.

Risk Assessment Reporting in Corporate Credit Unions

Purpose: To establish minimum reporting standards for corporate IT security reviews.

Background:

The Office of Corporate Credit Unions (OCCU) issued guidelines on network security in OCCU Guidance Letter 2001-02, dated August 17, 2001. This guidance established the parameters for network monitoring, vulnerability assessments and periodic penetration testing. The corporate industry has responded proactively in building appropriate defense structures in their networks and subjecting them to periodic testing.

However, corporate credit unions are deploying technology at a rapid rate. Networks are growing exponentially in their complexity and correspondingly in their vulnerability to system compromise. Networks are vital corporate assets that merit as much recognition and scrutiny as other important assets that form the corporate's structure. While a great deal of detailed information usually develops from vulnerability and penetration testing, summary reporting to corporate management is not always conveyed in a manner that adequately summarizes network risk factors. Management of technology risk mandates that the board have objective, understandable and independent assessments of the IT security infrastructure.

Problems commonly noted in the risk reporting process are:

- **Final report goes directly to IT director.** The report is summarized by the IT director, primarily because the final report is not summarized or presented in an executive level form.

- **The assessment is done by an organization that provides other IT services to the corporate**. This does not provide an independent review of the risk areas.

- **The vendor agreement does not spell out the objectives and operating parameters of the test.** In some cases, it appears the vendor determines the objectives without corporate involvement.

- **The agreement is not reviewed and approved by persons outside the IT organization.** As this is a corporate assessment, management and internal audit need to be involved.

- **There is no management level report**[1]. There should be a document that summarizes the overall security posture and provides management guidance with no security "jargon."

- **The test generates vast quantities of data about possible vulnerabilities with little analysis.** The vendor merely runs open source scanning tools.

- **The test is only for external attacks**. As the majority of computer security incidents are caused by insiders, testing needs to cover both internal and external networks.

- **External websites are not tested**[2]**.** Corporate management should know how secure its external web site is, e.g., risk of being defaced.

- **Risk definitions are vague**. Risk factors are not always clearly defined. How the vendor assigns risks to each device is not identified. Overall risk ratings are sometimes based on the raw results of the network scan rather than using scan results in the context of a complete system analysis.

Given the issues noted, it is in incumbent upon OCCU to apprise corporate management of expectations for security assessments and risk management reporting. However, the expectations should not be interpreted to be standards. There are several standards-making organizations that provide comprehensive security measurements. Corporate management is encouraged to assess these standards and implement them as needed[3].

[1] Management level refers to Executive Management (for example the CEO) and the corporate board of directors.

[2] External Website is referring to an outsourced Website.

[3] Three well know standards sources are:

ISO 17799 http://www.iso.ch/iso/en/IS00online.frontpage/

COBIT The Information Systems Audit and Control Association (ISACA) **http://www.isaca.org/cobit**

GASSP Generally Accepted System Security Principles sponsored by the International Information Security Foundation (I2SF) http://www.auerbach-publications.com/dynamic_data/2334_1221_gassp.pdf

Minimum Standards for Risk Assessment Reporting in Corporate IT Networks

Development of network security testing requirements. Development of the requirements for testing should involve corporate management, internal audit, security officer, or security committee. All parties should agree on the scope of the testing, report formats, risk definitions, and testing methodology. It is highly recommended that the testing address the corporate's compliance to appropriate laws, regulations, and selected standards.

Vendor selection criteria. Care should be taken to ensure the vendor selected is not providing services to the corporate that would question the vendor's independence. If the vendor is providing other services to the corporate, an assessment should be done to ensure that those services do not conflict with or potentially influence the results of the testing. As an example, a vendor providing firewall management or intrusion detection support would not be the appropriate choice for performing a network penetration test.

During the selection process, special consideration on the transfer of sensitive security configuration information outside of the corporate environment should be made before entering into an outsourcing arrangement.

Work scope. The work scope should encompass all internal and external network devices[4]. If there are any exclusions, they should be identified clearly in all reports with the justification for their exclusion. If the exclusion negates any of the testing methodologies utilized by the vendor, the vendor should state the impact clearly in contracts and in all reports. For example, a valid test network[5] could be excluded from the test without impacting the assessment. However, that exclusion should be clearly identified.

Careful consideration should be given to the tools the vendor will deploy for the assessment, the method of assessment, how vulnerabilities will be identified and the nature of social engineering efforts[6]. The extent of the vendor's penetration efforts should be clearly detailed as to what depth the penetration should proceed into the corporate network. Also, when a penetration is achieved, provision for notification to all management levels should be mandated[7]. The

[4] Devices include servers, workstations, network printers, routers and switches. In short, if any device can communicate within the corporates production network, then it should be included in the test.

[5] A test network would not engage in any fashion with the production network. It would be self contained with its own exclusive access points.

[6] Social Engineering is discussed in OCCU guidance letter 2001-02, dated May 17, 2001.

[7] Notification of the penetration should also be accompanied by the vendor's assessment of the risk involved. That is, would further exploitation of the penetration lead to system compromise.

level and method of notification depends on the organization's structure. In a typical corporate structure, IT staff would be notified immediately along with internal auditors. Prompt notification should initiate immediate corrective action. Notification to the corporate chief executive officer and the corporate board could be provided in formal reports or any other fashion agreed to during the engagement.

In addition to network infrastructure, if appropriate, the work scope should include testing of in-house applications and corporate data bases[8]. Appropriate applications would include Internet based systems that collect, transfer, or accumulate sensitive member information. Assessment of data base security could also be performed by internal audit staff or their designates, depending on the complexity of the corporate. However, at a minimum the audit should test whether the data base can be compromised from inside or outside the corporate network.

Rating criteria. A major function of network security assessment is to convey vast quantities of technical information into a summary risk assessment tool that corporate management can use to mitigate the risks. Therefore, it is vital that the risk ratings for network devices be clearly delineated prior to the implementation of the test. The rating should be more than a value assigned by a software tool. There needs to be a documented analysis process that the vendor uses to perform the analysis. The analysis process should be designed to provide the corporate with information that is accurate and assists them in mitigating the risk in high risk rated devices.

In addition to the rating for each individual device, it may be necessary to rate devices as a group in corporate networks with hundreds of devices. It is also common practice to assign an overall risk to each network involved. There may be variations in risk ratings and how they are applied; however, it is imperative that everyone understand the rating definitions and a consensus is obtained on their content by corporate management, IT management, internal audit and the vendor. The definitions will carry forward in the reports.

Management reporting. Two levels of reporting need to be established: (1) a detailed analysis for corporate IT staff and management, and (2) an executive summary.

Minimum components of the detailed report:

- Identification of network weaknesses, including penetrations made.

[8] There are several good reference works that outline the risks involved in databases and systems.
Database Security, Silvana Castano et.all Addison-Wesley publishing ISBN 0-201-59375-0
Building Secure Software – John Viega & Gary McGraw – Addison-Wesley ISBN-0-201-72152-X

- Individual risk ratings for network devices or system weaknesses identified.

- Provide sources for remediation of the noted problems[9].

- Detailed recommendations for improving network security.

Minimum components of the executive summary:

- A summary of the work performed, any exclusions from testing and their potential impact on the report.

- Provide an overall rating for the network as well as provide a summary of the rating process.

- Identify all penetrations made as well as their potential impact on the corporate network.

- Recommendations on improving network security.

Delivery of the executive summary should be in bound form and independently delivered from the vendor to corporate management[10]. Detailed reports should be made available as soon as possible to corporate IT staff so they can assess and effect changes as needed.

In summary, independent assessments of network security must be a corporate wide effort involving executive management and internal audit. Rules for the engagement should be well defined and accepted by all participants. The scope of the work should cover the entire network and provide for a comprehensive assessment of the IT infrastructure. It is imperative that understandable and meaningful rating systems are utilized in the reporting process. It is essential that quality risk assessment reporting is in place so that the corporate's board and management can fully assess the integrity of the organization's IT infrastructure.

[9] It may also be useful to have cost estimates included on what it would take to remediate the weaknesses.

[10] Delivery can be effected through internal audit, the supervisory committee or directly to the board as appropriate with corporate policy. Delivery should be effected on completion of a review and response by IT management, internal auditors and the vendor. The final report, however, needs to be independently prepared by the consultant performing the work.