

National Webcast Initiative
Performing a Cyber Security Risk Assessment:
Why? When? and How?
August 26, 2004
Question and Answer Transcript

The following is a compilation of questions submitted to the presenters through the written Q and A tool during the webcast. The transcript has been edited for relevance.

Q: Should an Awareness campaign not be the first step prior to initiating a Risk Assessment?

A: Certainly in initiating either a high-level or detailed risk assessment, there needs to be some upfront communication regarding the goals, scope, expected outcome and required involvement of parties. Awareness of security risks and controls is an element of any risk assessment and should be considered in identifying threats, vulnerabilities and controls.

Q: Are there sectors or verticals that are more vulnerable than others and should be performing more frequent security reviews?

A: At a macro-level all of the sectors identified as part of the nation's critical infrastructure should be performing risk assessments. Many industries have mandated requirements to perform some level of risk assessment (e.g., Banking, Utilities). In addition, there is increased focus on performing risk assessments within the federal government.

Q: Will these assessments and steps to prevent cyber attacks apply to the million of home users as well as corporations?

A: Home users should understand the risks associated with connecting their computers to the Internet especially using broadband connections such as DSL, Cable, or Satellite. There are also unique risks associated with using public WiFi (wireless) "hot spots" and wireless networks within the home. All home users are recommended to have up-to-date virus protection and utilize a personal firewall. Additional security controls should be considered for home users with wireless networks. A good web site for general information for protection of the home user is: <http://www.ftc.gov/infosecurity>.

National Webcast Initiative
Performing a Cyber Security Risk Assessment:
Why? When? and How?
August 26, 2004
Question and Answer Transcript

Q: Are there any real-world organizations that do continuous risk assessments?

A: Yes. Many organizations have developed an information security management system that includes continuous assessment of risk. For example, at least 844 organizations throughout the world have had their information security management system certified against BS7799-2. According to recent reports by GAO, there is also increasing coverage of risk assessments within the federal government.

Q: You mention that the RA is supported by Technology and Analysis tools.....what are some of those tools?

A: This topic was discussed in the presentation. The reference provided also contained links to tools. For further guidance on security testing tools I would recommend the following: NIST SP-800-46 Guideline on Network Security Testing.

Q: Are there any estimates as to the percentage of an IT budget increase necessary to maintain yearly assessments and upgrades?

A: Not to our knowledge.

Q: Isn't BS7799-2 a standard against which compliance can be assessed, rather than the ISO 17799, which is only for guidance?

A: Yes. BS7799 Part 2 contains the specifications for the design of an information security management system (“ISMS”) that includes detailed risk assessments. BS7799 Part 2 contains, as a normative model, all of the 127 recommended controls within ISO17799 but their application is determined based on the results of the risk assessments and design of the ISMS. Organizations can obtain certification under BS7799-2 from an accredited certification body. There are currently 9 organizations that have obtained this certification in the US. There are 844 organizations worldwide with BS7799-2 certification.

National Webcast Initiative
Performing a Cyber Security Risk Assessment:
Why? When? and How?
August 26, 2004
Question and Answer Transcript

Q: The risk assessment approach provided in the handouts appears simplistic. Why wasn't a more holistic reference source provided such as NSA IAM which takes in the totality of an organizations risk posture and provides a minimum of 18 categories that administrators can use immediately or at least use to build an RFP if they do not know how to implement a comprehensive assessment?

A: There were two handouts that showed risk assessments performed at different levels. One was performed at an organization level (“high level”) and was designed to show how a framework such as ISO17799 could be used to identify risks in the design of an overall security program. The second deliverable showed a “detailed level” view of a risk assessment performed on a specific system – on online motor vehicle registration system. Both example reports are illustrative of the type of information that might be presented. The examples are extracts from “real world” reports. NSA’s IAM methodology is another appropriate framework – its 18 categories map to ISO17799 which was the framework we used for our high-level report.

Q: If security is a continuous process, how does one convince management to undertake the fiscal support?

A: This topic was not covered in the webcast. We would briefly note there are several techniques used to justify increased investment in security controls. They include:

- *Educating senior management on the risks*
 - *Benchmarking against industry*
 - *ROI analysis*
-

Q: What was the name of that DB for risk assessment tracking he just mentioned?

A: NIST provides a free software program called ASSET to document and manage the risk assessment process. Refer to www.nist.gov for further information.

National Webcast Initiative
Performing a Cyber Security Risk Assessment:
Why? When? and How?
August 26, 2004
Question and Answer Transcript

Q: I often hear folks say using external resources poses a risk? Agree or disagree?

A: When you spend time identifying threats and vulnerabilities there is a risk that the information might be used for inappropriate purposes such as mounting an attack on the organization. This risk applies to both internal and external resources. Regardless of which are used the organization should be satisfied with the skills, competencies and trustworthiness of the individuals. For external resources we recommend using the services of a reputable company – for example one that performs background checks of its employees.

Q: Is it better to use a combination or just external resources?

A: This depends on the skill sets within, and maturity of your organization. External resources can provide you with methodology and expertise to help with the initial risk assessment(s). External resources can also provide a periodic third-party perspective, which may be useful to ensure your organization is aligned with what other similar organizations are doing. If you used external resources ensure they include knowledge transfer activities in their approach to help develop your internal capabilities and then involve an external party periodically for updates.

Q: What are some of the open source tools that can be used to perform a risk assessment?

A: Several were listed in the references document. Also for further guidance on security testing tools I would recommend the following: NIST SP-800-46 Guideline on Network Security Testing.

Q: If outsourcing the risk assessment, how do we go about costing? By number of ports, by number of users, number of applications?

A: The biggest cost driver would likely be number and complexity of applications (or group of applications) to be assessed. “Applications” in this sense would include the underlying operating system, network components, database and system interconnections.

National Webcast Initiative
Performing a Cyber Security Risk Assessment:
Why? When? and How?
August 26, 2004
Question and Answer Transcript

Q: How long should it take to risk assessment for a large enterprise? How many people should work on it?

A: This is a difficult question to answer in generalities. Several factors contribute to the estimate including the number and complexity of systems and the skill sets of the assessment team. We would recommend that you pilot an approach over a sample of your systems (perhaps one or two systems) and then extrapolate the effort over the entire enterprise. The complexity and diversity of systems in your environment may require a larger sample. You are also more likely to become more efficient as the team develops expertise in performing assessments and you refine your methodology.

Q: Please list the references for the Risk Assessment Workplan

A: In the presentation we referred to NIST SP-800-26 Security Self-Assessment Guide for Information Technology Systems. This publication includes a workplan.

Q: Can you clearly define the difference between penetration testing and vulnerability assessments?

A: Penetration testing is primarily designed to test the ability of a computer system to withstand intentional attempts to circumvent system security. Its objective is to test the system from the viewpoint of a specific threat-source (e.g., a hacker) and to identify potential failures in the IT system protection schemes.

Vulnerability assessment tools are typically used to scan a group of computers or a network for known vulnerabilities. These tools examine specific services that may be running on a system (e.g., system allows anonymous File Transfer Protocol [FTP], sendmail relaying). Vulnerability assessment tools may identify some potential vulnerabilities that do not represent real vulnerabilities in the context of the system environment – these are described as “false positives.” Many vulnerability assessment tools require software to be loaded on the system to be reviewed.

Q: Any recommended risk assessment methodologies?

A: We assume this question is asking about security risk assessment methodologies. As we discussed in the webcast, NIST publication SP-800-30 provides a good methodology

National Webcast Initiative
Performing a Cyber Security Risk Assessment:
Why? When? and How?
August 26, 2004
Question and Answer Transcript

for performing risk assessments. OCTAVE (see <http://www.cert.org/octave/>) is also a robust risk assessment methodology. A 1999 paper by the GAO provides case studies on methods used by four organizations to perform risk assessments – refer GAO/AIMD-00-33 (available at <http://www.gao.gov>).

Q: How are risks weighted? What do you use to assign severity or priority?

A: Ultimately all risk assessments require value judgments about (1) the probability (likelihood) of a threat-source exploiting a vulnerability; (2) the potential magnitude of the impact when this occurs; and (3) the effectiveness of controls to reduce the probability and/or minimize the impact. In the example report on the webcast website we described one approach that uses a high/medium/low rating based on certain attributes of threat and impact.

Q: Can you provide any references to learn more about conducting a risk assessment on ASPs that host applications for one's organization?

A: The same processes we described in the webcast can be used to assess application service providers. Ultimately we expect more standards to be developed around this area and are aware of efforts in certain industries (e.g., banking) to build standardized security assessment processes for third party vendors. Outside of the USA we have seen increasing adoption of BS7799-2 that specifies a security information management process and allows certification akin to ISO9000. We expect more US organizations to ultimately evolve to this type of a model.

Q: Once a risk is identified you will need to identify controls that will mitigate risk. Shouldn't those controls also be identified as part of a risk assessment?

A. Yes. In performing a risk assessment you need to consider the threats, vulnerabilities and the extent to which existing controls (if any) mitigate risk. The resulting residual risk should then be considered for further treatment based on management's risk tolerance and other factors discussed in the webcast.

National Webcast Initiative
Performing a Cyber Security Risk Assessment:
Why? When? and How?
August 26, 2004
Question and Answer Transcript

Q: Should a new assessment be done before or after each time technology is upgraded ... say changing operating systems?

A: It should be considered depending on the significance of the change. We would recommend that it be done prior to upgrading new systems.

Q: When you have limited resources (\$\$, staff, experience) to expend on all IT activities, where is best place to start? We are a state gov't agency and want to get the most bang for the buck...

A: We recommend performing a high-level risk assessment to identify potential high-risk systems and then narrow down on those systems for detailed risk assessment.

Q: Is there an email address or forum where we can suggest content for future webcasts?

A: You may forward suggestions to: isac@cscic.state.ny.us

Q: Given the fact that more and more risk assessments are being conducted by CPA firms, and other consulting professionals, and given that the entire universe of risks is large and perhaps never fully identifiable, how does the outside consulting firm: 1) establish correct expectations regarding the fact that there may be unidentified risks and 2) protect itself (from an error and omissions standpoint) for any unidentified risk that may later result in some harm to the enterprise?

A: The first part of your question is addressed by the methodology employed by the consulting firm. We recommend you consider the completeness of their approach in assessing risks. A comprehensive approach would consider people, process and technology risks and utilize historic data and experience. We agree that unforeseen risks may exist but believe an organization will be better equipped to deal with unforeseen risk if they have a good understanding of the threat/vulnerabilities and controls that exist today.

The second part of your question is frequently dealt with through contractual language with the consultant. Remember the consultant is really facilitating the risk assessment

National Webcast Initiative
Performing a Cyber Security Risk Assessment:
Why? When? and How?
August 26, 2004
Question and Answer Transcript

process, providing expertise and methodology and experience. Ultimately management must determine what are the appropriate risk treatments.

Q: How valuable would a SAS70 review be as part of the risk assessment?

A: A SAS-70 (Service Auditor's Report) is designed to provide assurance to auditors of customers of a service organization regarding the internal controls over key processes managed by the service organization. For example, if an ABC organization outsourced its payroll processing to a third-party service organization (XYZ Payroll Services) and XYZ had a SAS-70 report over its payroll processing, then ABC's auditors could use this report in evaluating controls over ABC's financial reporting processes. SAS-70's provide some useful information regarding controls over business processes and related systems and often include some component of security controls. They do not however replace the need for or substitute as a Cybersecurity risk assessment.

Q: Does the risk assessment involve the facility security? Who has access to the building, what physical security measures are in place? etc

A: The risk assessment should certainly consider physical threats and vulnerabilities such as natural disasters and breach of physical boundaries. We would recommend enlisting the services of your physical security and facilities personnel who have experience in evaluation of these matters.

Q: In addition to preparing for intrusion attempts, what measures would you advise to prepare for mass external denial of service attacks that do not actually enter the system?

A: A denial of service attack is designed to "flood" the system with communications that causes it to stop responding or fail in some dangerous fashion. Organizations may be impacted in two ways by mass denial of service attacks – they may be the target of the attack; or they may be a victim of an attack on another organization or the Internet infrastructure. In the first case where the organization is the target, we suggest blocking the source of the attack as a first step and then evaluating further tasks based on your incident response process. In the second instance there may be very little that the organization can do other than have good business continuity procedures in place to operate key functions when Internet connectivity is not available.

National Webcast Initiative
Performing a Cyber Security Risk Assessment:
Why? When? and How?
August 26, 2004
Question and Answer Transcript

Q: Who should dictate the timeline for remediation of the findings from the assessment?

A: This needs to be based on the risk and should be determined after discussion with the management of the assessed area. For example, some high risk findings may require immediate attention whereas lower risk items may be remediated over a longer timeframe. In some cases there may be regulatory or other reasons that require issues to be resolved immediately.

Q: Is there VA free ware that you would recommend?

A: NESSUS is a good tool. In addition, www.insecure.org/tools.html. This information was also provided in the webcast registration site materials.