@ISACA
RELEVANT, TIMELY NEWS
Volume 23, 10 November 2010

10 Things to Consider Before Providing a Vendor Security Questionnaire or Examination Result

By John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP

Vendor security questionnaires and assessments have become a popular and normal aspect of organizations' vendor security programs. They often ask for detailed information about the security and risk management capabilities of organizations they are evaluating. Here are 10 things you should consider before providing these data to a requesting organization:

1. **How are these data going to be used by the requesting organization?** Most often, vendor security data are used by information security and risk management organizations to assess the risk of working with third parties and allowing them access to sensitive data and an information infrastructure. These data can also be used by organizations for business activities such as leveraging negotiations, benchmarking their own capabilities, and identifying weaknesses and trends in information security and risk management. It is important to have a clear understanding of how the data are going to be used prior to disclosing the information and to ensure that you are comfortable with its use.
2. **How are the data provided to the requesting party going to be secured once they have been received?** Vendor security questionnaires and audit methods used by many organizations now include large amounts of sensitive information that can become an invaluable intelligence source and, potentially, a road map that an adversary could use to successfully attack your organization. It is important to understand what security and data handling standards and controls are going to be applied by the requesting organization prior to transmitting the data to them. These controls should include (but not be limited to) restricted access control procedures, encryption of data in transit and at rest, access to control logs, and regular access to log reviews by management.
3. **Legal agreements and acceptable use procedures between organizations are not sufficient for securing security questionnaires and audit reports.** Legal agreements that are in place between two organizations typically have provisions for data security that favor the requesting party and often do not have the same

provisions for protecting data provided by the vendor. Even if these provisions do exist, typically, they are applicable only in the recovery of damages in litigation, in the event of a misuse of the data, a data disclosure incident, or a malicious attack as a result of inappropriate access to or compromising of this information. If you are going to provide sensitive and detailed information about your information security and risk management capabilities to third parties, you should have legal language in place in agreements between both organizations that require mutually agreed-upon security measures be implemented to protect the data. The existence and appropriate operation of these measures should be verified on a regular basis during the time the requesting party has access to these data.

4. **Ensure that you are not in breach of contract with other arrangements as a result of disclosing vendor security questionnaires to third parties.** Many organizations are interested in maintaining the confidentiality, integrity and availability of the data they provide to vendors as well as the access they provide them to the information infrastructures. They also would like as few people as possible to have access to information about the information security and risk management capabilities of an organization that they are working with to enhance their own security posture. Organizations may include provisions in their contracts that prevent the disclosure of information about the organization's information security and risk management capabilities.
5. **Request a vendor security questionnaire and performing a vendor security audit of the requesting organization.** To ensure the proper handling and storage of the sensitive information, you should perform a vendor security audit, which can include your own questionnaire of the requesting party. If they are unwilling or unable to comply with this requirement, you should not transmit the security questionnaire to them. Instead, allow the requesting organization to review the completed vendor security questionnaire in person with an authorized member of your organization who can address questions or concerns that may arise as part of the review.
6. **Relay only the information that is relevant to the products and services that you provide to the requesting party.** Many vendor security questionnaires are extremely comprehensive and request information about your information security and risk management capabilities that exceed the scope of services you provide the requesting organization. To limit the exposure of sensitive data associated

with your capabilities, relay only the information that is applicable to the security of the services that will be provided to the requesting organization. If the organization requests information outside of this scope, provide it only when an appropriate business justification for its need has been presented and verified.

7. **Understand how the questionnaire or assessment will be evaluated by the reviewing organization.** Different organizations have different requirements and areas of interest regarding information security and risk management expectations of the vendors with which they work. It is important to understand these in advance of providing information to ensure that your current capabilities and approach are in alignment with their expectations. If you believe that they are not, it is important to contact the requester in advance of any response or examination to come to a mutually agreed-upon set of capabilities that will be used to meet their requirements.
8. **Do not be afraid to ask questions or push back on requirements identified in vendor security questionnaires or assessments.** Consider a vendor security questionnaire or examination a starting point in the conversation with a requesting party, instead of the authoritative set of requirements that you must meet to conduct business with them. Many organizations will use a generic security questionnaire for all vendors they work with that may not be applicable or appropriate to your business activities with them. If you disagree with or are unsure of some of the requesting organization's questions or requirements, engage the organization in a conversation. This will allow you to understand the threat it is trying to mitigate or the requirement it is trying to meet. Then, you can determine if you have an equivalent alternative that it has not yet considered.
9. **Utilize third-party examinations and certifications when possible to reduce the need for extensive data disclosure.** When possible, work with vendors to define a mutually agreed-upon examination or certification to be performed by a third party whose formal opinion will meet the requester's requirement of a review of your information security and risk management capabilities without having to disclose sensitive information to the requester. This can be to the benefit of both parties since it removes the liability and overhead associated with maintaining the security of this information from the requester and ensures an appropriate evaluation has been completed. Often, this approach will work with multiple vendors, which will reduce the time and expense associated with responses to

individual requests from numerous organizations.

10. **Ensure provisions exist for the destruction of questionnaires and assessment results if you no longer do business with a requester.** If you choose to provide questionnaires or allow assessments of your information security and risk management capabilities, it is important that you ensure that this information is destroyed once you no longer do business with the requesting organization. This assurance should not be limited to contractual obligations alone. It should also include a requirement of a certificate of destruction to be provided by the requesting party attesting that all existing and known copies of these questionnaires and assessments, including hard copies, electronic copies and all associated backups, have been destroyed in a manner that has been mutually agreed upon and accepted by both organizations.

John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP, is the president of IP Architects LLC.