Cybersecurity Issues for Agents – Security Education & Training

ACT™
AGENTS COUNCIL FOR TECHNOLOGY

I. New Employees

Make sure all new employees have signed an ISP (information security policy) and ensure that electronic safety is part of the on-board training.

1. Start with basic computer do's and don'ts.
2. Tackle email, flash drives, websites.
3. If there are laptops or tablets, review the "check in" procedure.
4. Explain what "unusual" means when it comes to computer behavior.
5. Passwords - explain the importance of confidentiality, and using a solid password strategy.
6. Review privacy of data and all information, laws that apply.

Some existing resources are:

InformationShield Employee Information Security Policy
SANS Employee Information Security Policy (ISP)
Downloadable free ISP Template - InstantSecurity
ACT's Cyber Information Security Policy (agency-wide)

II. Current Employees (each department)

1. At least annual IT update on what is going on for risks (preferably quarterly).

2. Have an emergency response plan that is reviewed on a regular basis.
   a. What do I do if…
      I clicked on a phishing email,
      My computer is locked by a virus,
      If I lost confidential information
   b. In the event of a suspected breach, who do I go to first?

3. Perform quarterly testing (at a minimum) to see how employees respond.
   a. Perform random, consistent Phishing-testing – Known resources are PhishMe and KnowBe4. These send out a customized bogus email that looks authentic, but creates click reports for leadership analysis and follow-up. The key is to train employee behavior to carefully review every email before opening, thereby reducing risk.
   b. Monitor website activity from IT reporting, and limit where ever applicable.
   c. Discuss what to look for in emails, websites, social posts, and all electronic interactions.

4. Daily: If a specific risk is identified each department should be notified, and employees should be guided on what happened, what steps are being taken to fix the incident, and what actions they should avoid.

III. Departing Employees

1. Walk departing employee(s) to the door and check any boxes, etc., even if leaving on good terms.
2. Whether leaving on good terms or not, have one check list created to ensure everything is covered.

a. Make sure that all passwords are changed prior to employee walking out the door.
b. Disable access to all information.
c. Ensure agency acquisition of physical security items (paperwork, keys, etc.) is completed.

Authors: *Mary Hauri (Insurance Concepts In Motion, Inc.), Ron Berg (ACT)*