tracesecurity
Compliance, simplified.

White Paper

2014 IT Risk-Based Audit Findings

An in-depth review of the top unimplemented risk controls

Herbert McMorris

CISSP, CISA, CISM and TraceSecurity Information Security Analyst

Executive Summary

The availability of critical systems and the confidentiality and integrity of customer data is paramount to the survival of organizations today. Unexpected events are at best distracting and at worst catastrophic for organizations, states the "Maximize Business Performance With A World-Class GRC Program" report published by Forrester Research, Inc., May 16, 2014. The report continues to say a critical element of any good GRC program is the ability to identify and understand risks that may damage the organization, then take proper precautions to prevent them from happening and to reduce the impact of the consequences should precautions fail.

In an effort to help organizations identify opportunities to enhance their security posture, a review of the 2014 IT risk-based audits performed by TraceSecurity information security analysts was conducted.

This white paper highlights the most common unimplemented risk controls as identified by TraceSecurity. The following results are not only considered industry best practices but also seen in guidance outlined by the FFIEC, specifically the FFIEC Information Security IT Examination Handbook and Business Continuity Planning IT Examination Handbook.

Top 2014 IT Risk-Based Audit Findings

Organizations must ensure they have the right processes and controls in place to avoid damaging events and build customer trust. Implementing the following risk controls will not only enable organizations to meet compliance requirements but also industry best practices related to data protection, business continuity and risk mitigation.

Establish and Maintain a System Hardening Standard and System Hardening Procedures

The most common unimplemented control discovered was the lack of system hardening procedures. In fact, 45% of audited organizations lacked system hardening procedures. System hardening is the systematic process of securing devices before placing them in production. The simplest exercise of system hardening is to utilize a checklist to ensure all steps are taken in configuring devices. For example, processes could include removing all default accounts, removing unneeded services, naming the device according to organizational standards, installing approved software, and installing and configuring anti-malware. Alternatively, system imaging is used where a device is configured to exacting standards, and the configuration is copied to an image, which is then copied to similar devices. Using the imaging process ensures devices can be implemented quickly and steps are not omitted during the hardening process. With a well-defined hardening process, organizations can lower the risk of attack due to default accounts, unpatched systems and flawed malware protection, among other things.

Install a Generator Sized to Support the Facility

Ideally, a generator will provide power to the entire office. Alternatively, power should be available to the data center, including all critical servers, switches, routers, firewalls, security systems, video surveillance and proximity readers. The absence of a generator could force an organization to invoke their disaster recovery plan for something as simple as a power outage. Power outages are extremely common in most parts of the country and can be caused by wide spread storms, such as hurricanes, tornado outbreaks, blizzards or even heat waves that cause the power grid to malfunction. Unfortunately, even traffic accidents can sometimes cause a localized outage. In such cases, a generator at the primary data center enables branch operations to continue even if the primary office is closed. Otherwise, all operations will cease until power is restored since critical systems will be unavailable.

Test the System Continuity Plan Regularly

Continuity plan testing is performed to ensure the process will work and the organization can continue to operate after a business interruption. The organization should consider the availability of critical staff, the equipment needed to resume operations, the methods needed to restore data, and the time it takes to restore services. The test should be performed annually. Both the business continuity and disaster recovery plan should be updated to reflect lessons learned from the testing event.

Establish and Maintain Documented List of Protocols, Ports, Applications, and Services to Essential Operations

Firewalls are composed of many access lists that allow traffic to flow in and out of the network. The required list should simply document the ports and services allowed to communicate through the firewall, which devices are allowed to communicate, and the business reason for the ports in use. If vendors have Virtual Private Network (VPN) access, the list should indicate the systems they are approved to communicate with and the allowed IP addresses of the vendor. The organization should periodically compare the lists to the firewall configuration and change management process that specified any changes. Any deviations should be documented.

Use Strong Data Encryption to Transmit Restricted Data or Restricted Information Over Public Networks

Most organizations assume that transmitting data over a public telephone line is safe. With the use of Point-to-Point and Multiprotocol Label Switching (MPLS) networks it would seem that data is not exposed to anyone outside of the company when transmitted in this fashion. However, data is transmitted over wires and switches and even traverses street side wiring pedestals. Encryption of all data leaving the physical safety of the office is the best defense against exposure due to misconfiguration or unscrupulous individuals.

Scan for Rogue and Other Network Devices and Deny Access Until Approval Has Been Received

The most frequently asked question during an audit is, "What is a rogue device?" A rogue device is any piece of equipment connected to a network that has not been authorized by the organization. A rogue device can be a wireless access point, an employee's personal laptop or a data switch. There are many risks associated with rogue devices. Consider the following situation: An intruder successfully gains access to an organization and quietly installs a wireless access point between a workstation and the wall jack. The intruder then exits the building and attacks the organization's systems from the parking lot or a neighboring building. Without rogue device detection, the wireless device will remain active for a considerable period of time, allowing the attack to continue. Rogue protection should block access to the network until the device has been checked by IT staff and specifically allowed to connect.

Communicate Security Awareness and the Internal Control Framework to All Constituents

A common organizational process is to communicate security awareness issues to new employees as part of their orientation, but often times organizations fail to repeat this process after the initial hiring period. The protection of information assets is the responsibility of everyone in the organization and requires continuing education. On-going training efforts should address new threats, as well as include reminders of common threats. The results of social engineering tests performed by TraceSecurity indicate most failures occur with staff who are aware of the security procedures but fail to follow them. It is recommended that organizations implement a formal security awareness program that, at a minimum, includes annual training.

Establish and Maintain a Configuration Management Policy

Configuration management is often vague. To have a policy governing it seems unnecessary, but a policy dictating the configurations of systems offers protection by indicating the types of systems to be purchased, what can and cannot be installed on systems, and how the security of the system should be configured. In addition, the policy protects the IT department by providing standardization and defining recourse if unauthorized software is installed or services are disabled. Policies, such as the configuration management policy, are normally authored by IT management and approved by executive management for implementation.

Establish and Maintain a Process to Control Patch Management

Patch management is simply the installation of software updates to mitigate known vulnerabilities in operating systems and software. Patch management can be managed through individual workstation downloads or via a centralized patch management system, such as TraceCSO Patch Management, Microsoft® Windows Server Update Services (WSUS) or Dell™ KACE, among others. To ensure all computers remain up-to-date and are not left vulnerable, an organization's patch management process should be monitored on an on-going basis, especially if individual workstations are allowed to download updates. Networking equipment should also be updated periodically as new operating system versions are released by the manufacturer.

Perform Penetration Testing and Vulnerability Scanning on a Regular Basis

Penetration testing and vulnerability scanning involve a three part security testing process: internal penetration testing, external penetration testing and automated vulnerability scans. In the audit context, all three portions should be implemented. Audit findings revealed two reasons testing is not performed: lack of understanding of the testing and budgetary constraints. The following includes clarification of the requirement.

Vulnerability Scanning

Vulnerability scanning is an automated process involving a managed system, such as TraceCSO Vulnerability Scanning or a third party scanning solution. The process involves testing systems on the network for known vulnerabilities a hacker could exploit to gain access to or prevent use of the system, which is referred to as a denial-of-service. Devices on the internal network as well as external-facing systems should be scanned, and the organization should review and mitigate the resulting vulnerabilities based on risk levels. Scanning should be performed on a systematic schedule. For example, conduct quarterly scans initially and adjust the schedule over time as organizational needs change.

Penetration Testing

Penetration testing refers to an active test performed by a qualified 'pen tester' or ethical hacker and is used to determine if an attacker can gain access to critical systems and corresponding data. Internal penetration testing is performed from within the perimeters of the organization's network and uses common hacking tools. It is designed to expose deficiencies in network credentials, default and easily guessed account information, unpatched systems, and unencrypted network traffic that is captured and analyzed. External penetration testing is performed remotely, and attacks are made on Internet-facing devices. The testing process is similar to internal penetration testing. One erroneous assumption is that most successful attacks originate from the Internet. In reality, the most successful attacks originate internally. Once the penetration tests are completed, reports are issued providing an explanation of the testing methodology and findings so the organization may take steps to mitigate the risks exposed. Both internal and external penetration testing should be performed, at a minimum, on an annual basis.

Establish Access Rights Based on Least Privilege

The "need-to-know" principle is the foundation for information security. Access to data should be limited based on job function. TraceSecurity audits have revealed many organizations establish users as local administrators on their workstations. As a result, users have access to all data. This is a critical issue. Access is to be granted in a granular fashion and is most easily managed by group memberships.

Conclusion: Practice Due Diligence to Protect Organizational Assets

There is nothing more potentially damaging to an organization than a security breach or an ineffective business continuity plan. Failing to implement controls that help safeguard assets can disable operations, result in regulatory violations and destroy an organization's brand. However, many organizations continue to fall short when it comes to effectively managing their risk exposure.

Reviewing controls currently in place and identifying potential areas of vulnerability enables organizations to manage risk proactively and reduce exposure. While there is no such thing as absolute protection, proper review and implementation of security controls, including those highlighted in this report in addition to others, will ensure an organization's ability to protect itself against significant risks.

About TraceSecurity

TraceSecurity is a leading provider of cybersecurity and compliance solutions that helps organizations of all sizes reduce the risk of cyber breaches and demonstrate compliance. With a combination of software and services, TraceSecurity can help organizations manage their information security program and supplement it with third-party validation.