

Raising the Standards for Managing a Security and Privacy Assessment

By Edward Johnson, CISSP
tedj@track-assets.com

With privacy laws expanding and the meaning and use of confidential information becoming more regulated, the management of information and assets has become increasingly complex.

Many organizations are crying out for more useful and useable assessments to help them reduce any significant potential losses to their assets and to help them keep compliant to the many new and diverse regulations and standards.

Core Elements in an Assessment

In security, privacy, business impact assessments, and risk assessments, many reports seem to miss essential, core issues. The focus of an assessment should be on the organization's critical and valuable assets and the relationships to the assets. These assets usually are an organization's people, processes, information, technology and supporting facilities.

Different values are normally attributed toward these assets, depending on the user, the owner, or the stakeholder of the asset. Likewise, these people will have diverse types and levels of concern for the exposures and vulnerabilities to the assets. There are many dependencies and inter-relationships among the security and privacy attributes, creating complexity.

With that in mind, there are basic key elements in an assessment that should be addressed and set the standard for an enterprise approach to asset tracking, so that the assessor can properly assign risks. The elements include capturing the following: context of the information to the enterprise, confidentiality and privacy attributes of the assets, integrity of assets, trail of accountability, availability, threats, vulnerabilities, and risks by impact. These eight areas taken together provide the platform for creating a standardized approach.

Current Practices and Issues

It is a commonly held understanding that many assessments are inadequate. Surveys have missed the mark or lost the scope of the subject of the assessment. It has been revealed that many organizations control their information by the "seat of their pants," just when information assets have moved into increasing hostile territory, with the Internet as the most hostile and riskiest area of all. Some client organizations have expended enormous amounts of energy and money to address threats only to find their controls are overly sophisticated and inappropriate.

Professional assessors are facing an increasingly complex client infrastructure, which must be fully understood. They are also facing an ever-growing list of audit and regulatory requirements to meet local, federal and international legislation. Add to this the complexity of maintaining control

under third party or outsource relationship, where the data is maintained off organization premises or even under another jurisdiction.

Whatever the client's business, security professionals need to be aware of these regulations, understand the impact to their organization, keep up with any changes, and be able to implement these capabilities quickly based upon upcoming deadlines. While there is no single "one size fits all" rule for compliance, professionals must consider regulations established by regulatory agencies, such as those governing privacy of information, human rights, electronic commerce, data protection, and now laws in attempt to control the threats of terrorism.

Six Issues with Risk, Privacy and Business Impact Assessments

Purpose. Professional assessors must never lose site of the purpose of the assessment. They must ask themselves how the client will use the results of the survey, the level of controls the recommendations call to implement, and address the standards of due diligence required for their sector.

Consistency. Survey results need to be consistent. Assessments are often done in many ways, with many different types of metrics. It is difficult to compare results from different surveys or determine how the results of a survey can apply to similar environments.

Scope. The assessor needs to understand scope and the level of the survey requirements. Because one aspect of a system happens to be more interesting, the survey must not lose its general focus.

Usability. Survey results need to be understandable, simple and usable. Professionals need to determine what information the client organization is trying to protect and how they want to protect it.


Security Standards. Assessments all have the same aim: to ensure the target system can be trusted to a specified level of security.

Reusable Results. Survey results need to be reusable. Security professionals preach the need to keep the risk management picture up to date, particularly after the client has made significant changes. The client must not be expected to complete a 20-day survey every time a change has been made to their environment or system. The survey should only focus on the effects of the changes as most of the details of their system most probably have remained the same.

Standard Enterprise Approach to Track Assets

Keeping the core elements of an assessment listed above in mind will provide a standardized approach that tracks security and privacy information about assets within an organization, a project or a system.

The standard enterprise approach guides the user to enter pertinent information on assets, including threats and vulnerabilities, by organizing and collecting data for future reference or re-appraisal. Professional assessors should be able to assign the risk, given the structured and ranked presentation of the data results. Assessors should not have to fight a standard enterprise approach, but rather be allowed to use their expertise once the relevant information is tracked.

The benefits far outweigh the cost of a proper assessment. Addressing all the elements in a standard enterprise approach will raise the bar for managing a security and privacy assessment and give organizations real value for managing their assets. 

Mr. Edward (Ted) Johnson is an Information Security Consultant with over 23 years' experience with information processing, including 15 years of specialization in computer security. Mr. Johnson has prepared policy, security specifications, business impact analysis and disaster recovery plans, audit and risk analysis, and engineering support for government and for industry. Mr. Johnson is president of Track-Assets.com, which has developed a tool for enterprise approach to track security and privacy information about assets within a project or a system.

