



The ASCnet Quarterly
2nd Quarter 2005



:: No Need to Be...Insecure

by Tim Woodcock

Insurance agencies who commit to the five phases of security compliancy reap the rewards.

With today's growing threats of information theft, identity theft, and privacy ramifications of inadequate data security on the rise, insurance agencies are overwhelmed with maintaining the security of their networks, while trying to meet information security guidelines of the federally mandated HIPAA, Sarbanes-Oxley and Graham-Leach-Bliley Acts.

Insurance agents can no longer afford to stand by and wait until a disaster occurs before investing in the security measures necessary to meet federal guidelines and customer commitments. By then it will be too late to react and the cost too high—loss of customer trust, lost income, severe penalties for noncompliance, and possible jail time.

Insurance agencies, who commit to investing the proper time and money in securing their network infrastructure, are enjoying the benefits of meeting the federal regulatory guidelines, improved network security, and reduced system down-time while increasing agency productivity. According to the IIABA 2004 Best Practices Study, Best Practices agencies and brokerages invest between 2 and 2.7 percent of their annual revenue into their information technology (IT) budgets.

There are five phases used by Best Practices agencies follow when investing in securing their infrastructure:

Phase One: Assessment

Action: Assessment of the current level of information security.

Result: Gap analysis between current state and federal requirements.

Phase Two: Design

Action: Design and documentation of policies, procedures and solutions to help mitigate security risks.

Result: Creation of gap closure plan.

Phase Three: Deployment

Action: Deployment of protection technology and services.

Result: Execute gap closure plan

Phase Four: Management and Support

Action: Continued management of security program to provide business continuity.

Result: Insures gaps remain closed and new gaps are not opened.

Phase Five: Education

Action: Education of organization on security best practices and best-of-breed technology.

Result: Ensures employees acknowledge their responsibilities with security best practices, documents and training.

Assessing the situation

The first step is to assess the agency's current situation. As with any assessment, a survey must be done of the current circumstances. This is accomplished by performing a comprehensive security audit. In order to obtain an unbiased assessment, best practice guidelines recommend utilizing the services of an independent IT vendor experienced in the audit and reporting process. The agency must first form a "security team" or committee to oversee and make final decisions regarding the security needs of the agency, what vendors to utilize, what steps to take after the audit, and the continued security management of the agency's network.

The team should consist of at least one principle or executive officer who has the authority to approve funds for security projects, and monitor the work. A manager or representative from each department with decision-making authority, and the manager of the IT department should be included on the team. Depending on the size of the agency, the team may consist of only one person.

The team should meet at regularly schedule times. Discussions should include measures to take regarding security procedures, emerging threats, and awareness. Decisions should be made based upon these discussions. A comprehensive audit will focus on various layers of security:

Security Policy Layer—Encompasses all aspects of employee awareness of security and responsibility to the network, e-mail, Internet usage, password usage, and handling of sensitive data.

Physical Layer—Addresses the need to ensure all computer equipment remains safe and secure from unauthorized access. Individual responsibility is assigned to critical equipment with the owner having the appropriate resources, skills, and information to fulfill this responsibility.

Data Layer—Controls the accessibility of data on the network. The desired outcome is one that restricts the access of data to only those users who are required to have access (access management).

Application Layer—Includes such applications as host-based antivirus software, anti-spyware software, and personal firewalls. These tools provide essential "last-resort" security for applications and data.

Network Perimeter Layer—With the proper utilization of firewalls, virtual private networks (VPNs), routers, intrusion detection/prevention tools, and Web content filtering, unauthorized access from outside the network can be prevented.

Management Layer—This important layer requires constant supervision to ensure consistency—assessing overall vulnerability, managing patches and updates for each software and policy. This layer includes the creation of the security framework that makes it possible to identify potential threats early, accurately analyze risks from emerging threats, and develop effective remediation strategies quickly.

Once the security assessment (audit) is finalized, the audit report will highlight all areas of risk and recommend solutions for mitigating each area of risk within the security layers, including the benefits of implementing each of the solutions (risk mitigation and increase productivity). These areas can then be addressed according to their level of risk. This will ensure all critical areas will be addressed first.

Designing the Right Solution

Once an audit is complete, the agency's assigned team can then begin the process of formulating or modifying a solid company-wide security policy with detailed descriptions of each area of concern.

Consideration and proper planning for implementing the recommended solutions must be performed. This will include a cost analysis and receipt of vendor quotes for each recommended solution. A budget for all immediate and "phased in" projects must be included, along with timelines for implementation. This will prevent cost overruns due to unnecessary purchases.

Deploying the Right Solutions

Once the planning and budgetary phase is complete, the agency can begin implementation. The recommended solutions will sometimes fall outside to agency's level of expertise. Best Practices include the expert services of vendors qualified to perform these tasks. These services should include the training of the agency's IT staff to perform the management tasks to properly maintain the solution.

Continued Management and Support is a Must

No matter the size of the network, security must remain at the forefront. Once security solutions have been implemented, the agency must remain vigilant to ensure these investments are properly maintained. If left unmanaged for any length of time, all will have been in vain.

A continued effort must be made in the areas of IT training. Systems monitoring, data security and retention, patch management, virus pattern updates, are just some of the management and support services of the agency's network that must be maintained. Many times, the agency does not have the necessary staff or funding to properly maintain these areas of concern. This is where outsourcing of certain managed services can be beneficial to the agency.

Continued Education and Awareness

A security policy remains effective only if it is practiced. Security education must remain constant and at the forefront throughout the agency's infrastructure. Some of the ways agencies are maintaining security awareness is by dedicating the time for discussion and 'what if' questions during scheduled departmental and company wide meetings, surprise inspections, security awareness posters within the agency, annual security audits and disaster recovery drills, and the receipt of weekly/monthly reports from the IT department.

Summation: The Time to Act is Now

Agencies can no longer afford to stand by and wait until a disaster occurs. The longer an agency waits, the greater the cost. You can have peace of mind and enjoy the benefits obtained through the implementation of security best practices.

To get started, visit the IIABA's Agent's Council for Technology (ACT) Web site to download The Independent Agent's Guide to Systems Security.

Tim Woodcock is president of Courtesy Computers (www.courtesycomputers.com) based in South Florida.