Managing Security Threats and Vulnerabilities for Small to Medium Enterprises

C. Onwubiko† and A. P. Lenaghan

Networking and Communications Research Group,
Faculty of Computing, Information Systems and Mathematics,
Kingston University, Penrhyn Road, Kingston Upon Thames, London, KT1 2EE, UK
{C.Onwubiko; A.Lenaghan}@kingston.ac.uk

Abstract* – The difficulty in managing security threats and vulnerabilities for small and medium-sized enterprises (SME) is investigated. A detailed conceptual framework for asset and threat classifications is proposed. This framework aims to assist SMEs to prevent and effectively mitigate threats and vulnerabilities in assets. The framework models security issues in terms of *owner, vulnerabilities, threat agents, threats, countermeasures, risks* and *assets,* and *their relationship; while the asset classification is a value-based approach, and threat classification is based on attack timeline.

***Keywords*— security threats, computer networks, vulnerabilities, asset classification**

I. INTRODUCTION

Managing security threats and vulnerabilities in assets are two fundamental challenges for SMEs. Vulnerabilities in assets are weaknesses in assets or the absence of security procedures, technical controls, or physical controls that could be exploited to harm or predispose assets to harm [1]. Harm to assets occurs in the form of *interruption*, d*estruction*, *disclosure*, *modification* of data, including *denial of service*.

For example, in 2001, the Code Red incident exploited a buffer overflow in a library module of Microsoft Windows' Internet Information Server. This allowed it to infect hundreds of thousands of computers [2], causing millions of dollars of damage. The Slammer [3], MSBlast [4], and Sasser [5] worms all exploited known vulnerabilities in computer systems. There are also accounts of security threats (for instance, computer worms) used as attack agents in denial of service (DoS) [6], and distributed denial of service (DDoS)[7] attacks. These types of threats affect the *confidentiality, integrity, reliability and availability* of computer network services.

The impact of threats on organisations in terms of financial losses is significant. According to the 11th Annual Computer Crime and Security Survey [8], the estimated total losses caused by various types of computer security incident in 2006‡ were $52.4 million. This was obtained from 313 respondents that were willing and able to estimate losses. The four top categories of threats that accounted for nearly **74.3%** of the total losses were: (i) *viruses*, (ii) *unauthorised access*, (iii) *laptop or mobile hardware theft* and (iv) *theft of proprietary information*. Similarly, in concurrent years, (2001 and 2002) according to the **CSI/FBI crime survey**, malicious codes (viruses) have been number-one [9], and the dominant threat for the past several years [10].

Since vulnerabilities in assets and threats that exploit them cannot be completely avoided [11], it is imperative that both must be appropriately mitigated. However existing defence models cannot defeat all known and potential threats. In part, this is because, existing models lack detailed representation of the dynamics of threat propagation in networks; narrowly focusing on isolated techniques to mitigate threats. Understanding vulnerabilities is critical to understanding the threats they represent [12].

Swiftly managing threats and vulnerabilities requires both a detailed understanding of security concepts and their relationships. Such an understanding can assist SMEs in implementing the right mix of protection controls to identify and mitigate both threats and vulnerabilities. Fundamental to this are models that richly represent security concepts and their relationships in terms of owner, *vulnerabilities, threat agents, threats, countermeasures, risks* and *assets.* The benifts of this approach to SMEs are that it allows them to : a) *properly classify valued assets b) carefully identify vulnerabilities in classified valued assets,* c) *identify and mitigate potential threats imposed on assets,* d) *appropriately evaluate associated risks,* e) *adequately classify threats and their threat agents;* and therefore provide appropriate and efficient *countermeasures* to reducing *risks* to valued *assets* in return.

Our contribution in this paper is therefore, *to investigate an approach to efficient security management through a conceptual framework that assist organisations to classify assets, identify and mitigate both vulnerabilities and threats.*

Models that evaluate both threats and vulnerabilities together provide countermeasures that are pertinently more efficient, appropriate and timely.

Section II discusses related work and definition of terms; section III examines the security conceptual framework in managing threats and vulnerabilities in assets. In section IV we investigate security threats, their impacts, classification and propagation dynamics based on attack timeline; and summarise with a discussion in section V.

II. RELATED WORK

Research into threats and vulnerabilities of computer systems continues to grow because its evolving nature and significant economic impact on organisations.

† Cyril Onwubiko is the principal author for which correspondence is made, and with the Faculty of Computing, Information Systems and Mathematics (CISM) at Kingston University, London, UK.

‡ The survey is conducted in 2006, but the incidents happened in 2005, as always, the survey is for the previous year.

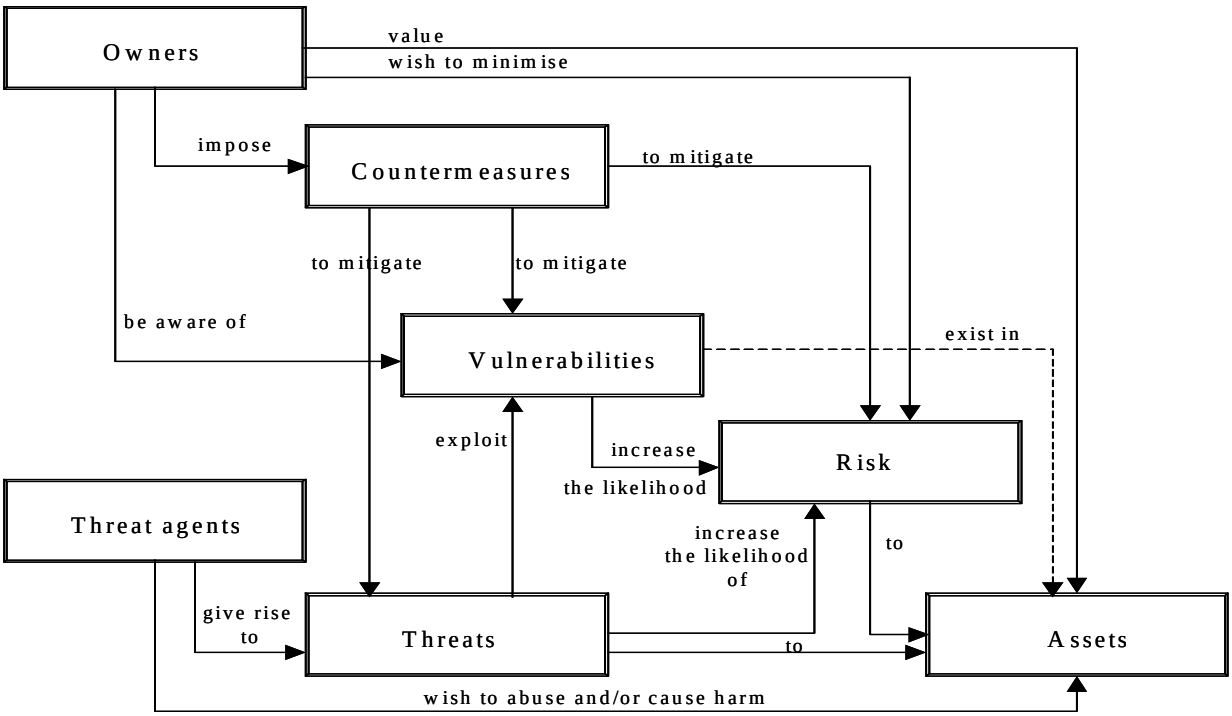

Figure 1.0: *Security Conceptual Framework*

The Common Criteria (CC) – *ISO/IEC 15408* contains one of few models that addresses threats and vulnerabilities together, showing representation and relationships of security concepts, in terms of *owner*, *safeguards*, *risks* and *assets* [13]. But the CC's model is limited in perspective because it neither includes *vulnerabilities in asset* in its representation nor *relationships* of *vulnerabilities* to other security concepts. The CC's model is useful for evaluating engineering products and therefore essential in its own rights, but the model needs to evolve to include other security concepts essential in protecting assets, given the ever-increasing incidents of vulnerabilities in assets.

A model of threat classification and control measures was proposed by Farahmand et al. [14], which aims to identify possible outcomes to an attack. The model focuses on attacks and their resulting outcomes, but relationships of security issues, such as vulnerabilities in assets were not explicitly covered.

Other contributions in the literature exist, but most of which are either specifically addressing *vulnerability* issues as in [14] or *threats* as in [13]. Thus, frameworks that possess the capabilities to model both threats and vulnerabilities issues together, and their relationships to other security concepts are pertinently a step forward.

A. Definition

Computer Security is the protection afforded to computer networks in order to attain the fundamental objectives of preserving the *confidentiality*, *integrity* and *availability* of information system resources, which includes hardware, software, firmware, information or data, and telecommunications [1]. Thus the primary objectives of *managing threats and vulnerabilities in system* are to protect computer networks and their communications in order to preserve the:

(a) Confidentiality of systems and communications. This is a requirement to avoid unauthorised disclosure of systems and communications either intentionally or inadvertently. (b) *Integrity* of computer networks, data and information. This is a requirement aimed to ascertain that computer networks and their offered services are *accurate, complete, consistent, authentic and timely. (c) Availability* of computer networks and its offered services. This is a requirement to ensure systems and their offered services are available at *accepted levels* to legitimate entities.

Threats to computer networks are defined as entities, events or circumstances with the capability to inflict harm or distort normal security operations by exploiting vulnerabilities in systems [15]. And *harm* is defined as the abuse or breach of the *confidentiality*, *integrity* or *availability* of computer networks, *in the form of destruction, disclosure, modification, interruption of data and/or denial of service*.

An asset is defined as anything that is of value and importance to the owner, which includes *information, programs, data, network and communications infrastructures*.

III. THE FRAMEWORK FOR MANAGING SECURITY THREATS AND VULNERABILITIES IN ASSETS

The investigated framework – security conceptual framework is adapted from ISO/IEC 15408 [13], and – logically defines seven security concepts and their relationships (see figure 1.0), as follows: a) Assets' ***Owners*** b) ***Vulnerabilities*** in assets c) ***Threat agents*** that give rise to threats d) ***Threats*** that exploit vulnerabilities in assets e) ***Risks*** that result due to threats and vulnerabilities f) ***Countermeasures*** imposed to prevent and mitigate threats, vulnerabilities and risks, and finally g) Valued ***Assets*** of the SME.

The conceptual framework (figure 1.0) assists organisations to fully understand what is required to be protected (assets), what should be protected from (vulnerabilities, threats and associated risks) and how they can be protected (countermeasures). Firstly, the framework assists SME to recognise important assets to them, determine what should be protected and weaknesses that exist in or within those assets. Secondly, to assess what can exploit these weaknesses, covering risks associated with vulnerabilities and potential threats that exploit vulnerabilities, and finally, to decide on what can be imposed to prevent and mitigate identified threats and vulnerabilities, as described in table 1.0.

Concept	Description
Owners	These are organisations or individuals who own the asset. Owners *value* their assets, they are sometimes *aware* of the vulnerabilities on their assets, but they ultimately want to *reduce the likelihood* of their asset been compromised by threats, so the *impose* countermeasures to prevent and/or mitigate vulnerabilities, threats and associated risks to assets.
Counter-measures	These are protection controls (s*afeguards) imposed* by the asset *owners to mitigate* vulnerabilities in assets, threats to assets and risk to assets.
Vulnerabilities	These are flaws in assets or the absence of security controls that could lead to a security breach when *exploited* by threats that *increases the likelihood* of risks to assets.
Threat agents	These are entities with the capability *to introduce* threats to assets.
Threats	These are entities that *exploit* vulnerabilities in assets, thereby *increasing the likelihood of* risks to harm or cause harm to assets.
Risk	The probability (likelihood) that assets may be compromised by threats.
Assets	Systems infrastructure, information, data, applications and programs owned by the owners.

Table 1.0: *Description of the Security Conceptual Framework*

A. Asset Classification

Asset classification schemes are utilised by organisations to determine which assets (*information, program, data, and infrastructure*) are crucial in their operations. We have developed an asset classification to assist organisations in doing this (see figure 2.0). The developed classification scheme is *simple, flexible* and *adaptive*. As a 'rough operations guideline', we decided on a classification that is robust, simple and fairly straightforward to implement, as opposed to classifications that require rigorous implementation time or/and numerous interpretations. Some classification schemes are even more difficult to understand than the process in which they intend to classify, therefore taking much time and consequently infeasible in operations environment. The asset classification model is flexible because it can be modified by an organisation to either include or exclude appropriately other fields. For example, an organisation may decide to include such fields as "Insignificant" – for assets not classified as minor, major or critical. With this, the classification changes from a 3-tier to a 4-tier classification as – *Insignificant, Minor, Major and Critical*. With "insignificant" assets, the failure of an asset leads to insignificant financial losses, and failures are only *potential*, for example, informational or warning threats, such as *software bugs* or *system caveats*. Similarly, the classification model is adaptive because it is not solely designed for use in computing; it is easily adaptable to other business operations.

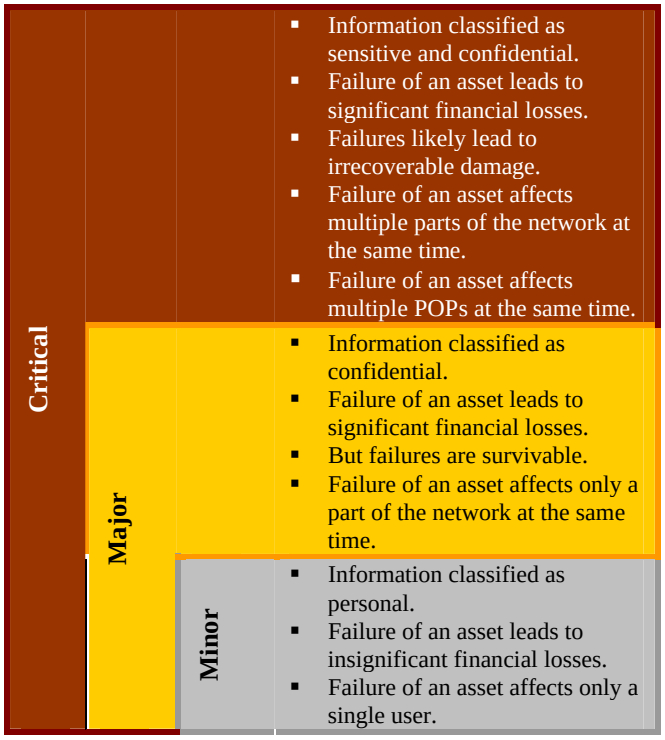

Figure 2.0: *Asset Classification Model*

B. Vulnerability Identification and Assessment

Vulnerability assessment is a review of the security posture of operational systems for the *purpose of identifying potential vulnerabilities* in assets. And when vulnerabilities are identified, appropriate mitigation controls are implemented to protect valued assets. Since vulnerability assessments are not exclusively conducted to identify potential vulnerabilities, but also to investigate missing countermeasures. It is therefore imperative that periodic vulnerability assessments are carried out to protect critical assets. The benefits of security vulnerability assessments include:

- To identify an organisation's **assets** (information, systems and network infrastructures, data, programs and applications).
- To classify assets identified according to their **importance** to the organisation, such as "critical" or "non-critical". This classification depends on the deployed methodology[§].
- To identify **critical assets** to an organisation, for example, *information*, such as (marketing database,

[§] Other methodologies and classifications exist, according to "**The Rainbow Books**" – NSC-TG-027, Library No. 5-238, 461, information assets can be classified as *'unclassified', 'sensitive unclassified', 'confidential', 'secret' and 'top secret'*

"classified" military information) and to identify which *infrastructure* (systems or networks) processes, stores, or transmits organisation's critical information.

- To determine the security posture of *assets* in order to identify **potential vulnerabilities** in them.
- To determine **associated security risks** on *asset* (*information*, *infrastructure*, *software and content*) as follows: end-user devices (PCs and PDAs), user-support devices and the actual content or otherwise.
- To determine **security requirements** and coordinate the right **mix of countermeasures.**
- To access **missing controls, protection measures** or requirements not implemented correctly, or not implemented at all, which should have been, for the purpose of protecting critical assets. And finally, to recommend **protection controls** (countermeasures) to prevent or mitigate identified vulnerabilities.

IV. THREATS, ATTACK TIMELINE AND CLASSIFICATION

A. Security Threats and Attack Timeline

To examine how threats exploit vulnerabilities in assets, a requirement is to investigate taxonomy of threats. In the literature, threats have been classified based on vulnerabilities, as in Brinkley and Schell [16]. Their classification focuses on identifying potential vulnerabilities an attacker exploits to harm an asset in order to provide appropriate countermeasures. We argue that to provide efficient and timely countermeasures a classification of threats based on attack timeline is essential. The purpose of classifying threats based on propagation timeline is to examine when in a threat propagation will the threat cause most significant harm (or damage) to assets, and what countermeasures are possible at each specific stage to efficiently and timely mitigate the threat. Thus, classification of threats based on attack timeline is recognised. The developed threat classification is a three-stage threat classification model based on attack timeline, namely: the *Probing*, *Penetration* and *Perpetuation* (the **3P**) stages, as shown in figure 3.0.

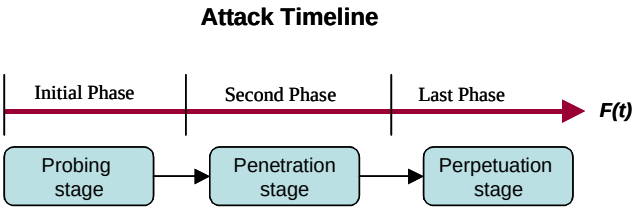

Figure 3.0: *Security threats attack timeline*

The three stages of threats attack timeline are explained, as follows:

a) ***Probing Stage:*** the earliest stage in a threat attack timeline also referred to as the *reconnaissance stage*. At this stage vulnerable networks and systems are discovered through such process as probing. For example, *an attacker may use port scan to discover and characterise networks and systems that are online and/or to find services, processes or applications running on certain systems.* Again, *social engineering deception techniques* can be engaged to gather information about a person or a system as part of the probing stage.

b) ***Penetration Stage:*** the second stage in an attack timeline. This occurs when an attacker (or threat agent) tries to circumvent security controls to create opportunities to cause harm or harm the system. Two sub-categories are recognised: i) *Unauthorised access:* when a threat intentionally (deliberately and maliciously) tries to bypass access control mechanism in order to harm or predispose a system to harm. For example, brute force attacks and dictionary attacks ii) *Denial of Service:* when a threat that does not require authorised access invades a system in order to deliberately and maliciously harm or cause harm to a system, for example, networks intrusions, computer worms, denial of service attacks (DoS) and distributed denial of service attacks (DDoS) - characterised by the attempt to exhaustively consume resources required to deliver services to legitimate users.

c) ***Perpetuation Stage:*** the last stage in an attack timeline. This occurs when threats have successfully penetrated networks or/and systems unlawfully for malicious intent. Four sub-categories are recognised: i) *Disclosure of information and data:* when the intent is for information or data or system disclosure, consequentially breaching the confidential of the system ii) *Manipulation of data:* when the intent is to alter information or data or system leading to abuse of the integrity of information or data or system iii) *Destruction of information or data or system:* when the intent is to destroy assets leading to abuse of *integrity and availability* iv) *Cleaning-up:* when the attacker removes traces of attack to prevent legitimate detection or forensic evidence in order to avoid criminal prosecution.

At each stage of the attack timeline different countermeasures are required. For example, at the probing stage, host and network-based intrusion detection systems are required to detect port scans. It is shown that this stage is very important towards a successful attack, as it is a precursor. According to the United States Army's Field Manual 100-5 [17], the success of an attack has a high correlation with the thoroughness of the reconnaissance [18]. At the penetration stage, strong access control mechanisms are required together with denial of service mitigation tools. For example, authentication, authorisation and accounting mechanisms, firewall systems, and DoS mitigation toolkits are all required. At the perpetuation stage, efficient forensic tools are required together with efficient network monitoring systems.

It is evident that at each stage of the timeline different mitigation controls are required. Therefore, a classification that investigates security threats in terms of attack timeline pertinently provides efficient and timely countermeasures to threat than taxonomies that investigate vulnerabilities without good understanding of threat propagation dynamics.

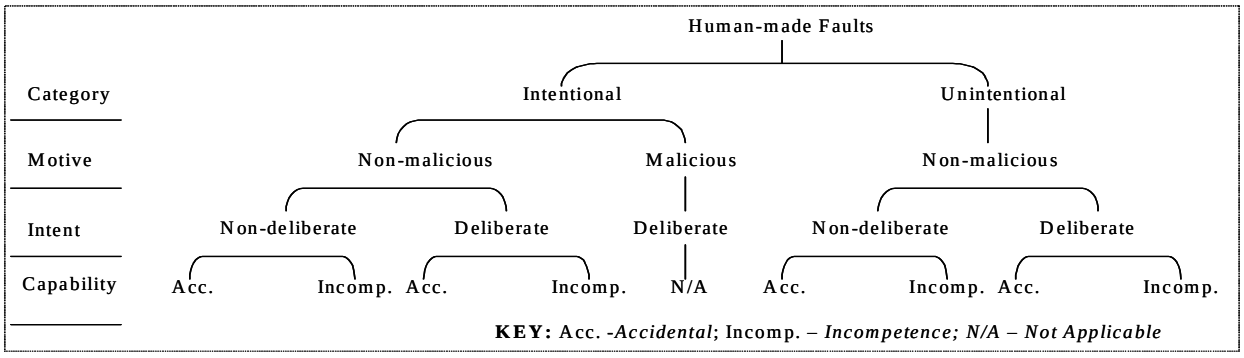

Figure 4.0: *Classification of Human-made fault*

B. Threats Classification

Threats to computer networks comprise of the following: *(i) Network errors*, ii) *Deliberate software threats***, (iii) *Natural disaster* (wildfire, flooding, earthquakes, and tidal waves - tsunami), (iv) *Cyber-threats* (terrorism, political warfare) and (v) *Insider threats* caused by disgruntled employees.

To classify threats to computer networks, two fundamental threat categories are identified: (a) *natural phenomena threats* and (b) *human-made threats* (see [19]). These threats cause failures in computer networks.

Natural phenomena threats are physical disasters that occur naturally without any human action, such as:
(i) *Tropical wildfire*, that occur in some African deserts, and seldom in Europe; (ii) *Flooding*, (iii) *Earthquakes* and (iv) *Tidal Waves* (for example, Tsunami)

Human-made threats: are threats through human actions that cause faults in systems, such as: (a) *Developmental faults, (b) Physical faults and (c) Interaction fau*lts. According to Avizienis et al. [20], faults are classified in two major categories, namely: (i) u*nintentional and (ii) intentional*, for detailed classification, see figure 4.0.

a) *Developmental Faults* include fault types that occur during development, such as *software "bugs"*, *hardware "errata"*, *design faults* (wrong design of equipment, error in dimension) and *system "caveats"*. These types of faults remain undetected during normal program or hardware development, but may manifest themselves during system operation, and often times during operational unexplainable circumstances.

b) *Physical faults* include fault types that affect hardware, such as *physical damage* to hardware systems or hardware content. For example, system failures due to excessive temperatures, environmental conditions (flooding, fire, earthquakes, and tsunami) affecting equipment performance or operation.

c) *Interaction Faults* include faults that occur due to external interaction on the system. For example, mistakes by systems operators, maintenance personnel and others with access to system that lead to *incorrect operation*, *accidental system shutdown*, or *accidental physical damage*, such as accidental disconnection of an equipment, or accidental cable cut.

Figure 4.0 is classification of human-action faults, *adapted from [17]*. This classification is used to evaluate and determine *category*, *motive* and *intent* of threats. For example,

I. **Network errors** (such as faulty systems design) are caused by *unintentional, non-deliberate, non-malicious, accidental human actions.*

II. **Deliberate software threats** *(such as viruses, computer worms),* are caused by *intentional, malicious, deliberate human-action*.

III. **Cyber-threats** *(such as, terrorist attack)* **and insiders' threats** *(such as, disgruntled employee)* are caused by *intentional, malicious, deliberate human actions.*

V. DISCUSSION

Effectively managing both threats and vulnerabilities for SMEs is increasingly difficult and challenging, especially because of the evolving nature of threats and the increasing number of vulnerability incidents in assets. Organisations need to adequately protect their valuable assets thereby reducing associated risks to their assets. Threats should not dictate how businesses are run. But threats can be a hindrance to this; threats to information assets can prevent their availability to legitimate users, at acceptable levels, thereby dictating how business operations function for an organisation.

As we have identified; to adequately manage both vulnerabilities and threats that exploit vulnerabilities in assets, a requirement is to implement appropriate countermeasures; but this is only attainable through models that possess the potential to comprehensively represent what needs to be protected, what it needs to be protected against and therefore through combined intelligence recommend appropriate controls that best protect valuable assets (see figure 1.0).

Contributions in this paper are regarded as essential, but preliminary objectives in managing security for SME; aimed primarily at providing comprehensive guidelines and frameworks to organisations that assist them fully understand their unique business requirements in managing security, such as, a) identifying exactly what needs to be protected (valued assets), b) being able to appropriately classify them c) assessing vulnerabilities in/within classified assets, d) identifying potential threats that could exploit identified vulnerabilities, e) evaluating associated risks to assets as a result of threats and vulnerabilities, f)

** 'Deliberate Software threats' include worms, viruses, macros and denial of service according to CSI/FBI Annual Computer Crime and Security Survey.

finally, recommending effective mix of countermeasures. It is needless implementing protection controls such as firewall or intrusion detection systems if these factors (a-f) have not been explicitly assessed and determined.

Among the distinguishing factors in managing security for small and medium-sized enterprises is finance. Small enterprises work on very minimal financial budgets for security compared to medium-sized enterprises. This cogent factor is recognised, as models proposed in this paper are those that combine multiple security facets together thereby reducing capital costs of both implementation and management. However, it is pertinent to distinguish that models with capabilities to address multiple security issues are a step forward compared to models that addresses specific but isolated security issues.

What is discussed in this paper is therefore a comprehensive process based approach in managing security for SMEs. That examines threats, vulnerabilities and associated risks to computer networks in order to provide adequate countermeasures in protecting valuable assets of an organisation.

REFERENCES

[1] Computer Security Handbook: *The NIST handbook, Special Publication 800-12, pp.*62

[2] D. Moore, C. Shannon, and J. Brown (2002) "Code-Red: a case study on the spread and victims of an Internet Worm", Proceedings *of the ACM/USENIX Internet Measurement Workshop, France, November, 2002*

[3] C. C. Zou, L. Gao, W. Gong, D. Towsley (2003), "Monitoring and Early Warning for Internet Worms", Proceedings *of the 10th ACM Conference on Computer and Communications Security; Washington, DC, USA, October 27-31 2003*

[4] Microsoft Security Bulletin MS03-026, (2003) "Buffer Overrun In RPC Interface Could Allow Code Execution (823980)", July 2003: [Online]: http://www.microsoft.com/technet/security/bulletin/MS03-026.mspx [Accessed 14th Dec. 2006]

[5] W32.Sasser.worm (2004), April 2004: [Online]: http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser.worm.html [Accessed 14th Dec. 2006]

[6] CERT/CC (2001), "Microsoft Internet Information Server 4.0 (IIS) vulnerable to DoS when URL Redirecting is enabled"; [Online]: http://www.kb.cert.org/vuls/id/544555,

[7] CERT/CC (2003) "W32/blaster worm advisory", [Online]: http://www.cert.org/advisories/CA-2003-20.html, August 2003

[8] L. A. Gordon, M. P. Loeb, W. Lucyshyn and R. Richardson (2006) "CSI/FBI Computer Crime and Security Survey – 2006", *11th Annual CSI/FBI Computer Crime and Security Survey, 2006*

[9] M. E. Whitman (2003) "Enemy at the Gate: Threats To Information Security", *Communications of the ACM, Vol. 46, No. 8, August 2003*

[10] R. Power (2002) "CSI/FBI Computer Crime and Security Survey", *Computer Security Issues & Trends, 8(**1**) (2002), pp. 1-24*

[11] C. Onwubiko, A. P. Lenaghan, L. Hebbes & R. Malyan (2005), "The Representation and use of Relation Information for the Detection of Threats by Security Information Management Systems", *Proceeding of European Conference on Computer Network Defence, EC2ND 2005, United Kingdom, Springer, December, University of Glamorgan, Wales UK, ISBN/ISSN 1-84628-311-6 (2005)*

[12] R. C. Seacord and A. D. Householder (2005) "A Structured Approach to Classifying Security Vulnerabilities" *Technical Note, CM/SEI-2005-TN-003, Survivable Systems, Carnegie Mellon Software Engineering Institute, Pittsburgh, PA 15213-3890, January 2005.*

[13] Common Criteria for Information Technology Security Evaluation, *Part 1: Introduction and General Model, Version 3.1, Revision 1, CCMB-2006-09-001, September 2006*

[14] F. Farahmand, S. B. Navathe, G. P. Sharp and P. H. Enslow (2003) "Managing Vulnerabilities of Information Systems to Security Incidents", *Proceedings of the ICEC 2003, Pittsburgh, PA ACM 1-58113-788-5/03/09*

[15] C Onwubiko, A. Lenaghan (2006), "Spatio-Temporal Relationships in the Analysis of Threats for Security Monitoring Systems", Proceedings of the *2nd International Conference on Computer Science & Information Systems, (ICCSIS 2006), Athens, Greece, ISBN:* 960-6672-07-7, *June 12-14 2006,*

[16] D. L. Brinkley and R. R. Schell (1995), "What is there to worry about? An Introduction to the Computer Security Problem", *Information Security: An Integrated Collection of Essays, pp. 11-39, 1995*

[17] Lieutenant Colonel Thomas C. McCarthy (1994), "U.S. Army Heavy Brigade Reconnaissance during Offensive Operations", Monograph, 1994.

[18] C. Gates (2003) "The Modeling and Detection of Distributed Port Scans: A Thesis Propsal", *Technical Report CS-2003-01, Faculty of Computer Science, 6050 University Ave. Halifax, Nova Scotia, B3H 1W5, Canada.*

[19] A. Avizienis (2000), "Design Diversity and the Immune System Paradigm: Cornerstones for Information System Survivability", *UCLA Computer Science Department, University of California, LA, CA 90095-1596*

[20] A. Avizienis, J-C Laprie, B. Randell and C. Landwehr (2004) "Basic Concepts and Taxonomy of Dependable and Secure Computing", *IEEE Transactions on Dependable and Secure Computing, Vol. 1, NO. 1, January-March 2004, pp. 11-33*