KFI WHITE PAPER:

Top 10 IT Security Vulnerabilities and Corresponding Controls Commonly Found in SOC Reports

The purpose of this whitepaper is to describe prevalent IT security vulnerabilities and the corresponding controls that companies deploy to respond to them. The baseline controls described in this whitepaper are applicable to most entities and are recommended for inclusion in all *System and Organization Controls* (SOC) reports. The controls address the most significant risks related to logical access, network security, change management and human resources control objectives (SOC 1) and Trust Services Criteria (SOC 2). The American Institute of Certified Public Accountants (AICPA) requires organizations undergoing a SOC examination to consider all relevant risks in designing their system of internal controls. This whitepaper is intended to help our clients comply with this requirement by linking critical risks to controls.

1. The Human Vulnerability: Individuals inside of an organization can unknowingly contribute to the success of a cyber-attack. Common attack vectors that exploit the human vulnerability include:

- Social Engineering
- Phishing
- Malware

Periodic (at least annual and upon hire) security awareness training is the most effective control to address the human vulnerability. It is a formal process for educating employees about IT security that includes education on corporate policies and procedures.

2. Missing, Blank, Weak, or Default Credentials: When passwords are weak or are not used at all, it becomes much easier for hackers to gain access to and/or destroy sensitive data and systems. Strong / complex password requirements are the most effective control to address this vulnerability. Another recommended control is the periodic review of password and configuration policies.

By Jamie Kilcoyne, CPA, CISA, CITP, CIA, CFE - K Financial

3. Password Re-Use: Occurs when an individual has one password that they use for more than one application, database or system. When a hacker breaches a system using a password, the potential for serious damage dramatically increases if that same password can be used to access multiple other applications, databases or systems.

The most effective controls to address this vulnerability are password policies and training designed to encourage employees to use effective and secure password practices.

4. Insecure Firewall Configuration: Firewalls can be effective tools for preventing outside access to an organization's network, systems and data. But if they are not configured properly, firewalls lose their value and networks, systems and data become easier to hack. An insecure firewall configuration may include the use of services, protocols and ports without business justification.

The most effective controls to address this vulnerability are firewall configuration policies and periodic reviews of firewall rules. Additionally, change management should be followed for all firewall rule changes.

5. Improper Privileged Account Management: This includes practices such as too many privileged accounts or shared privileged credentials.

The most effective controls to address this vulnerability are formal access request and authorization policies, user de-provisioning policies and periodic access reviews.

6. Broadcast Protocols: "Broadcasting" refers to transmitting a packet that will be received by every device on the network. Broadcasting may be abused to perform a type of DoS-attack known as a Smurf attack. The attacker sends fake ping requests with the source IP-address of the victim computer. The victim computer is then flooded by the replies from all computers in the domain.

The most effective controls to address this vulnerability are network configuration standards and security policies that include provisions for disabling broadcasting, when appropriate.

7. Unpatched Systems and Software: A patch is a piece of software designed to update, fix, or improve a computer program or its supporting data. This includes fixing security vulnerabilities and other bugs along with improving usability or performance. If computers are not patched, they become vulnerable to security threats that exploit weaknesses in software and operating systems.

The most effective controls to address this vulnerability are a patching policy and periodic penetration testing and vulnerability scanning.

8. Insecure Endpoint Configuration: Endpoint security is a methodology of protecting the business network when it is accessed via remote devices such as laptops or other wireless and mobile devices. Endpoint security is designed to secure each endpoint on the network created by these devices. Insecure endpoint configuration leaves companies vulnerable to a costly data breach. Insecure endpoint configurations include lack of endpoint logging and a failure to use anti-virus solutions.

The most common controls to address this vulnerability are endpoint logging, log monitoring and the use of anti-virus software.

9. Insecure Coding and/or Change Management Practices: Insecure coding practices lack specific steps to protect an organization against the accidental introduction of security vulnerabilities. Change management is insecure if it lacks standardized methods and procedures for preventing change related data breaches and other cyber-attacks.

The most effective controls to address this vulnerability are a formal systems development life cycle (SDLC) and / or change management policy.

10. Insecure Storage of Sensitive Information:
Most web applications store sensitive information, whether in a database or some form of file system. The information may include passwords, credit card numbers, account records or other proprietary information. Weak controls over the storage of this information make it easier for a hacker to access, steal or destroy.

The most effective controls to address this vulnerability are encryption of databases and other files that house sensitive data, strong / complex password requirements and security awareness training.

Conclusion:
There is no combination of controls that can provide absolute assurance and 100% protection of an organization's IT systems and data. However, by deploying the baseline controls described above, companies can take significant steps to protect themselves against the most common cyber incidents and can be confident that they are using best practices to address the most common vulnerabilities.