March 15, 2005

The Independent Agent's Guide to Systems Security

What Every Agency Principal Needs to Know

An Agents Council for Technology Report[1]

Table of Contents

Disclaimer
The purpose of this report is to assist agencies and brokers in considering issues relevant to developing plans to protect the security of their systems and data. The report includes only general information, and is not intended to provide advice tailored to any specific agency situations. It was prepared solely as a guide, and is not a substitute for agents and brokers independently evaluating any business, legal or other issues, and is not a recommendation that a particular course of action be adopted. If specific advice is required or desired, the services of an appropriate, competent professional should be sought.

[1] The Agents Council for Technology (ACT) is an association of agents, brokers, users groups, carriers, vendors, and industry associations dedicated to encouraging and facilitating the most effective use of technology and workflow within the Independent Agency System. ACT is a part of the Independent Insurance Agents & Brokers of America, Inc. (IIABA). See the ACT web site at www.independentagent.com/act for more information about ACT and its initiatives.

Copyright 2005 ©, Independent Insurance Agents & Brokers of America, Inc. All rights reserved. Permission to reprint is granted to ACT members.

Overview

The world has changed for independent agents and brokers. In the past, agencies primarily had to protect the paper within the physical perimeter of their agencies. Today, most of the information an agency relies upon has been digitized; most of the work is done on computer; and the agency is connected to the outside world through the Internet. These changes have been very beneficial, but they have greatly complicated the job of protecting the security of the agency's systems and data.

Today, a security breach can enable a virus or worm to plant itself in the agency's systems and bring these systems down, so that the agency's staff cannot function. A security breach can implant spyware that enables an external party to access confidential client information which may be protected by federal or state law. A security breach can result in the theft of agency expirations information, upon which the very value of the agency rests, or impose many other perils on the agency and its customers.

The privacy of confidential information is increasingly important to both the agency and its customers, and security breaches may put the agency at risk of regulatory action or civil or criminal litigation. Some federal and state laws require certain financial entities to implement comprehensive privacy policies. For example, the Gramm-Leach-Bliley Act of 1999 requires financial institutions, including independent agencies, to adopt administrative, technical and physical safeguards to ensure the security and confidentiality of non-public personal information and customer records.

As another example, California requires businesses to notify California residents if the business knows or "reasonably believes" that the security of their personal information has been breached.[2] ACT's report "Safeguarding Non-Public Personal Information"[3] goes into much more detail about these emerging privacy requirements, but safeguarding the security of the agency's systems and data are critical components to protecting this private information.

Individuals and businesses buy insurance and financial services products from independent agencies and brokerage firms because they are trusted entities in their communities. This "goodwill" is an important component of the overall firm's value. A preventable security breach exposing the personal information of the agency's policyholders could result in significant negative publicity for the agency and have a devastating impact on the agency's reputation.

In short, a security breach today can be every bit as serious to the ongoing success and viability of an agency as a major fire or other catastrophe.

---

[2] Section 1798.82, California Code. http://www.privacy.ca.gov/code/cc1798.291798.82.htm.

[3] The report is found at www.independentagent.com/act by clicking on the "Technology Reports" icon.

This report is focused on the specific technology-related security risks that agency principals and managers need to be aware of and to take action on in order to protect their agencies. While many agencies and brokers will employ or retain technology professionals to do security audits and implement specific security technologies, agency business leaders should be involved to assure adoption and implementation of appropriate processes.

It is easy for a discussion of security to become very technical and almost overwhelming for the average business leader. This report goes to great lengths to stay focused on the key principles and solutions that will be of interest to agency managers. More technical discussions are handled in the footnotes and the appendices.

In fact, agency principals will find the process of assessing security risk to be a very familiar one, given its similarity to the risk assessment process they engage in on daily basis with their clients to determine their insurance needs. Managing security risk is an ongoing and never-ending process. Just as one plugs a security hole, another one may emerge that must be addressed.

[Table of Contents]

Key Actions for Agency Principals to Consider Taking

Before we turn to the specific security issues that most independent agencies and brokers face, it is important to outline the role the agency principal can play in the adoption and implementation of a successful security policy in his or her firm.

The first step is for the agency business leader to understand, acknowledge, and communicate the importance of security. As an initial activity, the agency's business leaders can gain an overview of the major security issues their business faces, along with the impact various security breaches could have on the success of their firm. This report is designed to help the agency leader in this process.

Then the agency principal can make a comprehensive determination of where the agency currently stands with security. Two approaches could involve use of a security consultant, or having the agency conduct a self-assessment of security. Many agents engage an outside security expert to perform a security audit of their business, feeling that the level of knowledge and expertise required, plus the value of an independent view is best found in an outside resource. We have included some information in Appendix B to assist agents in selecting such a consultant.

A self-assessment may be an appealing initial step for an agency. In Appendix C, we have provided an "Agency Security Risk Self-Assessment Tool" to help the agency in doing a self evaluation of its security readiness. A self-assessment is, at least from a cash-flow perspective, less expensive than using an outside resource; but it may lack independence, and the agency may lack the expertise to do the assessment. Appendix D provides the agency with another helpful resource, definitions of the "Different Layers of Security" and an illustration.

A key decision the agency principal can consider is whether, and to what extent, the agency will engage an outside security consultant to assist the agency in its day-to-day security management. Once this decision is made, it needs to be clearly defined what ongoing security responsibilities the internal agency staff will perform, and which will be handled by the outside consultant.

Two extremely important functions that the agency principal can perform in the security area are to lead the agency in the development of a comprehensive security policy and its related procedures, and then to inspire the staff to implement this policy and to provide continuing support to it. This implementation includes training the staff on these policies and procedures and then monitoring and auditing them for compliance. The agency principal may want to schedule agenda time periodically at staff meetings to make sure the staff keeps the importance of security top-of-mind.

The agency will be in a much stronger position with respect to security if it has thought through, implemented, and then audited the implementation of its security policy. These pro-active actions demonstrate that the agency handles security in a systematic way, not just haphazardly when a problem arises. In addition, as this field evolves, businesses are increasingly turning to internationally recognized security frameworks, such as ISO 17799 and the Common Book of Knowledge® for guidance as they design their security policies.[4]

The agency principal can also work with the agency's technology and security staff and/or consultants to set up a pre-defined action plan should a security breach occur, rather than simply taking "ad hoc" action when an event occurs. The last section of this report provides some of the steps agencies can consider should a breach occur. The agency might also find ACT's report, "Key Considerations in Disaster Planning & Management for Independent Agencies & Brokerage Firms" to be a helpful resource in setting up a pre-defined action plan.[5]

We have included in Appendix E a sample agency security policy which is intended only as a template for the agency to use to customize the appropriate policy for its particular operations and systems.

Finally, in Appendix A, we provide the link to Microsoft's excellent glossary of security terms as a further resource to the reader.

[Table of Contents]

A Day in the Life of an Independent Agent

In today's world, independent agencies and brokers need to be concerned about security issues 24/7. Even after business hours, our networks churn away on our night processing

[4] ISO 17799:2005, International Organization for Standardization, www.iso.org; Common Book of Knowledge (CBK®), (ISC)[2], www.isc2.org.
[5] Report is found at www.independentagent.com/act under "Technology Reports."

and receive downloads of data from our carriers. Our web servers also are running to provide information to potential customers, and increasingly, to provide policyholders with access to their policy information from our systems. We also are faced with the traditional physical security issues 24/7—the security of our building and the files and data which they hold.

Each morning, we sit down at our desk, turn on our computer, and a whole world opens up to us. What we don't want to occur is that we also inadvertently open up any part of our agency systems and policyholder data to this outside world by overlooking or under-estimating the need for some critical security measure.

From our desktop, we login to our agency management system. This is typically where our entire agency database is held. A policyholder calls and requests some information. We access this from our desktop. Later in the morning, we need to use a carrier website to complete a change of a vehicle. And still before lunch, a policyholder requests a payment status, which we check using a real-time billing inquiry, and then sweep the necessary payment from the policyholder's bank account.

After replying to several email items, we head out for lunch. But on our desk, we may have left our computer screen on, and left various applications logged in with a policyholder's information in plain view on the screen. We may also have left client files open on our desk and left the file cabinet unlocked. We also may have password information posted all over our monitor on yellow sticky notes. We haven't thought much about the security implications of leaving all of this private information openly accessible for anyone to see who happens to pass by our desk.

The afternoon is filled with much of the same. We access information both from our agency management system and the companies' websites. We check our email, collect premium payments, issue policies, obtain quotes, and validate information. We give little thought to opening email attachments and downloading information we see on the web.

This afternoon we also say good-bye to a commercial lines CSR who is leaving to go with another agency across town. What are the security implications of this? Does the CSR have a clear understanding that all agency data is the property of the agency and is not to be copied onto the CSR's laptop, PDA, or USB drive, or emailed to another computer? Does the agency have a procedure to immediately turn off the CSR's access to the agency's systems as well as to the carriers' web sites and systems?

We finish our day by straightening up our desks, re-filing client files, and logging off of our computer and taking the laptop home with us. As we lock our door to the office, we are relieved to think that everything is secure—but is it?

In the evening, our agency networks are up and running. We are providing access for our clients 24 hours per day, seven days per week. Our night communication is running to obtain our policy downloads and our files are being updated. Our remote backup is running along with our tape backups.

We may have stopped at a grocery store for some food on the way home—with our laptop and perhaps some files in the car. After dinner and spending some time with the family, we sit down at our laptop to login for our email and to search the web. Our children are there and want to check something out on the web. They download some files to the laptop to burn into a CD. Once again, we have given little thought to the potential that this laptop when re-connected to the agency network could infect the entire agency's systems.

This sample "typical day" has illustrated the importance of an agency's fully assessing the security risks it faces and then developing a comprehensive security policy to manage these risks. This policy will mean nothing unless our staff is fully educated and trained to follow it, and we set the procedures in place to make sure our systems are monitored for compliance with the plan on an ongoing basis. Otherwise, each staff member and each connection to our network creates a potential exposure or place of entry for an unwanted person or activity.

[Table of Contents]

Identity and Access Management

Identity and access management are core security principles, because their processes determine who gets on your systems and what access they have once they logon. Identity management determines how you authenticate or identify a person requesting entry to your systems. Access management covers what access they are allowed once they are on your systems. Agencies should consider establishing clear policies and procedures for each of these areas and then assign specific responsibility to manage them. It is also important for the agencies to assess how well these policies are working and to continue to refine them to eliminate any weaknesses.

Identity Management

Each person requesting access to your system should have a digital ID to identify who he or she is. ACT recommends that digital ID's be unique to an individual and kept secure and private by that individual. Every employee should have a unique username and password. By providing unique ID's you have the capability to track activity and also reduce the exposure to loss by limiting activity to that related to that ID. There are several methods of authenticating a user. The most popular method is the use of static User IDs and passwords. Static passwords are ones that do not change very often. Static passwords are the easiest to use and deploy and are also the easiest to attack. You can reduce your vulnerability to brute force attacks of password guessing by using a complex password (combination of uppercase, lowercase, and numbers) as recommended by the ACT password guidelines. Static passwords are also subject to exposure through spyware and text capture tools.[6]

[6] In addition to static passwords you could use one-time passwords, which require a different password, from a predefined set of passwords, for each access.

If you are using static passwords, consider instituting a password aging process where passwords have to be changed on a regular basis. The more often passwords change, the more secure your systems will be, but also the more difficult it will be for your employees to remember their passwords. Use of complex passwords (those with mixed case and numbers) provide a much higher degree of security and should be carefully considered. Employees should be prohibited from posting passwords on their monitors, or otherwise keeping passwords in plain view. They should never give out a password to another employee or person (except to the agency's password administrator as provided in the agency's policies). They should also be prohibited from placing ID's and passwords in their PDA's and smart phones, in case they are lost. Care also should be taken to avoid hard copies of this information from being accessible to others, such as in address books/calendars, in word documents/emails stored online, and on rolodex cards in an office.

Agencies should not post ID's and passwords on their Intranets. There is too great a risk that these sites will be hacked or that the security will be inadequate to keep the information private. There are embarrassing cases where agency passwords have turned up in Google searches. To repeat, ID's and passwords should be safeguarded and kept confidential by the specific employee authorized to use them, and should not be disclosed to other employees or persons.

The ongoing administration and maintenance of passwords is a very important responsibility. It is often more time consuming than the initial ID setup and specific resources in your office need to be assigned to this task.

It is critical for the agency to revoke promptly the digital ID of any employee who leaves the agency both for the agency's systems and the carriers' systems. At a recent security conference, it was estimated that this step is overlooked as much as 30% of the time! It is easy to remember if it is added to the agency's standard checklist for exiting employees.

Strong authentication, sometimes called two-factor authentication, requires two components - something you know and something you have. The something you know is typically an ID, PIN number, or phrase. The something you have is usually a token producing card, software program or certificate, or smart card. Using two pieces of information to perform identity verification greatly reduces the chances of fraud. However, it also increases the administrative burden required to authenticate the person. A good example of this is bank ATM cards where you need both the physical card (smart card) and the PIN (something you know) to access an account. Either by itself is of no value, as account access is not permitted unless both are there.

The third method of authentication is based on biometrics or "something you are". This includes items like fingerprints, palm prints, iris scans, and voice recognition. Some biometric based identity management solutions are in use currently but additional research and new techniques are necessary to overcome some of the current limitations to widespread utilization. However, there may be benefit to evaluating this method in smaller scale operations such as login within an agency or remote access to systems within the agency. Fingerprint scanners are relatively inexpensive and can be obtained standalone or incorporated into various devices such as keyboards, mice, USB ports, or PCMCIA cards. Biometric authentication is an area to monitor as it has the potential to both simplify and improve in the identity management process.

Agency management systems today are increasingly managing multiple passwords for agents, initiating signons to carrier systems without the user having to enter each specific ID and password. In this scenario, the authentication of the designated user is critical to prevent an unauthorized user from gaining access not only to the agency's systems, but to the carrier systems.

Access Management

Once a digital ID is verified, access management comes into play by controlling what resources that person can use. Access management is the task of permitting or preventing usage of specific applications or data sources. Initial focus should be on control of the application level and by default this may also restrict access to the information needed to perform that function. Grouping users by role is a good method of determining what access rights a person needs to given functions. For example, the accountant and managers may need access to the agency's financial information, but the CSR's are not likely to need access to it.[7]

Logging and monitoring of activity, events, and exception conditions are necessary for adequate access management. Periodic audits are needed to insure that the controls in place are functioning and that unexpected access points have not been provided or created. Also, routine reviews of activity can detect abnormal actions such as after hour activity or unusually high transaction rates from unexpected sources. Be sure to comply with any applicable state laws that require notification to employees that monitoring may be conducted, including accessing their emails, and be sure that appropriate permissions are required to be obtained from senior management before emails of others are reviewed.

[Table of Contents]

Inbound & Outbound Email, Instant Messaging

Email has become a core communications tool in today's business. However, companies that use email are confronted with a number of threats that can be devastating to their organization if appropriate measures are not taken. With regard to inbound email, the major threats are Spam, Phishing, Trojans, Denial of Service (DoS) attacks, and of course, Viruses. With regard to outbound email, the major threats are that a private message will be intercepted and read or that valid email addresses will be used fraudulently (spoofed) by hackers.

To combat these threats, one must take strong, comprehensive measures. Where feasible, an organization may prefer a single supplier which can provide multiple areas of protection. This will create efficiencies in administration, and quite probably in cost, compared to a multi-vendor solution.

[7] There is some risk that technical staff could access the information via computer utility programs without having the primary applications.

In the following sections, we will explain each of these threats and then give suggestions to consider to combat them.

Inbound Email

Spam:
Unsolicited email ('Spam') is one of the most prevalent threats to organizations. Spam is not only offensive and annoying; it costs companies billions of dollars each year in lost productivity and creates a significant burden on systems in terms of bandwidth and storage consumption. An estimate of between 40%-50% of inbound Internet corporate e-mail is classified as Spam. That number is expected to grow to 60%-70% during the next two years. Spam reduces employee productivity by clogging already overflowing user inboxes, forcing users to delete (or forward) the messages. Spam often has inappropriate or offensive content. Spam may be sent to email addresses found on websites or other places with a publicly posted email address.

Anti-spam services can be implemented in-house or outsourced to an ASP, or a combination of both, depending on the size and requirements of the organization. It is more cost effective for small and medium-sized businesses to use an ASP managed service. Spam management can be a full time job for any organization. ASP's can also provide anti-virus scanning as part of their services. This is highly recommended since this would provide an organization with another level of protection. In addition, the centralized nature of a managed service supports real-time systems updates, allowing for more rapid protection against new forms of Spam, Viruses and DoS attacks.[8]

Spoofing:
Spoofing occurs when a "hacker"—an unauthorized user—successfully gains access to a list of valid email addresses in your computers, and uses those addresses as sending addresses for a fraudulent email campaign. This is often done to give the appearance of a valid source (e.g., a name in your agency), and may involve selling some expensive or offensive product.

Phishing:
Phishing is the newest type of spam attack. It utilizes spoofed emails and fraudulent websites designed to con recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. This type of attack was initially targeted at consumers, however, more attacks are being aimed at

[8] When considering any Anti-spam product for in-house or ASP based use, check for the following features:

1. Accuracy
2. Trusted-Sender Lists
3. End-User Quarantine Area
4. Anti-Virus Scanning
5. Update Frequency
6. Point System and Distribution Options
7. HTML-Based Spam Blocking

organizations to obtain corporate usernames, passwords, email address, etc. Phishers do this by posing as a trusted well-known bank, online retailer, credit card company, or other respected organization. It has been reported that Phishers are able to convince 3-5% of recipients to respond to these fraudulent emails.

Trojans:
Trojans are programs that have been designed to open a back door into a system. Most Trojans are used as proxies for mail relays and denial of service attacks. User systems get infected by Trojan viruses when users open attachments that are infected. Trojans in infected PC's remain dormant and can then be used by hackers to access the information on your computers or to perform denial of service attacks and other malicious acts.

AdWare:
Adware is a set of programs that come to your computers through emails or when you access other websites. Adware simply sits on the computer and logs where you go and what you do. It may send usage information to another site.

Spyware:
Spyware continues to grow at an alarming rate and has become a major privacy and security threat, as well as being a real nuisance. Spyware is also known as Adware, Malware, Scumware, Data-mining, aggressive advertising, Parasites, Trojans, Dialers, Browser Hijackers, and tracking components. When a PC is infected with Spyware, every keystroke, every web site visit, and every conversation could be recorded or monitored by the person or company that secretly installed the software on the user's system. The consequences of Spyware infections can include banking and identity theft, unusual computer problems, slow Internet access, changes in the browser homepage, search pages or favorites, and excessive numbers of pop-up ads even when you are not on the Web.

Denial of Service (DoS):
A new generation of threat to corporate inbound mail servers is Denial of Service. DoS attacks saturate the inbound mail servers by sending malicious emails, causing the servers to fail or be slow to respond to valid email. DoS is generally focused toward web servers and Internet gateways. However, mail server DoS is on the rise.

Viruses:
The most widely acknowledged threat is that of viruses. Viruses are often spread via email and can cause system down time, loss of productivity, loss of data, and in the worst-case scenario, exposure of confidential data. Mail-borne virus attacks via the Internet have been on the rise during the past several years. Virus cleanup has cost organizations millions of dollars and countless hours of the time of skilled IT personnel. Viruses have become more difficult to detect because they can be nested in attachments, zip files or other executables. Viruses are particularly destructive because of their ability to self-replicate. At a minimum, every organization needs to be scanning for viruses at the desktop and messaging server levels. A third tier of defense strategy is to scan emails

before they enter or leave your organization. This can be done at the Internet gateway level, scanning all traffic coming from, and going to, the Internet.

Immediate action by businesses should be taken to combat against these threats to secure their computer systems.

Generally, an agency may want to block certain types of files that scanning programs generally cannot penetrate, e.g. Zip files. As more and more users now have high bandwidth DSL or high speed access of some form, the agency should consider if zipping is something worthwhile. Zipping requires a set of manual steps to create and to expand.

Anti-virus software, including a firewall, to be most effective is implemented at the desktop, laptop, server and gateway levels to limit the threat of any virus infecting the organization. This software can also be loaded on machines not owned by the agency that employees can use to access the network when out of the office. When this course is followed, be sure to adhere to any licensing and fee requirements. Many businesses schedule daily and/or weekly scan engine and virus definition updates, as well as regular scans of mail server mailboxes. You need to check employee machines to make sure they remain current with virus protection, so that scans are being run and updates are being made automatically. Policies and procedures for handling virus outbreaks are best defined in advance of a virus infection.[9]

[Table of Contents]

Outbound Email

Privacy/Encryption:
Simple Mail Transport Protocol (SMTP) is used to communicate between mail servers over the Internet. SMTP provides the rules that enable email servers to locate each other across the Internet and then transmit messages between them. Email via SMTP over the Internet is notoriously insecure, and it is highly vulnerable to interception and forgery. Fundamentally, sending an email message via SMTP over the Internet is like sending an open-faced postcard through the U.S. mail.[10]

---

[9] Possible steps for a "Virus Found" procedure:

- Verify definitions are up to date
- Disconnect network connection
- Delete any infected files that were "left alone"
- Empty quarantine
- Empty Temporary Internet Files directory
- Empty Recycle Bin
- Run full system scan
    - If nothing found, reconnect cable & resume normal business
    - If infection found, delete them, and rescan.

[10] An email message, like a postcard, must first be composed using an email client like Microsoft Outlook or Lotus Notes, which are secured when used for internal communication within an enterprise. A service on the mail server then converts and sends the message to its destination via SMTP. The message, can transverse several servers before reaching its final destination. The originating server identifies the domain and passes the message to another server and/or gateway. This process is repeated until the correct server is

From a security standpoint, when an email message has been sent on its journey to its destination, it can be read by anyone who has the right technology and messaging knowledge. However, the person who is intentionally trying to read the message must sift through thousands or even millions of emails, requiring considerable effort and probably unlawful intent. In spite of the enormous effort that would be required to obtain the confidential information from email while it is in route, it remains a major exposure. Therefore, without proper protection, such as encryption, it is generally inadvisable to transfer sensitive information by email or to put too much trust on information received via email. Traditional mail and faxes are generally better alternatives for sending this confidential or sensitive information, although these forms of delivery are also susceptible to misdelivery or other interception. Agents also should have an understanding of the encryption policies of the entities with which they do business.

[Table of Contents]

Email Policy

Organizations may want to establish an email policy for what is appropriate to be sent over the Internet via unencrypted email.[11]

This email policy can also provide rules for the appropriate use and content of email by agency employees and spell out that the agency may audit emails to make sure users comply with the agency's policy.[12] This policy, coupled with appropriate monitoring and enforcement of the policy, may help limit the agency's legal exposure for inappropriate emails sent over the agency's network.

Many of the problems discussed in this section arise because an employee has opened an infected email attachment, music or video file, or has downloaded a non-business application from the Internet. The agency's email policy can prohibit employees from downloading or loading applications without prior approval. It also can restrict the employee from downloading music or video files and can instruct employees not to open any attachment where the email is from an unknown source or where the email contains an unusual caption even if it is from what appears to be a known source.

---

finally reached. The message is then placed in the user's inbox to be read. This complete process takes only a few seconds.

[11] Email can be made more secure by implementing Secure/Multipurpose Internet Mail Extensions (S/MIME). This protocol is supported in most messaging systems. However, a secure email system requires the user to take additional steps to encrypt the email and the email recipient may not have the compatible software to unencrypt the message. In the case of secure email technology, it has not kept pace with demand and all current solutions have drawbacks. Thus, many businesses will choose to defer deployment of secure email services until the market is more mature.

[12] It is important for the agency to comply with any applicable state laws that require notification to employees that monitoring may be conducted, including accessing their emails, and that appropriate permissions are required to be obtained from senior management before emails of others are reviewed.

Instant Messaging

More and more agencies are starting to use instant messaging as well as email to conduct business. Instant messaging can expose agency systems to viruses and worms in an even more insidious way than email, because the virus or worm can be spread through a weakness in the instant messaging software without the need for an attachment to be opened. Agencies using instant messaging should seek virus and worm protection software that also protects instant messaging applications. Also, some people "troll" IM users and try to get them to respond, often for illegitimate reasons.

Instant messaging also can create other exposures for a business. IM "style" is typically a very loose, free-form style, and may be overly casual, or use language or expressions not appropriate for use in customer interactions.

[Table of Contents]

Other Security Issues Arising Within the Agency Perimeter

Configuring Systems for Security & Security Patches

In addition to managing systems access and email, there are several other security issues that arise within the agency's perimeter. It is important that you have followed the agency management system vendor's recommendations, including on how to configure the agency management system to provide for multiple levels of security access to the computerized data records. Also make sure that your underlying desktop and server operating systems' security are up-to-date.[13]

As discussed above, it is prudent to take steps to make sure the agency stays current with virus definitions with regard to its virus and other software and to schedule virus definition updates to be downloaded on a daily basis.

With respect to updates of application software, such as Microsoft's frequent Windows updates, check with your vendor or with other users of the software as to whether it is timely to install it. Generally, if a patch causes a problem, the vendor will pull it, so a patch that is still available one week after release is likely to be safe to load. You also may want to have skilled IT personnel verify that the patches have been applied successfully.[14]

---

[13] Novell or Microsoft security templates are available at www.nist.gov. With the newer versions of the Microsoft Windows operating systems, patches can be installed automatically at a predetermined time. This generally causes few if any problems with the general patches. However, service packs can be another story. Generally you want to load Microsoft, Novell and other operating system patches within a week after they are released, but whenever possible, either the 2nd or 3rd day after release. You can check multiple systems at once for Microsoft patches by using easy to run software available from shavlik.com.

[14] These Microsoft patches can be found at: http://v4.windowsupdate.microsoft.com/en/default.asp.

Organizations with on-site IT personnel may wish to implement Microsoft's Systems Management Server (SMS), or a similar product, to automate patch distribution.

Microsoft recently released Service Pack 2 (SP2) for Windows XP which provides significant security enhancements, but at some exposure. Some reconfiguration of the desktop systems may be needed. Before

Implementation of firewalls at the desktop level, as well as at the agency perimeter (the entry point of any incoming traffic), is recommended as a further security measure.

Employee Security Restrictions, Encryption, & Confidentiality Agreements

The agency can develop an approved software list and restrict staff from downloading or loading any software that has not been included on that list or otherwise approved in advance. Agencies also may not want to allow agency employees to permit family members to use office computers and laptops, because of the risk the family member may download a game or music file full of viruses or access information they should not see.

The agency's security policy can also spell out that employees logoff their password protected systems when they leave their desks, that they keep client files that they are working with out of view, and keep files containing "Protected Health Information" (HIPAA) or other confidential policyholder or employee information in locked cabinets. Readers should review the recent ACT report, "Safeguarding Non-Public Personal Information; A Guide for Independent Agents and Brokers," for a more detailed treatment of steps agents can take to protect the privacy of their policyholders' confidential information.[15]

Agents should also consider policies that provide for storing electronic "Protected Health Information," and similar types of confidential policyholder information in an encrypted format, so that it is unintelligible to anyone other than authorized parties with the key and processes to decipher the data back to its original form.

Agencies may also want to have each employee sign a confidentiality agreement acknowledging the agency's ownership of all of its data and policyholder information; the employee's commitment to protect the confidentiality of this data and information; and the employee's commitment not to copy any of this data or information onto any computer, USB drive or other device, or to transmit it, post it to a web site, or print it, except as needed to conduct a transaction in the course of the agency's business.

Phone Calls, Office Visits, & Protection of Physical Agency Data

Just as an employee cannot logon to the agency's systems without a digital ID, the agency may also adopt procedures to spell out the steps agency employees follow to verify the identity of those who call on the phone, along with spelling out the limits on sharing client information over the phone.

Many agencies also require guests who visit the office should be required to sign in and then be escorted while in the office.

---

implementing, check with your Agency Management System vendor or similar agency users who have implemented SP2.

[15] The report is found at www.independentagent.com/act, by clicking on "Technology Reports."

Agency procedures can also provide that agency data contained on other media, such as back-up tapes, CD's, diskettes, or other media be safeguarded. Password protection on CD's should be considered. Paper being discarded with agency or policyholder information on it should be shredded. Diskettes should be "wiped" or destroyed before being discarded. Any computers returned at the termination of leases or discarded should have their drives "wiped" first. "Wiping" is a process that reformats the diskette or drive so that the former data is removed and not recoverable. "Erasing" these drives is not sufficient, since there are some programs that can be used to recover this "erased" information.

[Table of Contents]

Securing the Agency Perimeter from the External World

Firewalls, Wireless Networks, Monitoring, and Logging

The agency should install a firewall to control traffic moving in and out of the agency's network to prevent unauthorized parties from gaining access to the network.[16] It is also important for the agency to monitor this activity to not only check for security, but to check for employees wasting time. Employees should be informed about any office policy regarding the loading of unapproved applications on their desktops—whether via the Internet or purchased personally. As discussed above, this can be specifically covered in the agency's security policy. You will want to run software that checks for and removes spyware and adware. Your monitoring process can confirm that no software has been installed that is collecting information, such as customer credit card information that has been entered into the agency's system.

If a wireless network is being used by the agency, the various levels of security should be activated.[17] The wireless access point can be positioned in the center of the office so that the signal will radiate out to the windows, but not beyond. This may require professional support to get this adjusted correctly. Only purchase wireless access points that can accommodate security updates as they are developed. Also, beware that when you

[16] The four major types of firewalls are Packet Filtering, Application Gateway, Circuit-level Gateway, and Proxy Server. Packet filtering looks at each packet entering or leaving the network and accepts or rejects it based upon user-defined rules. Packet filtering, however, is susceptible to IP spoofing. The application gateway applies security mechanisms to specific applications. It is effective, but can lead to performance degradation. With the circuit-level gateway, the security mechanism is applied when the connection is established, and thereafter, packets can flow between the hosts without further checking. A proxy server intercepts all messages entering and leaving the network effectively hiding the true network addresses. If a Proxy Server is used, it is important to make sure its logs are not compromising user names and passwords.

[17] The first step is to enable the "WEP" which provides a basic level of encryption. This encryption is in a disabled mode when the "Wi-Fi" product first arrives. Second, the default "SSID" (service set identifier) should be changed, because the default setting is widely published. The ID used should be one that has little or no meaning, and should not be the agency name. You should also disable "broadcast SSID" on the access point, if you are able, to help hide your access point from any wireless device that does not enter the correct SSID. You should also change the default password on your access point or wireless router. A leading wireless firewall providing an IPSEC type of encryption will provide a higher level of security against hackers who have WEP cracking software easily available to them.

update the firmware on your wireless access point or wireless router, it might return your security adjustments back to the default (less secure) position, requiring you to make the adjustments again. There are also steps you can take to make your wireless router more secure.[18]

The agency should also actively manage the logs generated by its systems (firewall, wireless router, proxy server, fax server, file access, etc.) for any unusual activity. For example, are there any unusual patterns of file access that suggest a broad and inappropriate access to the agency's data? These logs of business transactions and system access should be kept for the period of years required by record retention or other laws, because of emerging privacy issues. More and more often, companies are being put in the position of having to prove that information leaks did not come from them, rather than an individual having to prove that they did. Archive these logs at least monthly onto a DVD or CD, and ensure that each system does not overwrite the logs prior to archiving them. It is also important to make sure that the logs do not create a security or privacy problem themselves by containing detailed policyholder information.

Laptops, PDA's, and USB Drives

A laptop brought into the network—perhaps from a producer who travels, an agent you partner with, or even a policyholder visiting your offices—can pose a significant security risk. Does the laptop have a virus or other "malware," and what unknown programs are on it? All laptops should be patched with the latest operating system patches, have an up-to-date firewall and virus protection installed, be inspected for spyware/worms, and have access only to the parts of the network needed for work functions. These laptops should also be backed up at regular intervals. It is also important for agency employees to know that when they use their laptops at public locations having wireless connections, they do not have the network level firewall and virus protection that they would have in the office. This makes it all the more important for their laptops to be up-to-date with these protections.

Laptops should also be configured so that they can connect to only one network at a time. Otherwise, when the laptop is plugged into the agency's wired network, a hacker may be able to use Wi-Fi to access the laptop and then tunnel through the laptop's wired connection, past the firewall, and into the agency's network.[19]

Whoever is responsible for systems security should periodically check the laptops accessing the network to be sure they have the right software and updates. In addition, agency security policies can provide that the content on laptops be inspected periodically to make sure that only necessary documents, files and settings are stored on them. This is

[18] If you're deploying a wireless router, think about assigning static IP addresses for your wireless NICs and turn off DHCP. It's true that it's more of an administrative overhead to manage, but we found a number of wireless networks that passed out IP addresses to us once we associated with the AP. Although a wireless sniffer could easily pick out IP addresses, by not passing them out, it just adds another barrier.

[19] This risk arises because Windows-based laptops with Wi-Fi capability can be configured with one click in "ad-hoc mode," which turns them into the equivalent of an access point for other nearby laptops to access, along with any network the laptop is connected to.

because if a laptop is stolen or lost and contains private policyholder information, it could cause a significant exposure for the agency. The agency should consider encrypting the data on laptops wherever possible to minimize this risk.

These office laptops also should not be shared with family members who may download a game or music file full of viruses or other malware, or have access to confidential information.

The agency may want to formulate a security policy on laptops that covers the monitoring of laptops for compliance, the types of information that can be kept on them, who may access them, and the steps to be taken when a new laptop is brought into the system.

For these reasons, an "unknown" laptop, such as that of a carrier or vendor marketing rep or policyholder, should never be allowed direct access to the agency's network.

The agency may also want to have a policy on the types of information that can be kept on PDA's. For example, the agency may not want agency login or password information to be copied to or stored in such a device, given the risk should it be lost or stolen. Agencies also may want employees who keep private information in their contact list to be required to set up a second contact list, without this private information, and to synchronize the PDA to the second list.

The agency may also want to have a policy that specifies which employees are authorized to use a USB "thumbnail" drive, and what types of information may be copied to it or from it.

Branch Offices, Remote Locations, Dial-up Access

The security policies adopted for an agency should apply and be monitored equally in all locations. Remote access to the network should be password protected, and access should be determined at the firewall level.[20] An employee should never give a password to another employee, remote or otherwise, unless he or she is sure of the identity of the remote individual, and the appropriateness of that person's access.

Many agencies have modem servers or communication servers that are used for remote dial-up access, and these systems have been left open, waiting for a connection. Often, these access points have been all but forgotten and are not being monitored. It is important to survey all phone lines and equipment to ensure the purpose for them is known and still needed, and that the appropriate passwords and security are in place to safeguard access. [Table of Contents]

[20] PC Anywhere and Terminal Services are services which provide the transport of the data from the remote connection to the main server. To make these transport mechanisms truly secure, you should have a Virtual Private Network (VPN). If using PC Anywhere consider using the callback feature. If using Terminal Services or even a Virtual Private Network (VPN), consider using a static IP at the remote and having the firewall at the main server block all IP's except those that are part of your range. If you have a dedicated line you are generally going to be secure from a networking perspective.

Steps to Consider if a Security Breach Occurs

You should work with your technology and security staffs and/or consultants to develop a pre-defined action plan to deploy in the event a security breach occurs. Do not wait until a breach occurs to think through how to react to the situation.

If you experience a security breach, here are some steps for you to consider to mitigate against further damage and to prevent a recurrence:

- Identify senior staff to whom reports of known or suspected security breaches should be made. It is important that someone be designated as the point person so reports are properly directed and acted on in a timely way.
- Determine if any personal, nonpublic information about your policyholders or employees has been stolen or accessed by unauthorized employees or third parties. If so, consult with your attorney or others knowledgeable about privacy laws to determine your obligations and next steps. These steps might include notifying the affected policyholders and employees of the breach or possible theft of their information, and suggesting some steps they might consider to safeguard against the misuse of their information. You also may need to notify law enforcement and/or your agency's professional liability carrier.
- Investigate the cause of the breach. If it has resulted from the compromising of your hardware or software, isolate the hardware and software involved by disconnecting it from the network and the rest of the agency's systems, as well as the external world.
- Work with your security and technology professionals to plug any holes in your systems to prevent further incidents or a spread of the problem. Remove or fully quarantine the infected files and/or other identifiable cause(s) of the problem. Notify security software vendors if you believe the breach is something they should be aware of or is potentially a new problem to them.
- If the security breach has resulted from actions taken by unauthorized employees or third parties, take appropriate and/or corrective measures, such as disciplining the employees in accordance with your personnel manual and policies (which may include suspension, termination or other measures), notifying the third parties' organizations, and/or notifying the appropriate law enforcement authorities.
- Notify your business partners (carriers, vendors, etc.) of the security breach in situations where the breach occurred through the use of their facilities or services, or in cases in which they may have been or may, in the future, be impacted by the breach. This notification will enable your business partners to safeguard their systems, limit access, or take other necessary protective and corrective actions.
- Determine the appropriate monitoring processes and procedures in an effort to prevent a recurrence of the security breach and implement them. This should include a review of the existing processes to see where they failed. Train your staff in any new processes and procedures and in the nature of the security risks they are designed to prevent, and update or revise your written policies and procedures to reflect these changes.

- Once the cause of the security breach has been removed or addressed, and corrective or preventive measures have been put in place, bring the isolated software and equipment back into operation after testing it to be sure it is no longer a problem.
- Consider whether the nature of the breach calls for an independent security audit of your agency by an outside security professional.

[Table of Contents]

The members of the ACT Agency Security Issues Work Group that produced this report include:

Brian Bartosh, Top O' Michigan Insurance Agency (chair)
Brad Allen, Selective Insurance
Steve Anderson, American Insurance Consultants
Bev Coats, CDH Insurance
Gavin Delaney, The Hartford
Ron Dudley, ACORD
Hani Esoo, Computers by Design
Barbara Flanigan, CNA Insurance
Mike Gray, Lehr Insurance Agency
Jeff Holman, Liberty Mutual RAM
Doug Johnston, Applied Systems
Alex Kuhn, The Hartford
William McCarthy, Liberty Mutual RAM
Rozalyn Murphy, The Hartford
Neil Nelson, Encompass Insurance/Allstate
Gray Nester, BB&T Insurance
Bob O'Connor, Consultant
Rebecca Partyka, St. Paul Travelers
Sandi Perillo, The Hartford
Sue Putnam, SCA Insurance
Roy Riley, Peel & Holland
Linda Rollings, AMS Users Group
Dave Schuppler, Schuppler Insurance
Greg Shiple, Applied Systems
Bob Slocum, The Slocum Agency
Clay Snellings, Snellings Walters Insurance
Angelyn Treutel, Treutel Insurance Agency
Alvito Vaz, Drive Insurance by Progressive
Rick Williams, Consultant
Tim Woodcock, Courtesy Computers
Tim Woods, idNet/Afni Insurance Services
Jeff Yates, ACT Executive Director

Debra Perkins, IIABA Executive Vice President and General Counsel also provided valuable input into this report.

For more information, contact Jeff Yates, ACT Executive Director, at jeff.yates@iiaba.net.

[Table of Contents]

Appendix A

Glossary of Security Terms

Microsoft has developed an excellent glossary of security terms and other security information which can be found by going to the Microsoft website (www.microsoft.com), and typing in "Microsoft Security Glossary" into the search tool at the top right of the home page.

[Table of Contents]

Appendix B

Securing Outside Security Help

Insurance agents face a growing number of security vulnerabilities in business today. The need to protect the bottom line, as well as corporate image and customer trust, drives the demand to effectively manage information security. However, agencies frequently do not have the resources to effectively manage and monitor their IT security. Security incidents can have a significant negative impact on business, interrupting operations and increasing costs in a very short period of time.

Agencies face a number of obstacles to achieving and maintaining in-house security programs:

- A shortage of qualified security professionals
- Insufficient resources and infrastructure to support comprehensive 24x7 network security program
- Rising complexity of security technology
- Lack of time to dedicate to security issues.

Today, many insurance agencies are effectively outsourcing their security management and monitoring services to trusted IT vendors and Managed Security Services Providers (MSSP) with industry certified credentials to lead them through the complex security field. Although there are a wide range of industry recognized "security certifications," each follow an evolving common set of principles relating to information systems security, including:

- Access Control Systems & Methodology
- Applications & Systems Development
- Business Continuity Planning
- Cryptography
- Law, Investigation & Ethics
- Operations Security

- Physical Security
- Security Architecture & Models
- Security Management Practices
- Telecommunications, Network & Internet Security.[21]

Among other benefits, outsourced managed security offers the following:

- Maintain positive company reputation
- Freedom to focus on company growth
- Improved information protection
- Possible reduction in cost of security management.

The IT industry has yet to establish standards to compare providers within the MSSP industry. Therefore, it is important to investigate MSSP vendors thoroughly, before engaging in their services.

When interviewing potential vendors, request documentation to gauge their strengths and weaknesses, including in the following areas:

- Financially Sound – They should be well-funded with a large client base in which to spread their costs. You may want to run a credit report or business report on the potential vendor to see if vulnerabilities exist.
- Years in business – Look for a vendor that has years of experience in the security business, and is familiar with the insurance industry.
- MSSP staff expertise – Ask for the biographies of the managing personnel. Look for experienced leadership and knowledge of detailed security tasks.
- Existing Customers – Check customer references, and how long their average customer stays with their services. If possible, ask for a list of existing insurance agency customers that utilize their services and check references.
- MSSP's Reputation – Perform due diligence by personally investigating the vendor. Review comments from analysts, industry trade writers, and third parties.
- What kind of background investigations do they do on their employees?

Offered Services

Determine if the MSSP's services are flexible enough to meet your agency's current and future needs. By asking several questions, you can evaluate their management, monitoring, and response techniques, such as:

- What IT products and services do they support? Do they maximize the use of existing security products by assisting with their installation, implementation and integration?
- How will the MSSP staff operate in an emergency? Does the MSSP offer guaranteed response times, including set levels of response per severity of threat?

[21] Businesses are increasingly looking at internationally recognized security frameworks when designing their comprehensive security policies. Examples include ISO 17799:2005 (International Organization for Standardization, www.iso.org); Common Book of Knowledge (CBK®, (ISC)², www.isc2.org).

- Does the vendor have policies and procedures for quickly adding qualified personnel to their staff, should the additional expertise become necessary?
- Does the security firm have the flexibility to meet your needs? Are there other features offered by the firm that mitigate against potential security breaches, reduce liability, and provide peace of mind? Do they constantly monitor security alerts and advisories?

Support Infrastructure

Additional questions should be asked, with respect to the MSSP's ability to ensure that client services are never interrupted, such as:

- Does the MSSP have access to or own a security operations center (SOC) facility? If so, is the facility equipped for redundancy to ensure continued operations (continuous power and communications, staffed 24/7, FEMA approved site, etc.).
- What is their philosophy and approach to hiring and retaining qualified competent staff?
- Do they require and support continued training of their IT personnel?
- How do they ensure client confidentiality?
- Are they a true 24/7 shop, providing flexible communications with their clients?
- How do they stay abreast of the latest industry trends, cyber threats, vulnerabilities, hacker techniques, and security developments?

One approach to the hiring of an MSSP is by personal recommendation. An MSSP that has provided satisfactory services to a similar agency is likely to be well prepared in providing your agency the same.

Security Services Provided by Outside Professionals

MSSPs can encompass various types of services, including consulting, remote perimeter management, managed security monitoring, vulnerability/penetration testing and compliance monitoring.

Some of the managed services that an MSSP may perform for the agency—that the agency might otherwise overlook—include:

- Actively monitor network and servers
- Central management of systems, users and resources
- Network, operating system and application patch management
- Disaster recovery planning
- Data backup/ restore testing and log review
- Network usage log review and reporting
- Network vulnerability detection and reporting
- Virus, SPAM, and spyware management
- IDS (intrusion detection system) management
- Internet abuse reporting
- Annual security audit and reporting

- Software license compliance review.

Reminder…
Always make certain that you first analyze what services you wish to outsource. Then choose the most qualified vendor, based on your due diligence. Most importantly, ensure that you remain in control of your network systems, not the vendor.

Industry Security Certifications

The table below displays many of the industry recognized security certifications currently available. This list will help in assessing the qualifications of the MSSP's support staff.

International Information Systems Security Certification Consortium (ISC)^2
Vendor Site
CISSP - Certified Information System Security Professional ®
SSCP - Systems Security Certified Practitioner

Prosoft
Vendor Site
CIW - Security Professional

SANS
Vendor Site
GSE - GIAC Security Engineer

RSA Security
Vendor Site
RSA/CSE - RSA Certified Systems Engineer
RSA/CA - RSA Certified Administrator
RSA/CI - RSA Certified Instructors

CheckPoint
Vendor Site
CCSA - Check Point Certified Security Administrator
CCSE - Check Point Certified Security Engineer

Cisco
Vendor Site
Cisco Firewall Specialist
Cisco VPN Specialist
Cisco IDS Specialist
CCSP - Cisco Certified Security Professional

TruSecure
Vendor Site

TICSA - TruSecure ICSA Certified Security Associate
TICSE - TruSecure ICSA Certified Security Engineer

BrainBench
Vendor Site
BIS - Brainbench Internet Security Certification
BNS - Brainbench Network Security Certification

Learning Tree
Vendor Site
NSCP - Network Security Certified Professional

CompTIA
Vendor Site
Security+

Security Certified Program
Vendor Site
SCNP - Security Certified Network Professional
SCNA - Security Certified Network Architect

[Table of Contents]

Appendix C

Agency Security Risk Self Assessment Tool

Maximizing the security of the agency's information systems—whether for electronic or paper information—is an important part of protecting the agency's critical information and assuring the continuity of the agency's operations. It is vital for agents to understand that a single security breach can bring your agency's work to a standstill and even jeopardize the ongoing viability of the agency. This checklist is designed to alert you to the major security issues you should be considering.

Overall Agency Focus on Security

1. Principal and staff involvement.
    a. Agency principals provide security direction with technical input. This involves a balancing of the extent of the risks presented against the costs of various options to protect against these risks.
    b. Agency security officer or its equivalent is appointed to take ownership of the implementation of the agency's security program and to keep continuing focus on it.
    c. Staff is trained on agency's security policy and on its importance.
    d. Staff signs applicable agreements to adhere to agency security policy and to protect confidentiality of agency information.

2. Implement security policy, monitor, audit, and continue to refine policy.
    a. Has the agency had a security audit performed by an outside expert?
    b. Does the agency have security policy which it reviews periodically? This policy can include employee responsibilities, restrictions on the use of the Internet and email, restrictions on re-using others' information without permission, protecting the confidentiality of employee passwords and agency data, preventing computer access by unauthorized parties, and other security issues identified by the agency. Have employees been advised that their emails and systems may be monitored and have applicable state laws covering employee monitoring and notification been checked for adherence?
    c. Does the agency have procedures to monitor and audit security policy compliance, approve exceptions, and handle violations?
    d. Does the agency have procedures to monitor network traffic to detect any unusual activities, whether caused by a third party secretly making use of the agency's systems or an employee improperly transferring agency information to external sources? Is the agency actively managing the logs produced by its firewall, wireless router, proxy server, fax server, etc., and keeping them for the period required by record retention or other laws because of emerging privacy issues?
    e. Has the agency considered implementing an intrusion detection system?
    f. Does agency have procedures to identify security holes, to evaluate the cause of the failure, and to document and implement corrections?
    g. Does the security policy spell out the types of agency information that is permitted to be loaded onto employee laptops and PDA-type devices in case of loss?
    h. Has the agency developed a pre-defined action plan should a security breach occur?

3. Evaluate backup security and disaster recovery plan.
    a. Are data backups completed daily?
    b. Are backups stored in a secure location?
    c. Are backups regularly stored off-site in an environmentally protected and secure location?
    d. Are backups tested at least quarterly? These tests should be done as a restore from the backup tapes, not just a validation that the backup process ran "successfully."
    e. Has the agency developed and tested a disaster recovery plan?

Protecting Against Threats External to the Agency

4. Evaluate external access to your computer network.
    a. Do you have a router and firewall to block and regulate access to the agency's systems, a Virtual Private Network (VPN) to provide a secure connection from external sources, and anti-virus software scanning on the

network, servers (including mail server), and desktops to prevent inbound viruses or the lodging of worms, spyware, or Trojan horses in the agency's systems?

b. Does this protection software run a scan on any executable file received through the Internet, a diskette, or other memory device?
c. Have you activated the automatic update features to keep this protection software up-to-date? Are you staying current with the security patches and updates for all of your operating systems and testing them before full deployment to prevent systems crashes?
d. Have you implemented a server based or outsourced SPAM blocker?
e. Establish who is authorized to make changes to the agency's firewall and what the approval process is for such changes.
f. Are you current with security updates for your agency's software, and have you established that these updates are automatically installed at a time convenient to the agency?
g. Do you keep track of security bulletins from your vendors?
h. Consider shutting off open Ethernet ports in the office.
i. Keep Wireless Access Points off of the trusted network (on your DMZ).
j. Have a firewall that, by default, has all ports closed unless needed (and opened only to the IP addresses it needs to access).
k. Evaluate and properly secure any network access 'holes' (PPP, VPN, etc) on your network.
l. Does your policy prevent unauthorized parties from using agency desktops or laptops because of the risks such action creates to compromise agency data?
m. Does your policy restrict employees from downloading any software not on the approved list without advance approval? Does your policy restrict employees from downloading non-work files, such as music or video material? Does your policy restrict an employee from opening any email attachment from an unknown source or with an unusual caption?
n. Has the agency implemented virus and worm protection software to protect its instant messaging applications?
o. Is the agency continuing to monitor any remaining dial-up connection points to the agency's systems?
p. Do you "wipe", not just "erase" all information from diskettes, drives, and computers before discarding them or turning them in?

5. Application and data access controls.
    a. Do you have access control installed on all agency computers?
    b. Have you determined the appropriate access for each employee or category of employee?

6. Remote access.
    a. Does your policy cover the firewalls and virus protection software that should be in place when employees access the agency's systems from home?

   b. Are remote locations and employee desktop computers regularly checked to make sure they are running the same security software as the rest of the agency's systems?
   c. Do you require that remote access to the corporate network be through a secured and encrypted connection, such as through a virtual private network (VPN)?
   d. Have you changed default security settings and secured wireless access so that unauthorized parties cannot access the agency's system through the wireless connection?

7. Evaluate ease of access to your building.
   a. Can guests at your agency walk around your building without escort and/or name badges?
   b. Do you log guests that visit your agency?

8. Evaluate policy on sharing of information.
   a. Is policy set on identity verification of callers?
   b. Is policy set on what types of information can be disseminated, and by what authority process?

Protecting Against Threats Within the Agency

9. Evaluate the agency's password management policy.
   a. Do employees understand the importance of keeping their passwords private and not posting them on their monitors or leaving them in visible locations? Do employees understand the importance of not sharing these passwords with other employees or individuals (except the agency's password administrator as provided in the agency's policies)?
   b. Are procedures in place so that passwords of former employees are terminated immediately to all of the agency's systems and to the systems of the agency's carriers and other entities with which the agency does business?
   c. Has the agency assigned the responsibility for the administration and maintenance of passwords; are individually based, complex passwords combination of uppercase, lower case, and numbers) used? Are passwords changed on a regular basis?
   d. Is the requirement to keep passwords confidential explicitly covered in the office manual and employee's written confidentiality agreement?

10. Establish data access based upon "need to know."
   a. Do you have a policy set for data to be accessed on a "need to know" basis?
   b. Have you secured all databases, networks, data storage, and other paper and electronic files to enforce this "need to know" policy?
   c. Do you have policy in place to safeguard non-public client information?

d. Do you have policy on what types of information can be sent by email, since it is not a confidential medium?
e. Do you have access control software installed on all employee laptops containing agency information or access to agency systems?
f. Do you have mailroom and fax procedures to safeguard the transmission, receipt, and routing of non-public client information?
g. Have you evaluated what type of information you will let clients access electronically, while protecting the security of the agency's systems?
h. Has the agency implemented privacy screens on monitors to guard against bystanders seeing confidential screens?
i. Do employees logoff their password protected desktops when they leave their desks?

11. Restrict employee downloads and opening of attachments from unknown sources.
    a. Does your security policy cover the prior approval process before employees are permitted to download applications into agency laptops and desktops? Is compliance monitored?
    b. Are employees restricted from opening attachments from unknown sources or with unusual captions?

12. Evaluate policy on non-trusted devices and software. (Non-trusted means devices and software that pose a security risk because they are unknown, not pre-approved, or not protected and monitored pursuant to the agency's security policy.)
    a. Can staff/guests use personal laptops and hardware on your computers and network?
    b. Can staff/guests install software on systems, or open documents from CD/ floppy?

13. Evaluate access to paper information.
    a. Are client documents left on desks when the employee is away from his/her desk (e.g., at lunch or in a meeting) or at the end of the workday?
    b. What security is applied to client charts/folders?
    c. Are files locked at the end of each work day, and are files containing non-public client information locked whenever an authorized employee is not at the file location?
    d. Is the fax machine checked regularly to remove any non-public client information?
    e. Is discarded client and agency information properly shredded when appropriate?

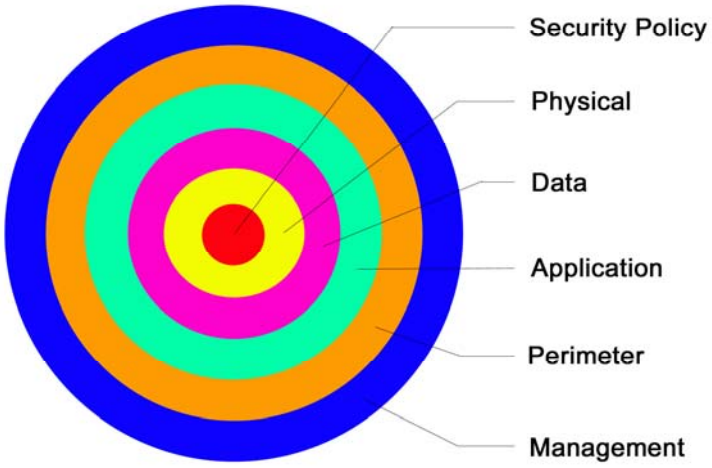
[Table of Contents]

Appendix D

Different Layers of Security

Security attacks are becoming more frequent and more sophisticated. Investing in single layer security systems is of limited use. A wiser course is to develop a multi-layered security architecture that recognizes the strengths and the limitations of each individual security layer.

Concentric Ring Illustration of the Different Security Layers



Each layer focuses on a different area of security in your agency.

Security Policy Layer: The Security Policy Layer, which is substantial in its application and scope, should encompass all aspects of employee awareness of security and responsibility to the network, email, Internet usage, and password usage.

Physical Layer: Keep your computers (servers, workstations, portable devices, software media, data backup media, switches, routers, firewall, etc.) locked down and safe from physical theft and intrusion. Each device must have a designated owner who is responsible for its security. The owner should have appropriate resources, skills, and information to fulfill this responsibility. Network equipment and software should be restricted to authorized personnel.

Data Layer: The Data Layer is limited to the accessibility of data on any given network. The desired outcome is one that restricts access to data to only those users who are required to have access. This protects privacy and provides accountability. Web application gateways, email spam filters, XML security systems and Secure Sockets Layer virtual private networks help ensure that application traffic is clean, efficient and secure.

Application Layer: The Application Layer provides an automated security layer to protect configurations on hosts and includes host-based antivirus applications, intrusion-prevention software, spyware tools and personal firewalls. These products provide essential "last-resort" security for applications. These products provide any given network with the most advanced set of tools to thwart any potential threat. However, as with most software, human intervention is required to ensure the solution is constantly updated.

Network Perimeter Layer: The Network Perimeter Layer (NPL) utilizes hardware and conceptual design to provide a layer of protection from outside the network. To create this layer of protection, the NPL utilizes firewalls, Virtual Private Networks (VPN's), routers, intrusion detection and prevention software, and Web Content filtering.

Management Layer: The Management Layer is critical to the continued security of the overall network. Consolidate your approach to security management, assess your overall vulnerability, and manage patches and updates carefully. Persistently monitor all security layers for compliance and vulnerabilities. This includes creating a security framework that makes it possible to identify potential threats early, accurately analyze risks from emerging threats, and develop effective remediation strategies quickly and protect the entire organization, from the borders of the corporate network down to each individual computer. In general, this requires supervision to ensure consistency in assessing overall vulnerability, managing patches and updates for each software and policy.

[Table of Contents]

Appendix E

Agency Information Security Policy (Sample)

Disclaimer
This is a sample policy on agency information security that some agencies may want to use by tailoring it to their individual circumstances. As with all other tools, it was prepared solely as a guide. It is not a substitute for agents and brokers independently evaluating the business, legal or other issues applicable to them and is not a recommendation that a particular course of action be adopted. Various state and federal laws may govern issues covered by this sample policy, and adherence to them is critical. If specific advice is required or desired, the services of an appropriate, competent professional should be sought.

This sample policy is intended to serve as a possible framework—a starting point—for your own information security policy or to compare to the one your organization has on the books. Please add to this framework as you address the specific issues covered in the body of this report as well as in the Agency Security Risk Self-Assessment Tool in Appendix C.

To ensure that employees understand the policy that you adopt, the agency should provide a copy for each employee. The agency can also consider a special employee meeting to go over the policy and its importance to the agency. Issues addressed in this policy can be raised at staff meetings regularly, so that the policies become top-of-mind with your employees.

After reading the policy, employees can be required to sign a form acknowledging that they have read the policy, understand it, and agree to abide by it. We've included a sample form on the last page.

To make sure that the agency is following its own policies, the agency should conduct routine compliance audits. Employees should be notified about the monitoring and compliance activities that will take place, especially as they relate to employee emails and other information on their systems. The agency should make sure it is fully complying with any state laws governing the monitoring of such employee information and any required employee notifications.

Introduction

Computer information systems and networks are an integral part of business at "Agency Name". The agency has made a substantial investment in human and financial resources to create these systems.

The enclosed policies and directives have been established in order to:

- Protect this investment.
- Safeguard the information contained within these systems.
- Reduce business and legal risk.
- Protect the good name of the agency.

Violations

Violations may result in disciplinary action in accordance with the human resources manual. Factors that may be considered in determining disciplinary action may include, but are not limited to the type and severity of the violation, whether it causes any liability or loss to the agency, and/or the presence of any repeated violation(s).

Administration

The information services manager (IS manager) is responsible for the administration of this policy.

Contents

The topics covered in this document include:

- Statement of responsibility
- Manager responsibilities
- IS manager responsibilities
- The Internet and e-mail
- Computer viruses
- Access codes and passwords
- Physical security
- Copyrights and license agreements

Statement of responsibility

This policy specifies general responsibilities for which all employees are responsible, except where specific responsibilities are assigned to specific categories of employees.

Manager responsibilities

Managers and supervisors must:

Ensure that all appropriate personnel are aware of and comply with this policy.
Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy.

IS manager responsibilities

The IS manager:

1. Develops and maintains written standards and procedures necessary to ensure implementation of and compliance with these policy directives.
2. Provides appropriate support and guidance to assist employees to fulfill their responsibilities under this directive.

The Internet and E-mail

The Internet is a very large, publicly accessible network that has millions of connected users and organizations worldwide. One popular feature of the Internet is e-mail.

Access to the Internet is provided to employees for the benefit of "Agency Name" and its policyholders. Employees are able to connect to a variety of business information resources around the world.

Conversely, the Internet is also replete with risks and inappropriate material. To ensure that all employees are responsible and productive Internet users and to protect the agency's interests, the following rules have been established for using the Internet and e-mail.

Acceptable use

Employees using the Internet are representing the agency. Employees are responsible for ensuring that the Internet is used in an effective and lawful manner. Examples of acceptable use are:

- Using Web browsers to obtain business information from commercial Web sites.
- Accessing databases for information as needed for agency business.
- Using e-mail for business communications.

Unacceptable use

Employees must not use the Internet for purposes that are illegal, harmful to the agency, or nonproductive. Examples of unacceptable use are:

- Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.
- Conducting personal business using agency resources.
- Transmitting any content that is offensive, harassing, or fraudulent.

Downloads

File downloads from the Internet are not permitted unless specifically authorized in advance and in writing by the IS manager.

Employee responsibilities

An employee who uses the Internet or Internet e-mail shall:

1. Limit use to agency business. Any personal use should be minimal and not interfere with the employee's productivity.
2. Be responsible for the content of all text, audio, or images that the employee places or sends over the Internet. All communications should be identifiable as from the employee and reflect the professionalism of the agency.
3. Not use or transmit copyrighted materials without permission.
4. Know and abide by all applicable agency policies, including dealing with security and confidentiality of agency records.
5. Run a virus scan on any executable file(s) received through the Internet.
6. Avoid transmission of "Information" protected under HIPAA, Gramm-Leach-Bliley or other applicable laws (confidential policyholder information) over the Internet, except in a manner specifically approved by agency procedures. and it is sent in encrypted form. This is because the Internet is not a confidential medium. Where it is permitted to transmit nonpublic personal information, employees are required to take steps reasonably intended to ensure that information is delivered to the proper person who is authorized to receive such information for a legitimate use.

Copyrights

Employees using the Internet are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express prior permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action by the agency and/or legal action by the copyright owner.

Monitoring

All messages created, sent, or retrieved using office tools, equipment or resources, including but not limited to computer equipment or software licensed by the agency are the property of the agency and *are not the personal property of the employee.* "Agency Name" reserves the right to access the contents of any messages sent using its tools and resources, without advance notice to employees.

Computer viruses

Computer viruses are programs designed to make unauthorized changes to programs and data. Therefore, viruses can cause destruction of corporate resources.

Background

It is important to know that:

- Computer viruses are much easier to prevent than to cure.

- Defenses against computer viruses include, at both the network and desktop levels, protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

IS responsibilities

IS shall:

1. Install and maintain appropriate antivirus software on all computers.
2. Respond to all virus attacks, destroy any virus detected, and document each incident.

Employee responsibilities

1. Employees shall not knowingly introduce a computer virus into agency computers.
2. Employees shall not open any attachment from an unknown source or from a known source with an unusual title or e-mail message.
3. Employees shall not load diskettes or CD's of unknown origin.
4. Employees shall not download non-business files (e.g., music or video files) without permission from IS.
5. Incoming diskettes and CD's shall be scanned for viruses before they are read.
6. Any employee who suspects that his/her workstation has been infected by a virus shall IMMEDIATELY POWER OFF the workstation and call the IS manager.
7. Employees may only access agency systems from their home computers, if those home computers are approved for use on agency business by the agency and are running the security software specified by the agency, including the automatic updating of virus definitions.
8. Employees shall make sure their laptops are running the security software specified by the agency, including the automatic updating of virus definitions.

Access codes and passwords

The confidentiality and integrity of data stored on agency computer systems must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those capabilities that are appropriate to each employee's job duties.

IS responsibilities

The IS manager shall be responsible for the administration of access controls to all agency computer systems. The IS manager will process adds, deletions, and changes upon receipt of a written request from the end user's supervisor.

Deletions may be processed by an oral request prior to reception of the written request. The IS manager will maintain a list of administrative access codes and passwords and keep this list in a secure area.

Employee responsibilities

Each employee:

1. Shall be responsible for all computer transactions that are made by him/her.
2. Shall not disclose passwords to others. Passwords must be changed immediately if it is suspected that they may have become known to others. Passwords should not be

recorded where they may be easily obtained. Passwords should always be kept out of view and not be placed on the monitor or be visible on the desk area. Passwords should not be saved onto a PDA type device.
3. Will change passwords according to agency policy. (ACT recommends passwords be changed at least every 90 days.)
4. Should use passwords that contain a combination of all three of the following: upper and lower case letters and numbers. Employees should use passwords that will not be easily guessed by others.
5. Should log out when leaving a workstation for a meeting, a break, lunch, or at the end of the day.
6. AGREES THAT HE/SHE WILL NOT USE PASSWORDS FOR ANY PURPOSE AFTER TERMINATION FROM THE AGENCY.

Supervisor's responsibility

Managers and supervisors should notify the IS manager promptly whenever an employee leaves the agency or transfers to another department so that his/her access can be revoked or adjusted, as appropriate. Terminations must be reported concurrent with the termination.

Human resources responsibility

[Agency may prefer to put the responsibility to notify the IS manager of employee transfers and terminations as discussed in the above paragraph on the human resources manager.]

Physical security

It is agency policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

IS Responsibilities

1. Critical computer equipment, e.g., file servers, must be protected by an uninterruptible power supply (UPS). Other computer equipment should be protected by a surge suppressor.
2. Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided.

Employee responsibilities

1. Diskettes, CD's, DVD's, USB "thumbnail" drives, and tapes should be kept out of view and should be locked up when not in use. These media also should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.
2. Since the IS manager is responsible for all equipment installations, disconnections, modifications, and relocations, employees are not to perform these activities. This does not apply to temporary moves of portable computers for which an initial connection has been set up by IS.
3. Employees shall not take shared portable equipment such as laptop computers out of the agency without the advance consent of their department manager. Advance

consent means that the manager agrees that the equipment can be taken from the office, what data is on it, and for what purpose it will be used.
4. Employees should exercise care to safeguard the valuable equipment assigned to them. Employees who neglect this duty may be accountable for any loss or damage that may result.
5. Employees may only save the types of agency information to laptops, PDA's, USB drives, CD's, DVD's, and diskettes that is permitted by agency procedures.
6. All agency guests shall be logged in at the receptionist and then be escorted while in the office.

Phone Conversations

1. Employees should confirm the identities of callers pursuant to agency procedures before disclosing non-public or other agency information to them.
2. Employees should follow agency procedures with regard to what types of information they may disclose to various categories of caller.

Copyrights and license agreements

It is Agency's policy to comply with all laws respecting the ownership rights of others in intellectual property (e.g., software, web content, books and reports), including but not limited to U.S. copyright and trademark laws. There are severe civil and criminal penalties that can result from the violation of these laws.

IS responsibilities

The IS manager will:

1. Maintain records of software licenses executed by, or on behalf of the agency.
2. Periodically scan agency computers to verify that only authorized software is installed.

Employee responsibilities

Employees shall not:

1. Install software unless authorized in advance by IS. Only software that is licensed to or owned by Agency is to be installed on Agency computers.
2. Copy software unless authorized in advance by IS.
3. Download software unless authorized in advance by IS.
4. Copy, incorporate, or transmit the information contained on web sites without securing the permission of the owner of that information in advance. Copy, incorporate, or transmit links to internal website pages, without securing the permission of the owner of that information in advance.

Acknowledgment of Agency Information Security Policy and Ownership of Agency Information (Sample)

This form is used to acknowledge receipt of, and compliance with, the "Agency Name" Information Security Policy.

Procedure

Complete the following steps:

1. Read the Information Security Policy.
2. Sign and date in the spaces provided below.
3. Return this page only to the information services manager.

Signature

By signing below, I agree to the following terms:

i. I have received and read a copy of the "Information Security Policy." I understand it and agree to abide by this policy in its entirety;

ii. I understand and agree that any computers, software, storage media, and documents provided to me by the agency contains proprietary and confidential information about "Agency Name" and its customers or its vendors, and that this is and remains the sole property of the agency at all times;

iii. I agree that I shall not copy, duplicate (except for backup purposes as part of my job here at "Agency Name"), otherwise disclose, or allow anyone else to copy or duplicate any of this information or software;

iv. I agree to use special care to safeguard the privacy of "Protected Health Information" and other confidential customer information and to not disclose it to anyone, including fellow employees, except as necessary in the course of business and as specifically permitted by agency procedures.

v. I agree to use special care to safeguard the confidentiality of my passwords, to not disclose them to fellow employees or other persons at any time (except to the password administrator), and not to use these passwords for any purpose after termination from the agency.

vi. I agree that, if I leave "Agency Name" for any reason, I shall immediately return to the agency the original and copies of any and all software, computer materials, or computer equipment and any other agency property that I may have received from the agency that is either in my possession or otherwise directly or indirectly under my control.

vii. I agree to abide by all of the provisions contained in the "Information Security Policy," even though they have not been singled out and repeated in this Acknowledgment form.

Employee signature: _____

Employee name: _____

Date: _____

Department:_____

[Table of Contents]