"Successful businesses understand the value of timely, accurate information, good communications and secrecy. Information security is as much about exploiting the opportunities of our interconnected world as it is about risk management"
- ISO27001:2013[1]

Security Risk Assessment

Technical Point-of-View

Security risk assessments should identify, quantify, and prioritize information security risks against defined criteria for risk acceptance and objectives relevant to the organization[1]. The results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks. Assessing risks and selecting controls may need to be performed repeatedly across different parts of the organization and information systems, and to respond to changes. The process should systematically estimate the magnitude of risks (risk analysis) and compare risks against risk criteria to determine their significance (risk evaluation).

The integrated security risk assessment and audit approach attempts to strike a balance between business and IT risks and controls within the various layers and infrastructure implemented within a university, i.e. financial reporting, business process, application, database, platform and network. This newsletter will describe process, methodology, impact and approach to address limitations for carrying out security risk assessment activities[1,2].

Common Challenges

While security risk assessment provides the means to identify and address potential risk factors, failure to perform assessments effectively can lead to missed opportunities, both to avoid and capitalize on risk events. Common business challenges include the following.

1. ***Cost***, especially unbudgeted costs. Regardless, business and even IT units do not want to spend money on security controls unless they are absolutely necessary and usually tied to regulatory compliance or an audit citation. The business unit will minimize the privacy or security risk to avoid spending the money.

2. ***Unplanned activity,*** Any unplanned activity, whether it is part of a project or part of a yearly operating plan, will generate, at minimum, tension or push back. Project teams and management in general are inherently averse to doing any tasks they did not plan for.

3. ***Miscommunication***: Many times, security managers communicate in terms of missing control risks or a policy non-compliance risk, not in terms of the operations or educational risk. As a result, it's hard to achieve consensus to mitigate the risk(s), regardless of what control should be implemented.

4. ***User or customer impact***: Any security control that changes the user experience will create resistance. Even if it's as benign such as increasing the length of passwords, it creates anxieties for business managers. Therefore, they will likely overstate implementation costs and try to delay implementation.

"In an assessment, the assessor should have the full cooperation of the organization being assessed. The organization grants access to its facilities, provides network access, outlines detailed information about the network, etc. All parties acknowledge that the goal is to study security and identify improvements to secure the systems. An assessment is potentially the most useful of all security tests, but it is also the hardest to define"
-SANS [6]

5. ***Incorrect estimating the costs of security controls.*** Sometimes the business or IT unit is uncertain about the implementation cost, and will incorrectly estimate the cost of the security controls.

6. ***Improperly relying on mitigating controls*** that do not effectively address the risk. A good example might be to rely on a manual review of system event logs instead of implementing an event monitoring system.

Universities need to understand and appreciate the importance of security controls. The vast majority of the controls outlined in the generally accepted security standards bodies, (e.g. COBIT, ISO, etc) are required in some shape or form in universities that manages IT infrastructure, even if it is outsourced[2].

Performing Security Risk Assessment

Universities have many reasons for taking a proactive and repetitive approach to addressing information security concerns. Legal and regulatory requirements aimed at protecting sensitive or personal data, as well as general public security requirements, create an expectation for companies of all sizes to devote the utmost attention and priority to information security risks. Security risk assessment takes on many names and can vary greatly in terms of method, rigor and scope, but the core goal remains the same: identify and quantify the risks to the universities' information assets. This information is used to determine how best to mitigate those risks and effectively preserve the universities' mission[4,5].

Assessment Process

The security risk assessment and security risk management processes comprise the heart of the information security framework. These are the processes that establish the rules and guidelines of the security policy while transforming the objectives of an information security framework into specific plans for the implementation of key controls and mechanisms that minimize threats and vulnerabilities.

Methodologies

The assessment approach or methodology analyzes the relationships among assets, threats, vulnerabilities and other elements. There are numerous methodologies, but in general they can be classified into two main types: quantitative and qualitative analysis. The methodology chosen should be able to produce a quantitative statement about the impact of the risk and the effect of the security issues, together with some qualitative statements describing the significance and the appropriate security measures for minimizing these risks.

By default, all relevant information should be considered, irrespective of storage format. Typical information that will be collected for assessment include:

- Security requirements and objectives
- System or network architecture and infrastructure, such as a network diagram showing how assets are configured and interconnected
- Information available to the public or accessible from the universities' web site
- Physical assets, such as hardware, including those in the data centre, network, and communication

"To help understand threats and their impact on assets, a mapping of threats with impact is necessary. The following four impact categories lists threats, both direct and indirect, and indicates areas where a given threat may have an impact."
- *SANS[8]*

components and peripherals (e.g., desktop, laptop, smartphone even BYOD)
- Operating systems, such as PC and server operating systems, and network management systems
- Data repositories, such as database management systems and files
- Security systems in use, such as access control mechanisms, change control, antivirus, spam control and network monitoring
- Governance and compliance pertaining to minimum security control requirements

The project scope and objectives can influence the style of analysis and types of deliverables of the security risk assessment. The scope may cover the connection of the internal network with the Internet, the security protection for a computer center, a specific department's use of the IT infrastructure or the IT security of the entire organization. The security requirements should be based on business needs, which are typically driven by senior management, to identify the desired level of security protection. A key component of any risk assessment should be the relevant regulatory requirements such as ISO/IEC 27001:2013 and the Personal Data Privacy Ordinance.

The following are common tasks that should be performed during security risk assessment:

- Identify business needs and changes to requirements that may affect overall IT and security direction.
- Review adequacy of existing security policies, standards, guidelines and procedures.
- Analyze assets, threats and vulnerabilities, including their impacts and likelihood.
- Assess physical protection applied to computing equipment and other network components.
- Conduct technical and procedural review and analysis of the network architecture, protocols and components to ensure that they are implemented according to the security policies.
- Review and check the configuration, implementation and usage of remote access systems, servers, firewalls and external network connections, including the client Internet connection.
- Review logical access and other authentication mechanisms.
- Review current level of security awareness and commitment of staff within the organization.
- Review agreements involving services or products from vendors and contractors.
- Develop practical technical recommendations to address the vulnerabilities identified, and reduce the level of security risk.

Mapping threats to assets and vulnerabilities can help identify their possible combinations. Each threat can be associated with a specific vulnerability, or even multiple vulnerabilities. Unless a threat can exploit vulnerability, it is not a risk to an asset.

The range of all possible combinations should be reduced prior to performing a risk analysis. Some combinations may not make sense or are not feasible. This interrelationship of assets, threats and vulnerabilities is critical to the analysis of security risks, but factors such as project scope, budget and constraints may also affect the levels and magnitude of mappings[12].

"When considering the impact of a successful attack, it's important to realize that there are two kinds of impacts. The first is the "technical impact" on the application, the data it uses, and the functions it provides. The other is the "business impact" on the business and company operating the application."
OWASP Risk Rating[13]

Once the assets, threats and vulnerabilities are identified, impact and likelihood of security risks should be determined.

Impact Assessment

An impact assessment (also known as impact analysis or consequence assessment) estimates the degree of overall harm or loss that could occur as a result of the exploitation of security vulnerability. Quantifiable elements of impact are those on revenues, profits, cost, service levels, regulations and reputation. It is necessary to consider the level of risk that can be tolerated and how, what and when assets could be affected by such risks. The more severe the consequences of a threat, the higher the risk. For example, if the research IP are compromised, the cost to the university would be a plagiarism from the original research work and the loss of intellectual property work.

Likelihood Assessment

A likelihood assessment estimates the probability of a threat occurring. In this type of assessment, it is necessary to determine the circumstances that will affect the likelihood of the risk occurring. Normally, the likelihood of a threat increases with the number of authorized users. The likelihood can be expressed in terms of the frequency of occurrence, such as once in a day, once in a month or once in a year. The greater the likelihood of a threat occurring, the higher is the risk. It can be difficult to reasonably quantify likelihood for many parameters; therefore, to simplify relative like hood would be wise using High / Medium / Low as measurement.

A systems example is the high likelihood of an attempt to exploit a new vulnerability to an installed operating system as soon as the vulnerability is published. If the system affected is classified as critical, the impact is also high. As a result, the risk of this threat is high.

For each identified risk, its impact and likelihood must be determined to give an overall estimated level of risk. Assumptions should be clearly defined when making the estimation. This two-dimensional measurement of risk makes for an easy visual representation of the conclusions of the assessment. See figure 1 for an example risk map.

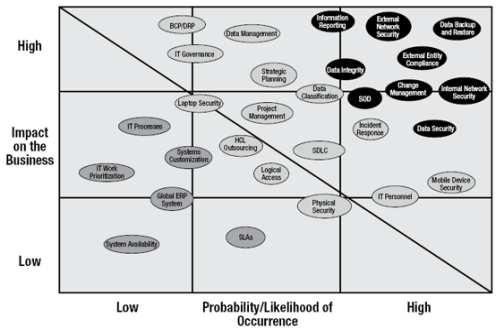

Figure 1: Risk Map

Value Creation

Institutionalizing a practical risk assessment program is important to supporting an education institution activities and provides several benefits[10]:

1. Security risk assessments programs help ensure that the greatest risks to the IT department are identified and addressed on a continuing basis. Such programs help ensure that the expertise and best judgments of personnel, both in IT and the larger organization, are tapped to develop reasonable steps for preventing or mitigating situations that could interfere with accomplishing the universities' mission.

2. Security risk assessments help personnel throughout the organization better understand risks

Case Study:

"At Notre Dame University,. The executive vice president created—and personally chairs—a group known as the Institutional Risk and Compliance Committee. This group is composed of senior members of management, including functional roles like finance, IT and research, and covers each of the major business areas of the university. It is a diverse group with a big impact.

What makes the group different from many management teams is how it looks at risks, and how it reacts to risks. This diverse group has created a simple process of yearly assessments conducted by each major business area in the university. Risks must affect the university as a whole, and they're categorized on a simple high, medium and low scale for probability and impact, and coloured red, yellow or green. Each one is then rated on its current status: un-handled and needs a plan; in progress with a plan; or handled as well as it can be handled. Again, each risk is red, yellow or green based on its status—a separate rating from its probability and impact. A quick glance at a chart tells the group what needs attention or a status check. Red risks with a red status rating get attention quickly!"

- *Security Tech Target*[11]

to institutional operations. They also teach them how to avoid risky practices, such as disclosing passwords or other sensitive information, and recognize suspicious events. This understanding grows, in part, from improved communication among senior management, system support staff and security specialists.

3. Security risk assessments provide a mechanism for reaching a consensus as to which risks are the greatest and what steps are appropriate for mitigating them. The processes used encourage discussion and generally require that disagreements be resolved. This, in turn, makes it more likely that senior management will understand the need for agreed-upon controls, feel that the controls are aligned with the universities' goals and support their effective implementation.

4. A formal security risk assessment program provides an efficient means for communicating assessment findings and recommending actions to senior management. Standard report formats and the periodic nature of the assessments provide universities a means of readily understanding reported information and comparing results between units over time.

Ultimately, security risk assessments performed with measurably appropriate care are an indispensable part of prioritizing security concerns. Carrying out such assessments informally can be a valuable addition to a security issue tracking process, and formal assessments are of critical importance when determining time and budget allocations in large universities.

In contrast, taking a haphazard approach to security concern prioritization can lead to disaster, particularly if a problem falls into a high-risk category and then ends up neglected. IT-specific benefits of performing security risk assessment include:

- Providing an objective approach for IT security expenditure budgeting and cost estimation
- Enabling a strategic approach to IT security management by providing alternative solutions for decision making and consideration
- Providing a basis for future comparisons of changes made in IT security measures

Conclusion

An information security framework is important because it provides a road map for the implementation, evaluation and improvement of information security practices. As a university implements its framework, it will be able to articulate goals and drive ownership of them, evaluate the security of information over time, and determine the need for additional measures.

A common element in most security best practices is the need for the support of senior management, but few documents clarify how that support is to be given. This may represent the biggest challenge for the universities' ongoing security initiatives, as it addresses or prioritizes its risks.

Specifically, security risk assessment is intended to be suitable for the following, which could be specific to any university:

- A way to ensure that security risks are managed in a cost-effective manner

- A process framework for the implementation and management of controls to ensure that the specific security objectives of an university are met
- A definition of new information security management processes
- Use by management to determine the status of information security management activities
- Use by internal and external auditors to determine the degree of compliance with the policies, directives and standards adopted by the university
- For implementation of business-enabling information security
- To provide relevant information about information security to customer

Overall, universities must have a solid base for its information security framework. The risks and vulnerabilities of universities will change over time; however, if universities continue to follow their frameworks, they will be in good position to address any new risks and/or vulnerabilities that arise.

References

1. "ISO/IEC 27001:2013, Information Technology – Security Techniques – Information Security Management Systems, 2nd Edition" 25 SEPT 2013, WEB, 13 February 2015
2. "ISO/IEC 27002:2013, Information Technology – Security Techniques – Code of Practice for Information Security Management, 1st Edition" 13 OCT 2013, PDF, 13 February 2015.
3. "NISTIR 7328, Security Assessment Provider Requirements and Customer Responsibilities: Building a Security Assessment" SEPT 2007, PDF, 13 February 2015.
4. "NIST Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans" JUN 2010, PDF, 13 February 2015.
5. "Technical Guide to Information Security Testing and Assessment" SEPT 2008, PDF, 13 February 2015.
6. "Implementing a Successful Security Assessment Process" AUG 2001, PDF, 13 February 2015.
7. "Prioritizing Information Security Risk with Threat Agent Risk Assessment" DEC 2009, PDF, 13 February 2015.
8. "Critical Security Controls: From Adoption to Implementation" SEPT 2014, PDF, 13 February 2015.
9. "Security Assessment" WEB, 13 February 2015
10. "The transformation of IT Risk Management" PDF, 13 February 2015
11. “Security-Risk-Assessment-Process-a-Team-Effort-at-Notre-Dame” WEB, 13 February 2015
12. “A Perspective on Threats in the Risk Analysis Process” PDF, 13 February 2015
13. “Using Risk Assessment To Prioritize Security Tasks And Processes” WEB, 13 February 2015

Copyright Statement