Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Facilitating the Qualitative Security Assessment: Overview of the Process of Defining and Delivering

The Security Assessment represents a process that is used to help ensure that the appropriate security measures are identified and applied to meet management's expectations for a secure and trusted computing environment. There are two aspects of this process that contribute to its success. The first is the need to provide management with a clear understanding of the security issues and the related threats that impact the processes they are responsible for. The second aspect involves the identification and delivery of s...

Copyright SANS Institute
Author Retains Full Rights

AD

Facilitating the Qualitative Security Assessment:

Overview of the Process of Defining and Delivering Security Requirements for Application Systems

Mike Kleckner (assignment version 1.2e)

July 24, 2001

The Security Assessment represents a process that is used to help ensure that the appropriate security measures are identified and applied to meet management's expectations for a secure and trusted computing environment. There are two aspects of this process that contribute to its success. The first is the need to provide management with a clear understanding of the security issues and the related threats that impact the processes they are responsible for. The second aspect involves the identification and delivery of solution options and their associated costs, offered by appropriate, qualified solution providers.

The result of an effective security assessment is that management is in a better position to make informed decisions concerning the delivery of appropriate security controls for their business processes. It is the intent of this paper to provide an overview of how to involve the appropriate decision makers and the solution providers in the delivery of cost-effective security controls for application systems. The primary beneficiary of this overview is the individual who is charged with facilitating the security assessment process.

Overview of the Process

Performing a security assessment involves three types of individuals. It relies upon

- a facilitator who is familiar with information security concepts,
- a manager, (from the business side), who is responsible for the data and the associated business processes, (the data/process owner), and
- solution providers who are experts familiar with delivering and supporting solutions that protect and support business processes.

The security assessment starts with the data/process owner establishing the need for an evaluation of the vulnerabilities[1] that threaten a business process that they are responsible for. The data/process owner will enlist the services of a security advisor to facilitate the security assessment process. The result will be to identify the security threats and document the business requirements that define acceptable levels of risk.

Once the security requirements have been defined by the data/process owners, experts familiar with improving the business process(es), the solution providers, are familiarized

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

with the security requirements. Solution providers tend to include, but are not limited to, internal and external technical experts, professional trainers and legal specialists. The facilitator will ensure that the solution providers have a clear understanding of the data/process owner's expectations by conducting a meeting to review the documented requirements. This will place the solution providers in a better position to investigate the various options that can be used to deliver solutions that provide the level of security expected by the data/process owner.

The data/process owner then reviews the options and costs that have been offered by the solution providers to determine the balance between controls the business can afford to implement and the amount of risk that is acceptable.

Critical to the success of the security assessment is a general understanding of security concepts and the timing of when the security assessment is performed. Security assessments should be encouraged[1]:

- when the security of an existing system needs to be evaluated,
- when it is necessary to determine the impact of changes to a system, or
- when a new system is being developed.

Greater success will be achieved when the assessment is performed while system functional requirements are being defined. Retrofitting security into the later stages of system development is likely to delay projects and drive up project costs.

Facilitating the Assessment Process

In preparation for a security assessment, the facilitator needs to be familiar with security concepts and have a general understanding of the business process that is being evaluated. This will allow the facilitator to more clearly articulate the value of the security elements and how they support the business requirements. At a minimum, the security elements that should be considered consist of:

- Authentication
- Authorization
- Confidentiality and Reliability
- Monitoring
- Backup and Recovery
- Physical Security
- Change Management
- Legal Requirements
- Training and Awareness
- Contingency Planning

When a security assessment is requested, the facilitator should first schedule a meeting with the data/process owner to introduce the overall security assessment process. The facilitator will then describe each security element to the business owner. This leads into a discussion concerning whether the element poses a risk to the business process. The facilitator is responsible for helping the data/process owner to:

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- understand pertinent risks and vulnerabilities
- select security elements and safeguards that protect the resource consistent with management expectations and their level of risk tolerance
- be familiar with security best practices.

Every element should be considered, but some elements may not apply or may be already provided by the current infrastructure. As each element is reviewed, the data/process owner is positioned to make informed decisions about system components they need to protect and the amount of risk they are willing to assume.

When the security requirements have been defined by the data/process owner, the facilitator needs to identify the experts who are in a position to provide remedies that can address the identified risks. These experts will then be assembled to review the business requirements, ask questions and discuss any concerns that they may have. Discussion at this point is valuable since the solution providers will need to work together to ensure that the ultimate solutions integrate and deliver on the requirements defined by the data/process owner.

After the solution providers offer their solution options, the facilitator will help the data/process owner to understand how the various options contribute to create the level of trust that is expected. Contracts can then be drawn up with the solution providers once the desired solutions are selected.

Establishing Ownership and Owner Responsibilities

The key to the success of a security assessment is an individual, the data/process owner, who accepts ownership responsibilities for a business and its processes. This person must be willing to drive the security assessment and take ownership of the action plan. The data/process owner has a vested interest in protecting their data and the related process and cannot assume that anyone else, including information systems staff, will make the 'best' decisions on their behalf. The data/process owner needs to become comfortable with a few basic security concepts and must be willing to determine the value of their data and the systems that make their data useful. With this foundation, they will be in a good position to ask questions, scrutinize solution options and determine the appropriate investments in controls to mitigate the risks that threaten their data and process(es)[2]. The action plan for the implementation of the controls needs to be chosen by the data/process owner[2].

The primary objectives of the data/process owner are to[3]:

- identify the value of the assets involved, including hardware, software, information, people and procedures
- classify the data used by the process and identify the highest level of sensitivity and criticality involved
- identify the threats to the data and associated processes and consider the likelihood of their occurrence

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- select the security elements that will protect the information resources in a manner consistent with management expectations, and
- document the business requirements as they relate to the security elements.

The data/process owner is responsible for selecting security that protects the information resources that they are responsible for, consistent with their level of risk tolerance. The data/process owner should establish this tolerance level by considering:

- the pertinent threats, (human, machine or nature), that can affect the value of an asset
- the vulnerabilities, or the means by which a threat can be realized[3]
- the resulting damage, including the loss of access, unauthorized access, modification, disclosure or destruction of data
- what executive management's expectations are, (as stated in corporate information security policies)[2]
- the legal requirements that govern the handling of certain types of data, and
- the costs that can be justified in light of the value and sensitivity of the data[2].

After the solution providers have responded with their documented solution options, the data/process owner is placed in a position of performing risk management[4] by identifying what should be done to reduce identified threats to an acceptable level. The data/process owner should recognize how the security solutions are intended to:

- reduce the likelihood of a threat from occurring
- reduce the impact of a threat if it occurs
- detect the threat when it occurs and
- recover from the threat when it occurs.

A meeting facilitated by the security advisor should help data/process owners to understand and select the security options within each of the security elements that best suit their tolerance for risk and cost. It is the owner who has the vested interest in protecting the data and its processes, and should therefore be making informed decisions on the costs[2] that should be expended to provide an affordable level of protection.

Educating the Data/Process Owner

Information protection objectives are to ensure that the information is protected from unauthorized or undesirable modification or corruption, (integrity), that it has not undergone unauthorized or undesirable disclosure, (confidentiality), and that it available to those who are properly authorized to use it, (availability)[1]. It is necessary to identify the risks that that would have a negative impact on these objectives and the controls or measures that should be taken to prevent, detect, reduce or eliminate risk[4].

Providing the data/process owner with a general understanding of security concepts is essential to the success of the assessment. The ten security elements described below need to be considered in the assessment discussions.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Evaluating each of these elements will shed light on how security concepts can be utilized by the business processes to provide the opportunities that can be achieved when a trusted environment is created. Information on each element should be provided by the facilitator to help understand the various elements of information security, appreciate the risks mitigated by the security element and select a combination of security elements that:

- protect the information resource,
- mitigate related risks, and
- meet management's objectives for creating a cost-justified trusted environment[2].

Authentication is the security element which establishes the level of confidence that individuals accessing the information are who they claim to be[5]. If users are not truly known to the system, it is not possible to accurately identify the source of the problems or malicious activities.

Lack of accountability, or not knowing who accessed or changed your information, is the major risk of poor authentication practices. As a result, if there is an incident of fraud or a breach of confidentiality, it is unlikely that the responsible party can be identified or pursued through legal channels.

Security policies should establish baseline authentication requirements, but additional requirements may be identified to strengthen the use of passwords or identify where other authentication options may be desired, using tokens, smart cards and biometrics.

The data/process owner should be aware of additional risks that are introduced when their data passes through several computers, applications and networks. This may require authentication at multiple locations and restrictions on the use of generic, guest and process userid's.

Authorization describes the process by which persons or processes are allowed to access information. This should limit individuals to access data or perform only those actions that the data/process owner has approved for them[5]. This is enabled through the use of operating or application system controls.

Improper authorization leaves the data vulnerable to intentional or unintentional tampering or viewing. If users are permitted to perform more actions on the data than their job requires, it is possible they may inadvertently change or delete information. They may see information that is restricted or that they have no business need to see. It is possible they may fall under suspicion for activity not related to their immediate job responsibilities because their authorization is too generous. The principle of least privilege needs to be appreciated so that only the data and processes required to perform one's job duties is allowed.

Confidentiality is the security element which establishes the level of privacy that is utilized so that data is restricted to authorized individuals. Reliability ensures that information is received exactly as it was sent (*data integrity*) and that the transaction cannot be denied (*nonrepudiation.)*.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Corporate policy[6] should prohibit the inappropriate disclosure of information classified as Confidential or Internal Use Only. Disclosure of sensitive information to unauthorized persons can result in financial loss, gains to competitors, significant embarrassment to your company, sizable loss of customer confidence, lost opportunity and notable reduction of corporate standing in the community. Unreliable data provides misleading information to decision making processes (computerized or human).

Technologies including encryption and digital signatures should be considered for mitigating risks introduced by this security element. The business owner needs to consider that it may be necessary to encrypt sensitive information while stored on a computer (server or local PC hard drive) as well as in transit over a network. Unprotected information traversing public lines can be seen by an unpredictable number of computers managed by a variety of individuals and businesses, all who can read information as it passes through their computer systems.

Monitoring the activities of people and programs accessing data and processes is generally accomplished by evaluating activity that has been written to log files. These logs can be useful for:

- determining who has access to the data or what activities were carried out regarding the data
- establishing a record which can provide proof of unauthorized activity
- establishing a baseline of 'normal and usual' activity
- identifying where new policies or procedures may need to be established
- ensuring that the system is secured in accordance with management expectations[2]
- providing forensic evidence in a case of fraud, a breach in security, or other abuse or criminal activity.

Certain levels of security allow an individual to give access to other persons or processes. Periodic checking for entities having access can reveal:

- additional persons or processes other than those originally authorized by the data/process owner who may have been given access
- persons having access that is no longer needed because they have left the Company or have changed responsibilities
- processes having access that are no longer needed because they have become obsolete.

It is also important to secure the log files themselves to preserve their integrity. Unauthorized persons may tamper with unsecured logs to cover their tracks.

Backup and recovery procedures are required to recover and resume operations in the event of intentional or unintentional data loss due to virus attack, fraud incidents, data tampering, or accidental activity. It may be impossible to recover the system in a timely and cost effective manner if data and software used in the business process are not available. There may be legal risks to consider if archived information cannot be made available or if business operations cannot be resumed in a certain period of time (e.g.,

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

timing requirements for claims processing). Often overlooked is the fact that backed up data should be protected to the same degree as information on the production system.

Physical security considers how easy or difficult it is to access the computer hardware containing electronic data, as well as non-electronic information that reside on media such as paper and microfiche. It is important to ensure that confidential information is properly stored, retained and disposed of. Under consideration should be processes for removing sensitive information from disks, tapes and obsolete servers and personal computers. It is also valuable to keep track of individuals who are allowed to use corporate computer hardware, especially portable devices such as laptops and personal digital assistants.

Physical access to computer hardware presents the risk of:

- Unauthorized removal of equipment, hardware and information
- Loss of sensitive information stored on local PC hard drives
- Disclosure of sensitive information
- Tampering with servers, routers and other computer hardware to read information, change configurations, corrupt data, install 'sniffer' equipment or malicious software, etc.

Access to data centers, communication centers and tape/disk libraries should be denied to personnel other than those who have a business need to enter those areas. Any exceptions need to be logged and investigated.

A change management process, with its related procedures, (such as version control), assists with life cycle management by controlling changes to code running in the production environment. This is critical to protecting the production processes.

A controlled change management process can:

- prevent malicious or faulty code from being introduced into the production environment
- prevent accidental changes to the production code
- determine who made changes to production code
- make it easier to back out code changes to prior working versions
- coordinate multiple changes to a system
- identify when changes took place to the production process
- ensure that testing and user acceptance has been completed.

Formal test plans and scripts should be created at the start of the project to minimize the risk of compromised data integrity and system failure. Modifications to software may dictate changes to interfaces, procedures and access control definitions.

Legal requirements (state or federal) may impose restrictions on business processes. For example, federal HIPAA regulations require that medical data be encrypted whenever it is transmitted or stored. It is in this area where the assistance of legal experts is critical. The delivery of non-technical solutions, such as confidentiality agreements and contracts

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

become very critical to protecting a business and its partner relationships. There may be certain steps required when transacting business in an electronic environment to ensure that a legally binding transaction took place resulting in a valid contract. Date and time stamping of an electronic transaction may be necessary to establish the timing of contractual agreements. Litigation issues, fines, and incarceration concerns need to be revealed if governmental regulations are violated. If nothing else, the Federal Sentencing Guidelines as they relate to information security should catch the attention of any responsible manager. These guidelines provide a summary of actions that can be taken against companies, (and their management), that violate federal regulations regarding privacy and due diligence.

A partial list of legal requirements and governmental regulations which may need to be considered consist of:

- data privacy laws
- release or reporting to a governmental agency
- information that may be released due to "public right to know" laws
- contract law in cyberspace issues
- legal or governmental jurisdiction and sovereignty
- security monitoring issues
- systems or data affected by "threat to national security" rules
- retention practices to conform to legal requirements.

Training and awareness[5] can establish a level of understanding necessary for users to appreciate the sensitivity, integrity, and accessibility issues that apply to an application process. Current practices may be sufficient, however, new behaviors may need to be encouraged or new skills may need to be developed.

Threats that compromise the owner-defined security objectives include accidental or intentional mishandling or disclosure of proprietary information. As technologists, we tend to believe that security relies upon technical solutions. In reality, a significant amount of security depends upon the employee attitudes and ethics that contribute to the corporate culture. A motivated individual can subvert even the best technical controls.

A Contingency Plan, also called a Business Continuity plan, is necessary for managing the risks related to a sudden and unplanned interruption of the business process. The plan establishes a Recovery Time Objective that defines a maximum acceptable time that the business unit cannot function without serious impact to customers and determines strategies to restore functions within that projected time. In addition to rebuilding computer systems, this plan will consider requirements for moving a business operation to new facilities, enlisting additional human support and providing supplies necessary to resume business processes.

Solution Providers

Solution providers can include internal and external technicians, vendors, contractors, application service providers and legal specialists. Providing reasonable and valuable

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

solution options requires that the solution provider have a clear understanding of the business objectives that need to be met. Some of the responsibilities of the solution provider include:

- offering options, including the associated cost estimates, for meeting the data/process owner's security expectations
- adhering to information security policies and standards and
- testing and implementing the security components requested by the data/process owner.

Solution providers may also be responsible for the ongoing maintenance of controls that secure the computing environment. Solution Providers test, implement and maintain the security required by the data/process owner. It is valuable to involve the data/process owners in the monitoring of important security elements to ensure the security is working or is applied as required. The solution provider must ensure that the technical implementation coincides with the business requirements defined by the data/process owner.

An additional consideration involves the use of external service providers. Management needs to appreciate the fact that they will assume the vulnerabilities that exist in the external providers environment[7]. It should be expected that external providers meet or exceed the policies, standards and functional requirements defined by their corporate executives. Legal expertise becomes very important in establishing reliable expectations for these arrangements[7].

Conclusion

The assessment process is most effective when the data/process owners take ownership of the security assessment and identify it as a necessary function, similar to any other process that establishes business requirements. The facilitator, who is often a security specialist or advisor, should be perceived as the one who is working for the data/process owner to offer insight and experience in bridging the gap between those who define the security requirements and those who provide the solutions. The facilitator will need to understand the business objectives and must be able to convey the value of the security elements in the context of the business requirements. Once the data/process owner justifies the security assessment, the business case is made. It then becomes the responsibility of the solution providers to offer their services and the associated costs. In the more traditional model, where a security department is charged with determining what appropriate security controls should be, there tends to be resistance from those who perceive security to be authoritarian, intrusive and optional.

It must be understood that the assessment is intended to support the business needs and that the business side of the equation is charged with making the decisions concerning the security of their data and processes. No security control can be expected to be one hundred percent effective, so trade-offs must be made to achieve business objectives by balancing acceptable levels of risk and cost. In the words of Bruce Schneier,

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Some risk needs to be accepted as a cost of doing business, some risk is reduced through technical and/or procedural means, and some risk is transferred, through contracts or insurance.[4]

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

References:

Online:

1. Peltier, Tom; "The New Risk Analysis; A Facilitated Approach" CSI Educational Resource Center Seminar 1998.
2. Johnson, John D.; "Developing a Successful Information Security Process: Risk Assessments" SecurityPortal.March 2001. URLhttp://securityportal.com/articles/risk20010329.html
3. Johnson, John D.; "Conducting Risk Analysis to Evaluate Enterprise Security" SecurityPortal.November 1999 URLhttp://securityportal.com/direct.cgi?/topnews/conduct-risk.html
4. Schneier, Bruce; "Closing the Window of Exposure" Counterpane.February 2001 URLhttp://www.counterpane.com/window.html
5. Internet Security Task Force; "Initial Recommendations for Conducting Secure eBusiness" ISTF.March 2000 URLhttp://www.ca.com/ISTF/recommendations.htm#8
6. Robinson, Chad; "Good Security Puts Policy First" CIO.June 2001 URLhttp://www.cio.com/analyst/060801_rfgonline_content.html
7. Tuesday, Vince; "Security Outsourcing:Don't Bet on It – Yet" ComputerWorld.June 2001 URLhttp://www.computerworld.com/cwi/community/story/0,3201,NAV65-663_STO61232,00.html

Other Reading

Textbooks:

1. Schneier, Bruce; "Secrets & Lies: Digital Security in a Networked World" New York, NY: John Wiley & Sons,Inc. 2000

Magazines/Publications:

1. Oppliger, Rolf; "Trouble Ahead, Trouble Behind: The Future of Computer Security" Computer Security Journal.Winter 2001
2. Computer Security Institute Information Protection Assessment Kit, 1997
3. Brink, Derek; "The Gentle Art of Managing Risk" Info Security News.April 1999
4. Miora, Michael; "7 Steps to Assessing Your Security Risk" Security Advisor.Premiere 1998
5. Paller, Alan; "Key Security Queries" ComputerWorld.August 1999
6. Pabrai, Uday and McCright, Matt; "Integrating Network and Security Infrastructures" Business Security Advisor.June 2001
7. Winkler, Ira; "Audits Assessments & Tests" Information Security.July 2000
8. Columbus, Louis: "ASP Planning: Create a Strategy for Scalability" E-Business Advisor.March 2001
9. Rutkowski, Therese; "Are Your Systems Safe?" Insurance Networking.April 2001
10. Forte, Dario; "Security Risk Assessment" Internet World.August 2000
11. Schneier, Bruce; "The Process of Security" Information Security.April 2000
12. Paul, Brooke; "How Much Risk Is Too Much?" InformationWeek.November 2000

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced