Business Impact Assessment

Does your organisation struggle to value information security?

Do you have problems justifying investment to manage risk?

There is a common misconception by some CEOs and Boards that security has no tangible return on investment.

Business impact assessment is the process of understanding the value of information assets in a structured way, using a graduated scale defined in terms the business understands.

Assets are valued in collaboration with the business, helping the wider business to understand and get involved in managing information risk.

This drives better buy-in from the wider organisation, helps justify investment where required and also drives other positive business benefits such as identifying a catalogue of information that can be re-used, improving efficiency.

The Business Impact Assessment essentially defines the impact of a compromise of Confidentiality, Integrity or Availability (C, I or A) of an information asset in business terms. The impact could be material, reputational, political, or life-threatening, but will always have a financial aspect whatever your business.

The objective of the BIA is to obtain business ownership and agreement of the BIA and effectively communicate to all stakeholders the potential business impact associated with the business or system and its ability to continue to perform its business function.

This supports the effective management of information risk, which should be a key governance process in today's information-driven age.

Failure to conduct an appropriate BIA will mean misguided business expenditure by under or over mitigation of relatively unsubstantiated risks, failure of the business to buy into the process of managing information risk, or successful compromise of valuable information assets through failing to properly identify the items that need protecting.

First, some basics:

Information, in its simplest term, is the basis of competitive advantage.

An **Information Asset** (information, IPR, hardware, software, etc) has **Vulnerabilities** (weaknesses), which are endangered by **Threats** (a possible way in which an asset can have its security requirements breached).

Confidentiality is the property that information is not made available or disclosed to

unauthorised individuals, entities, or processes.

Integrity is the property of safeguarding the accuracy and completeness of assets - this may include the ability to prove an action or event has taken place, such that it cannot be repudiated later.

Availability is the property of being accessible and usable upon demand by an authorised entity.

Threat is the possibility of a harmful event.

Threat Actor/Agent is a person/group or thing that is likely to inflict a harmful act.

Threats should be further analysed to consider likelihood that a harmful event will occur, the likely impact that a particular harmful would have, and the motivation that a Threat Actor/Agent has, or may have, to inflict that harm.

Information Risk is perceived as a threat of compromise to the C, I or A of Assets (or Resources) and is defined as a combination of Threat and Vulnerability.

These components are at the heart of a BIA.

The BIA in Context

A BIA can only be done in the context of your business. For example, in a government or Ministry of Defence (MoD) environment, information has seven Impact Levels (IL) - 0 to 6.

As far as Confidentiality is concerned, these ILs can be easily calculated in line with the potential harm that the loss/theft of an item of information could have. Often these ILs can increase depending on the amount of information at stake – known as aggregation.

In the case of Integrity; an IL must be derived from the possibility of an information asset or resource being corrupted. For example, in the case of a communications link between the Battle Group headquarters and the commander of a heavy logistics patrol; if an encrypted data message on that communications link was deliberately corrupted by a known threat agent, using known corruption techniques, and the received coordinates for a safe stop-over were a few digits out from those actually transmitted, then the whole patrol could be in for a long night (or worse). Equally, the Integrity of an organisations accounts, customer information, orders and invoices need to be protected. Arguably, an information asset isn't worth keeping unless its Integrity is adequately protected!

In the case of Availability: What if the military communications link was totally disabled? Or what if a leading online auction website were to be taken offline?

The IL needs to be balanced though; the difference between a compromise resulting in, for example; undermining of the financial viability of a number of UK small businesses, as opposed to; major, long term damage to global trade or commerce; could mean all the difference when proposing solutions to guard against this type of compromise at the national infrastructure level. Although in private sector business terms, the disruption of a local area network server may be critical to the business and so should be allotted the respective business impact level.

In a business context, where financial profit is the driver, business impact levels may be much more granular and the loss of an information asset or resource should ideally be given a monetary value, thereby providing a 'quantitative' estimate. This is usually based on the cost/time to fix or replace a specific asset in order to resume normal business. Confidentiality should not be ruled out though; businesses dealing with personal data, even employee data are subject to the Data Protection Act and the Freedom Of Information Act. Breaches of this legislation could mean substantial fines from the Information Commissioner; of course the loss of client-owned data could be devastating to your reputation and your business. Furthermore, the loss (or theft) of, for example, a bid document for the next £1M/B contract, could mean losing out to a competitor.

Government, local authorities, MoD and other similar organisations, usually prioritise the Confidentiality of an information asset ahead of its Integrity or Availability. Regency ITC understands that the needs of plant equipment or SCADA networks as control communications moves from analogue to digital, reverses the typical order so that the priority becomes Availability, Integrity, Confidentiality.

Regency ITC has worked with partners to develop risk assessment methodologies that are tailored to the needs of SCADA networks, and that are simple to use, presenting results in business language. We have also developed the first active defence methodology, partnering tried and tested plant-proven security devices with malware

defences designed to target SCADA based threats. Contact us to find out more.

Board Level Support

The BIA must have Board-level support, as only the Board will truly know the business strategy and therefore the significance and value of each information asset and resource. In some instances cooperation may be required down at the technical level to derive a value for specific items of technology or component parts, but the largest part of this assessment must be supported by top-level decision-makers.

BIA in Brief

Identify Priorities

The first BIA task is to identify your business priorities; deciding on what business processes that if obstructed would slow or cease your business output. An ideal method, but not always possible in less mature businesses or systems, is to consider an outage from a time-criticality perspective. So if a particular process is affected for 30 minutes, you would calculate how much this 30-minute outage would cost you. Furthermore, you would derive a maximum time a business process can be inoperable without causing irreparable harm to the business. These processes and their time-factors would need to be listed throughout the scope of the business (or project). This task is best done by specific business area representatives. When all business area representatives have concluded their priorities, then a master list should be configured through the entire business (within scope). Some heads of small but mature businesses may be able to put this information together over their morning coffee!

Threat Identification

Next, you will need to consider all the threats posed to the business. The threats should be considered in the human or non-human form and with implementer and aggravator capacity, such as:

- Threat to valuable intellectual property, from commercial competitors, organised crime and more.
- The threat of 'hacktivist' activity following a new wave of on-line protesting which have lead to harmful denial of service attacks or successful hacks and embarrassment to companies.
- Organised criminals or an opportunistic intruder - in this case, the former could encourage or support the latter;
- Amateur or opportunistic hackers, with their own kudos goals, or committed hackers funded by large antagonist organisations;
- 3rd party organisations, or individuals, employed to conduct specific tasks on behalf of the business, but instead making a profit from their unsupervised activities[1];
- Insiders - the very personnel employed to operate or support systems or information you need to protect. Again, these threat actors could be persuaded to cause harm, or remove sensitive information by competitors or others;
- Government systems are threatened by more strategically-focused foreign organisations;
- The weather, or weather-based threats, such as storms, blizzards, floods, etc;
- Local or national power failures.

Threat Assessment

You will then need to consider threat capabilities and, where relevant in the human form, motivation levels. Don't for one moment think that because yours is a small business with what you may believe to be little to offer a would-be hacker that they won't attack you. Hackers go for the path of least resistance[2]; why would they try to penetrate GCHQ if they knew it would take years to find a route in to an ever-evolving security profile, when they could target lots of small businesses with poor security at their logical perimeters providing them with a reliable regular income, or an adequate degree of satisfaction.

Likelihood / Risk Assessment

The risk assessment should include the level of impact that a particular threat would have on a particular business process or processes - remember this may increase if the threat actor is influenced by an aggravating source.

You now need to add some realism to the BIA by putting the risks into context. Consider the likelihood that, as examples:

- A tsunami will engulf your middle-England facility compromising the Availability of all your business processes.
- A brand-new employee on the IT Administration team drafted in by

[1] http://www.ico.gov.uk/news/latest_news/2012/nhs-trust-fined-325000-following-data-breach-affecting-thousands-of-patients-and-staff-01062012.aspx

[2] http://www.informationweek.com/smb/security/how-cybercriminals-choose-their-targets/240007409

international recruitment with no previous professional or character references or screening will attempt to compromise the Confidentiality of your business information.

Only now can risks be prioritised and appropriate treatment implemented.

Regency IT Consulting

Regency ITC has a great deal of experience in performing BIAs as part of the Information Risk Management (IRM) and Business Continuity Planning (BCP) process for public and private sector organisations. We can provide you with tailored assistance with as much or as little involvement by you as you require. Once your BIA is finalised we can then assist you with an appropriate risk assessment and treatment plan. If required, this would be the basis for submission for accreditation or certification (ISO27001, PCI DSS, etc).