The Risk Advisor

IT Risk Management Issues: Staying Safe and Compliant in the Technology Era

In recent years the importance of information security has taken center stage with media attention given to massive disclosures and geopolitical security incidents involving *WikiLeaks*, the "hacktivist" group *Anonymous* and alleged cyber-warfare involving government entities. Larger organizations, in our experience, have stepped up security as a result by taking a more proactive approach. These organizations generally had effective information security programs in place because of the more stringent regulations, such as Sarbanes Oxley, PCI and HIPAA, under which large organizations operate, and the enactment of legislation in the U.S. and Europe requiring notification of security breaches to affected parties. However, the shift from mere legal and regulatory compliance to this more proactive approach has led to increased investment in security systems and services, resulting in significant progress. Smaller businesses, however, have generally viewed these incidents and compliance issues as a problem for large companies or government entities. Recently, we have seen that direct experience with a security incident, ranging from identity theft of an individual to a malware outbreak at a company, has been the catalyst for the more proactive security stance taken at small companies because the likelihood and impact of an incident made the transition from an abstract concept to a measurable quantity.

Despite these recent improvements, information security professionals seem to share the fate of the mythological Sisyphus, doomed to an eternity of rolling a bolder up a hill only to see it roll back down. Even those companies that managed to defend their perimeters with the likes of firewalls, proxy servers, proper network architecture and properly secured desktops and servers soon discovered that those perimeters were no longer clearly defined. The increase in mobile computing, which brings with it VPN access, portable devices such as laptops, smart phones and tablets, and cloud computing, has increased business efficiency and responsiveness while introducing a host of additional security risks to be addressed, including the loss of the physical layer of security over organizational information and the increased complexity of the IT infrastructure. Keeping mind that many organizations still suffer from basic vulnerabilities such as improper access control management and improper patch management, especially of applications (as opposed to operating systems), the task of achieving adequate security can seem rather daunting, but there is hope.

(continued on page 2)

CBIZ®
our business is growing yours
www.cbiz.com

Network Security Assessment

Every journey, no matter how long, begins with a single step. In our world that first step is a risk assessment. Ideally, those charged with securing organizational information will already have the support of management when beginning a risk assessment. For those who do not have this support, a risk assessment can be a good tool for clearly presenting to management, in business terms, the risk posed to the organization by a lack of security, thus presenting the business case for implementing or improving an information security program. Although this can often be an intensive process, it is not without tangential benefits, including increased integration between the business and IT and enhanced visibility into business continuity management via the identification of critical information assets and related processes. Additionally, increased security is often implemented via automation or infrastructure changes, such as automated log analysis and correlation, virtual desktop infrastructure or server virtualization, which can bring with them operational efficiencies that, over time, defray the cost of the security investment. Although a risk assessment should be customized for the specific organization, security standards can be used as a framework to ensure holistic coverage and aid in the development of resulting security policies and resources. For one, the *SANS Consensus Audit Guidelines: 20 Critical Security Controls* can be used to prioritize the implementation of additional security controls.

Information Security (Infosec) Assessments can be broken down into three basic categories:

- Level I – Basic External Network Assessment
- Level II – Full Information Security and Network Assessment
- Level III – Penetration Assessment

The overall objective of a network security assessment is to provide the client's executive staff with a confidential and independent assessment of their current information security infrastructure. Potential vulnerabilities will be disclosed and recommendations for addressing them will be provided.

The custom component of the Level II assessment is that vulnerabilities will be exploited and elements of penetration testing will be employed. Level III Penetration assessments are typically run against hardened targets (e.g., banks, financial institutions, government agencies and similar critical infrastructure companies) with long timelines. The proposed customized Level II assessment for a client will incorporate many elements of a Penetration assessment that would normally be included in assessing a "hardened"

target, but with the cooperation and active participation of the client staff, project timelines of several months for penetration testing will be able to be collapsed to a span of only two to four weeks.

Specifications of our services are detailed below and include:

- Identify external and internal network vulnerabilities of all client networks using manual and automated probes.
- Conduct social engineering email campaigns to entice client users to load benign (no payload) Trojans and viruses on workstations and simultaneously test corporate antivirus systems for specified users.
- Review firewall, intrusion prevention and network access control (NAC) systems and policies.
- Provide tailored written policies for our clients using SANS Security Policy Templates.
- Conduct NSA Router Assessment Tests (RAT) for Cisco routers.
- Conduct employee interviews to assess and raise security awareness for our clients.
- Assess wireless networks in the physical work location and surrounding area.
- Coordinate with service providers and staff to ensure minimal disruption of network services.
- Provide a discreet proprietary report directly to the client contracting agent.

(continued on page 3)

Network Penetration Testing

There are plenty of reasons for performing internal and external network penetration testing. The obvious reason is to find vulnerabilities and fix them before an "unethical" attacker has the chance to interrupt or compromise your company's information. While your IT department may be aware of reported vulnerabilities, they sometimes need an outside expert to officially report them so that management will approve the resources necessary to fix them. Lastly, penetration testing will also provide internal controls and process on how your IT department responds when an actual attack does occur.

Additionally, having a second set of eyes check out a critical computer system is a good audit security practice. It is important to keep in mind that you are dealing with a 'Test'. A penetration test is like any other test in the sense that it is a sampling of all possible systems and configurations. If an outside source is hired to test only a single system, they will be unable to identify and penetrate ***all*** possible systems using all possible vulnerabilities. As such, any Penetration Test is a sampling of the environment. Security vulnerabilities, such as weak configurations, un-patched systems and botched architectures, continue to plague organizations. Enterprises need people who can find these flaws in a professional manner to help eradicate them from their infrastructures. While many consultants claim to have penetration testing, ethical hacking and security assessment skills, a precious few can apply these skills in a methodical regimen of professional testing to help make an organization more secure.

The professionals at CBIZ Risk & Advisory Services will conduct an active analysis of your company's system for any potential vulnerabilities that could result from poor or improper system configuration, either known and unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. Our comprehensive testing and analysis methodology is carried out from the position of a potential attacker and can involve active exploitation of your internal and external network vulnerabilities. Our customized approach matches viable test information with an accurate assessment of the potential impacts to the organization and outlines a range of technical and procedural countermeasures to reduce risks. Let our ethically reliable methodology work for you.

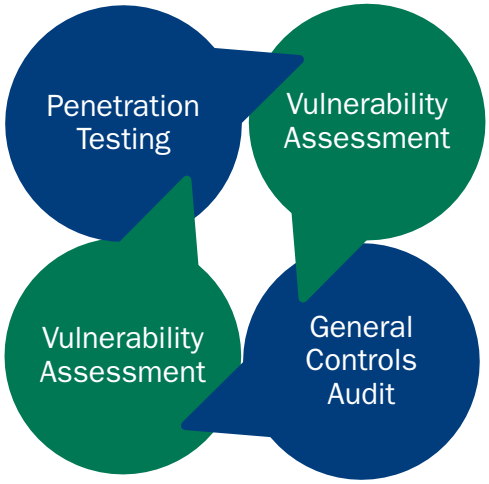
Penetration tests are valuable for several reasons:

1. Determining the feasibility of a particular set of attack vectors
2. Identifying higher-risk vulnerabilities that result from a combination of lower-risk vulnerabilities exploited in a particular sequence
3. Identifying vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software
4. Assessing the magnitude of potential business and operational impacts of successful attacks
5. Testing the ability of network defenders to successfully detect and respond to the attacks
6. Provides evidence to support increased investments in security personnel and technology

In Conclusion

The Process can be summarized accordingly:

Network vulnerability assessments and penetration testing can be an invaluable technique to any organization's information security and compliance program. As technology advances, and its use in organizations continues to evolve, so will the threats to organizations' information security. At any given time, attackers/hackers are employing any number of automated tools and network attacks, looking for ways to penetrate systems. The slow pace of legislation is no match for the speed of this evolution, making a proactive approach to security a necessity. Treating an information security program as a living, breathing organism that requires ongoing attention gives organizations the best opportunity to keep up with, or even stay ahead of, those who wish to exploit their the defenses. Remember that ultimate responsibility for the security of IT assets rests with Management. This responsibility rests with management because it is they, not the administrators, who decide what the acceptable level of risk is for the organization.



CBIZ

our business
is growing yours

© Copyright 2013. CBIZ, Inc. NYSE Listed: CBZ. All rights reserved.

Let the CBIZ Risk & Advisory Services Information Technology group help keep you compliant, mitigate network security risks and keep your company's and clients' critical information safe. For more information please contact us at: **1-866-956-1983** or **RASInfo@cbiz.com.**

Employee Services

- ☐ EMPLOYEE BENEFITS
- ☐ RETIREMENT SERVICES
- ☐ PAYROLL / FLEX / COBRA
- ☐ PROPERTY & CASUALTY INSURANCE
- ☐ RISK MANAGEMENT
- ☐ LIFE INSURANCE
- ☐ EXECUTIVE SEARCH
- ☐ COMPENSATION CONSULTING
- ☐ HUMAN CAPITAL SERVICES
- ☐ TIME & ATTENDANCE
- ☐ HRIS

Financial Services

- ☐ ACCOUNTING & TAX
- ☐ LITIGATION SUPPORT
- ☐ VALUATION
- ☐ INTERNAL AUDIT
- ☐ MERGERS & ACQUISITIONS
- ☐ FINANCIAL ADVISORY
- ☐ RISK & ADVISORY SERVICES
- ☐ CORPORATE RECOVERY
- ☐ FAMILY OFFICE SERVICES

CBIZ also provides specialized services, including Real Estate Services and Health Care Solutions