Analyzing Threat Agents & Their Attributes

Dr. Stilianos Vidalis[1], Dr. Andrew Jones[2]

[1] 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

[2]Research Group Leader,
BT Group,
Security Research Centre
0044 1473 647133

Andrew.28.jones@bt.com

Table of Contents

List of Figures

List of Tables

Abstract:

Modern risk assessment techniques recognize that there is a need to perform a threat assessment in order to identify the threats that a system is facing, and the agents that are able to manifest them. Most of them though do not incorporate the process of identifying and analyzing threat agents. Gathering IDS data and analyzing them is a challenge on its own, but identifying threat agents, and analyzing their attributes is a different game altogether. Is an agent motivated enough to pursue his/her target? Does the agent have the technical capability and the knowledge required to exploit a vulnerability? Our intention is not to put labels in certain categories of people, rather to try and understand these and stimulate the discussion between all those of good faith.

Keywords: threat agent, threat agent identification & analysis, threat agent categorization, threat agent metrics

1. Setting the Scene

Information systems have changed our lives drastically. The global economy depends on computing infrastructures that are scattered around the world, functioning in different environments, having to face different types of threats (see (Hinde 2001)). "*The increasing use of interconnected networks makes these crimes [computer crimes] easier than ever*" (Icove, Seger et al. 1995). The Internet has made computer fraud much easier, and the corporate world, over the past decade, actually equipped threat agents with the means to perform computer crimes. "*…technological advances…including communications…were often accompanied by lack of foresight, thereby inadvertently opening doors to new forms of vulnerabilities following deployment*" (Ghosh 2004). The introduction of the personal computer to every household, the development and use of "unsecured" operating systems and software, and the use of broadband connectivity, are the aforementioned means. In the martial arts field, knowledge and responsibility are tied together. In the "cyberworld" of today, most threat agents have the knowledge without the responsibility and/or or the maturity, for using it.

Protecting the enterprise networks from the different computer criminals is not a straightforward procedure. Techno phobic grey men, sitting behind their wide wooden desks in dark offices cannot estimate cyber threats and cannot provide solutions in today's environment. Organizations are allocating vast amount of resources for protecting their infrastructures, but not always with the expected result. Agreeing with (Hinde 2003), it is the threat agents that manage the threats, and not the security officers. Modern threat assessment methodologies acknowledge that there is a need to analyze and understand the range of the threat agents that a system is facing and/or will have to face in the future. For the purposes of this paper, we will use the following definition for threat assessment:
A threat assessment is a statement of threats that are related to vulnerabilities, an organisation's assets, and threat agents, and also a statement of the believed capabilities that those threat agents possess.

The concise oxford dictionary 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 1996).
- A weakness in the security system that might be exploited to cause harm or loss (Pfleeger 1997).

- Some weakness of a system that could allow security to be violated (Blyth and Kovacich 2001).

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

> *Vulnerability is a measure of the exploitability of a weakness.*

When it comes to threat, there is a range of valid definitions. The concise oxford dictionary 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 (Blyth and Kovacich 2001) 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 paper, threat is a function of a threat agent's motivation, capability, opportunity, and the impact that a successful attack would have on an organization.
- Threat = Function (Motivation, Capability, Opportunity, Impact)

1.1 Motivation

The concise oxford dictionary 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 2002), there are some commonly accepted motivational drivers, which are: political, secular, personal gain, religious, revenge, power, terrorism, and curiosity. For the purpose of this paper 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 threat agent to consider attacking a computer system. Analysis of computer criminals suggests that the primary motivations include the following, sometimes in combination:

- The need to resolve intense personal problems such as job related difficulties, mental instability, debt, drug addiction (Stoll 1989), loneliness, jealousy, and the desire for revenge,
- Peer pressure and other challenges, for example, among malevolent hackers,
- Idealism and extreme advocacy, for example, by espionage agents and terrorists,
  Financial gain.

1.2 Capability

The concise oxford dictionary 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 to use the tools and techniques correctly.
- The availability of education and training to support the correct use of various tools and techniques.
- The level of resource that a threat agent has, or can acquire over a certain time.

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

1.3 Opportunity

The concise oxford dictionary defines the word opportunity as meaning, a favorable occasion for action. Sun Tzu (Denning 1999) 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 he must have the correct conditions to do so, and in order for his 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 should to do is making sure that threat agents will be in no position of creating that opportunity for themselves.

1.4 Impact

The term impact is used to denote the result of a threat reaching an asset (J.D.Nosworthy 2000). The threat impact can be on the market share of the company, or even more important the user trust. These impacts cannot be easily assigned a financial value 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. The classification of threat impact levels that will be used in this paper is the following:

- Insignificant: unauthorized use of asset without actual loss, no other effect in enterprise
- Minor: minor loss of 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 is realized

The impact level is related to the enterprise. An impact that is moderate for one enterprise might be insignificant for another. For example, the loss of the only web server of an SME that is offering on-line services will probably be catastrophic. On the other hand, the loss of a web server that is part of the British Petroleum infrastructure will probably be insignificant. Some of the enterprise attributes that affect the impact level are: the number of staff, the size of the enterprise and of its supply chain, the revenues of the enterprise and its capital, the level of exposure and sensitivity to market pressure and of course the type of business that the enterprise is conducting.

1. Threat agents? What threat agents…?

In the old days, the public used to mistakenly call most of the individuals that were attacking computers "hackers". No matter who they were, no matter what technique they used for attacking, no matter what type of attack they performed, they were all addressed as "hackers" (see (Rees 1996)). Nowadays though, people are more literate, and they understand that the term "hacker" does not necessarily describe an individual with malicious intend (for a definition of the hacker see later section), neither is able to describe all the individuals that have an interest on a computing system. Instead, computer literate people are using the term "threat agent" for describing individuals and/or groups that might have an interest in performing one or more types of attacks against a computing infrastructure. For the purposes of this paper the following definition will be used:

> The term **threat agent** is used to denote an individual or group that can manifest a threat.

These individuals and groups are classified in figure 1. The "old style" InfoSec officers could immediately argue with the following figure. Obvious categories such as: hackers, crackers, amateurs, and insiders are not included. That is because we have followed a different approach. The nature of "computer crime" has changed over the past decade, so the perspectives under which we examine it, have to change as well. Any threat agent can by an insider. We will define the insider as:

An **insider** to an organization is a threat agent who is directly or indirectly employed by that organization, and has access to the system or sensitive information not otherwise disclosed to him and to the general public.

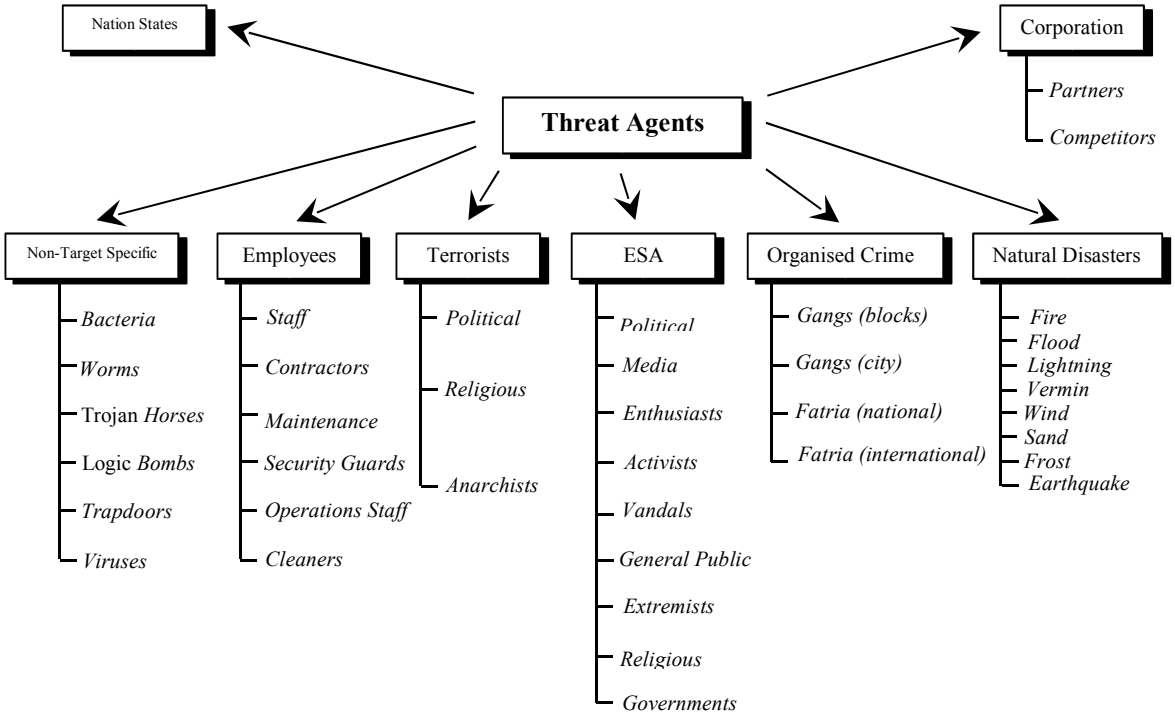

Figure 1: Threat Agent Classification

More of the point, most threat agents are insiders, as they are employed by one or more organizations (Kovacich 2000), hence making the distinction between insiders and outsiders is not considered efficient and helpful for an effective threat assessment. Instead, the status of the agent towards the organization has to be considered as an attribute of the agent. An insider prediction tool was presented by (Maglaras and Furnell 2002) where is quoted: "…49% of the respondents faced IT security incidents due to the actions of legitimate users". Statistics on "insiders" in the UK can be seen in the UKs National High-Tech Crime Unit survey (NHTCU 2004) and in the US on the FBI survey (Richardson 2003).

Threat agents will be Hackers, crackers, or amateurs (script-kiddies), depending on their knowledge and attitude about computers. Hackers under no circumstances should be confused with crackers. The following definitions will be used:

> **Hackers** are persons interested in the arcane workings of computing systems. Hackers constantly seek to further and freely distribute knowledge. Hackers will never intentionally disrupt data.
>
> **Crackers** are persons who violate the system integrity, with malicious intent. Crackers enjoy this abuse and the temporary power that it gives them.

When considering threat agents under the context of cyber-security, then all of them fall under one of the following: hacker, cracker, amateur, so it is more efficient to use the structure presented in figure 1, and then differentiate our threat scenarios depending on the agent. There is only one exemption in the above statement. Agreeing with (Conway 2003), terrorists are not likely to hire hackers, but they can train themselves up into “acquiring” that “status”.

Of course, in addition to individual people and groups, Mother Nature can be a threat agent as well. Natural disasters such as fire, floods, lightning, and earthquakes can have a major impact to the survivability of a corporation. Natural disasters may or may not have a human agent in the background. For example, a laboratory inside a tropical rainforest has taken all the necessary precautions, and according to calculations, the fire threat from Mother Nature has been nullified. The scenario of a human agent helping Mother Nature though, ensuring that certain “amplifiers” (see (Jones 2002)) will be in place, greatly change the level of the threat. Other natural causes that fall under this category are damage from: extreme temperature, sand storms, windstorms, vermin and earthquakes.

One more concern of the authors is that of malicious software, and if we can classify these programs as a different threat agent category. According to (Blyth and Kovacich 2001), (Forcht 1994), and (Smith 1993) the largest component of the unintentional threat agents arises from the use of software. Software can never be exhaustively tested for bugs, and the larger a piece of software the greater the chance of encountering a bug when using it. Malicious programs are everywhere and in great numbers. They are probably one of the most sophisticated threats to a computer system. The following figure illustrates the different types of malicious programs (source (Stalling 2000)).

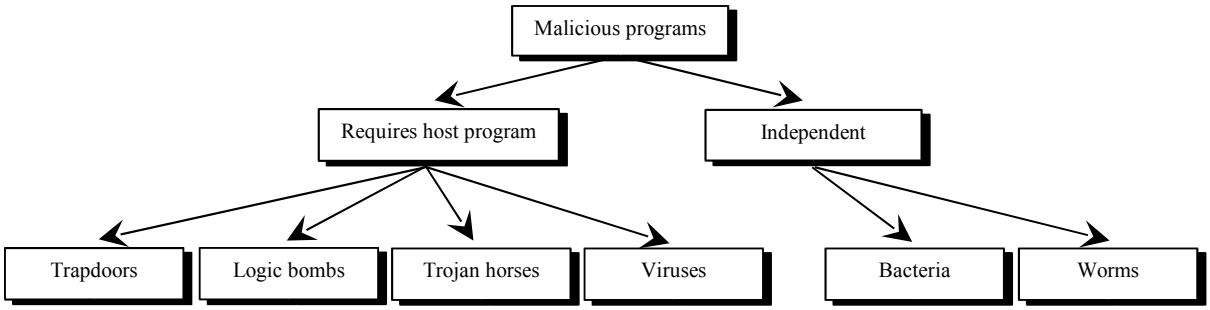

Figure 2: Malicious Programs (source Stalling 2000)

Our argument is that with today’s technology, using certain artificial intelligence techniques, one could develop a malicious program able to “understand” the environment it is in, and react to certain stimuli. In the hypothetical case of such a program attacking a computer system, then the threat agent the enterprise is facing is not the programmer that developed the malicious program, but the program itself. Two very dangerous and important attributes of malicious software are the polymorphism and the metamorphism (Skoudis 2004). Analysing the different types of malicious programs goes beyond the scope of this paper, but needless to say, the most dangerous types are those that do not need a host program to run, are platform independent, and can mutate over time according to external or internal stimuli.

2. Threat Agent Identification

In agreement with (Summers 1977) and (Nosworthy 2000), the threat agent identification should be a continuous process as their attributes change constantly. Information from different sources should be collected and combined where appropriate, and threat agents should be identified and classified according to their nature and the scope of the assessment. Once an entry is recorded it should not be deleted as threat agents can exist in different states (active, inactive, dormant, dead…). It is accepted that threat agents may mutate over time, acquiring new capabilities. We believe that it is important, and completely ethical, to observe threat agents and record their movements throughout their lifetime. It is often that one threat agent arose like the phoenix from the ashes of an old one. The following inputs could be used to identify threat agents:

- Threat agent catalogue – standard catalogues of threat agents acquired from the national and international authorities.

- Historical threat agent data – data about the activity of threat agents collected by the enterprise and other private and/or public organizations.
- Enterprise technical environment reports – based on the Porters' model (Johnson and Scholes 1999), examining the technical environment we will be able to identify the nature of threat agents that are active (or inactive) in that environment.
- Business environment reports – examining the business environment we will be able to identify the nature of threat agents that are active (or inactive) in that environment.
- Physical environment reports - examining the physical environment we will be able to identify the nature of threat agents that are active (or inactive) in that environment.
- Current knowledge of senior managers – senior managers will have knowledge of the main incidents that occurred in the past.
- Current knowledge of stakeholders – stakeholders will have a high level view of the history of incidents.
- Current knowledge of staff – staff will have detailed knowledge of most incidents.
- Stakeholder List – identified stakeholders might be associated with threat agents.

One threat agent attribute that will have to be taken into consideration in a threat assessment is the hostility intention. Figure 3 presents the "hostility" structure.

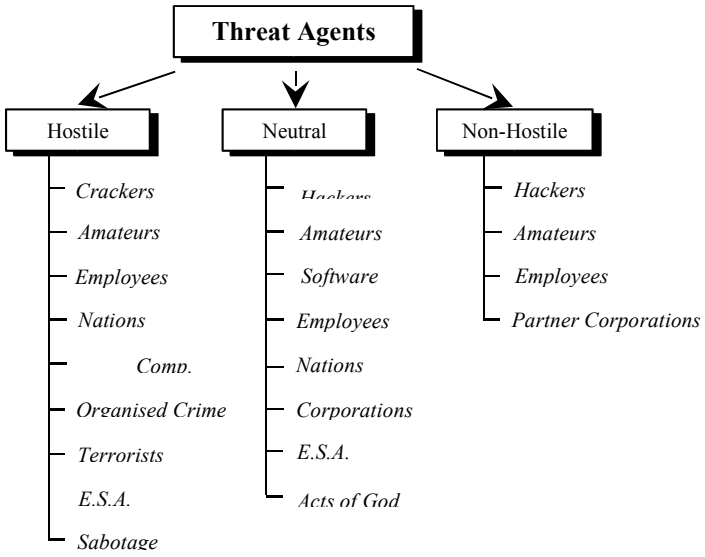

Figure 3: Hostility Diagram

We use the term "hostile" to express an intention towards the system, and if they have identified it as a target. From their nature career criminals and crackers can only be hostile towards a system. On the other hand, amateurs and hackers can cause either intentional or unintentional damage. Hackers though, by definition, will never be hostile towards a system. Should this happen, then they convert into crackers. Amateurs, most of the times, have no good idea of their actions or of their side-effects, hence they can cause unintentional damage while browsing the network for example. Hackers, although computer literate, most of the times are not able to fully understand the system they are exploiting, and the side effects of their actions to that system. It is not difficult to cause an unintentional disruption to the system simply by following an information gathering technique (see (Scambray, McClure et al. 2001), (Stoll 1989)). The same person can very easily be transformed from a non-hostile agent to a hostile one. The hostility attribute of an agent will change as the agent mutates over time.

Hostile threat agents are those that knowingly set out to cause loss or damage to a system. Crackers are probably the most dangerous hostile threat for a computing system. They are so because they have a brain! That is, they have the knowledge, and the motivation to perform active attacks, and they have the capabilities to create the opportunities needed in order to perform them (the attacks). No information security officer can be so naïve as to claim that he/she is able to predict all the possible actions of a human attacker. The human mind has the unique ability to see a problem from different angles, and should there are no more; it will invent some new ones! Never the less, attackers follow

distinct patterns, which are depended on their knowledge, procedure and scope. These patterns can be used in order to predict the "future" of the attack.

3.2 Likelihood & Importance Analysis

The purpose of a threat assessment can be either preventive or corrective, and the threat assessment can take place either before a system has gone live or after. If there are threat data, then we need to use them for calculating the likelihood of each threat agent. According to Carroll(Carroll 1996) and Stalling(Stalling 2000), threat data can be gathered from: the general population, from a similar system, estimation of number of occurrences in a given time period, and by using the DELPHI approach.

It is obvious that during the likelihood calculation we should ensure that the time period value remains the same for all the agents under analysis. The likelihood calculation activity may use the following inputs:

- Threat Agent Preference List – listing the threat agents that are selected for further investigation,
- History Threat Agent Data – details of threat agent activity from internal and external sources,
- Current knowledge of senior managers – their perspective about threat agent activity,
- Current knowledge of stakeholders – their perspective about threat agent activity,
- Current knowledge of staff – their perspective about threat agent activity.

According to the reports analyzing the environment of the enterprise (based on the five forces from the Porters' model (Johnson and Scholes 1999)), threat agents will be more, or less important in the assessment. For all the entries in the Threat Agent Preference List, we must calculate their importance. The value of the importance property will be a natural number $x : x \in \mathrm{N}$ ranging from 0, for the lowest importance, to a positive number, for the highest important. Threats with an importance of 0 should be excluded from any further investigation, but not from the Threat Agent List, as very easily the assessment variables may change. The importance calculation activity may use the following inputs:

- Threat Agent Preference List – listing the threat agents selected for further investigation,
- Technical Environment Report – examining the technical environment into which the enterprise is operating,
- Business Environment Report – examining the business environment into which the enterprise is operating,
- Physical Environment Report – examining the physical environment into which the enterprise is operating.

4. Threat Agent Attributes

According to (Pfleeger 1997), for a threat agent to be able to exploit a vulnerability, three factors must be in place: the capability factor, the motivation factor and the opportunity factor. For calculating the threat agent attributes, there is a need for a three-dimensional matrix. In the x-axis there will be the selected vulnerabilities of the assets included in the Asset Preference List (list that contains the assets that were selected for further investigation in the threat assessment). In the y-axis there will be the threat agents included in the Threat Agent Preference List. In the z-axis there will be the above three factors (capability, motivation, opportunity), which are of the Boolean data type. They can be either true or false. The following is a graphical representation of such a matrix.

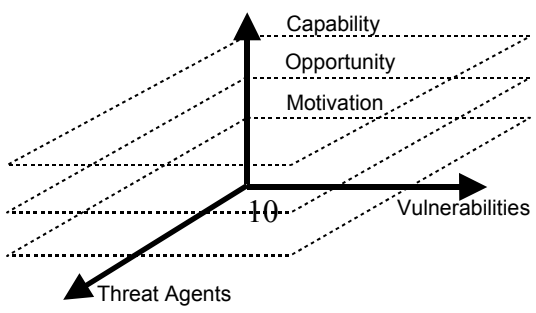

Figure 4: Threat Agent / Vulnerability Matrix

The threats that should "qualify" for further investigation will only be the ones that exist in all three layers of the third dimension.

4.1 Threat Agent Capability Calculation

This activity calculates the capability of each selected threat agent to exploit the selected vulnerabilities of the assets that were included in the assessment. The capability value of each threat agent will have to be examined against the complexity value of each asset's vulnerability. The complexity value is being calculated in another process. The metrics for calculating the threat agent capability can be seen in the following tables. The source of the metrics is (Jones 2002), and the tables are printed after permission from A. Jones.

Table 1: Nation-State Metrics

Factor	Weighting Value				
	1	2	3	4	5
Adult Population	<1M	1–10M	10–50M	50–100M	>100M
Literacy Level	<50%	51-65%	66-80%	81-90%	>91%
Internet Access	V. Low	Low	Medium	High	V. High
History of Relevant Activity	None	Intermittent	Occasional	Regular	Regular & Widespread
Technical Expertise	None	V. Limited	Limited	Adequate	H. Level
Gross Domestic Product per Capita	<$1K	$1-$5K	$5-$10K	$10-$20K	>$20K
Allied Nation Capability	None	Limited	Medium	High	V. High
Indigenous IW Capability	None	Limited	Medium	High	V. High
Other Factors					Religious Fundamentalism, Support of International Terrorism

After taking under consideration the above metrics, the capability is calculated using the following formula:

> Nation-State Capability = (Adult Population of Country * Literacy + Other Factors) + (History of Relevant Activity * 6) + (Technical Expertise * 2 + Indigenous IW Capability * 2 + Internet Access * 2) + GDP per Capita + Allied Nation Capability

Table 2: Terrorism & Terrorist Groups Metrics

Factor	Weighting Value				
	1	2	3	4	5
Number of Activists	<500	501-1k	1k-5k	5k-10k	>10000
Education Level	V. Low	Low	Medium	High	V. high
Internet Access	V. Low	Low	Medium	High	V. High
History of Relevant Activity	None	Intermittent	Occasional	Regular	Regular & Widespread
Technical Expertise	None	V. Limited	Limited	Adequate	H. Level
Funding	None	V. Limited	Limited	Adequate	Unlimited

After taking under consideration the above metrics, the capability of the "Terrorist Groups" is:

> Terrorist Group Capability = (Number of Activists * 5 + Level of Education * 2) + (History of Relevant Activity * 7 + Technical Expertise * 2 + Internet Access * 2) + (Funding * 2)

Table 3: ESA Metrics

Factor	Weighting Value				
	1	2	3	4	5
Spread of Membership	1-5	6-10	11-20	21-30	>31
Number of Members	<500	501-1K	1K–5K	5K–10K	>10K
Funding	None	V. Limited	Limited	Adequate	Unlimited
Target Type	Local	National	National, High Profile	International	International, High Profile
History of Relevant Activity	None	Intermittent	Occasional	Regular	Regular & Widespread
Sponsoring Countries or Organizations	1-5	6-10	11-20	21-30	>31

After taking under consideration the above metrics, the capability of the "ESA" threat agent is calculated using the following formula:

ESA Capability = (Number of Activists * 5 + Spread of membership * 2) + (History of Relevant Activity * 7) + Target Type * 2) + (Attack Characteristics) + (Sponsorship) + (Funding * 2)

Table 4: "Corporation" Metrics

Factor	Weighting Value				
	1	2	3	4	5
Market State	Decline	Static	Volatile	Buoyant	Turmoil
Organization Size	1 - 500	501- 1K	1K – 5K	5K – 10K	Over 10K
Target Type	Local	National	National, High Interest	International	International, High Interest
History of Relevant Activity	None	Intermittent	Occasional	Regular	Regular & Widespread
Technical Expertise	None	Very Limited	Limited	Adequate	High Level

After taking under consideration the above metrics, the capability of the "Corporation" threat agent is calculated using the following formula:

Corporation Capability = (Market State * 4) + (Organization Size * 4) + (Type of Target * 2) + (History of Relevant Activity * 7)

Table 5: "Criminal Groups" metrics

Factor	Weighting Value				
	1	2	3	4	5
Geographic Group Range	Decline	Static	Volatile	Buoyant	Turmoil
Group Size	<500	501-1K	1K–5K	5K–10K	>10K
Type of Crime	Prostitution, Usery, Protection	Construction, Debt Collection	Fraud	Money Laundering, Gambling	Industrial Espionage, Smuggling
History of Relevant Activity	None	Intermittent	Occasional	Regular	Regular & Widespread
Technical Expertise	None	V. Limited	Limited	Adequate	H. Level

After taking under consideration the above metrics, the capability of the "Criminal Groups" threat agent is calculated using the following formula:

Criminal Group Capability = (Group Range * 3) + (Group Size * 3) + (Type of Crime * 4) + (History of Relevant Activity * 4) + (Technical Expertise * 7)

Table 6: "Hacker/Cracker/Amateur Groups" metrics.

Factor	Weighting Value				
	1	2	3	4	5
Group Size	<50	51-100	101–200	201–300	>300
History of Relevant Activity	None	Intermittent	Occasional	Regular	Regular & Widespread
Technical Expertise	None	V. Limited	Limited	Adequate	H. Level
Reason for Target Selection	Curiosity	Rebellion	Criminal Gain	Belief	Revenge, Religion, Racism, Nationalism

After taking under consideration the above metrics, the capability of the "Hacker/Cracker/Amateur Groups" threat agent is calculated using the following formula:

> Hacker/Cracker/Amateur Group Capability = (Group Size * 4) + (History of Relevant Activity * 7) + (Technical Expertise * 3) + (Target Selection * 6)

The activity for calculating the threat agent capability could use the following inputs:

- Threat Agent Metrics – tables containing metrics for each threat agent category,
- Historical threat agent data – threat agent data from internal and external to the enterprise sources
- Threat Agent Preference List – listing the threat agents selected for further investigation.
- Vulnerability List – listing vulnerabilities of the assets listed in the Asset Preference List,
- Vulnerability Preference List – listing vulnerabilities selected for further analysis.

4.2 Threat Agent Opportunity Calculation

This activity calculates the opportunities that are presented to each selected threat agent for exploiting the selected vulnerabilities of the assets that were included in the threat assessment. The opportunity factor is affected by the following variables:

- Access to Information – an agent that does not know of a vulnerability cannot exploit it,
- Changing Technologies – new technology might give the means to an agent to exploit a previously countered vulnerability,
- Target Vulnerability – a vulnerability that either is not discovered or not countered by the enterprise.
- Target profile – the profile of an enterprise might offer an opportunity to an agent, e.g.: a university has to maintain an "open" network.
- Public Perception – perception is an important factor with a range of weightings. Depending on the agent and on the enterprise, public perception might have a tremendous weighting on the opportunity factor, e.g.: a pharmaceutical company is perceived to be conducting illegal experiments to animas; activists now have the opportunity to legitimately attack the above company, having the public support in their side.

The concept of metrics is not feasible in this calculation. The assessor will have to use the reports analyzing the environment of the enterprise, and the perspective of the stakeholders in order to identify the opportunities that are presented to the threat agents listed in the Threat Agent Preference List.

The activity could use the following inputs:

- Threat Agent Preference List – listing the threat agents selected for further investigation.
- Current knowledge of stakeholders – their perception and opinion on the types that should be further examined.
- Technical Environment Report – examining the technical environment into which the enterprise is operating,
- Business Environment Report – examining the business environment into which the enterprise is operating,
- Physical Environment Report – examining the physical environment into which the enterprise is operating.

- Vulnerability List – listing vulnerabilities of the assets listed in the Asset Preference List,
- Vulnerability Preference List – listing vulnerabilities selected for further analysis.
- The existence of all inputs is not obligatory. Based on the state of the enterprise and the experience of the assessor other inputs might be available.

4.3 Threat Agent Motivation Calculation

This activity calculates the motivation of each selected threat agent for exploiting the selected vulnerabilities of the assets that were included in the threat assessment. The activity uses the information about threat agents in conjunction with the vulnerability information from this stage to calculate the motivational factor of each agent.

According to Jones (Jones 2002), the factors that motivate a threat agent are diverse and might operate singly or in unison. According to the previous author the primary groupings of threat agent motivators are the following:

- Political –
- Secular – supporting secular believes will motivate the agents to a high level of action,
- Personal Gain – it can be financial gain, acquisition of knowledge, and/or peer recognition. Hackers will be highly motivated when they are hunting for knowledge, crackers will be highly motivated when they are trying to be recognized, and organized criminal groups will be highly motivated when there is a financial gain behind their actions.
- Religion – This is one of the most regularly observed motivational factors. “Holy” wars have been fought throughout history. While the traditional wars are mutating to become informational wars, this motivational factor is expected to become one of the most important ones. People are ready to die to fulfill their religious believes and will proceed to extreme actions for doing so. Attacks caused by this motivational factor are expected to be conclusive.
- Terrorism – Cyber-terrorism is expected to be the next mutation of terrorism, as we know it in the 21st century. Although most recognized terrorist groups do not have the capability to enter such a phase, there are more than one instances of such groups displaying cyber-terrorist actions. Traditional terrorist actions have the unique goal of causing terror. Cyber-terrorist actions will have exactly the same goal, so the attacks will have quite a large impact on the enterprise.
- Curiosity – Hacker’s main line of defense. A hacker moved by curiosity is expected to go in an extreme way in order to fulfill this basic need. Attacks initiated by this factor are expected to succeed as time becomes of no importance. An agent will not spend extreme resources, but it will try a variety of methods in order to acquire the necessary information.

The activity could use the following inputs:

- Current knowledge of senior managers –
- Current knowledge of stakeholders –
- Threat Agent Preference List – listing the threat agents selected for further investigation,
- Threat Agent List – listing the identified threat agent individuals and groups,
- History threat agent data – threat agent data from internal and external to the enterprise sources,
- Threat Agent Metrics – tables containing metrics for each threat agent category,
- Vulnerability List – listing vulnerabilities of the assets listed in the Asset Preference List (O5.2),
- Vulnerability Preference List – listing vulnerabilities selected for further analysis.

The existence of all inputs is not obligatory. Based on the state of the enterprise and the experience of the assessor other inputs might be available.

5. Conclusion

It is accepted by the EU that there are several “cyber-threats” (see (Pounder 2001)) and that all member-countries should collectively find a solution for minimizing those threats. Despite the warnings

though, the worldwide economic damage due to “cyber-threats”, in 2002 was more than $35.000m (source (Goodwin 2002)). Based on these figures, it is apparent that old solutions cannot address and manage modern risks. Modern security management methods now acknowledge that most risks cannot be completely eliminated and that they need to be managed in a cost effective manner.

We have argued that the information security officers should be concerned with the threats that their system is facing and not with the risks. Our modern computing world demands the development of new methods for effectively and accurately tackling threats. Our approach is trying to manage threat by examining its source, the threat agent. It is our belief that by taking away from the threat agents the capability of creating the opportunities for exploiting vulnerabilities, we can effectively minimize the “cyber-threats” that are responsible for millions in financial losses every year.

A system that will effectively monitor threat agents and their actions in cyberspace is being developed by the Information Security Research Group (ISRG) of the University of Glamorgan. The system is called G4DS and is using GRID technology to exchange knowledge about security incidents and countermeasures.

6. References

(Barber '01). Barber, R. (2001). "*Hacking Techniques*", Computer Fraud & Security, 2001(3): 9-12.

(Barber '01). Barber, R. (2001). "*Hackers Profiled - who are they and what are their motivations*", Computer Fraud & Security, 2001(2): 14-17.

(Bequai '01). Bequai, A. (2001). "*Organized Crime Goes Cyber*", Computers & Security, 20(6): 475-478.

(Blyth '01). Blyth, A. J. C., L. Kovacich (2001). “*Information Assurance: Computer Communications & Networks*”. UK, Springer-Verley.

(Brown Commission '96). Brown Commission (1996). “*Roles and Capabilities of the United States Intelligence Community*”, p27, http://www.fas.org/irp/congress/1996_hr/s9606053.htm

(Carroll '96). Carroll, J. M. (1996). “*Computer Security*”, Butterworth-Heinemann.

(Conway '04). Conway, M. (2004). “*Cyberterrorism: academic perspectives*”, 3rd European Conference on Information Warfare & Security, 2004, Royal Holloway, University of London, UK.

(Cushing '02). Cushing, K. (2002). “*IT Directors Must Review Security Every 90 Days*”, 19 December, Computer Weekly: 4

(Denning '99). Denning, D. E. (1999), “*Information warfare & security*”, Addison-Wesley.

(Denning '01). Denning, D. E. (2001). "*Cyber-warriors: activists and terrorists turn to cyberspace*", Harvard International Review, 23(2): 70-75

(Daughtrey '01). Daughtrey, T. (2001). "*Costs of trust for e-business*." Quality Progress.

(Forcht '94). Forcht, K. A. (1994). “*Computer Security Management*”, Boyd & Fraser.

(Goodwin '02). Goodwin, B. (2002). “*Record Wave of Hacking Targets UK Business*”, 31 October, Computer Weekly: 6

(Goodwin '03). Goodwin, B. (2003). “*Whitehall acts to marshal UK's security expertise in fight against cybercrime*”, 17 June, Computer Weekly: 18

(Goodwin '04). Goodwin, B. (2004). “*Viruses cost SMEs £9.5m*”, 30 March, Computer Weekly: 14