our IA distribution channel has increased significantly regarding Protected Health Information ("PHI") and Personally Identifiable Information (PII). Agents must be aware of the state and federal laws regarding this information, and what data is kept, where it is stored, and who has access to it.

Overview of Possible Solutions(s): Conduct a risk analysis to identify and document where all the PHI and PII is located at in your organization. Complete compliance gap assessments. Minimize the amount of PHI and PII these that the agency retains if possible. Develop, train and monitor policies and procedures with staff. Implement a "need to know" access policy. Be aware of the **Breach Notification Rule**.

Resource(s):
ACT article: HIPAA Omnibus Rule will have Big Impact on "Business Associates"
PCI.org - PCI Compliance Guide
HIPAA Security Rule Toolkit
Gramm-Leach-Bliley ACT (GLBA)
HIPAA/HITECH Breach Notification Rule
Federal Trade Commission - Identity Theft and Assumption Deterrence Act

---

Topic: **Document Destruction**

Critical Risk (to industry):
Document destruction is not just about paper files and dumpster diving. Considerations in addition to paper include electronic files and emails (retention) and the destruction of files that can be located on LAN's, cloud drives, local hard drives, mobile devices and USB or external drives. Federal and State Laws require business to properly destroy customer records that are no longer to be retained. Destruction includes shredding, or otherwise modifying the personal information in those records so that it is unreadable.

Overview of Possible Solutions(s):
To establish a policy and processes for the proper destruction of documents follow the 5 steps:

1. Take stock and inventory – Where is information kept, agency management systems, fax, email, paper, physical drives, cloud services, 3rd party.
2. Scale down – Consolidate and restrict the storage of information to controlled and manageable locations.
3. Secure it – lock paper drawers, secure server access, password protect files, screen savers.
4. Pitch it – properly destroy or remove documents and files that no longer NEED to be retained.
5. Plan – establish procedures and monitor and train for compliance. Incorporate training into new employee orientation and make security a part of your culture.

Resource(s):
Federal Trade Commission - Disposing of Consumer Report Information Guidelines
ShredOne Security Topics Blog

Topic: **Encrypting Databases**

Critical Risk (to industry): With the continuing complexity and sophistication of hackers, data security and electronic transmission of data, this is possibly the single most critical business risk business today.

Overview of Possible Solution (s): Critical is Agency compliance with State Privacy and Personal Information Regulations, adhering to the strictest state in client database.

Resource(s):
Mintz-Levin - State Data Security Breach Notification Laws
Symantec - PGP Background, Tools BitLocker Drive Encryption

Topic: **IP Phone System Security**

Critical Risk (to industry): Convergence of voice and data networks presents a multitude of advantages and cost savings to small business. When implementing VoIP service, one must also understand the associated security and fraud risks and take measures to mitigate these risks. Three of the more prevalent risks are: interception of calls and privacy concerns, interruption of service, and theft of service or toll fraud.

Overview of Possible Solutions(s): Overall security of your data infrastructure becomes increasingly important when implementing a VoIP system. Unencrypted VoIP traffic can easily be captured. Through the use of encryption protocols such as TLS, voice traffic is encrypted the same as data traffic for secure transmission over a network. Implementation of larger premise based VoIP systems should also consider the use of a Session Border Controller (SBC).

Resource(s):
VoIP-info.org - VoIP Phone Security Issues
SANS.org - Security Issues and Countermeasures for VoIP

Topic: **Remote Access of Agency Systems**

Critical Risk (to industry): Remote access adds flexibility and requires awareness to adequately mitigate risks associated with this capability. The three primary areas to consider are: improved authentication, entry point validation, and secure data during transmission.

Overview of Possible Solutions(s): Use strong authentication with two-factor capability. Available solutions include remote access, certificates, SMS PIN codes, or biometric validation. Also evaluate restricting access to some systems via remote access. Consider an Intrusion Detection/ Prevention System (IDS, IPS) sitting in-line, between the remote access point and your internal network, to prevent security exposure. This reduces risk from hacking software and viruses from the connecting device. Use a Virtual Private Network (VPN) to secure data during the transmission from remote locations.

With attention to the authentication process, traffic coming from remote access points, and data security in-flight you will reduce the risk of a security breach via remote access points.

Resource(s):
Best Remote PC Access Software 2015 Citrix Server Background, Getting Started

---