



Using an Information Security Audit to Avoid a Security Incident

By Richard A. Diamond ■ *InformaTouch, LLC*

You have a choice as a business executive: live in fear or ensure your organization's protection by having a security audit performed on your information systems. Most managers are familiar with other types of audits such as the financial audit, while many have yet to be a party to a security audit. Auditing how information is processed through your organization, as well as how confidential the data is kept has become one of the

How is the security audit performed?

Part of the job of any auditor is to do an enterprise wide network inspection to see what is attached to it. They walk around and check out the network physically. They take a complete inventory or check it against the latest inventory on file. They look at them electronically to ensure that they are configured the way that they are supposed to be. Additionally, one must

Work on the audit is typically performed through personal interviews, vulnerability scans, examination of operating system settings, analyses of network shares, and historical data. Auditors are concerned primarily with how security policies are actually used. Here are some key questions that your security audit should address:

- Are passwords in place and difficult to crack?
- Are there access control lists in place on network devices?
- How is backup media stored, who has access and is it up to date?
- Have all custom written applications been written with security in mind?
- Have custom applications been tested for security flaws?
- Are the operating systems and commercial applications patched to current levels?

"Your have a choice as a business executive: live in fear or ensure your organization's protection by having a security audit performed on your information systems."

most important processes a business can review. No business can afford the costs associated with a security breach; nor can they afford to lose the time that it takes to get a business back on track after an incident. How bad would it look if your company lost important proprietary information? Ask your board members this question and see what type of answers you get. Without a regular security audit procedure in place, you may be "@Risk."

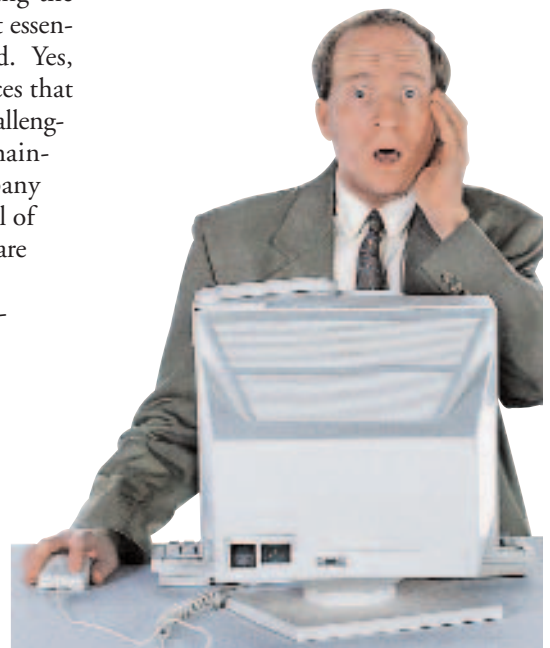
What is a security audit?

Simply put, an information security audit is a technical assessment of how your company's security policy is followed. Do you have a security policy? This is the first step on the list of getting your information security under control and the subject of an article that will be presented in the next few months.

make sure that network administrators are actually changing passwords when they're supposed to and keeping the firewalls set to block out all but essential access to the outside world. Yes, this may take time and resources that you do not have. Security is challenging at best but needs to be maintained and made a high company priority. Be sure to consider all of the different security tools that are available.

The five basic internal security controls used by most companies are as follows:

- Authorization
- Identification of users and systems
- Authentication
- Integrity (including backups, checks and balances on data)
- Monitoring



- How are configurations and code changes documented at every level?
- How are records reviewed and who conducts the reviews?
- Are there audit logs to record who has accessed data?
- Is there a disaster recovery plan in place and have all of the key participants reviewed and rehearsed the plan?

Dealing with security breaches

All vulnerabilities are not of the same magnitude. Some repairs yield significant returns on investment, many others do not. Make sure to identify critical information assets by figuring out which could put the company out of business if they were compromised or damaged. Some vulnerabilities may be accepted by the business because mitigation is too costly. That is a business decision. The level of control needs to match the level of risk.

Many problems that are found

through a security audit are actually produced by an organization's own internal users or employees and experts agree that these users are the most likely to compromise a company's network.

ity structure will change as well. An IT audit program will not happen overnight. Keeping this in mind, the information security audit is not just a one time event, but a continual effort to improve data protection. The audit

"Simply put, an information security audit is a technical assessment of how your company's security policy is followed."

Using outside IT Security companies

Some companies with complex security needs, such as a legal obligation to protect customer or patient privacy, it makes sense to contract an IT security firm that specializes in working with companies like yours.

Security audit timing

As an organization grows, their secu-

measures the company's security policy and provides an analysis of the effectiveness of that policy within the context of the organization's structure, objectives and activities. The audit should build on previous audit efforts to help refine the policy and correct deficiencies that are discovered through the audit process. The audit is less about using the latest and greatest tools and more about the use of consistent,

TeleGuide

Two of the most important channels on your lineup.

TV Listings Channel and the **Community Information Channel**

Both satellite-delivered and completely updateable through your web browser



www.4teleguide.com



organized, accurate, data collection and analysis to produce findings that can be measurably corrected.

Conclusion

In reality, most companies do not have very high levels of security so don't worry about creating the perfect security program as it does not exist. Instead, define which areas are most vulnerable. Map out the process to get your information security audit completed. Work with professionals to guide the audit and get moving on addressing the vulnerabilities that are uncovered. Take care of all of this and you will no longer be "@Risk". ■

About the Author

Richard A. Diamond is President of InformaTouch, a leading provider of in-room interactive, business & guest services aimed at the hospitality industry. The author may be reached with questions or comments via email at rdiamond@stradass.com

Coming in November:

Broadband Properties 2nd Annual

Buyers Guide

The Broadband Properties Buyers Guide is the premiere resource for companies representing cable, Internet and telecommunications products and services to the multifamily (MDU) or commercial property (MTU) marketplace.

For details on how to include your company, please contact Irene Gonzales at irene@broadbandproperties.com or call 877-588-1649.

