PenTest magazine
Aud&Stand

The Information

Security Risk Assessment Security for the Enterprise

As the saying goes, nothing can ever be 100% secure and we all know that in practice security is always a trade-off between competing forces such as user requirements, cost, government regulations and the like. Risk management provides the overarching framework for this trade-off and one of the most fundamental parts of the risk management process is the risk assessment.

As the saying goes, nothing can ever be 100% secure and we all know that in practice security is always a trade-off between competing forces such as user requirements, cost, government regulations and the like. Risk management provides the overarching framework for this trade-off and one of the most fundamental parts of the risk management process is the risk assessment.

In this article I will cover how you can carry out a detailed Information Security Risk Assessment and deliver genuine value to the end business. This is a process that I, and others, have used with numerous businesses, across all market sectors, and has proven to be resilient and straightforward to deliver.

What you will learn in this article

- Why you need an information security risk assessment.
- The basics of carrying out an information security risk assessment.
- What you need to do with your findings.

Risk management for dummies

Risks are everywhere – when we cross the road, when we take a flight, when we eat sushi, we are taking a risk. We do this automatically, because throughout our lives we have taken on board the lessons of our parents, teachers and own experiences as to what risks are likely to happen and if so how much they will hurt us. We then weigh this up against what our benefit will be and decide how we will act (Figure 1). For most people, this becomes so much "second nature" it happens without any conscious thought.

This is risk management on a personal level and while it may not be perfect (accidents still happen), it generally serves people throughout their lives and enables them to reap the benefits of taking occasional controlled risks.

The same principle applies to businesses [1] whereby taking risks allows them to open up new markets, deliver better services, or just enhance the quality of their offerings. Any business that re-

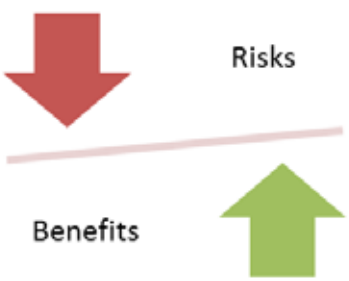

Figure 1. *Risk Management*

fuses to take any risks is certainly doomed to failure.

The difficulty is that what we are used to as part of our personal risk management process (look both ways before crossing the road) doesn't really apply to business decisions. When it comes to the risks around IT assets this problem gets even worse. Most enterprises comprising more than one or two computers develop complicated sets of risks based on factors that can frequently change from day to day. With the proliferation of smart phones connecting to the enterprise from potentially anywhere in the world, this risk landscape quickly becomes impossible to manage using our "normal" processes for day to day life.

As a result of this complexity, several international risk management standards have been developed over the years. Three of the most commonly known Information Risk standards are:

- ISO / IEC 27005:2008 Information technology – Security techniques – Information security risk management. (commonly referred to as ISO 27005)
- ISACA's Risk IT Framework
- The Open Group's Factor Analysis for Information Risk (FAIR) model

(In addition, the UK Government's Cabinet Office has published "The Orange Book: Management of Risk - Principles and Concepts" which covers a holistic range of risk management issues and is suitable for any organisation or enterprise).

Despite these standards coming from different interest groups in different countries, there is a common theme in what the approach to risk management should look like (Figure 2).

While the exact title of each step varies between the standards (for example, ISO 27005 uses the phrase Context Establishment to mean reviewing the enterprise to see what is where), this cycle pretty much forms the bedrock of any risk management approach.

When it comes to enterprise IT and other information systems, the Information Security Risk Assessment (ISRA) allows you to identify the risks you face and provides the frame of reference you need to analyse what this risk means to your business. Using the generic model above, the ISRA covers: "Review the enterprise", "identify risk" and "Analyse risks."

Carrying out an ISRA enables the organisation to properly manage its risks and, as a direct result, opens up routes for opportunities which may not have been known as well as giving warning of where the risks are too big, too dangerous or simply pointless. Proper risk assessments will also ensure that the resources spent on security are allocated in the way that best suits the organisation, not a 3rd party vendor or other unrelated entity.

Information Security Risk Assessments

What an information security risk assessment is (and is not)

An ISRA is a tool used to determine what impact changes will have to an existing environment. In an ideal world, the ISRA is used to enable risk managers to maintain a continuing level of awareness about what risks they face, however occasionally (especially in organisations with an immature risk management strategy) the ISRA can be used to drive a ground up understanding of the risks present.

The value of the ISRA is dependent on two main factors: the knowledge and skill of the person carrying out the assessment and the level of information available. An inexperienced or poorly skilled assessor is likely to overlook key issues creating an incorrect risk assessment and, likewise, even the most skilled assessor can only assess what is available. If key facts are withheld then the risk assessment is never going to be correct.

In any risk management setting, an incorrect assessment is frequently worse than no assessment at all and is likely to lead to costly mistakes. Recently, while consulting with a large blue-chip cli-

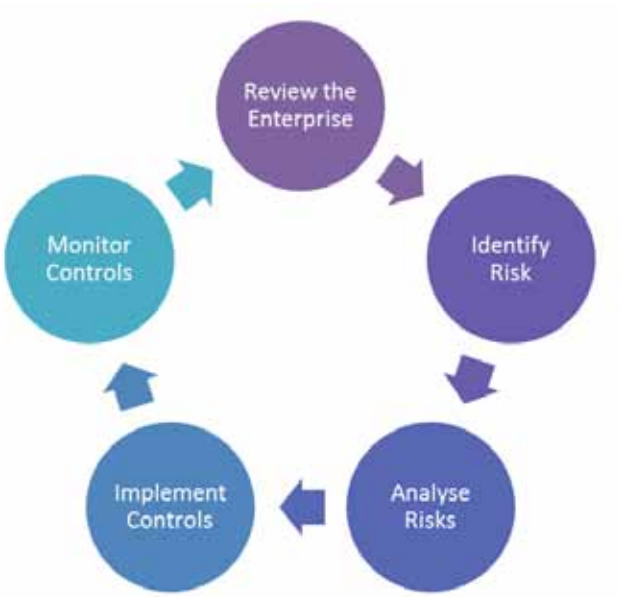

Figure 2. *Generic Risk Management Cycle*

ent, I discovered that the majority of their problems stemmed from decisions which had been based on a terrible set of risk assessments. As a result of this, they had spent outrageous sums of money on unnecessary security controls and were still suffering significant breaches because the real risks they faced had been ignored.

With this in mind, it is important to be aware that an ISRA is not a substitute for detailed testing of the environment; rather it complements and drives the testing requirements. An ISRA is also not a substitute for security controls, instead it is the first step of the process allowing Security to determine where best to apply controls and where they aren't cost effective.

The majority of organisations where I have delivered an ISRA have had the sense to back this up with a penetration test to verify the controls. The ISRA has proven to be invaluable in defining the test scope, and for two recent clients has enabled them to save thousands over the initial suggestions of the testing company.

The final point to always keep in mind is that all risk assessments are subjective to at least some extent. Even the best will never be perfect and, a fundamental principle that every organisation has to realise is that even very low probability risks occasionally occur. Nothing is ever totally secure and no possible risk is ever totally mitigated.

Figure 3. *Six steps*

How you conduct an information security risk assessment

The specifics of how you carry out your risk assessment will vary between organisations and risk assessors, but there are six fundamental steps (Figure 3) that should always be part of your process. When it comes to developing your own risk management strategy, these steps should all be addressed in sequence.

All of this assumes you are working within a clearly defined scope and the term asset is used here to describe the target of your risk assessment. In practice this can range from small tasks like an email server changing operating system, to large scale projects where a new global enterprise resource is being deployed. For organisations new to risk management, the initial assessment may well be "everything" but it is crucial that the scope of assessment is agreed beforehand.

Step 1: Engage key stakeholders

The first step of the ISRA is to determine who in the organisation has vital roles regarding the assessment and ensure that you have proper buy-in for the task to work. For most enterprises, where Information Technology assets are being assessed, the principal roles are:

- *Senior Management*. As with all security processes, senior management buy in is totally essential. It is possible that your assessment will uncover painful information about the state of the enterprise and the risks you identify will need to be managed properly. Without senior management buy in, the risk assessment is compromised from the outset and should be abandoned.
- *Information Asset Owner (IAO).* This is the person within the organisation who is responsible for the assets being assessed. If this is an en-

terprise wide assessment, this is normally the IT Director or equivalent, however, if this is an assessment of a particular application or infrastructure change, then it may have a localised owner. The IAO needs to be responsible for ensuring you have access to relevant technical documentation and that the assessment is properly resourced.

- *Technical Contacts*. The information security aspects of the ISRA mean that there needs to be detailed technical information available. Ideally this is in the form of technical documents (often called "High Level Designs", "Low Level Designs" and "Infrastructure Solution Designs") which detail things like interfaces, data flows, network paths etc., but in smaller organisations this may only be available by talking to the technical managers.
- *Security & Policy*. Unless the ISRA is taking place in a completely new environment where no security has been considered previously, it has to take into account existing security controls and policies, so security involvement is essential. At the most basic level, existing security policies set the environment which the assessment is comparing changes to. Without these, the assessment has to fall back onto an agreed standard – such as ISO27001 or the ISF Standard of Good Practice for Information Security.

In some organisations, especially within the small – medium enterprise sector, several (or all) roles can be carried out by the same person.

The only role which routinely needs to be independent from the others is that of the risk assessors themselves. It is difficult, if not impossible, for an accurate assessment to be carried out by the person directly responsible for the management or implementation of the asset.

Additionally, cases where the assessor reports to any of the individuals above can cause doubts over the veracity of the details and in the organisation I mentioned previously for having a very poor risk assessment, the subsequent investigation discovered that the assessment had been carried out by an employee who directly reported to the risk owner, and had been given specific instructions as to what to report, rather than to assess. This must be avoided at all costs.

Step 2: Gather Information and Assess

This is the first "proper" stage of the assessment and involves the assessor carrying out a function similar to that of auditors. It is for this very reason that early buy in is required – remember no one likes auditors and it is very likely that the people providing you with information will be defensive. It is the assessor's job to overcome this and ensure that they have access to all the appropriate data on the asset being assessed.

The scope of the assessment will dictate what information is required but common artefacts are as follows:

- Technical diagrams [2]
- Data flow diagrams
- Configuration / Build standard documents
- User instruction guides
- Firewall rule sets
- Interface diagrams
- Encryption details
- User account requirements

As assessor, you need to make sure that you have enough information to properly understand how the asset works, how it interfaces with the outside world, how users use it, how it is maintained, and how it will be disposed of when it is no longer needed. If you aren't sure about something, make sure you ask.

Where the asset (or part of the asset) is looked after by an external party or outsourced to a service provider, this creates a new area of risk and, in most cases, should be subjected to its own ISRA.

Step 3: Identify Risks

Once you have collected all the information you need, the next stage is to review the documents to identify areas where risks are present. Remember, here we are using the guiding principle that a risk is something where there is vulnerability *and* a threat actor that can exploit that vulnerability – this means someone who is able to reach out and connect to the vulnerability and is likely to want to exploit it (Figure 4). As an example, if you are assessing an application on a computer with no external connections, XSS vulnerabilities are not likely to be a real risk [3], the vulnerability exists and there are people who would want to attack it (script kiddies looking to vandalise if nothing else), but there is no vector for them to mount the attack.

This step can often be the most time consuming as, initially at least, risks are everywhere. The emphasis now moves towards the risk assessor working with the stakeholders to determine what the organisation's baseline level of risk is.

Normally this can be identified from previous risk assessments, existing security controls and the current enterprise structure. Where these are available, the risk assessor should concentrate on areas where change is taking place to determine if this lowers or raises the existing risk profile.

However, frequently you will find yourself faced with the situation where there is no existing documentation or you are carrying out an enterprise-wide assessment. In these situations the best approach is to document all the risks you identify.

Step 4: Assess Risks

Once you have identified the risks (and this can be done either as you identify each risk or when you have created an overall risk picture listing all of them), you need to assess them to generate a prioritised risk management approach which will allow for mitigation (treatment) of risks where required.

The risk assessment process is probably the most important step and the one that requires the most effort and judgement. It is also likely to be the step which needs the most subjective decisions based on experience and collateral reporting.

Entire books are written on how risks should be assessed, and there is not enough space in this article to go into it in great depth, but the basic principle is that risks should be categorised based on the likelihood (probability) of them happening and, if they do occur, how much harm they will cause (impact).

At its most simple, the assessor should take the list of identified risks and grade each on how significant they are. The most common approach is to create a system which breaks these two variables down into a rating from 1 (lowest) to 5 (highest) then multiplying the two we get a "risk score" which can then be graded from very low (1) to very high (25). (See Table 1 for an example). This table shows a hypothetical risk assessment matrix for an organisation whereby it has been determined that scores 1 – 5 are "low risks", 6 – 19 are "medium" and 20+ is a "high" risk.

The exact details will vary by organisation, but it is good practice to retain three broad categories to assist risk management decisions later on. Frequently this will consist of requiring urgent mitigation for the red risks and being prepared to tolerate (at least for a period of time) the green risks.

Where possible, historical data should be used to grade the risks and this can come from a variety of sources, depending on the nature of the risk. Some examples for the probability assessment include records of how often attacks have occurred previously, how often natural disasters have occurred and similar. The impact should be business driven and can include things like how much revenue will be lost if an asset is taken out of service, how much a replacement will cost or how much a regulatory fine will levy against the organisation.

Unfortunately, there will be a lot of situations whereby a totally subjective judgement has to be taken as to how likely the event will be and how much harm it will cause. The reason for this is that you will frequently be identifying new risks for an organisation, meaning there is no existing baseline – this is the reason for the ISRA in the first place. In situations like this, the risk assessor should use a combination of professional judgement, published reports & metrics from other organisations and security resources (such as the Internet Watch foundation reporting), to form an informed position.

Risk assessments should be carried out for all identified risks, and the resulting information produces the overall risk profile.

Step 5: Determine controls

Once you have a finalised risk profile, it is important that you identify what controls exist and where

Table 1. *Generic risk grading table*

		Probability				
		1 LOW	2	3	4	5 HIGH
Impact	5 HIGH	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1 LOW	1	2	3	4	5

Figure 4. *What constitutes a risk*

there are no existing controls (or the controls are unsuitable), what controls are required.

Ideally the risks should be addressed in order with the highest rated risks first as it stands to reason that these are the areas of greatest importance.

When determining controls you should look for options that reduce the probability that the risk will occur or ones that reduce any resulting impact [IV] (see Figure 5). Occasionally controls will reduce both, but you should be wary if you are struggling to determine which aspect is reduced and not assume it will be both, as this is likely to result in you increasing the impact of the control over and above what it really delivers.

In selecting controls, you should always consider a wide range of options and not just fall back on the simplest technical measures and make sure you fully consider the business processes in use. There will be occasions when you get the "light bulb" moment and realise simply disconnecting a device from the internet controls most of the risks, unfortunately there will also be times when you need to build in a whole array of compensating controls to manage the risk.

If you are struggling to find good controls, review Figure 4 again and remember, all you fundamentally need to do is to knock out one step – fix the vulnerability or prevent the attacker getting access (it is normally very difficult to eliminate all threat actors, but in some circumstances you might be able to do this – however, the process for managing this needs to be subjected to a much more detailed assessment and is out of the scope for this document).

When you have determined the controls, you should produce a second risk score showing the effect the controls have on each risk – frequently referred to as the "controlled risk rating" or "residual risk score."

Under normal circumstances, controls should be added to each risk until the residual risk score reaches an acceptable level (i.e. a green score on Table 1). Where this is not possible for valid business reasons, the situation should be escalated to a suitable level of authority within the organisation to make a decision based on the needs of the business.

Where controls do not exist, or existing controls aren't suitable, recommended ones should be documented along with an implementation and verification plan. In this situation, the residual risk score should remain unchanged, but a note kept and when the controls have been implemented a new score assigned. Care should always be taken to ensure that the residual risk score is an accurate assessment of the current status rather than an estimate of the future – it is inevitable that problems, accidents and business pressures will warp any implementation plan.

Step 6: Report findings

The final stage of the risk assessment is to convey the business intelligence that you have gone to great lengths to produce to the relevant stakeholders. While this is frequently seen as a tedious

Figure 5. *Risk Reduction*

step, it can be the most important output from the ISRA process and, done properly, the risk reporting is what allows the business to benefit from the assessment.

It is important that the ISRA output report is presented in a manner that the business stakeholders can understand, and if necessary act upon. To this end, where an organisation has an existing risk reporting process, the ISRA should fit into this.

If one does not currently exist, the most straightforward way to present the output report is to provide an executive summary; recommended controls implementation & verification plan and a risk assessment table – in the manner of a risk register. This should break down the risks, and hopefully the enterprise will remain within the bounds of the ideal "risk pyramid" shown at Figure 6. If there are excessive medium and high risks, there may be a more fundamental problem that needs identifying and addressing.

It is always good practice to get formal acknowledgement of the output report from the relevant executives, and where risks remain outside the acceptable risk zone (e.g., amber on table 1 above), then this becomes essential to ensure that an auditable record of the risk treatment is maintained.

Every organisation will have a different stance over who is allowed to see the ISRA output reports and you should ensure you comply with this. Where there is any doubt however, you need to remember that this report identifies all the weaknesses present in the organisation and, if it falls into the wrong hands, can lead to significant compromises. As a result, it should always be considered a sensitive document, and if you are carrying out an assessment as a consultant, you must never allow one organisation's findings to be shared with another.

This may seem like the end of the process, but in a good risk management environment, the ISRA output will drive future assessments and, at the very least, assets should be re-assessed on a regular basis.

Summary

- The ISRA is a superb tool that enables you to provide an organisation with a rigorously carried out assessment of the risks their enterprise faces, along with an assessment of the state of controls. In turn, this process allows you to help the organisation drive changes and the ever-important "continual improvement" which underpins all good security regimes.
- The ISRA is a deceptively simple tool – there are six fundamental steps that need to be carried out, although the exact specifics will vary between organisations. If you ensure all six steps are covered off, you can be confident that your assessments are valid and accurate.
- For most security professionals, the interesting part is looking at what the risks are and how to control them but it is very important that you also make sure you document your findings properly and provide this information to the relevant executives in the organisation. This is doubly important when you have areas of risks that are uncontrolled or for some reason remain significant.
- Security controls can appear complicated and sometimes people struggle to select the right ones, but if you use the ISRA to guide your choices you can be sure you have implemented the most cost effective measures for your enterprise.

References

[1] For the purposes of this article, I will use the term "business" interchangeably with "organisation" to mean any organisation, public, private, non-profit etc., that has a need for security advice.
[2] These can be variously referred to as "solution designs", "high level designs", "low level designs" etc. The exact term doesn't matter.
[3] While in most circumstances this would not equate to a real risk, you may decide it is still worth identifying this in case the utilisation of either the application or the machine change in the future. Normally this would be something decided between the risk assessor and the key stakeholders.
[4] If more detail is required, you can consider adding in an additional dimension of controls documenting ones which treat the risk (reduce probability or impact), transfer the risk to others or eliminate the risky activity (normally this means cease entirely). This level of risk treatment is out of the scope of this article.

TAROT "TAZ" WAKE

Taz is a Security and Risk Management Consultant, currently providing global IT security risk assessment services to a major Anglo-Dutch multinational.
With almost twenty years' experience improving the security posture of major global brands, government departments and the military, Taz currently runs Halkyn Consulting Ltd, a company that provides a full range of expertise in security and risk management consulting for organisations and individuals. He can be reached at t.wake@halkynconsulting.co.uk.