Information Security Risk Assessments – Why Conduct Them and Avoiding Common Pitfalls

Need to Improve Information Security

Most organisations are aware of the need to improve the security of the information under their control. There may be a variety of reasons for wanting to do this. It may be quite simply that senior management want to demonstrate externally that the organisation protects its information, possibly in order to gain a competitive advantage and attract more clients. Alternatively, the organisation may be working in a regulated environment, part of which requires that it manages the security of its information assets. Another often quoted reason is that it may be as a response to one or more of its clients, which have stipulated it as a prerequisite of engagement.

Whatever the reason, effective information security controls will help to prevent security breaches, reduce the impact of breaches should they occur and will help to minimise any adverse publicity. Whoever said ‘there’s no such thing as bad publicity’ probably never ran their own business!

Cost of Jumping Straight in

One of the biggest mistakes made by organisations looking to increase the effectiveness of their information security is that they jump straight in and start implementing security controls without thinking through the process fully. This is a bad idea on two counts. Firstly, they may be implementing controls which provide little in the way of improved security as they do not protect the organisation’s most important or valuable assets. The implementation and ongoing management may be a costly exercise with little or no return on investment. Secondly and conversely, key controls which need to be implemented may go unidentified or have a low priority. The information security controls implemented need to be cost effective and be appropriate to the objectives of the organisation.

Another common pitfall for many organisations is the assumption that information security risks are all associated with IT and that by simply deploying anti-virus systems and firewalls, the problem will go away. However, security breach surveys have repeatedly shown that the biggest source of security breaches is human related, be that user error, user ignorance or malicious acts. For example, a firewall will not prevent someone from stealing all the laptops and the confidential information stored on their hard-drives along with them.

A single solution is, very rarely, sufficient to prevent an information security breach and risk reduction is not always necessary. The answer is to deploy layers of security which include a combination of IT, people, policies, processes and physical security controls.

The six million dollar question then, is how do you determine which risk treatment option needs to be implemented? The simple answer is to start with an information security risk assessment.

Risk Assessment

There are a number of different ways of conducting an information security risk assessment, including manual and tool based approaches. No matter what methodology is chosen, URM recommends that three basic steps are taken.

1. **Identification**

   Before any levels of risk can be analysed and evaluated, a ‘picture’ of risk needs to be built up. There can be no benefit from trying to implement security controls if the business does not know what it is trying to protect and from what in the first place.

   In order to identify a level of risk (yet to be determined) organisations need a sound understanding of:

   - Their information **Assets** and values
   - **Threats** to these assets

© 2016 Ultima Risk Management Ltd

- **Vulnerabilities** within the assets.

The first thing to do is ascertain the information that needs protecting and determine how important those assets are in terms of their confidentiality, integrity and availability to the business. Or, to put it another way, what would be the impact on the business if one or all of those three things were breached? The second aspect of identification is to understand where the information is held/stored/processed both physically and logically, what format the information is in and who has access to the information, both internally and externally.

Threats and vulnerabilities to these asset types, i.e. information (in all formats), premises, people, technology and suppliers can then be identified to determine the risk picture.

Threats come in all shapes and sizes and include everything from computer viruses, floods and fire, to user error, disgruntled employees and theft. Once the relevant threats have been identified, it should be determined if there are any vulnerabilities associated with them, such as no anti-virus systems in place, HQ being on a flood plain, no sprinkler system, lack of documented policies and procedures or insufficient locks on the doors. When the threats and vulnerabilities are understood, the likelihood that those threats will occur can be determined, based on an understanding of the defences already in place and local circumstance.

Obtaining a thorough understanding of our risk picture enables a comprehensive and robust risk analysis to be undertaken.

2. Analysis

Analysis involves understanding levels of risk and is determined by multiplying the **impact** of a security breach by the organisation's understanding of **likelihood,** taking into account the value of information (and supporting assets) and the threats and vulnerabilities identified during the previous stage of the risk assessment process.

Dependant on the scoring mechanism used, upon completing the analysis exercise, the organisation should have an understanding of the levels of risk associated to the information and supporting assets used to support its service delivery.

On a simple scale, the organisation will most likely have some high, medium and low levels of risk and can begin to evaluate what needs to be done to effectively assist in the management of risk. It is useful at this stage to state confidence levels for the risk scores identified, e.g. we are 99% confident that the level of risk associated with the flooding of HQ is 'high'. The justification for this confidence level is that the impact would be high (based on the value of the HQ) and the likelihood is high due to the fact that we are on a flood plain, we get flooded every year and the experts (Environment Agency) are themselves stating a high level of flood risk.

It is crucial that the organisation has confidence in the risk assessment results, therefore it is important that the appropriate knowledge is obtained to ensure we know enough about a particular threat or vulnerability, or is more research/expert opinion needed? Once we are confident that the risk level is accurate, then we can then move onto the next stage of evaluation.

3. Evaluation

The final stage of risk assessment involves evaluating the levels of risk found during the analysis element of the risk assessment process against the **risk appetite** of the organisation in order to determine appropriate risk treatment options needed, as well as priority for treatment.

Risk Treatment

Risk treatment follows on from risk assessment and allows the organisation to determine what can be done to address the risks identified. There are essentially four options.

- **Reduce / Modify -**The first and most commonly applied option is to reduce the risk by implementing more controls to reduce the likelihood, or the impact of the risk.
- **Transfer** -This typically involves outsourcing to a third party or taking out additional insurance. Accountability for the risk still remains with the organisation.
- **Avoid / Terminate / Eliminate** -The risk can be avoided by stopping the practice altogether
- **Accept** / **Tolerate** -The risk can be accepted.

The acceptance of risks must be done knowingly and objectively.

Risk Management

The information security risk assessment and risk treatment is part of the bigger 'Risk Management' piece. A core and essential tenet of risk management is the need for repeated risk assessments in order to allow organisations to manage risks as they evolve and appear. As time goes on, historical data can be added to the process allowing for assessments and treatments to become more accurate.

Another common pitfall for organisations is taking their 'foot off the gas' once the initial risk assessment has been conducted. Best practice suggests that to gain the maximum benefit, risk assessments are conducted on a regular basis, i.e. annually. They should also be undertaken if there are any changes, for example, new business processes, mergers and acquisitions, new information assets added into the mix, significant increase in security incidents or the emergence of new cyber or non-cyber related threats.

In summary, a risk assessment should be carried out to understand possible risks the organisation faces, actual levels of risk the organisation has and, taking into account the executive's appetite for risk, what action may need to be taken. Any significant change to the organisation's asset profile, threat landscape, maturity of controls, local circumstance and risk appetite should be a trigger to review and possibly undertake a further risk assessment to gain a new understanding of risk and what may or may not need to be done to enable effective management.

© 2016 Ultima Risk Management Ltd