



YOI-YIO: Contextual Risk Analysis

Document Version V1-1

Document Set: **QCC Risk Methodology**

Date 07/11/2008

Prepared By Neil Hare-Brown



Document Control

Change History

Version	Date	Name	Revision Description
V1-0	2008	N. Hare-Brown	Original Version

Approbation

Version	Date Approved	Approver	Position
V1-0	October 2008	CEO	Executive Committee

Distribution List

Name	Title
All internal staff (inc long term contractors, temps or consultants)	
Customers	
Industry Analysts	
Academic Partners	

Related Documents

Document Title	Date	Revision	Author
An Introduction to FAIR (draft)			Jack A. Jones
IS calcs (UK HMG) – Restricted			



YOI-YIO: Your Outside [looking] In – Your Inside [looking] Out

Contextual Risk Analysis

Introduction

This document describes an approach to risk analysis which gives a new (or perhaps simply a clarified) view of risk. This view is one that is both natural and contextual and it flies in the face of over complicated and over simplified analysis methodologies that do not seem to give a realistic, accurate or scientifically accountable picture of risk.

The major problems with risk assessment and analysis at present are;

- The terminology is confused and all-to-often misused; even by experts, with terms being used out of context and often not properly defined.
- The factors making up risk are misused by the security product industry as sexy selling terms and very few products actually use terms correctly in their literature let alone embrace them correctly in their functionality.
- Many sources claim to have determined risk when analysis of such determinations shows that calculations have not been made or are extremely simple. Quite often the vital factors required to complete formula and derive risk are missing. Examples include risk determination which excludes asset value and determinations that claim risk to be the inverse of control compliance.
- The two camps of qualitative and quantitative risk analysis supporters spend more time in critical analysis of the opposing approach than they do in positive critique of their own. Mother Nature knows better! She has had millions of years of practice and has found that risk assessment by experience (a combination of qualitative and quantitative analysis) always gives more reliable results.
- The realistic appreciation of time is underused in risk analysis. Risk is often presented in terms of possibility as opposed to probability and as you can see from the definition below, it is probability which is a key component of effective risk analysis. Time, or rather chronological timeline, is also the ether in which risk exists; assets vary in value, controls degrade, impacts vary, threats become more or less prevalent. Many risk analysis methodologies fail to adequately appreciate all of the time factors that matter and that risk is fluid because of time.

What is YOI-YIO (simply pronounced “Yo-Yo”)

The YOI-YIO technique is a way of building up realistic models of both specific and overall risk to which assets are exposed in a 2-stage process of analysis; one of **exposure** and the other of **cover**.

The process is modelled using natural thinking and by arranging the various risk objects such as assets, threats, exploits, impacts and risk treatment techniques incorporating vulnerabilities and controls, in the correct context as follows;

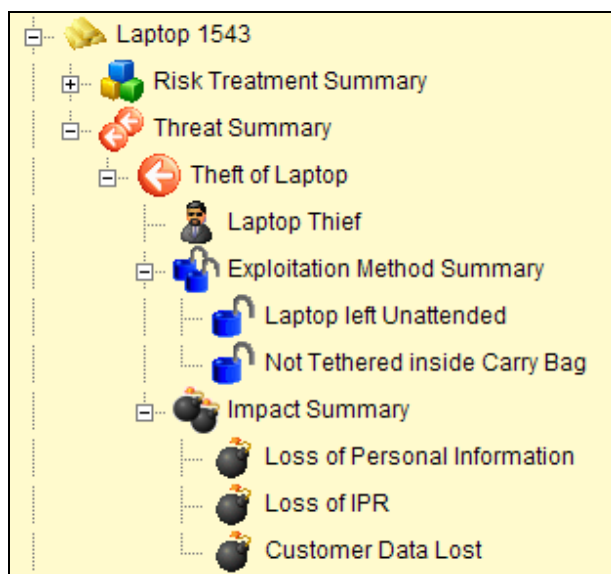
1. Assets are *exposed* to Risk.
2. Assets have *value*.
3. Threats are the “Potential to cause Harm”
4. **One or more Threats can act on an Asset.**



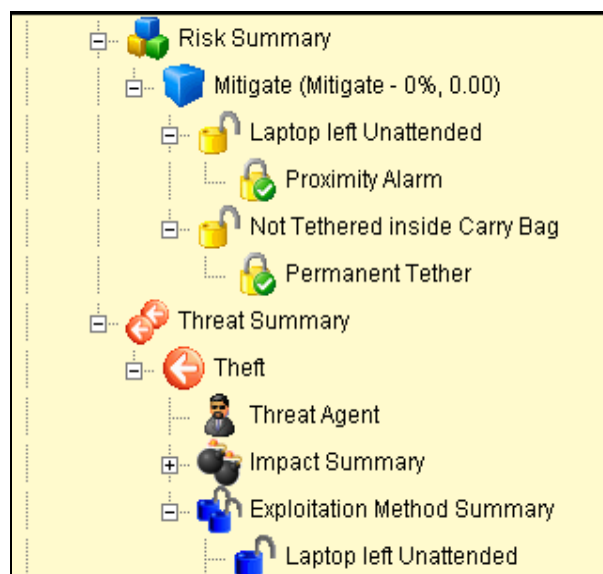
5. Each Threat has a Threat Agent (representing a person, natural phenomenon).
6. Threat Agents possess an *intent* to drive the Threat to be *realised*.
7. **Threat Agents use one or more Exploits.**
8. Threat Agents have varying *capability* to *execute* each Exploit.
9. **Realised Threats result in one or more Impacts¹ on the Asset upon which they act.**
10. An Impact can be a *primary*, *secondary* or *tertiary* loss.
11. Risk is the *probable frequency* and *probable magnitude* of future loss².
12. Risk can be *experienced* when all the objects in a risk model move from potential occurrence to actual occurrence i.e. in an incident.
13. **Risk can be treated with one or a combination of 4 methods** which will reduce or *cover* the probable frequency or probable magnitude of future loss;
 - a. **Risk Reduction** or Mitigation: The process of *addressing* Vulnerabilities with Controls.
 - b. **Risk Transfer**: The process of agreeing for a 3rd party to take the risk.
 - c. **Risk Avoidance**: Avoiding use of the Asset in the way that was planned.
 - d. **Risk Retention**: The process of accepting or tolerating risk i.e. accepting the Impact(s) should Risk be *experienced*.
14. When risk treatment methods are initially applied, the calculated risk value can be seen as a resulting *exposure* or *cover*.
15. Further rounds of risk treatment should ideally result in a null value called the RTSS (Risk Treatment Sweet Spot).

Here is an example of a simple risk model using objects “in-context”.

Exposure Analysis Half (YOI)



Cover Analysis Half (YIO)



¹ The Impact might result in a loss which is negligible all the way to considerable.

² Definition taken from an Introduction to FAIR by Jack A. Jones



YOI-YIO Risk Models are built in trees which mimic the correct³ context; outlined in bold text above. As the models are built the Risk is calculated using the following formula;

$$\text{Risk} = \text{Threat} \times \text{Impact} \times \text{Vulnerability} \times \text{Likelihood}$$

In order to complete the factors needed by the formula, YOI-YIO uses objects to describe each of the factors (or those that make up each factor such as Threat = Intent x Capability) described above and a set of metrics to describe the properties for each object as follows;

- **Assets** – Name, type and monetary value
- **Threats** – Name and type
- **Threat Agent (describing Intent)** – Name, Options (Natural Force, Man-Made, Structured, Hostile), Reason, Maturity, Trust, Motive and Estimated Attacks per annum.
- **Exploit (describing the Capability of a Threat Agent)** – Name, Type, Experience⁴, Skill, Qualifications. Instinct.
- **Impact** – Name, Type and [the affect on the Asset in terms of loss of] Confidentiality, Integrity, Availability, Accountability and Collateral Damage
- **Risk Treatment - Reduce** supporting;
 - **Vulnerability** – Name, Type, CVSS: Access Complexity, Authentication, Access Vector; Distribution, Exploitability, Remediation Level, Report Confidence and Experience²
 - **Control** – Name, Type and [the effectiveness terms of preventing a loss of] Confidentiality, Integrity, Availability, Accountability and Collateral Damage in relation to the Asset.
- **Risk Treatment – Transfer** supporting;
 - Supplier (to whom the risk is transferred)
 - Amount transferred as % Asset value and/or fixed amount
- **Risk Treatment – Accept** supporting;
 - **Risk Owner** (who accepts the risk)
 - **Amount** transferred as a % Asset value and/or fixed amount
- **Risk Treatment – Avoid** supporting;
 - Name and Amount avoided as a % Asset value and/or fixed amount

³ See the section YOI-YIO: A Natural Way of Thinking

⁴ Data fed into the process from recorded risk experience through incidents i.e. empirical data



YOI-YIO: A Natural Way of Thinking

The contextual arrangement of YOI-YIO risk models is crucial to their success and there is nothing revolutionary to this design. It is born from the common sense instilled into us by Mother Nature. An often subconscious arrangement of the components described above which enables us to understand the risk to ourselves and others and fundamentally to maximise our survival.

A contextual arrangement of entities or 'objects', representing the components of risk, which is performed by all life on earth, whether acting as predator or prey. Simply, it goes like this;

1. You have an asset – perhaps this asset is you?
2. Threats act on assets; therefore there is not much point in analysis of threats unless they act on the assets which are important to us. We determine that a threat may act on an asset by four methods of deduction;
 - a) We have an experience of the threat acting on our own assets (or ourselves)
 - b) We have knowledge of a threat acting on another asset (or person)
 - c) We can imagine or project a threat acting on an asset by morphing a known scenario and deducing from point a. or b;
 - d) We can use pure imagination; usually the stuff of science fiction.

The options a to d here are in order of confidence i.e. we have considerably more confidence that a threat will act on an asset in option a) than we do in option d). In nature a large percentage of non-human⁵ threat identification is only made through option a) and a small percentage (in some species) through option b) with options c) being the domain of primates and d) being exclusively the domain of humans.

3. Threats are driven by Threat Agents. Threat Agents can be seen as being either environmental or human in nature and can be described as comprising some degree of both Intent and Capability. Here are (just) some threat examples;
 - a) Tornados; total intent, capability varying depending on many environmental conditions.
 - b) Terrorist; high intent (although this may vary), capability based on skills and resources.
 - c) Thief; medium intent (driven by greed), capability based on available skills and resources.
 - d) Bad Driver; low intent (and even less thought), capability high based on lack of driving skills, awareness and speed and nature of vehicle.

There is also a probability aspect to threats and an important window where both the factors of Intent and Capability coincide to have contact with an asset resulting in threat realisation.

4. In YOI-YIO, Threat Agents possess intent and their capability is expressed through one or more 'Exploits'. Examples of exploits include;
 - a) The Sea exploiting coastal defences
 - b) A Hacker exploiting a buffer overflow
 - c) A Thief exploiting an open window
 - d) An Archer exploiting a hole in a battlement

⁵ Other animal and plant life



5. The key in YOI-YIO is the ability to apply perspective. The perspective of an attacker and that of a defender. It's an age old relationship that enables us to determine the vulnerability factor needed for our understanding of risk. It relies on a concept that an Exploit for an attacker is a vulnerability for a defender. The hole in the battlement is a good example of this concept.

When our minds are determining risk (which happens almost constantly in our subconscious), they are positioning first in attack mode and then defence mode. As children we begin to learn our ability to determine risk (in our regular environment) reasonably accurately through play, trips & falls and as we get older through sometimes higher impact experience, fights, car crashes, arguments.

Other life forms have similar experiences in often very different environments and timescales. It is interesting (and perhaps a reflection of the physical world in which we live) that we have developed a range of controls to reduce risk to our physical bodies but by comparison have only basic controls to mitigate emotional harm and are only just beginning to implement effective safeguards in the new and complex logical world of information technology.

6. YOI-YIO considers that an exploit from one perspective is a vulnerability from another. The two are like different sides of the same coin! And (just like a coin) each has different descriptors; an Exploit, as previously mentioned, describes the Capability of a Threat Agent. A Vulnerability however needs to be described from a defenders perspective and so we have adopted the Common Vulnerability Scoring System (CVSS) as a suitable set of metrics.

7. Assets have a degree of innate control strength⁶ and so just because they experience contact with a threat doesn't mean that harm will necessarily result, or if it does it may be negligible.

The assessment of risk in life forms on earth is passed down the generations as a determinant factor in their survival, referred to by many such as Richard Dawkins in his book "The Selfish Gene" as 'instinct', it is hard-wired into genes. Those species in which modifications occur which negatively affect their ability to assess risk soon suffer a well-known type of impact called "Extinction".

As described above, most day-to-day risk assessment in humans is not a conscious act just as it isn't in other life forms. In a way this is evidence of the primeval nature of risk assessment, perhaps it has been part of life since the beginning of life itself.

Time: The Elusive "Pimpernel" Factor

Although I have not expressly referred to time in the definition of risk it is actually the most important factor of all. Risk constantly varies over time as a consequence of probabilities occurring in both exposure and cover, i.e. our ability to treat risk.

To quote Jack A. Jones again, "Risk is not about possibilities but probabilities". If you conveniently take time out of the risk equation then it can be expressed as a possibility because given infinite time available any and every threat must be realised and every risk experienced.

This world of "possibility" is one inhabited by many who make their living as purveyors of products and services sold through conveyance of fear, uncertainty and doubt but it is not the world of the real security and risk professional.

Whilst it is true that we must never discount catastrophe but as we do not (apparently) live in a world of chaos where extremely high impact events occur with extremely high probability (thankfully they are in opposition) we must discount the "possibility" approach and adopt one which describes "probability" in a practical and contextual way.

⁶ Referred to by Jack Jones in FAIR as "Resistance Strength"



Probability as it Applies to the Factors of Risk

Literally every component of the risk picture has a time factor although through our qualitative analysis we generally automatically build time into the factors of our assessment.

To give concise examples let's start at the top;

Assets vary in value over time, they might appreciate or depreciate both as a general trend and at specific key points where they are particularly needed.

Threats can be extremely complex because their root causes may be numerous and each of these causes subject to a time factor. An avalanche for example, occurs as a result of many underlying factors; weight of snow, type of snow, atmospheric pressure, wind, gradient of slope, natural or man-made breaks, presence of sound. Each of these factors occurs or collides in a timeframe which may or may not be causal to an avalanche.

Threat Agents possess Intent. Human threat agents either singular or in groups, are subject to changes in their belief systems; faith, greed, pro-active defence which all may vary over time. Natural threat agents can be thought to have complete intent but are still maintained within a chronological straightjacket which determines their likelihood to drive a threat to realisation. An avalanche in the Alps, for example is unlikely to occur in high summer.

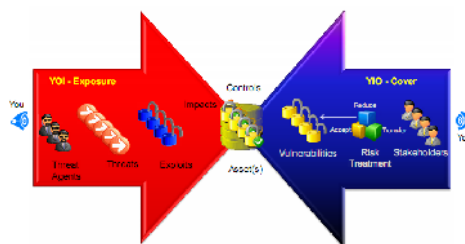
Exploits possess metrics which describe the Capability of the Threat Agent to use one or more exploits effectively⁷ also varies over time. The capability of a living threat agent will depend on recent experience over time and the ability they may have to employ previously successful or learned exploits. Non-living threat agents capability will depend on the alignment of certain natural phenomena which when aligned both physically and at the same point in time may cause the threat to be realised. In such cases intent and capability might be thought to coincidental (see incidence and coincidence below).

Impact is particularly subject to chronological variation. Jack Jones presented impact with clarity as primary and secondary degrees of loss. Primary being the impact recorded as a direct consequence of a single or combination of loss events resulting from an incident. The secondary impacts occur as indirect loss events, sometimes quite a long period of time after the primary impacts and even after an incident might be considered to be closed.

Vulnerabilities vary over time in direct relation to exploits. A vulnerability determined by experience or knowledge through a verified report is, by its nature evidence of a successful exploit. The time factors important to vulnerabilities are largely related to past experience and resultant probabilities.

100-POWER(2.0,LOG({days since first exploit}/{no. of days with exploits}))

Controls degrade in their effectiveness to adequately address the vulnerabilities which they address. Whether physical, technological or organisational⁸, the degradation of a control will be determined by its type. For instance, the degradation of a lock on a gate will have a different rate of degradation from a firewall rule or an awareness campaign focussed on preventing password sharing.



⁷ Effectively means to result in the realisation of a threat.

⁸ people/process



Incidence and Coincidence

It would seem that probability analysis as it applies to a single factor or component in isolation generally gives an inaccurate understanding of risk. As we will see later, because true risk is derived from an analysis of both exposure and cover and because time applies to various factors of the risk equation in varying degrees, it is not possible that a single factor analysis can result in a true understanding of risk.

However, if probabilities applying to all the factors at distinct times of assessment are unidirectional then assessment of any single factor is likely to indicate the trend in the overall resultant risk and because the factors in the risk equation are multiplied the single factor assessment will at least be proportional.

In YOI-YIO, the probabilities associated with each component each signal one or more points of incidence. For example, in our avalanche scenario a number of causal factors can be incidental in leading to threat realisation i.e. snowfall, temperature, humidity, pressure (inc. sound), wind, surface conditions terrain/vegetation, slope angle and orientation. In reality, any single factor or even a few of them occurring coincidentally may not result in threat realisation. However, as the factors increasingly become coincidental the probability of threat realisation grows.

In our avalanche example, the Intent factor can be given a value of 1 and the various causal factors (represented by Exploits) given values representing the Capability for each to result in threat realisation. In practice each of the factors is contributory and so it is when the probabilities for each of these factors coincide on a timeline that they become resultant and either more or less likely to lead to threat realisation.

So the probability of factor coincidence within a designated time period e.g. a year, is much higher than at other times and so this forms the basis of a more accurate overall understanding of probability. The objective therefore is to determine individual probabilities by understanding the incidences where factors peak or trough and then to determine on a common timeline where coincidences occur. It follows that if factor peaks or troughs are coincidental then it will have considerable effect on the overall probabilities in the risk equation.

For more about Yo-Yo contact Neil Hare-Brown: neilhb@qccis.com or join the [Linkedin group](#)