Components of Information Risk

CESG, the National Technical Authority for Information Assurance, has a number of definitions for Risk, the simplest being: '*A particular combination of **Threat**, **Vulnerability** and Impact.*' Although this is expanded in another instance to include: '*The probability or likelihood of an attack succeeding or of damage being sustained as a result of compromise to an **Asset**.*'

It's the combination of **Asset**, **Threat** and **Vulnerability** that form the **Risk** triad, together with their major sub-components that this document seeks to summarise.

The ultimate aim of Information Assurance is to eliminate, or to reduce to an appropriate level (to within 'Risk Appetite'), one of these components.

- If the Asset is removed the Threat will be void of an objective and so there is no Risk.
- If all Threats were eliminated, then the Asset would not need to be protected against them.
- If the Asset were attack-proof (void of all vulnerabilities), then the Threat's compromise methods would be useless.

Asset

The Asset is your information; or the information system, which stores or processes it. The information can be Intellectual Property, research and development analysis, Government protectively marked, or personal data (as defined by the Data Protection Act 1998). Information may be open-source, but the simple fact that your organisation *needs* that information may be sensitive in itself. Information can be IT-based, in transit on a communications bearer, on portable electronic or optical media, or within a hard-copy filing system. Your organisation's information assets are what make your business tick. If that information were to become known to a competitor or journalist your business would potentially suffer to the competitive edge or may become the topic of an unwanted media campaign, as such, it needs to be protected.

The degree of protection that you afford that information, to provide you or your stakeholders with a proportionate level of security assurance, is known as Information Assurance.

Criticality

Criticality is based primarily on the security principle of Availability – an interruption in the Availability of a specific information asset or business process could have negative consequences on an organisation's effectiveness.

Furthermore, the security principle of Integrity is also a factor. If the information asset or business process were affected sufficiently to cause a false output, then this could also have negative consequences to the organisation's effectiveness.

The above terms 'could' and 'negative' will need to be measured in the context of the organisation, the asset, and the time-scale for which it is affected.

Criticality Assessment

Defining the relative criticality of information assets is an essential Business Impact Assessment (BIA) step in an organisation's Disaster Recovery (DR) and Business Continuity Planning (BCP) process. For example, if the operation of an information asset, for instance your email application, were to be disrupted (or corrupted) for one hour during a normal business day, you will need to calculate the expected impact (loss of revenue) that this disruption would have on your organisation. Disregard for the time-being how much it would cost to fix or replace, and also the fact that in this particular case that you could probably employ alternative methods for certain communications, these are mitigation measures that you'll get to later once you have the hard figures in front of you. Once you've calculated the impact over one hour, calculate the impact for a full working day, then for a week, and a month. The increase in time may be more than a matter of multiplication, business-critical events that occur weekly or monthly for instance will have an impact on the longer term calculations, or you may have a special marketing event January through to April during which the Availability/ Integrity of particular systems may be of upmost importance.

Of course, revenue is one factor to consider, but also take into account the impact on your reputation, relationships with business partners, sponsors, etc. Ask yourself how these 3rd parties would view, with this particular example in mind, not being able to communicate with you over email for a specific period. Consider if they would appreciate that systems need to be taken offline for an hour or so, say for security updates (which may be considered by some as a normal and important business process). Then consider their perception if the outage were drawn out over a week or more, and finally, if you were unable, for example, to transfer key flyers during your marketing event.

Once you've conducted this exercise for all of your information systems and business processes you could then consider applying Criticality Levels (CL) to each information asset.

Criticality Levels can be used to gauge the impact of any disruption to an information system, or exploitation of any information they contain. Their purpose is to help in deciding where security resources can be most effectively applied. While it may only be possible to assign a single CL to an entire system, it will sometimes be preferable to establish CLs for each of its constituent services and infrastructures.

The following are four adapted CLs, which are described in decreasing order of impact.

Criticality Level 1 (CL1)
Systems where the impact of any disruption or exploitation of any information they contain would cause *exceptional* damage to your organisation.

Criticality Level 2 (CL2)
Systems where the impact of any disruption or exploitation of any information they contain would cause *serious* damage to your organisation.

Criticality Level 3 (CL3)
Systems where the impact of any disruption or exploitation of any information they contain would *materially* damage your organisation.

Criticality Level 4 (CL4)
All other systems.

Impact

When considering the impact of a risk to an information asset, organisations must consider both direct and indirect impacts. Whilst the realisation of a risk may not impact directly on the organisation, for example, as an explosion at your main operating station might, instead it may indirectly impact through third party services, staffing levels or supply chains.

Take the Swine Flu pandemic of the summer of 2009 for instance; in an attempt to weigh up the potential costs to the UK economy, in mid-

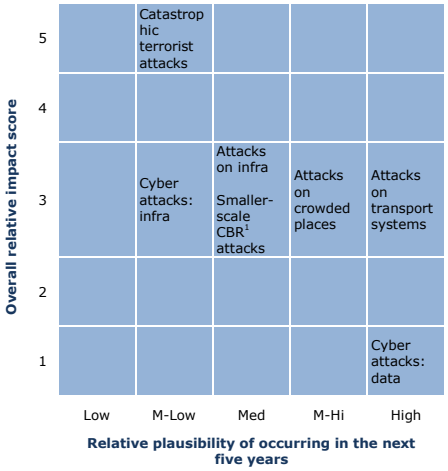
flow of the pandemic, the government suggested that up to 12% of the UK workforce could have been off work because of illness during the peak weeks. Of a workforce that is normally absent once every 30 working days, the figures protracted at the peak of the pandemic were an additional 10 working days. Analysts expected school closures, which would have had the knock-on effect of parents staying at home to look after their children. Of course with any pandemic, employees who may not have actually contracted the disease may err on the side of caution and stay away from colleagues and fellow commuters in order to minimise their ~~and~~ chances of becoming one of the statistics. This type of risk, however, can be reduced for some IT-based roles, where a well-practiced home-working policy is implemented.

Another example of an indirect impact would be an affected supply chain by a local or national incident in the vicinity of a third party supplier. This risk may be mitigated by having a number of alternative suppliers in widespread locations.

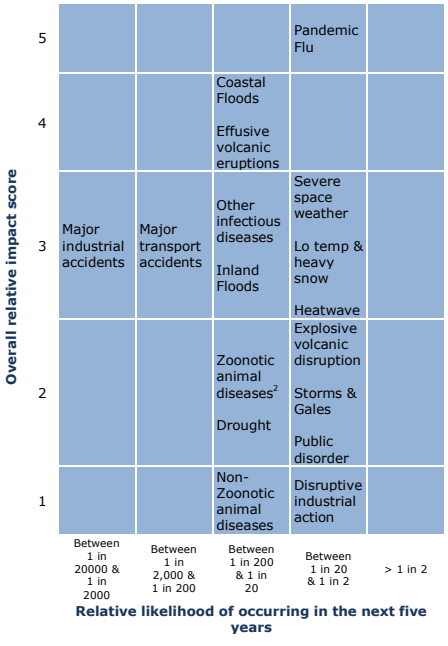
The Cabinet Office National Risk Register provides an assessment of the most significant emergencies which the UK and its citizens could face over the next five years, summarised into three categories:

- Accidents;
- Natural events (collectively known as hazards); and,
- Malicious attacks (or threats).

January 2012's National Risk Assessment is summarised in the tables below. The first table shows *risks of terrorist and other malicious attacks*. It shows attacks on transport systems and cyber attacks as the most likely risks to be realised.



The next table shows *risks of natural hazards and major accidents*. It shows the most serious impact coming from Flu Pandemics, the impact of which only marginally outweighs the likelihood.



[1] Chemical, Biological & Radiological.
[2] Zoonoses are infections and diseases that are naturally transmissible between vertebrate animals and humans.

Threat

CESG define Threat as: '*A potential cause of an incident that may result in harm to a system or an organisation.*'

A reasonable presumption to make is that you will not be *threatened* by a human Threat Source/Actor before an attack is attempted; human attacks on information are usually of a surreptitious nature.

Other relevant CESG definitions for a Threat Source and Threat Actor are as follows:

CESG define Threat Source as: '*A person or organisation that seeks to breach security and ultimately will benefit from the breach in some way.*'

The benefit gained by the Threat Source can vary drastically, whether the intent is to use the ill-gotten information to gain international military supremacy over a rival nation; for a corrupt journalist to grab the latest scoop; or a close competitor seeking bid proposal information with intent to undercut.

CESG define Threat Actor as: '*A person, or group of people who are in a position to exploit a vulnerability. The threat actor is a person who actually performs an attack or, in the case of accidents, will cause the accident.*'

A Threat Actor's intended gains may be more personal. One Threat Actor, which may be overlooked as a likely attacker to an organisation's information assets is the employee (or User). Employers often think that employees have the same goals as themselves; to build the company and make substantial profits. Employees may have their own goals less tuned to

the advancement of the company. They could have intent to illicitly profit from the company in their own right, or even have malicious objectives set on its demise. Additionally, attitudes can change and malice cultivated; individuals once loyal may change their allegiances if sidelined for a promotion, if dissatisfied in their role, or if they've become disaffected with somebody in their reporting chain. Users with Administrative privileges (Privileged Users) pose the greatest threat and so a great deal of consideration should be given to whom you employ in those roles. Their access to information, types, amounts, should be given a great deal of thought.

Employees are one thing, but how much trust do you have for the other members of the Board? Logical separation of duties throughout the organisation is the best approach (for example denying the Finance Director access to R&D analysis).

Local crime rates and environmental issues should feature as deciding factors in your risk assessment, although consideration should also be given to those with a national and even international footprint – e.g., cyber criminals (hackers).

Measurement of Threat

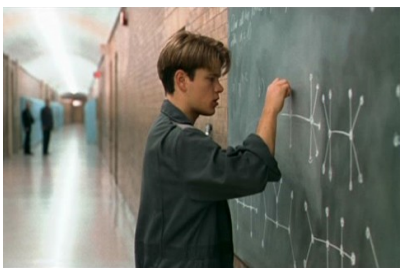
All relevant Threat Sources and Actors should be considered in your risk assessment including their Capability, if they are Motivated in any way, and the Probability or Likelihood of their attack. All of these need to be determined in the context of your organisation's information assets. Threat information may come from:

- knowledge within your industry;
- from the press;
- via Community Risk Registers compiled and updated, with scoring scales produced by the Cabinet Office, by Local Resilience Forums, and;
- the Centre for the Protection of National Infrastructure (CPNI), who specialise in sharing UK-generic threat information between government and industry with the aim of maintaining national cyber security.

This information would serve to influence your own tailored in-house Threat Assessment, whether that's for a simple standalone information system or a multi-national organisation; conducted by your own internal suitably qualified personnel or you may contract a specialist organisation, like **Regency IT Consulting**, to undertake a comprehensive Threat Assessment specifically on behalf of your organisation.

Capability

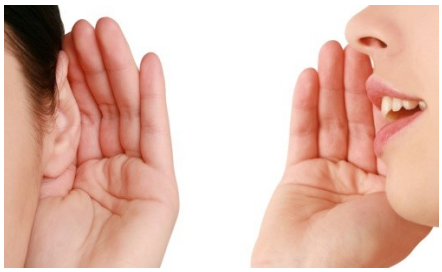
Capability ('*to exploit the flaw*') is the degree of ability to mount a technical attack. It is dependent on factors such as skills, knowledge and access to resources. For example, consider the Capability of your IT Manager against that of your Cleaner. Factors to consider are their access to information assets and technical expertise. Although the Cleaner may partake in more technical pursuits in his spare time!



Vulnerability

CESG define Vulnerability as: '*A security weakness that may allow realisation of a **threat** to compromise an **asset**.*' The US Department of Defense (DoD) Software Protection Initiative (SPI) defines System Vulnerability as: '*The intersection of a system susceptibility or flaw, access to the flaw, and the capability to exploit the flaw.*'

As long as you are providing access to your information assets then you must assume vulnerabilities are present in your systems.



When you allow an employee to remove information (for instance a document or a Laptop) from the protection of your organisation the information is susceptible to surveillance or theft including; from the employee himself, who now has unfettered access to the information meaning he could make copies, etc. If you allow an employee to access your network from a remote location (their home, or another site) your network will be susceptible to attack from anywhere in the world via the internet. Vulnerabilities can be reduced, for example documents could be carried in a locked briefcase, and illicit access to information on a stolen laptop could be hindered by encryption (file or full disk). You could employ a Virtual Private Network (VPN) infrastructure for remote access to your information. With Availability

in mind, what if an employee (accidentally or otherwise) deletes all the information from your corporate share drive. This is a vulnerability that could be reduced by minimising types of access privileges, or by incorporating a backup strategy to recover from such a disruption.

Exposure

Another tangent of Vulnerability is Exposure (‘*access to the flaw*’). Exposure could be a measure of Vulnerability, but is also the period of time for which the Vulnerability exists. For example an unencrypted laptop holding sensitive information is vulnerable to external Threats whilst in transit (during the daily commute, etc). The Vulnerability is likely to be reduced once the device is taken inside a secure office or home.

Regency IT Consulting

Regency has a team of very experienced Consultants that specialise in information risk management in both the public and private sectors. Our consultants working within your organisation will establish or improve an information risk management regime tailored to meet your business requirements.

If an organisation simply wants to assess its security profile for its own or its stakeholders’ peace of mind, Regency can conduct bespoke risk assessments and provide guidance on risk treatments in line with the business need and risk appetite.

Where necessary, Regency ITC can employ a fully automated information risk management tool, CiticusOne, to assess an organisation’s extant security controls against compliance with the relevant policy and standards (e.g., Security Policy Framework, Privacy Impact Assessment, JSP 440, Information Assurance Maturity Model, ISO27001, Sarbanes-Oxley, CoBit, SCADA, etc). Other standards bespoke to an individual business area can also be utilised.

The use of Citicus will not only reduce the time it will take for the security practitioner to carry out the information risk management process, but will also reduce the costs of maintaining a real-time effective information risk management regime that once adopted can be updated on demand when the threats, vulnerabilities, scope, etc, change.

As the sole UK-based implementation partner, Regency can host and manage CiticusOne in our ISO/IEC 27001 Certified secure data centre and also provide the expertise to carry out independent evaluations. We can also arrange the training for personnel to use the software to maintain and update their risks and actions by using our hosting service via secure HMG VPN encrypted connections.

IS 548043