Establishing the Scope for a Cyber Security Audit
by: Mitchell H. Levine, CISA - Audit Serve, Inc.

With the level of hacking into corporate networks increasing at an alarming rate over the last few months, audit departments are confronted with the requirement to include cyber-security audits within their Audit Universe. In the past, companies relied on penetration tests performed by independent security firms to provide the corporate “higher ups” peace of mind that their companies will not be embarrassed by a media release that they have their companies have been hacked and even worse that there was a release of private customer data. Paying for an independent firm to perform a penetration test using the approach of an external hacker is not sufficient to validate the adequacy of cyber-security controls which need to be built within an organization. Since most penetration tests are designed to be only internet based attacks, this type of test only partially addresses the external threats from the internet and does not address internal threats which include employees, contractors, and business partner connections.

Just analyzing the individual components from the definition of Cybersecurity, “the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access”, an auditor can relate these components to existing IT Infrastructure audits that are typically listed as standalone audits within the Audit Universe. The most common IT Infrastructure audits which relate directly to the which scope should be included within a Cyber-security audit include Data Privacy Audits, Vulnerability and Threat Management Audits, Network Security Audits, Data Access Audits, Mid-Tier audits, Operating System Domain/Server Audits and certain aspects of an IT Governance Audit.

Over the past two years US Federal Government and Federal/State regulatory agencies have issued frameworks for improving cyber-security controls. In addition, these agencies have mandated control initiatives to be established within government agencies and private sector companies and have also mandated that independent third-party cyber-security audits be performed on an annual basis.

For instance to meet the State of New York Public Service Commission Order (CASE 13-M-0178 – In the matter of Comprehensive Review of Security for the Protection of Personally Identifiable Customer Information), the order required water and sewer companies to conduct a 3rd party cyber-security audits of its New York Operations. The New York Public Service Commission Order was very specific on what it required to be included in the scope of the audits which included:

- Policies and standards relating to overall data security at the network, host, database and application levels have been established.
• Policies, standards and procedures have been established regarding the handling and protection of PII (Personally Identifiable Information) data.

• Data Loss Prevention (DLP) measures have been deployed.

• Effective Network Access Controls have been implemented.

• Intrusion Prevention/Detection (IPS/IDS) systems have been deployed.

• Privacy training has been conducted.

• Physical and logical security controls have been established at all sites containing PII data.

• An effective incident response program has been implemented.

• Customer PII data has been properly separated from corporate data.

When planning a Cyber Security audit the first question is whether a Cyber Security Framework has been established by the organization which defines the key controls which comprise the cyber security program. If this IT Governance initiative has not occurred this should be escalated as an IT Governance issue and then the audit approach should proceed with the auditor pre-defining control areas to be included in the scope of the audit based on a Cyber Security framework which have been established within the industry such as NIST:


NIST does a good job in defining the functions within a Cyber Security Framework (Identify, Protect, Detect, Respond and Recover) which truly reflects the stages an organization needs to go through to protect themselves and respond to a cyber security attack. The NIST Framework also uses a logical approach for grouping categories with these functions (e.g., Asset Management, Risk Assessment and Governance Categories within the “Identity” function).

However, the NIST defined controls within these Categories/Functions in many cases includes controls which are unrelated to identify, preventing and responding to a cyber security attack. For instance requiring a “SDLC to manage systems is implemented (PR-IP-2)” which is listed under NIST “Prevent” controls seems not be a control which belongs in any phase of a cyber security program. The auditor when establishing a list of controls to include in the scope of the Cyber Security Audit should perform a detailed reviewed on all of the NIST controls and “cherry pick” the controls which truly represents controls that would identify, prevent and recover from a cyber security attack.
There are also cases where it would be unrealistic to be able to cover certain NIST specified controls because they would require testing across an entire organization. For example “PR.DS-1: Data-at-rest is protected” would require a review of all of the production data across all production application systems which is a type of audit that cannot be performed as a single audit.

One other critical item to consider when establishing the scope of the Cyber Security Audit is to understand that some of the controls included within the scope of the Cyber Security Audit may have been performed in a prior audit in which credit can be taken that these controls have already been tested.

The overall end product of the scope of the Cyber Security Audit scope document is to establish a list of NIST controls mapped to the NIST functions which includes a specification of whether the each of the detailed audit procedures will be executed as part of the Cyber Security Audit or if they will be linked to past audits which were performed in which the audit procedures were previously executed.

Mitchell Levine, CISA, Founder and President of Audit Serve Inc. www.auditserve.com and his consulting team have conducted several cyber-security audits and related audits over the past three years for the financial, utility and government sectors. Contact Mr. Levine Levinemh@auditserve.com if you looking to have a cyber-security audit performed within your organization. Audit Serve conducts these audits using an outsourcing audit model or using a co-sourcing module working with audit departments in order to share our knowledge with our audit colleagues.