GeoBureau
Geographic Information Specialists

Ordnance Survey Developer Partner

ESRI Technology AUTHORIZED DEVELOPER

A Critical Discussion of Risk and Threat Analysis Methods and Methodologies

Stilianos Vidalis

Information Security Consultant
Geo-Bureau Ltd, 47 Cowbridge Road,
Pontyclun, Rhondda Cynon Taf,
UK, CF72 9EB
e-mail: stilianos.vidalis@geobureau.co.uk
Tel: +44 (0) 845 603 10 10
Fax: +44 (0) 1443 48 23 29

Table of Contents

List of Figures

List of Tables

Abstract

In this report we will examine the state of the art on the various risk and threat analysis techniques. The objective of this report is to examine the applicability of current risk assessment techniques to assess modern electronic threats. We will analyse the concepts of risk, vulnerability, threat agent and threat, and examine threat statistics from around the world and from various sources. Before discussing the concept of threat assessment though, we will examine the state of the art on the risk assessment field in order to spark the argument on the reasons that risk assessment methodologies and models are obsolete weapons in the hands of the IS officers (based on (Gerber '01), and that they cannot address the needs/problems of the modern electronic era. In agreement with Hinde (Hinde '03), concentrating on the risks issues is both a poor motivator and an unmanageable activity as risk is actually managed by the threat agents and not us.

Risk Assessment Overview

Risk assessment is the heart of risk management. Risk management is the process of:

- Establishing and maintaining information system security within an organization (Wright '99),
- The identification and management of opportunities and threats (Walker '01).

Risk assessment provides the means by which systems risks are identified and assessed in order to justify safeguards (Carroll '96). And of course in our case, protect the system from digital attacks. According to Cushing (Cushing '02), IT directors should perform a risk assessment every 90 days in order to efficiently protect their systems. According to Carroll (Carroll '96), risk analysis is applied in many contexts, such as:

1. Assessing the security postures of IT systems,
2. Formulating IT security strategy,
3. Prioritizing the implementation of safeguards,
4. Auditing IT systems for compliance with security standards,
5. Preparing for imminent attack or disaster,
6. Security training and awareness,
7. Justifying the cost of safeguards,
8. Allocating responsibilities for IT security

Risk has been defined as:

1. "Risk is the probability that a threat agent (cause) will exploit a system vulnerability (weakness) and thereby create an effect detrimental to the system." (Carroll '96)
2. "A risk represents the likelihood of a threat happening/causing a problem." (Nosworthy '00)
3. The term risk is used to describe the possibility of a threat taking advantage of an asset's' vulnerability (Martin)
4. "A risk is an unwanted event that has negative consequences " (Pfleeger '00)

According to (Walker '01), there are four main general areas of risk:

1. Strategic,
2. Market,
3. Credit, and
4. Operational risk.

Risk analysis is a process that examines the risk of something going wrong. Although people do not realize it they perform some sort of risk analysis in their everyday lives. Crossing the road, buying a lottery ticket, flying a plane, and indeed going to work in the morning are actions that involve some sort of a risk. According to the individual's' analysis, one can choose to perform the action or act otherwise. Once people analyse their options, they try to perform their desirable action in a best possible way, often taking care of various parameters in order to do so. That process is exactly like the process in which professionals are deploying countermeasures for minimizing the risk of certain events. People accept the fact that their lives are full of different types of risks, and in the same way organizations accept that they cannot do business without some sort of a risk being involved. What organizations were doing in the past though is performing a risk analysis assessment in order to identify those risks and analyse the way in which countermeasures could efficiently be deployed in order to minimize those risks. Based on Wright (Wright '01): "…that approach is failing as we move towards even more open networks and business models."

Risk Assessment Approaches

Based on (Nosworthy '00), (Martin), (Summers '77), (Tregear '01) there are four approaches to risk assessment.

- Quantitative Approach: Quantitative risk analysis is a mathematical approach to the problem. It involves taking a number of steps to measure the amount of damage dome to an asset as a result of a compromise. Such an approach requires hard facts and figures and is a time consuming and expensive exercise. The solutions of the approach are based on probabilities. There is a number of tools developed over the years that are able to conduct a quantitative risk analysis and a selection of them can be seen in following sections of this thesis. Most of these tools are using complex algorithms for calculating the threat frequency and the likelihood of the occurrence. Both terms are analyzed in a following section.
- Qualitative Approach: This approach is far simpler than the qualitative approach. Probabilities are not required and only estimated potential loss is used. The parameter values are described using phrases such as "high", "medium", and "low". The qualitative approach involves less uncertainty and takes under consideration the knowledge and the judgments of those doing the analysis. In the last years, the qualitative approach is considered to be better able to address the requirements of computing systems. It is accepted that most threats defy any sort of probability analysis as humans are too chaotic to be categorized in any well-established patterns. Hence, this approach, which is not using probabilities, is better able to analyse this type of threats.
- Knowledge-Based Approach: Knowledge based analysis involves reusing "best practice" from similar systems. This approach was extensively used in the old years of computing, where the number of assets and their vulnerabilities could be counted using human fingers.
- Model-Based Approach: Such an approach is using object-oriented modeling to describe and analyse the risk. A tool that is using this approach is CORAS (Dimitrakos '01). The CORAS methodology integrates aspects of various tools and methodologies. It is model-based in the sense that it gives detailed recommendations for the use of UML-oriented modeling in conjunction with assessment. It employs modeling technology for three main purposes:
    - To describe the target of assessment at the right level of abstraction.
    - As a medium for communication and interaction between different groups of stakeholders involved in risk assessment.
    - To document risk assessment results and the assumptions on which these results depend.

  The tool will be further analyzed in a following section of this thesis.

The Evolution of Risk Analysis

Computers have come a long way since the days that were invented. During the last two decades though their evolution rate was extraordinary. From simple stand-alone batch applications in a single-user environment we now have computers able for real-time control, multitasking and distributed processing in a true distributed environment (Cerutti '93). Computers went through at least three phases during their history.

Up to the early 1980's the world was based on batch jobs. There were no overlaps between departments. Figure 1 (source (Gerber '01)) illustrates the organizational infrastructure of a typical business at the time. As we can see the computer department is in the middle, taking care of the batch jobs that its' satellites (the other departments) were producing. The era was called computer-centric era.

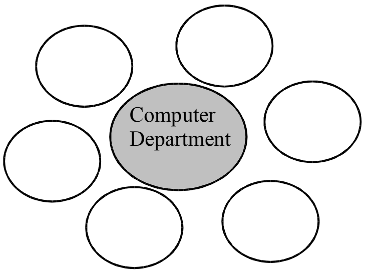

Figure 1 – Computer-centric Environment

In that era the biggest asset was thought to be the computer up time. The protection of the computing facilities was conducted by implementing physical countermeasures around and within the mainframe room. Risk analysis had the form of an experienced employee going around with a checklist making sure that most of the controls on the list were implemented, and threat assessment was non-existent as threat environments were fixed. That was the first generation risk assessment method (Wright '99). The word that characterizes it best is "static".

At the beginning of the 1990's though the picture was slowly changing. The departments started sharing information with the computer department, which was renamed to be the Information Technology (IT) department. New activities emerged such as multi-tasking, multi-processing, real time control and distributed processing. Slowly but effectively a flow of information between the different departments was starting taking place. Figure 2 (source (Gerber '01)) illustrates the new status quo at the time.

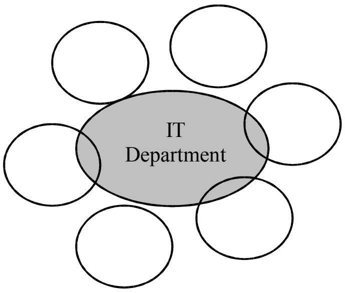

Figure 2 – IT-centric Environment

Naturally the risk assessment methodologies had to evolve to address the new requirements, which were: user identification and authentication, access control and encryption of communication lines. The concepts of asset, vulnerability, threat, impact and likelihood were introduced to the assessment. The biggest asset of the era was though to be the communications. Most departments were depended in the IT department for communicating and completing their work, and here is where the main problem was. Most assets are intangible, and not easy to measure and associate with a monetary value. Furthermore, data are associated with more than one asset and can be influenced by more than one factor. To solve the problem, impact values were used, and the concept of threat was introduced to the risk assessment process (Gerber '01). The results though were very subjective as there were no formal ways to interpret and calculate the threat impact, or even the likelihood of the threat. That was the second generation of the risk assessment methods, that based on M. Wright (Wright '99): "…enabled the analyst to identify and valuate individual system assets, undertake threat and exposure assessments, conduct quantitative risk analyses and enumerate and prioritize controls."

The risk analysis process was under heavy fire when the computers went under another phase, the Information Centric era. The electronic commerce and the on-line services were the new concepts introduced in our everyday lives but with them came new threats (the web threats (Highland '97)) that destabilized the balance on the security field. Information is the most important asset. Having the right information at the right time can make the difference between survival and bankruptcy. Figure 3 (source (Gerber '01)) illustrates the organizational structure of today's business.

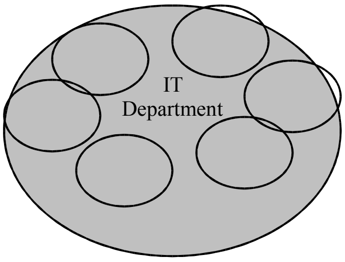

Figure 3 – Information-centric Environment

Security countermeasures had to evolve from protecting infrastructures to protecting information. The classical risk analysis methodologies using assets, vulnerabilities and threats focus on the computing infrastructure, and not on the information as per say. There was a need for a third generation to surface, a generation that would be able to address the system as whole. This new generation will have to be able to examine the interrelationships between systems, user behaviors and the history of the environment that the system is functioning in. In other words it will be able to analyze the core business of the company (Forte '00). All these new requirements can be seen in the examined implementations of commercial electronic payment systems. The commercial systems have a number of subsystems, they are functioning in a number of different environments, and different types of stakeholders are involved. According to M. Wright (Wright '99), the 3rd generation practices must encompass four risk management principles:

1. Explore and assess business operations
2. Determine policies, standards and controls that are worth implementing
3. Promote awareness amongst all stakeholders
4. Assess compliance and control effectiveness.

Threat Assessment Overview

For the purpose of this research we will use the following definition for threat assessment:

> A **threat assessment** is a statement of threats that are related to vulnerabilities of company assets and threat agents, and also a statement of the believed capabilities that those threat agents possess.

The definitions of the terms are given further down in this report. Threats are best realized under the context of information security. The only definition of the term, which the author agrees with, is provided by Anderson (Anderson '03):

> **Information security** is a well-informed sense of assurance that information risks and controls are in balance

Information security can be seen like a huge blank sheet of paper, but it should not be seen differently from other key business objectives or missions (Parkin '98). It is difficult to define a start and an end or put context to the term. Based on King (King '02), security needs to be addressed as a continued lifecycle in order to be effective. Security is more than just a firewall, or a user-name and password login (Hinde '01), (Wright '01). It is a trade-of between cost, ease-of-use, and business flexibility (Wood '97). Based on (? '02), (A.J.C.Blyth '01), (M.Smith '93), (Pfleeger '97), (Summers '77), (Finne '00) information security is concerned with the integrity, confidentiality, availability, authentication and non-repudiation of the following:

- Software,
- Communications,
- Data,
- Hardware,
- Physical & Environmental,
- Personnel,
- Administrative & Organizational.

Confidentiality means that the assets of the system are only accessed by authorized parties (Pfleeger '97). Stalling (Stalling '00) is giving another aspect in confidentiality by saying that the traffic flow is also protected by any kind of "outside" analysis. This requires that an attacker will not be able to identify any asset in a transaction, such us the sender, the receiver and the context.

Integrity means that the assets of the system can be modified by authorized parties only, and in authorized ways (Pfleeger '97). Here there is a concept of "inside" and "outside" integrity. Not only we want the "outsiders" not to be able to modify system data, but we also want the insiders not to be able to proceed in any sort of malicious operations with the system data.

Availability means that the assets of a system are always available to the authorized parties (Pfleeger '97). As explained, availability is of the essence due to the nature of the systems and their users. Having one or two of the above goals achieved is relatively easy. The difficulty lies in achieving all three of them as each one is going "against the other" in some sort of manner.

Non-repudiation prevents either the sender or the receiver form denying a transmitted or received message (Stalling '00). It can be seen that non-repudiation is essential for the operation of the system, as it will prevent clients from denying having made a payment and also the system from denying that it had received one.

Authentication is assuring that a communication is authentic (Stalling '00). Due to the financial nature of the system it is important to authenticate all communications and being able to identify masqueraders that are trying to conduct fraudulent transactions.

Furthermore, according to B. von Solms(Solms '01) information security has different dimensions:

- The strategic/corporate governance dimension,
- The governance/organizational dimension,
- The policy dimension,
- The best practice dimension,
- The ethical dimension,
- The certification dimension,
- The legal dimension,
- The insurance dimension,
- The personnel/human dimension,
- The awareness dimension,
- The technical dimension,
- The measurement/metrics dimension,
- The audit dimension.

The above five terms are considered to be the main goals of the science of information security, and should be addressed in all of its dimensions in order to establish a really secure environment. The terms has been analyzed by a number of people and discussed in depth. The purpose of this research is not to redefine information security; hence we will not expand on them any more. In order to understand information security and how it relates to electronic commerce though, we need to have a precise set of definitions as to what we mean by: threat, threat agent, and vulnerability.

Threat Agent

The term threat agent is used to denote an individual or group that can manifest a threat. Based on (A.J.C.Blyth '01), (Hinde '01), (Vidalis '01), (D. Kove '95), these individuals and groups can be classified as follows:

- Hostile Nations: Most governments now recognize the need to protect the information assets that their country has created. These assets have a financial value for business and can have a value in terms of national security. Intelligence agencies seek the military, diplomatic, and economic secrets of foreign governments, foreign corporations, and foreign adversaries. They always have; however, they can now do it remotely and with less risk due to information systems vulnerabilities. In addition, intelligence and law enforcement agencies seek to protect the information assets of the nation by targeting the activities of criminals and foreign intelligence operatives. In times of war, a government may target the CNII of another country in order to help it achieve its objectives. For example: in the Gulf War, the allied forces targeted and partially destroyed the CNII (physical and information) of Iraq. In fact, in probably every war fought in the last hundred years, examples can be found of targeting the adversary's infrastructures. The people who perform these attacks are:
  - Highly trained and highly funded.
  - Backed by substantial scientific capabilities, directed towards specific goals, and skilful in avoiding detection.
  - Very dangerous to life and property.

- Terrorism and Terrorist Groups. Terrorists are of particular interest because of the damage that they can cause against the information infrastructure such as emergency services, utilities such as water and electricity, and financial services. Terrorists are politically motivated and have their own political agenda that they use to select targets. Before the 11th of September, terrorists had been slow to use offensive IW tactics. Why? No one really knew for sure, but since then a wave of terrorist cyber attacks hit the UK and the US SMEs (see Goodwin (Goodwin '02)). Although Destroying buildings and “blood in the streets” still seem to have more of a major propaganda value on the six o’clock news than showing a burned out computer, the terrorists were quick to realize the impact they can have manifesting cyber threats. Terrorists use attacks to inflict fear and to achieve either social or political change.
- The Corporation. Corporations engage in offensive IW when they actively seek intelligence about their competitors or steal their sensitive information, e.g. trade secrets. Money, market position and competitive stance are examples of some of the corporate motivations for using IW tactics. In addition, corporations have always engaged in a form of IW even before the term was first used. This type of IW is called advertising and marketing. Back in 1996 the FBI conducted a survey amongst US corporations, financial and academic institutions and government agencies. From the 4971 questionnaires that were sent out, only 8,6% were returned. From those it was reported that 42% of the examined organizations admitted experiencing some sort of an attack within the last 12 months, and over 50% of those were believed to be from competitors from their marketplace. The source of the statistics is (U.S.Senate '96). Corporations often employ individuals (criminals) to perform netspionage (Kovacich '00).
- Organized Crime and Criminals. Criminals target information that is of value to them, such as bank accounts, credit cards or intellectual property that can be converted into money. For example: the Pennsylvania State lottery was presented with a winning lottery ticket worth $15.2 million that had been printed after the drawing by someone who had browsed through the online file of still-valid unclaimed winning combinations. The scam was detected because the ticket had been printed on card stock that was different from that of the legitimate ticket. The main motivation in this case was money. Criminals will often make use of insiders to help them. They may be in collusion with the insiders or use such tactics as threats, blackmail and the like. Criminals can be subdivided using the following structure:
    - Amateurs: In today’s interconnected world, WWW is a huge knowledge depot. There are a lot of hacking tools (Barber '01) and “hacking-related” information in the public domain, readily available to anyone with a computer attached to the Internet. Furthermore, hacking is seen by the majority of the people as some sort of magic. It is very popular amongst the youngsters of the world, especially in the western hemisphere. All these people come under this category. They have minimal knowledge of the art of computing and “hacking”, they use of-the-self ambiguous “hacking-called” tools downloaded from the Internet, and can cause no real damage expect increased network traffic. Their motivation is to “show-off”.
    - Hackers: There are a lot of arguments for a definition of the hacker. Some observations about this type of people are the following. A hacker will never admit in being a hacker. A hacker is interested in knowledge and not in destruction. A hacker is not only someone dealing with computers, but everyone who is interested in the way things are working, everyone who is trying to analyze what is going on behind the scenes, and everyone who is not happy with whatever is on the surface. A hacker does not think that what he does is bad, evil or illegal. A hacker does not want to realize that what he does is bad, evil or illegal. Most hackers have a very good knowledge on one of the many aspects of computers. Most hackers use sophisticated tools and have the knowledge to cause a real havoc to a computer system. Fortunately, most hackers do not normally abuse their power unless they are prompted. There are hackers with different “experience levels”. The low level hackers can be traced back most of the times. The high level hackers tend to stay low and use someone else for their “dirty” work. Their motivation is to acquire knowledge. Hackers are not necessarily criminals. They can be divided in “black hats” and “white hats”. The “black hats” are breaking the law and the “white hats” are making their “experiments” in isolated environments without breaking any laws, intentionally or unintentionally. This last category can be a great asset to an organization employing a number of these individuals working as security experts, testing thy systems against potential threats (Rees '96).
    - Crackers: Crackers can be seen as the “evil” hackers. They are aware of their power and they like abusing it. They are not interesting in just acquiring knowledge, but also using the knowledge they have to cause havoc to legitimate computer users and corporate networks. The bigger the goal, the more resources will allocate in cracking it. Their motivation is to hack and crack as many computer systems as they can, cause as much damage as they can, bring community operations to a standstill, and leave their signature behind. That is also their weakness. In their pursue for power they need to let people know who they are. UK has acknowledged the problem and is formulating a strategy to help secure and install computer systems (Goodwin '03)

Organized crime is around since the dawn of mankind and has outlived all the big empires. A very good comment that comes from Bequai (Bequai '01): “Like the one celled amoeba it has outlived those who sought to destroy it…”. The Mafia provided the high esteemed brokers of Wall Street with what ever they need (drugs, prostitutes…) and in exchange they provide them with sensitive financial data. In the US organized crime is a half-a-trillion dollar business (Bequai '01).

- The Empowered Small Agent (ESA). The term empowered small agent is used to denote an individual or group who is motivated for a) ideological principles, b) political principles, c) religious principles or d) the intellectual challenge. For example Political Dissidents are people who are attempting to use information and information technology to achieve a political objective, in particular they are using information technology to:
    - Inform the civilian population and other organizations or individuals about the alleged activities of their government.
    - Gather (via legal, or illegal means) information relating to the activities of their government.
    - Disrupt or undermine the activities of their government.

As it was mentioned, corporations are using on-line systems to offer services to their customers. More and more small businesses are being depended on some sort of EPS for their revenues. Each one of these small businesses constitutes a vulnerability to the Critical National Information Infrastructure (CNII). According to the "Brown Report" (Brown_Commission '96) collecting information about the threats against the CNII is a legitimate mission of the intelligence community, and not an unethical action violating human rights.

Of course, except the individual persons, Mother Nature can constitute a threat agent as well. Natural disasters like fire, floods, lightning, earthquakes and others can have a major impact to the survivability of a corporation. Natural disasters can have a human agent in the background or not. For example, a laboratory inside a tropical rainforest has taken all the necessary precautions, and according to threat calculations fire from Mother Nature does not constitute a threat. The scenario of a human agent helping Mother Nature though, ensuring that certain "amplifiers" (see Jones (Jones '02)) will be in place, greatly change the level of the threat.

The structure presented in this section can be seen in figure 4, which is presented underneath.

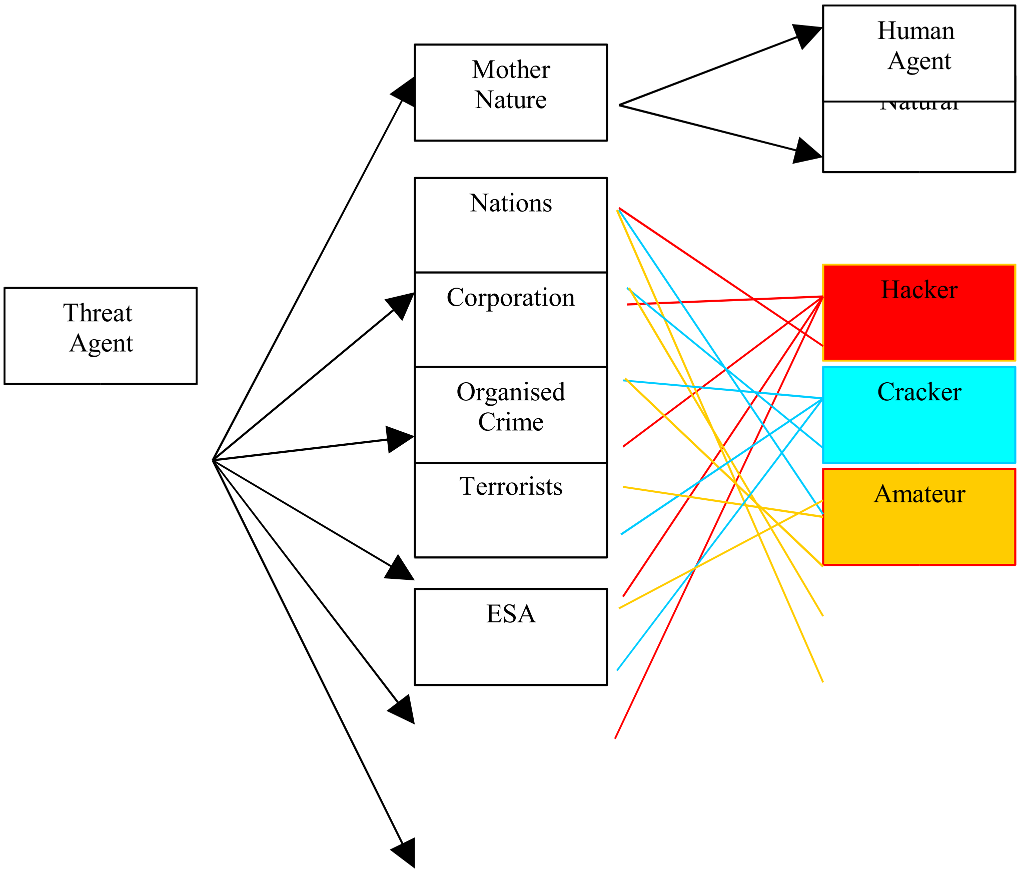

Figure 4 – Threat Agent Categories

Nations, corporations, organized crime, terrorists, and the ESA can employ hackers, crackers and amateurs to achieve their goals. Hackers, crackers, and amateurs can be part of the aforementioned groups. We can think of it as a two-way inheritance. Each combination has different attributes, and more than one combination can exist in any one group.

Vulnerability

The concise oxford dictionary (Sykes '81), defines the term Vulnerability to mean: is susceptible to damage. Vulnerability has been defined as follows:

- A point where a system is susceptible to attack (Kabay '96).
- A weakness in the security system that might be exploited to cause harm or loss (Pfleeger '97).
- Some weakness of a system that could allow security to be violated (A.J.C.Blyth '01).

However for the purpose of a threat assessment we require a definition that is more general to information security and encompasses both, information technology, communication systems and business processes. Therefore we will use the following definition:

Vulnerability is a measure of the exploitability of a weakness.

According to (A.J.C.Blyth '01), (Pfleeger '97), (Summers '77), there are six types of vulnerabilities that can exist in any system, and these are:

- Physical: intruders can break into computing facilities. Once they get in, they can sabotage and/or vandalize computers, and they can steal hardware, diskettes, printouts etc. What is the point of spending thousands of pounds in buying and configuring a firewall to protect the servers of the finance department, if there are no locks in the windows that the servers are situated and those windows face a public street.
- Natural: computers may be vulnerable to natural disasters and to environmental threats. Disasters such as fire, flood, earthquakes and power loss can wreck your computer and destroy information. What is the point of installing the server room over the main water pipe? Simply, you do not do that, even if the building is brand new.

- Hardware/Software: certain kinds of hardware and software failures can compromise the state of a computer system. Software failures of any kind may cause systems to fail, and may open up systems to penetration, or make systems so unreliable that they can't be trusted. Customers will be the first ones to go away, and then the employees will follow. The bigger the system the more vulnerable to this type of vulnerabilities is. An example of a hardware vulnerability is the overheat problems the early AMD processors had. An example of a software vulnerability is the remote exploits of the sendmail daemon.
- Media: disk packs and tapes can be stolen or damaged by such mundane perils as dust and ballpoint pens. If your headquarters were next to a beach you would not leave the window to your server room open on a windy day…and definitely you would not allow any of your employees to walk in the server room with their mugs of coffee.
- Communication: if your computer is attached to a network then its message can be intercepted, and possibly modified or misrouted. The Man-in-the-Middle attack[1] (Toxen '01), (Bhansali '01) is the best example that illustrates the severity of these types of vulnerabilities.
- Human: the people who administer and use your computer facilities represent the greatest vulnerability of all. They may be vulnerable to greed, revenge, blackmail and the like. The customers of a company offering an on-line service are its greatest vulnerability because there is no way to police someone, which is half the world away from you. Furthermore, it is extremely difficult to distinguish between a legitimate customer and a malicious customer that is employed by a rival company for gathering information about your system. In agreement to Nosworthy (Nosworthy '00), the only way out is customer and user training (see Furnell (Furnell '00)) and a reflective information security policy.

New vulnerabilities are being discovered every day. Approximate values of new vulnerabilities discovered over the years, taken from Goodwin (Goodwin '02) can be seen in table 1.

Year	No of Vulnerabilities
1995	Less than 100
1996	125
1997	260
1998	260
1999	900
2000	1010
2001	1550
2002	1350

Table 1 - Discovered Vulnerabilities since 1995

It can be seen from the above table that the last four years there was an explosive increase on the vulnerabilities that were discovered in computing systems. It is the belief of the author that the more we move towards a more open and interconnected architecture the more vulnerabilities will be discovered every year. This is natural as companies that are merging business, are also merging their systems, and each system is having its own vulnerabilities and/or mutate existing vulnerabilities of their individual infrastructures. Furthermore, companies fail to realize the existence of vulnerabilities in their infrastructures, and keep on expanding and upgrading their systems, which soon look like "giants with feet from sand". Penetration tests in UK revealed vulnerabilities the existence of which is due to human stupidity (see Jones (Jones '97)).

Threat

The concise oxford dictionary (Sykes '81) defines the word **threat** as meaning:

> *Declaration of intention to punish or hurt; menace of bodily hurt or injury to reputation or property, such as may restrain a person's freedom of action indication of something undesirable coming.*

According to A.J.C. Blyth (A.J.C.Blyth '01) a threat to a system can also be defined as:

> A circumstance or event that has the potential to cause harm by violating security.

For the purposes of this research, threat is a function of a threat agent's motivation, their capability, the opportunity, and the impact that a successful attack would have on an organization.

Threat = Function (Motivation, Capability, Opportunity, Impact)

Each of the terms utilized in the threat function are defined as follows:

[1] The man in the middle or TCP hijacking attack is a well-known attack where an attacker sniffs packets from a network modifies them and inserts them back into the network. There are a few programs/source codes available for doing a TCP hijack.

- Motivation. The concise oxford dictionary (Sykes '81) defines the word **motivation** as meaning:

  > Supply a motive to cause a person to act in a particular way. In the context of a threat, motivation is considered to be identification of both the reasons why someone would launch an attack and a measure of the degree to which the attack would be pressed home.

  According to Jones (Jones '02), there are some commonly accepted motivational drivers, which are: political, secular, personal gain, religious, revenge, power, terrorism, and curiosity. For the purpose of this research we will consider motivation to be the degree to which an aggressor is prepared to implement a threat. The motivational factors are the specific real-world elements that drive a hacker to consider penetrating a computer system. Analysis of computer criminals (Carroll '96) suggests that the primary motivations include the following, sometimes in combination:

  1. The need to resolve intense personal problems such as job related difficulties, mental instability, debt, drug addition (Stoll '89) loneliness, jealousy, and the desire for revenge,
  2. Peer pressure and other challenges, for example, among malevolent hackers,
  3. Idealism and extreme advocacy, for example, by espionage agents and terrorists,
  4. Financial gain.

  Motivational factors in and of themselves cannot be detected by IDS technology – at least, not with the current state of the art. However, important motivational elements can be observed in the records that are collected and maintained by a variety of network security systems: they represent important information that can and should be analysed. Abstracting such profiles is part and parcel of the objective of this new-generation IDS technology, allowing confident identification of individuals to be supported.

- Capability. The concise oxford dictionary (Sykes '81) defines the word capability as meaning the power to do something. In terms of Information Security the term capability is used as a measure of:

  - The availability of a number of tools and techniques to implement an attack, and the ability tot use the tools and techniques correctly.
  - The availability of education and training to support the correct use of various tools and techniques.

  For the purposes of this report we will use the term capability to mean the degree to which an aggressor is able to implement a threat.

- Opportunity. The concise oxford dictionary defines the word opportunity as meaning, a favourable occasion for action. Sun Tzu (Denning '99) stated: “The good fighters of old first put themselves beyond the possibility of defeat, and then waited for an opportunity of defeating the enemy”.

  Consequently in order for a threat agent to bring its capability to bear against a target they must have the correct conditions to do so, and in order for their capabilities to be effective and have an impact on the target, the target must be vulnerable to attack. Hence, the target must present the threat agent with an opportunity of attack. What the information security officers are trying to do is to make sure that the threat agents will be in no position of creating that opportunity for themselves.
- *Impact. The term Impact is used to denote the result of a threat reaching an asset (J.D.Nosworthy '00). A threat impact can be towards the market share of the company, or even more important the user trust. These impacts are not easily calculated and only speculations can be made for their size. A golden rule is that any threat that could be realized from the users will have a catastrophic impact to the user trust and any threat that can be realized from the suppliers or generally the stakeholders of the company will have catastrophic results to the market share of the company. Another classification of threat impacts is the following:*
  - *Minor: minor loss of a business asset, no change in business order*
  - *Moderate: business disruption, moderate changes in way of conducting business*
  - *Major: out of business unless countermeasures are deployed immediately*

- *Catastrophic: out of business from the moment that the threat was realized*

The impact of a threat can cause disruption in more than one field. The following impact fields were identified during the development of the model. Different types of businesses could have different types of impact fields.

- *Human Resources:* Any kind of organization is depended on its employees. If the employees are demoralized, scared or not able to perform up to the management's expectations in any way due to the manifestation of a threat, then the business will be at a loss.
- *Supply Chain:* All businesses are dependent on their supply chain. The majority of the businesses are like functions in a software program. They take something as an input, do specific operations with the input, and produce an output, which they pass over to either another function or to one of the standard output devices of a computer system. If there is a disruption in that chain, then the function is not able to operate. Exactly the same principle applies to the businesses, only in a larger scale. Once there is a disruption in the supply chain, the business will survive only if it has good continuity plans.
- *Market Share:* The market share is essential for the survivability of a business as it declares more or less its ability to sell the product that is producing. If there is a major disruption or change in the market share of the business, then it is unlikely that the business will be able to recover in a short term, if ever at all.
- *Business Capital:* The capital of the business could be impacted by the manifestation of certain threats. The result of that will be a further disruption on the ability of the business to continue offering its services.
- *User Trust:* User trust is one of the most important survivability factors for a business using a micro-payment system (Daughtrey '01). The user trust is closely related to the market share, with one distinction. It is easier to regain market share following marketing tricks and procedures. The user trust on the other hand is an asset that takes ages to develop and minutes to loose.

Threats can be classified according to the motivation of their associated threat agent. Figure 5 presents that classification.

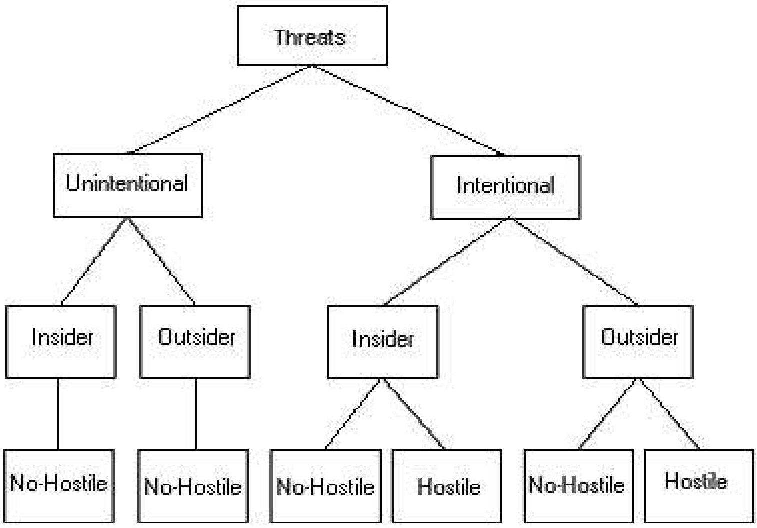

Figure 5 - Motivational Threat Classification

All threats can be either intentional or unintentional. Natural threats can fall under either category depending on the threat agent. For example the natural threat of a flood can be unintentional (caused by mother nature), but it can also be an intentional sabotage caused by an outsider threat agent. The above classification can be used in the preference structuring of the threats. Of course it is easily understood that the threat agent associated with an intentional threat will be willing to spend or assign more resources in achieving his/her goals, hence all these threats will have to be treated differently than the other types. Table 2 presents the top 10 countries that suffered digital attacks over 2002. The source of the table is (Cushing '02). The results presented could be expected as the foreign affairs of the US provide with motivation hundreds of threat agents. The fact that the US is greatly computerized, gives to those threat agents, the opportunity to perform the attacks. Hence any threat agent of an adequate capability will most likely perform some sort of an attack against a US target, be it military or civilian, as those two concepts are not easy to distinguish of late.

Rank	Country	No of Attacks
1	US	28.519
2	Brazil	6.204
3	UK	5.099
4	Germany	4.736
5	Italy	2.738
6	Canada	2.345
7	France	2.022
8	Denmark	2.004
9	Australia	1.317
10	South Korea	1.259

Table 2 – Digital Attacks in 2002

Based on a survey conducted by the Computer weekly newspaper (see Goodwin (Goodwin '02)) the worst threat to IT security is the viruses, which is followed by theft of electronic context. The results of the survey are presented in table 3.

Threats	% of Respondents
Denial of Service	49%
Web Site Defacement	27%
Viruses	59%
E-Mail Interception	39%
Internal Fraud	39%
Fraud affecting a third-party service such as a credit card	26%
Theft of confidential information of electronic documents	54%
Threat from disgruntled employees or contractors	41%
Interception of wireless LAN communications	43%

Table 3 – Worst Threats to IT Security

Based on various reports talking about cyber crime (see (Bequai '01), (Goodwin '03), (Goodwin '02), (Hinde '03), (Pounder '01)) that are trying to foresee the future, the cyber crime will increase and become a bigger threat to the companies. According to the UK's' government figures, computer hacking and virus attacks are costing UK businesses as much as £10bn each year (see Hinde (Hinde '03)). The same author observed a change in the threats of late. Although in the past most attacks were coming from within a company, nowadays 60 – 70% is coming from the Internet.

Threat & Risk Assessment Methodologies & Methods Overview

Until now, threat assessment was merely a part of the risk analysis process. There are quite a few commercially available risk analysis methods and tools (see (Tregear '01), (S.A. Kokolakis '00)). Based in "The Evolution of Risk Analysis" section, a number of tools from each generation was selected and examined in order to understand the state of the art in the field of risk analysis. Risk analysis is a process to assist management in defining where time and money should be spend (J.D.Nosworthy '00). According to Pfleeger (Pfleeger '00) risk is defined as: "…an unwanted event that has negative consequences." The difference between the risk and the threat lies on the point of reference. When we examine the risk we do not really examine the causes, we are only interested on the way that our system will react and how to better defend against it. Today though, we cannot afford to ignore the causes of the risk. It is accepted that the only way to minimise losses is to be proactive, and to deal with threats rather that risks. As it was realised, all the different methodologies (Carroll '96), (Nosworthy '00), (Summers '77), (D. Kove '95), (Pfleeger '00), (Brewer '00), (Katzke '88), (R.C. Reid '01), (Smith '95), (Bayne '02) were assuming that the user knew about the threats and the threat agents that his system had to face. That assumption might be adequate for a risk analysis, but in today's ever-changing world a threat assessment cannot and should not make that mistake. There are a lot of different methodologies for conducting a risk assessment of a computing system. In this section we examine some of them, and discuss their pros and cons. All of the following risk assessment methodologies fall under the classical risk analysis model described by R.C. Reid (R.C. Reid '01).

Risk Analysis Methodologies

Summers

Summers (Summers '77) in her book suggests the following steps in a risk methodology:

1. Identify assets and assign monetary values
2. Identify threats and vulnerabilities
    a. Estimate likelihood of occurrence for each threat
    b. Estimate impact of each threat
3. Calculate exposure of each asset to each threat
4. Identify potential safeguards and their costs

The user has to first identify the assets of his system and then do a simplistic and subjective assignment of monetary values to each one. The first way is by "standard accounting", where the user assigns the value that is recorded in the asset register of the organisation. This is ideal for the tangible assets but can cause a headache otherwise. The second way is the "replacement cost". It is most suited for intangible assets and assigns the value that a replacement of the asset would cost. In calculating their final value the user must include the value of their security attributes, which are: confidentiality, integrity and availability. The second step is the identification of possible threats and vulnerabilities. According to Summers a threat is the exploitation of vulnerability by a threat agent. Unfortunately no metrics are given on how to objectively make these identifications, and probabilities are being used for estimating the likelihood of each threat. The method is trying to predict the importance/severity of each threat towards the system, based on probabilities. Unfortunately, threat agents defy all of the probabilistic rules and equations, as humans follow a chaotic way of thinking. Summers is examining the impact of each threat only from the financial aspect. Let 'I' be the threat impact, let 'A' be the availability, 'In' the integrity, 'C' the confidentiality and 'L' the likelihood. The equation is:

$$F(I) = [\ f(A) + f(In) + f(C)\ ] * f(L)$$

In our opinion though, there are other more important long-term impacts that any business should be worried about. For linking threats and vulnerabilities the users have to calculate the exposure of each asset to each threat. The last step of the method is the identification of available safeguards.

Icove

The Federal Bureau of Investigation in USA is running a course in conducting risk assessments. In the textbook (D. Kove '95) of the course the following procedure is identified:

1. Ask questions (threat & asset identifications),
2. Apply intelligence reports,
3. Conduct vulnerability analysis,
4. Develop security countermeasures,
5. Document the findings.

FBI makes a distinction in the types of threats and vulnerabilities, which may be categorised as either static or dynamic. Intelligence reports can be obtained from the police, other law enforcement offices, private investigators, and interviews. By applying this stage we can understand the relevance of each identified threat. Unfortunately these reports are not always available for the public, and the ones that are in the public domain are out of date. The third step is a discussion of the system under investigation. This step contains the creation of a list of all the possible vulnerabilities of the system, and each one is related to the identified threats. According to the size of the system this stage can take so much time that can render the results of the model out of date and unusable. It is very difficult for a user to be able to complete with success this stage. Throughout this method, users are forced to make assumptions, and with each one made, the result are becoming more unreliable and with no value.

Carroll

Carroll in her book (Carroll '96), identifies the following procedure:

1. Threat assessment
    a. Likelihood estimation
    b. Severity prediction
2. Asset evaluation (importance, exposure, attractiveness)
    a. Vulnerability assessment
3. Impact assessment
    a. Threat & asset interaction
4. Safeguard evaluation

Carroll makes a distinction between deliberate threats and accidental threats. The attacker, for "manifesting" a threat, must have the capability to perform the attack, the motivation and the opportunity to do it. Each threat has two properties: likelihood and severity. Likelihood is the number of occurrences of the threat per year, and severity is the consequence of the realisation of the threat. Asset evaluation is dependent from three factors: the asset importance, its exposure and its attractiveness. The method can only be used reactively as it needs history data for the threats. Furthermore, it fails to appoint the threat agent investigation and identification problem.

Pfleeger

Pfleeger in his book (Pfleeger '97), describes the following methodology:

1. Identify assets,
2. Determine vulnerabilities,
3. Estimate likelihood,
4. Compute expected annual loss,
5. Survey applicable controls and their costs, and
6. Project annual savings of controls.

The method looks like a procedure developed from a finance person to be used in the finance department. Likelihood estimation is a rather sensitive part. Pfleeger suggests the following methods: (a) Probability from observed data of the general population, (b) Probability from observed data for a specific system, (c) Estimate of number of occurrences in a given time period, (d) Estimate of likelihood from a table, (e) The DELPHI[2] approach. Excluding the DELPHI approach, all other methods are subjective and because are based on probabilities are dangerous to use. The DELPHI approach can only be used reactively and the amount of time that it takes to be completed renders the results unusable. Data from other systems cannot be used as each computing system no matter how similar might look to another will always be unique unless it is its exact image. The likelihood calculation is based on a subjective table that is based on the frequency of the threat occurrence. The table is presented underneath.

Frequency	Rating
More than once a day	10
Once a day	9
Once every three days	8
Once a week	7
Once in two weeks	6
Once a month	5
Once every four months	4
Once a year	3
Once every three years	2
Less than once in three years	1

Table 4 – Pfleeger's' Likelihood Estimates

Next step is the annual loss calculation. Should a vulnerability of the system is exploited it will cause a certain loss. By multiplying that with the number of occurrences of the incident we get the annual loss expectancy. The least that can be said is that the above statement is simplistic. The short-term financial loss is the least that any business should worry about in the case of the manifestation of an attack against its system.

Following the investigation on the different risk assessment methodologies, we did an investigation on the different models that claim to be able to successfully assess and secure a computing system. Some of the results of the above search can be seen underneath.

FRAP

Peltier Associates' FRAP methodology is based on the concept of information ownership. The methodology enables rapid decisions that affect the security of the information asset. The methodology helps the client to identify control weaknesses, analyze the cost of controls and develop an action plan where action items are assigned to the client's own subject matter experts. The methodology uses a five-step process to help the client review any task, project or idea. By learning the basic concepts of risk analysis, the client can use FRAP to determine if a project should be started, if a product should be purchased or if a new control should be implemented. The process is presented underneath:

1. Interview to establish business objectives
2. Study assets to identify risks
3. Analyse risks with information owners
4. Identify control plans to implement
5. Final report & presentation

[2] DELPHI approach [(Webster '97). Webster, R. (1997). The DELPHI Research Methodology. **2001**.http://www.geocities.com/ResearchTriangle/4681/]: It is a qualitative forecasting methodology that is used where either data is non-existent or where high uncertainty, complexity and uniqueness disallow the use of quantitative methods. The technique uses a series of questionnaires administered in phases to interrogate a panel of experts. Information and opinion feedback on progressive outcomes between phases are provided to the panel. The panel is then requested to respond to the outcomes of the preceding phase as follows:

Phase one: A questionnaire is sent and the panel is asked to pass opinion regarding future events. The panel co-ordinator analyses responses and compiles them into a document that lists and describes all predicted future occurrences identified by the panel.

Phase two: The panel is sent the compilation of phase one responses and asked to rank and comment on both the probability and nature of effect of the predicted occurrences. Phase two responses are then compiled into a document that identifies occurrences about which there is general agreement and occurrences about which there is divergence of thought.

Phase three: The panel is sent the compilation of phase two responses and asked to comment on and possibly review widely divergent predictions that were made.

The resulting responses are then compiled into a final report that details; predicted future events about which there is a general agreement; any significantly divergent opinion from the general opinion and reasons for this divergence; and, those events around which there is significant uncertainty.

Like most methodologies, FRAP fails to examine the threat agents and their motivations, and accept as inputs only the data collected from the stakeholders and the users of the assets. The difference of this methodology is the stakeholder identification and the evaluation process.

Risk Analysis Models

CRAMM

CRAMM is widely used in the UK and although longwinded it produces some meaningful results. A CRAMM analysis begins, as expected, by identifying the assets, assigning monetary values and calculating impacts. CRAMM makes a distinction between four kinds of impacts: disclosure, modification, unavailability and destruction. The distinction is done with the help of questionnaires provided by the model to the asset owners. The question here is the suitability of the owners, and how the different views of the same assets are getting combined. Assets are organized into groups and each group is handled as a unit. This is a dangerous operation as each asset has unique attributes and it only takes an exploitation of one to create a security breach. After that, CRAMM is using an internal list of generic threat agents for constructing links between group vulnerabilities and threats. Each link is characterized as low, medium or high. CRAMM then calculates a risk number from 1 to 5 for each impact (disclosure, modification, unavailability and destruction). The output of the CRAMM review is a set of countermeasures that are proposed to be necessary in order to minimize the identified risks.

The author believes that the identification of threat agents should be continuous, as nothing is staying stable in our world. Having a generic list is a drawback, unless it is being updated constantly. The characteristics of the threat agents are easily changed by worldwide incidents and any kind of human acts inside and outside of the business under review. The last step in the model is to consider the countermeasures. CRAMM is directly linked with another model, the SSADM. Both models are monolithic, produce a vast amount of output that makes difficult to distinguish any useful information and the risk analysis is not integrated into the methodology. The details for CRAMM were taken from Carroll (Carroll '96), Summers (Summers '77), and (CCTA '93).

ARiES

ARiES stands for the Aerospace Risk Evaluation System and it is using a quantitative risk analysis methodology. The model uses assets, threats, controls and impacts for estimating risks. The main equation of the model says that a risk is a combination of the threat agent, its path to the asset, the asset itself, the impact of the threat and the countermeasures. Let ‘EF’ be the expected annual frequency of the threat, let ‘PCF’ be the probability of failure in the deployed countermeasures, and let ‘MPL’ be the impact of the threat to the business. The risk is then calculated from the following equation:

$$R = EF \times PCF \times MPL$$

The methodology has six stages: project planning, information gathering and management input, risk definition and screening, risk acceptability assessment, cost-benefit assessment and prioritization of control sets. Stage 2 is all about asset identification, stage three is the threat identification and impact calculation, stage 4 is the countermeasure proposals, stage 5 is the cost calculation of the countermeasures against the cost of the impact, and stage six is the final set off countermeasures. Likewise CRAMM, ARiES follows a series of steps in order to come up with a set of countermeasures that will reduce all risks against the system. It follows the waterfall model of development, and as a result it hasn’t got the necessary flexibility to overcome the speed in which the threats are mutating today. Should there is a mistake or a change in the data, the model has to be re-run. The details for ARiES were taken from Summers (Summers '77).

COBRA

COBRA (C&A_Systems_Security '02) stands for Consultative Objective & Bi-functional Risk Analysis. The model consists of three stages:

1. Questionnaire Building,
2. Risk Surveying, and
3. Report Generation

The tool uses the same methodology as CRAMM but operates on a smaller set of countermeasures. It is using questionnaires to gather the necessary information. The design of the tool is modular, which allows for greater flexibility and ability to address change. New organization specific modules can be developed and attached to the model. The limitations of the model leys to the business impact module that all questionnaires are based on. Not all assets can be assigned fiscal values. Furthermore, the generated countermeasures are at a very high level.

STIR

STIR (Martin) stands for Simple Technique for Illustrating Risk. It is a two-step process:

1. Identifying Assets, Threats and Safeguards,
2. Discovering Patterns

In the first step assets, threats and safeguards are illustrated in a diagrammatic form. Knowledge-based risk analysis is used for their identification. The diagrammatic form is known as Asset-Threat-Safeguard (ATS)

Diagram and it is based on the UML Use Case diagram with the addition of custom tags that define assets, threats and safeguards. Assets are added as Use Cases with the Asset tag (also known as a stereotype). Threats are added as Actors with the Threat tag. Safeguards are added as Actors with the Safeguard tag. Threats and safeguards are associated with assets using Associations. These associations indicate that the threat is capable of compromising the asset and the safeguard is capable of protecting the asset. In the second step the diagrams are being reviewed for unusual or unexpected patterns. The technique can be used to combine knowledge-based risk analysis with quantitative/qualitative risk analysis.

The technique assumes that assets, threats and safeguards will have already been identified using knowledge-based risk analysis. It fails to examine threat agents and their capabilities, or any other of their characteristics for that. It is simple and effective, but nothing more than a technique to be used for illustrating purposes.

FIRM

FIRM is a toolset, developed by the International Security Forum (ISF), which includes SPRINT (Simplified Process for Risk Identification), SARA (Simple to Apply Risk Management), and Oscar. The toolset adopts a high level approach to risk management. Its most significant stages are:

1. Identification of resources to be monitored,
2. Information gathering,
3. Analysis of results,
4. Advising of results, and
5. Report production.

According to Jones (Jones '02), the threat in this method is considered to exist, and there is no attempt to allocate any form of metric in order to perform some sort of structuring.

Threat Assessment Methodologies

Jones

The first threat assessment methodology that the author was able to identify was the one developed by A. Jones (see (Jones '02), (Jones '02)). The methodology is illustrated in figure 6 (source (Jones '02)) and has five distinct processes:

1. Causal Factor Identification,
2. Threat Amplifiers Analysis,
3. Threat Inhibitors Analysis,
4. Threat Catalysts Analysis, and
5. Threat Agent Motivators Identification.

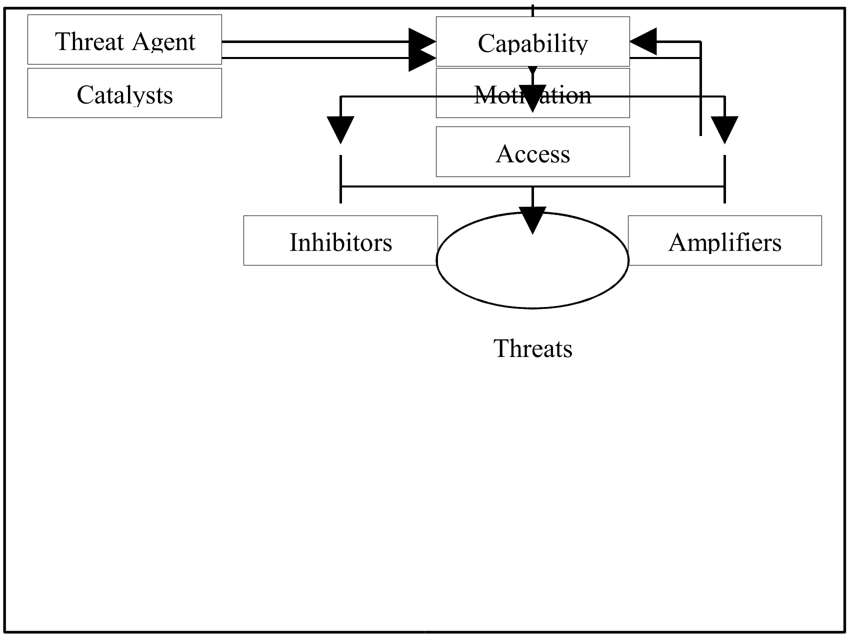

Figure 6 – Jones' Threat Assessment Methodology

The threat agents are getting identified and categorized, and their capabilities are getting analyzed. In another process, catalysts that influence the motivational factor of the agents are being examined. Once a threat agent is being identified as having both the capabilities and the motivations to perform an attack, then two new processes examine the inhibitors and the amplifiers of the threat.

The above methodology is addressing the CNII of a nation hence it fails to realize the needs of corporations that are using electronic payment systems. Although the metrics that are used can very effectively analyse threat agents and their capabilities in manifesting a threat, there is no distinct processes for analyzing the target organization, the needs of the business and the assets used by the system. Furthermore there is no process for identifying vulnerabilities and analyzing the impact of their interrelationships.

VIM

VIM stands for Vulnerability Instantiation Methodology. It is a two-stage method that is using vulnerabilities and their relationships in order to identify and analyse threats. The model has a set of prerequisites. It requires the user to run one of the many commercial vulnerability detection tools in order to identify the vulnerabilities of the examined system, and be used as input. Secondly it requires an information security policy document in order to:

- Identify a threat agent preference structuring and selection,
- Specify which asset are to be secured, and
- Specify the scope of the assessment.

For each identified vulnerability, VIM is concerned with two things:

- The effort required by the threat agent to exploit it, and
- The assets that it will put at risk after its exploitation.

The first stage of the model discards those vulnerabilities that are too “expensive” so as to fall outside the scope of the assessment, specified by the information security policy document. The “expensive” term is examined under the context of:

- Collusion: the level of authorization to the system in order to exploit its vulnerability
- Connection: the type of connection to the target machine
- Time: the time required to exploit a vulnerability
- Expertise: the knowledge required to exploit the vulnerability

The second stage of the model removes anything that does not threaten a protected asset.

VIM is more of a tool that can be used inside a threat assessment methodology, rather than a threat assessment methodology itself. There is no business analysis, and no interaction with the stakeholders. The model takes input from the policy document and the vulnerability identification tools “as is” and without asking any questions. It cannot address change as although it examines the threat agent capabilities, the calculations are based on the policy document. The author does not believe that the model can effectively understand all the interrelationships of the vulnerabilities, and as a result it fails to effectively analyse all the threats. Impact calculation is not existent, but that was never one of the goals of the model. Vim’s’ approach is that all threats that can potentially harm an asset specified in the policy document should be protected. The source for VIM is (Barker '98).

Threat Assessment Models

OCTAVE

OCTAVE (Alberts '99), (Alberts '01) stands for Operationally Critical Threat, Asset, and Vulnerability Evaluation Framework and was developed by the Carnegie Mellon University. It is a framework for identifying and managing information security risks. It allows an organization to identify the information assets that are important to the mission of that organization, the threats to those assets, and the vulnerabilities that may expose those assets to the threats. It contains three phases and eight processes.

- Build Enterprise-Wide Security Requirements
  - Identify Enterprise Knowledge,
  - Identify Operational Area Knowledge,
  - Identify Staff Knowledge, and
  - Establish Security Requirements.
- Identify Infrastructure Vulnerabilities
  - Map High-Priority Information Assets to Information Infrastructure, and
  - Perform Infrastructure Vulnerability Evaluation.
- Determine Security Risk Management Strategy
  - Conduct Multi-Dimensional Risk Analysis, and
  - Develop Protection Strategy.

Phase 1, “Build Enterprise-Wide Security Requirements”, examines the organization by eliciting information from people working in different levels. By combining the different perspectives it allows for the security analyst to have a greater understanding of the business. Having the process for obtaining information about the assets of the business is considered to be best practice. Having the same process though for obtaining information about the threats that those assets are facing is wrong. We cannot expect that the user of a system will be able to know the above information. There is nothing wrong in involving the user in the threat identification process. Quite the contrary, the user of a system should be involved, as he/she has the best knowledge of the system. Having the user performing a threat assessment though is a totally different matter. In this phase the assessor is performing the steps of business analysis, boundary identification, asset identification and threat generation.

Phase 2, “Identify Infrastructure Vulnerabilities”, uses the asset and threat information gathered form phase 1 to perform a preference structuring of the information infrastructure, and an evaluation in order to identify vulnerabilities. In this phase information about threats, and assets are combined with staff knowledge. Intrusion scenarios are being put together in order to identify missing policies and practices as well as infrastructure vulnerabilities. In this phase the assessor is performing the steps of modeling, scenario construction, vulnerability identification and vulnerability preference structuring. The identified shortcoming is the use of standard catalogs of intrusion scenarios and vulnerabilities. That means that there is no threat agent identification and/or threat agent capability analysis. The concept of change is very important in today’s electronic era, and the time interval of that concept is very small.

Phase 3, “Determine Security Risk Management Strategy”, analyses the results gathered in the first two phases in order to identify and prioritize risks to the enterprise. The assessor performs the steps of impact analysis, probability estimation, risk preference structuring, and countermeasure proposal. The impact and the probability of the risk are used to perform the preference structuring. As with other methodologies, the use of probabilities with the concept of risk constitutes a major shortcoming.

Amenaza IT Threat Tree Modeling System

Amenaza Technologies Ltd. has developed a system that is using hierarchy trees to model threats. It is using a probabilistic approach to assign downtime values to the assets of the system. The down time is used to calculate the risk of the threat, which is then multiplied with the impact of the threat to give as the risk value. The system has two distinct phases and eight processes:

- Vulnerability Identification & Threat Analysis
  - Scope,
  - Threats & Vulnerabilities in Tree Format,
  - Threat Agents,
  - Threat Indicator Functions, and
  - Analysis of Environmental Threats.
- Incident Impact & Threat Mitigation
  - Identifying Threats that Require Mitigation, and
  - Neutralizing Danger by Mitigating Threats.

In the first phase the scope of the assessment is being determined, and the threats against system vulnerabilities are being put together in a diagrammatic tree form. Once the trees are completed the threat agents are being identified and analyzed in order to realize their capabilities. Because threats are associated with a different complexity, the threat indicators are analyzed in order to be able to perform the threat elimination stage based on the characteristics of the threat agents. The threats that will “survive” the first phase will constitute the input of the second one, where their impact is getting analyzed, and mitigation procedures are being considered.

The author would argue that using threats as nodes for the tree models is not logical. In the initial stage the assessor cannot possibly know all the existing threats, and/or those that will have to exclude or include based on other parameters from other processes of the model. It seams like extra work that can be avoided. During a live threat assessment the concept of time is a very expensive commodity.

The threat indicators that are used to examine the capabilities of the threat agents are: the cost of the attack, the apprehension probability, and the technical ability. The model fails to address the motivational factor of the agents; hence it has a difficulty assessing irrational agents and/or their actions. During the lifetime of this research, the author has concluded that motivation is the main factor that “guides” a threat agent to certain actions. The likelihood factor is nice only in paper, for the financial people that cannot accept certainty. When dealing with sensitive computer systems that are offering an online service, it only takes one individual to cause havoc. One in the billions of online computer literate persons on the planet, given the right circumstances can bring any company down to its knees.

The model is calculating threat impact by analyzing the breach of confidentiality, integrity and availability of the assets in the following business fields:

- Safety,
- Customer impact,
- Environmental,
- Public perception,
- Regulatory, and
- Financial.

The above is not considered to be complete, especially for systems where more than one type of stakeholder is being involved.

The model is approaching the problem of proposing countermeasures from a mathematical point of view. It is trying to mitigate risks and not threats, which today in most situations is misleading. The proposed countermeasure techniques are grouped in the following categories:

- Authentication,
- Authorization,
- Encryption,
- Hardware,
- PKI, and
- Policies and practices.

The user is then comparing the cost of the mitigation towards the cost of the risk and if the mitigation is cost effective then countermeasures can be deployed. The major shortcoming of this approach is that not all risks can have accurate monetary values associated with them, and that most of the time it is difficult for an assessor to fully understand the full consequences of a risk, hence be certain for the deployment (or not) of countermeasures.

Conclusion - Critical Comparison of Examined Methods

The examined methodologies and models have a number of shortcomings. Comprehensive quantitative risk analysis is time consuming and expensive. Qualitative approaches, although reducing the complexity of the problem, are not scientifically well defined, and there is a lot of uncertainty in the field. All of the examined methodologies and models are following the waterfall method (Pressman '01) for calculating and producing results. That means that they are not flexible enough and cannot cope with the amount of changes that their inputs have to go thought during the lifetime of the assessment. UKERNA is supporting that the most conservative statistics indicate that every single computer system in the whole of the world, which is connected to the Internet will be the target of an attack across the network, at least once a week (see Cormack (Cormack '02)). All the models do not examine the sources of the threats but wrongly assume that the users are already familiar with the concept of the threat agents. Furthermore, they are using probabilities for calculating the likelihood of the threat, without examining the likelihood of the agent. Just the concept of using probabilities greatly undermines the validity of the methods. The collected data are interpreted according to the experience of the analyst and results are often not reproducible (see Jones (Jones '02)). None of the methods is trying to model the examined systems in the business environment hence various assumptions are made. These assumptions can lead to wrong estimations on threats and vulnerabilities. Most of the models only think of the threat impact as only causing a financial loss. A threat though can have an impact on various levels and aspects of a business. The generic framework for electronic commerce (see Kalakota (R. Kalakota '97)) represents a fine example of all these different levels. The proposed model must be able to understand the flows and powers to and from these levels in order to understand how the business is using electronic commerce, and be able to address the multidimensional character (Solms '01) of information security at those levels.

If we imagine the existing methodologies and models as being a black box then the process start with the users placing inputs inside the box. What is already in the box cannot see what the users are going to place in the box, and in their turn, the users cannot see / understand what is already in the box. After the end of the “input” phase, the users give the box a good shake, and wait for some output. There is always a probability of getting something meaningful out of the box, but corporations today do not like probabilities when their own survivability is at stake (feature '02), (S. Garfinkel '97).

The other way of thinking about the existing methodologies is the making of the Greek coffee. Everybody knows how to make Greek coffee as long as they are Hellenes, or being taught by Hellenes. Everybody has his own perception about what the Greek coffee is and what is the proper way for making one, but only Hellenes really know how. The proper result is based on the concept of probability, as there is no real measurement on how much coffee and sugar to put in the shaker, only estimations. Furthermore, the result is totally subjective as each person has a totally different taste.

Table 5 presents a critical comparison of the examined risk assessment methodologies & models.

	CRAMM	ARiES	Pfleeger	Carroll	Summers	COBRA	FRAP	TAME
Explore & Assess IS Threats to Business Operations in relation to Type of Business								
Boundaries ID	Yes	No	No	No	No	No	No	Yes
Scenario Construction	Yes	No	No	No	No	No	No	Yes
Business Analysis	No	No	No	No	No	Yes	Yes	Yes
Threat Agent Identification & Selection	No	No	No	No	Yes	No	No	Yes
Threat Agent Preference structuring	Yes	No	No	No	No	No	No	Yes
Business Modelling	No	No	No	No	No	No	No	Yes
Asset ID	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Determine what Policies, Standards & Controls are worth implementing to reduce identified threats								
Impact Analysis	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Vulnerability Identification	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Vulnerability complexity calculation	No	No	No	No	No		No	Yes
Promote awareness & understanding amongst all stakeholders								
Stakeholder Analysis	No	No	No	No	No	No	Yes	Yes
Evaluation of results	Yes	No	No	No	No	No	Yes	Yes
Assess compliance with standards & control effectiveness								
ISO 17799	Yes	No	No	No	No	Yes	Yes	No
ISO 15408	No	No	No	No	No	No	No	No
Ability to evolve and react to external stimuli as they happen								
Top Down Approach	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Bottom Up approach	No	No	No	No	No	No	No	Yes
Threat agent capabilities analysis	No	No	No	No	No	No	No	Yes
Countermeasure analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Use of formal methods in threat calculations								
Probabilistic approach	Yes	Yes	Yes	Yes	Yes		Yes	No
Hierarchical approach	Yes	No	No	No	No		No	Yes

Table 5 – Critical Comparison of Risk Assessment Methodologies & Models

Table 6 presents a critical comparison of the examined threat assessment methodologies and models.

	Jones	OCTAVE	AMEZANA	TAME	VIM
Explore & Assess IS Threats to Business Operations in relation to Type of Business					
Boundaries ID	No	No	No	Yes	No
Scenario Construction	No	Yes	No	Yes	No
Business Analysis	No	Yes	No	Yes	No
Threat Agent Identification & Selection	Yes	No	Yes	Yes	Yes
Threat Agent Preference structuring	Yes	Yes	Yes	Yes	Yes
Business Modelling	No	Yes	Yes	Yes	No
Asset ID	No	Yes	No	Yes	Yes
Determine what Policies, Standards & Controls are worth implementing to reduce identified threats					
Impact Analysis	Yes	Yes	Yes	Yes	No
Vulnerability Identification	No	Yes	No	Yes	No
Vulnerability complexity calculation	No	No	Yes	Yes	Yes
Promote awareness & understanding amongst all stakeholders					
Stakeholder Analysis	No	Yes	Yes	Yes	No
Evaluation of results	No	Yes	No	Yes	No
Assess compliance with standards & control effectiveness					
ISO 17799	No	No	No	No	No
ISO 15408	No	No	No	No	No
Ability to evolve and react to external stimuli as they happen					
Top Down Approach		Yes	Yes	Yes	Yes
Bottom Up approach		No	No	Yes	No
Threat agent capabilities analysis	Yes	No	Yes	Yes	Yes
Countermeasure analysis	No	Yes		No	No
Use of formal methods in threat calculations					
Probabilistic approach	No	No	Yes	No	No
Hierarchical approach	Yes	Yes	Yes	Yes	Yes

Table 6 – Critical Comparison of Threat Assessment Methodologies & Models

From the sections on threat agents, vulnerabilities and threats we can see how the field of cyber crime has change over the past few years. Threat agents constantly mutate becoming bigger and better, new vulnerabilities are being discovered every year or old ones merge and mutate, and the nature of threats has greatly changed. The “old” methodologies that we had to analyse and manage risk are not adequate any more, and indeed risk and trying to manage it is not considered to be best practice any more. That is why there is a need for a 3rd generation threat assessment methodology that will be able to address change in every field, be modular in order to be efficient, and in the same time user friendly as security is already expensive without ambitious security consultants trying to become richer by introducing a sophisticated and complex methodology.

References