CPA
Practice Advisor

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

The Threat From Inside

Column: The eSecurity Advisor

Aug. 01, 2008

From the August 2008 Issue

Many accountants are familiar with the threats faced by our organizations from the outside — hackers, viruses, spyware, Trojans, and other various malicious software and people. However, many of us fail to think about the threat from inside the organization —employees, vendors, consultants and clients.

It is fairly easy to look at the security vulnerabilities outside the organization because it receives more coverage, but internal security vulnerabilities are often overlooked or ignored. We all like to trust our employees and believe that they are serving the best interests of our firm. While the vast majority of employees are honest and forthright in their dealings, there may be a time when we become victim to an insider threat.

What are the threats?
The threats come in many forms and have various degrees of severity ranging from fairly benign threats (such as an employee losing a client's records) to more severe threats (such as an employee stealing client information and selling it to an identity thief).

Here is a list of some inside threats faced by an accounting firm:

- Losing client records
- Theft of client records

- Unauthorized discussions with third parties about client information
- Removing client records for personal use or for sale
- Using client information to commit a crime (theft of money or a client's identity by employee or an associate of the employee)
- Theft of company information
- Sale of company information (sale of the processes used by the firm, most likely to a competitor)
- Misuse of position to obtain benefits from clients
- Misuse of position to obtain benefits from vendors
- Theft of company property whether electronic (software) or physical assets

Many other items could be added to this list. Take a few minutes to write down any that come to mind that might be specific to your firm.

What to do about the threats

One of the most important aspects in dealing with internal threats is through control. You want to control access to documents and ensure that only those who should have access are actually the only ones who do. Document control can take several forms including the following:

- Using passwords to gain access to network resources as well as within a document in order to secure sensitive information
- Using document management software to control access to documents
- Using the file security system built into the server operating system to secure documents in folders with access controlled to only those users who require access
- Rotation of duties to ensure that employees who might be thinking of leaving cannot take a group of clients with them because of unrestricted access
- Limiting access to only those documents required to complete the work assigned

Let's take a closer look at each of these areas to gain some insight into how each will help bring about effective internal control over documents and threats from the inside.

Passwords

Use of passwords provides access control to documents and the network. By using passwords on document(s) and the network to either open or edit the document, you control the ability to prevent non-authorized employees from looking at or changing a document. Passwords address internal vulnerabilities, especially from employees who might desire to use the information for inappropriate activities.

Passwords also provide means of controlling access to resources on the network. And by not having authorization to access a particular area, the user is prevented from obtaining information from that area.

Document Management

Properly designed document management software provides a means for not only managing the various documents in your environment, but also for securing them. Most document management products make it very easy to assign rights to particular documents or folders. By only allowing access to documents by employees who need access, you prevent the ability of other employees to use that information for inappropriate means. Document management software can also be used to track who last accessed a file so you can determine the history of who was in the file. The better document management programs track this so you can monitor for inappropriate use.

File Security on the Server

Most accounting firms use Windows Server operating systems, but Linux and Unix are also used on occasion. Each of these operating systems has built-in file permission structures. While assigning file permissions on your server is not as easy as it would be in a document management tool, it is a means for controlling access to documents and preventing unauthorized use if set up properly. The network administrator would need to build a folder structure to fit your organization.

Once set up, users would only be able to access the folders and files stored within based on their permissions. This is similar to the document management solutions except that it is done at the server level and users cannot easily make security changes without the assistance of their network administrator. Considerable thought also needs to be put into the structure to ensure that users do not have rights to files they should not be able to see.

Rotation of Duties

We always advise clients to rotate duties to guard against stealing. The same thing can be done in an accounting firm to prevent familiarity from becoming a liability to the organization. Employees who are too familiar with clients can (and sometimes do) decide to leave a firm and start their own. They often take the clients with whom they are most familiar (or those clients follow them) because of the personal relationship that has developed between them. One of the easiest ways to prevent this type of familiarity from becoming a liability for your firm is to rotate the employee's work so that every two or three

years, they are working on a new set of clients. This provides stability for the client relationship but does not allow it to become too familiar.

Limiting Access to Assigned Work

Many of the engagement tools available today have the means for assigning work to specific employees and preventing other employees from accessing those documents.

By assigning only certain documents to certain employees, no single employee can gain the full picture of the client's financial state. This helps to ensure that employees cannot engage in activities of an inappropriate nature because they do not have enough information to undertake the inappropriate activity.

Collusion would be the only way employees could gain enough information to be able to conduct an illegal activity. Breaking up work assignments can also be an important deterrent. By only giving an employee a piece of the work, they don't have sufficient pieces to be able to create mischief. This could be especially important to new employees who might be more prone to use information inappropriately versus older, more senior employees who are more trusted. This is no guarantee, however, as senior "more trusted" employees can compromise procedures just as much as younger less-experienced employees.

Other Steps

Software monitoring tools can help monitor and lock down your internal network from internal threats and look for inappropriate access and activities inside the network. While these tools may make sense for a large firm of 100+ employees, most smaller accounting firms are going to want to utilize the tools already available as part of the existing software they are using and already own.

Summary

Just as an accounting firm looks at its outside security issues, it also needs to look at its internal security issues. Employees might have many reasons for wanting to take advantage of inadequate controls over client information No matter what the reason, it is important for accounting firms to look internally to ensure they are not providing a means for employees to utilize the information in the organization in an inappropriate manner.

Article

CPAPA is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.

© 2023 Firmworks, LLC. All rights reserved