Using Fuzzy Cognitive Maps (FCMs) to Evaluate the Vulnerabilities with ICT Assets Disposal Policies

Yeboah-Boateng, Ezer Osei

Published in:
International Journal of Electrical & Computer Sciences

Publication date:
2012

Document Version
Early version, also known as pre-print

Using Fuzzy Cognitive Maps (FCMs) to Evaluate the Vulnerabilities with ICT Assets Disposal Policies

By Ezer Osei Yeboah-Boateng*
*Ph.D. Fellow at the Center for Communications, Media & Information Technologies (CMI), Dept. of Electronic Systems, Aalborg University, Copenhagen
Contact Author: Ezer Yeboah-Boateng: ezer@cmi.aau.dk or ezer@es.aau.dk

***Abstract*-- This paper evaluates the possible vulnerabilities of ICT assets disposal policies and the associated impact that can affect the SMEs. A poorly implemented policy or unenforced policy is "potentially the weakest link" in the cyber-security chain. Do SMEs have an idea of vulnerabilities or threats due to assets disposal?**

In the event of breaches, the SMEs pay for the cost of notifying the concerned stakeholders, compensate affected parties, invest in improved mitigation technologies and also may be subjected to unwarranted public scrutiny. ICT assets at the end-of-useful life span usually have data left on the hard disk drives or storage media, which is a source of data confidentiality vulnerability. SMEs were surveyed in developing economies on their assets disposal policies. The perceived correlations were analyzed using fuzzy cognitive maps (FCMs) to ascertain if any cyber-security vulnerabilities inherent in a particular policy have implications on others.

The study endeavored to show that, SMEs ought to have appropriate assets disposal policies in place. Then, these policies ought to be signed off by all stakeholders as a matter of responsibility. By employing the FCM approach with fuzzy matrix operations, the results indicate positive correlations exist amongst the policy constructs. Thus, vulnerabilities with one policy have implications on others.

***Index Term*-- Fuzzy Cognitive Maps, Vulnerabilities, ICT Assets Policies, Data Confidentiality, Risks, Threats.**

1. INTRODUCTION

Fuzzy system modeling is concerned with identifying semantically subjective and vague concepts, by converting them to fuzzy sets for modeling purposes. Using fuzzy cognitive map (FCM) preserves the apparent fuzziness of the experts' reasoning whilst utilizing the computational capabilities of the model [1]. As ICT assets reach the end-of-useful-life span, it is required of small and medium-sized enterprises (SMEs)[1] to protect the cyber-security threats to confidential data exposure to unsuspecting persons. Key issues at stake are the information assets destruction and e-waste disposal methods. Are there elaborate policies to deal with these threats? Do SMEs have an idea of vulnerabilities or threats due to asset disposal? How do SMEs dispose of corporate information? Do they use outside disposal contractors?

For the purposes of this paper, ICT asset disposal policies shall encompass physical asset disposal policy, e-waste disposal policy, including data destruction policies, regulations governing ICT assets disposal, Acceptable Internet Use policy and remote access policy.

Convergence of technologies and services could create the need to re-evaluate SMEs ICT assets, especially hardware assets. It may require consolidation and integration with state-of-the-art technologies, e.g. virtualization[2]. When this happens, some hardware assets are made redundant (e.g. legacy hardware) and often disposed of. The data contained therein ought to be appropriately and securely disposed of within the requisite regulations.

ICT asset disposal has become, in recent times, fast-breaking news events, not only from the proponents of green ICT or e-waste environmentalist, but also, issues bothering on data confidentiality breaches and regulation compliance lapses. Most large companies may outsource their asset disposal and data destruction. This option could be economical and makes business sense, if and only if, proper cyber-security measures are followed. Secured ICT assets disposal and destruction is a continuous process and business owners ought to be aware of the threats present, and the need to understand the options available to them.

[1] This research defines SMEs as businesses with less than 10 employees as a Micro Enterprise, between 10 and 50 as Small Enterprises, and between 50 to 250 employees as Medium sized enterprises. This definition falls within those applied in Ghana and Nigeria, which are the case studies for this research, and it is also consistent with similar research works in ICT [26].

[2] Virtualization is the use of multiple virtual machines with multiple OSs on a physical machine to improve efficiency and availability of ICT assets or resources.

Whatever the approach, care must be taken in the disposal or destruction of confidential information, to prevent unauthorized access to the information.

SMEs ought to know that when a file or data is said to be "deleted", the data is not removed from the hard disk per se. Rather, that file's pointers are deleted, its accessibility status rendered inaccessible, and the actual data remains on the sector of the hard disk from where it can be retrieved. The storage area is labeled "deleted" and it is made available as re-usable storage. Until that sector is over-written to by specialized software, the data shall remain recoverable through many different techniques.

Recognizing that these threats confront SMEs is indeed a step in the right direction. But this ought to be translated into devising a strategy to protect and minimize the inherent risks of being vulnerable. A simple path towards ensuring security commences with the recognition and identification of vulnerabilities, threats, and risks. It is followed by the analysis of the impact in the unlikely event of the vulnerabilities being exploited, or threats being realized. For instance, what would be the cost and legalities, if sensitive customer data get into public domain? What if malwares infect the finance department's PCs and wipe out the hard disk drives (HDDs)? Or, what if a sales guy gets robbed of his laptop? There must also be the regulation of how the system should be used, and monitoring of the activities , including what services are permitted; HTML, FTP, SMTP or P2P?

These processes culminate in the formulation of cyber-security policies which must be enforced. The policies must consist of the general rules, goals, objectives and responsibilities of all entities or end-users. A poorly implemented policy or unenforced policy is "potentially the weakest link" in the cyber-security chain [2] [3].

In the absence of appropriate and enforceable policies, SMEs are susceptible to vulnerabilities as a result of indiscriminate asset disposal. P. Ahonen et al., [4] measure the economic value of data confidentiality breaches by evaluating the resulting costs borne by companies when corporate data or customers' information found their way into the public domain. In the event of such breaches, the company pays for the cost of notifying concerned stakeholders, compensates affected parties, invests in improved mitigation techniques and also may be subjected to unwarranted public scrutiny.

Connections to SME networks from remote locations are extremely vulnerable and adequate security measures must be put in place to protect the networks. It is in order to place restrictions on authorized users from accessing the network remotely based on one's job functions. No elevated or highly privileged access must be permitted remotely. Remote access policy stipulates the guidelines for permitting authorized entities to access and connect to the corporate network from outside locations, usually via modems. The remote access policy must ensure that precautionary measures are in place to provide secured and reliable access with appropriate encryption. The policy ensures the data integrity during transmission or sessions.

Most enterprises have come to use Remote Access Dial-In User Service (RADIUS[3]) servers for remote access services, especially with multiple users who can share authentication databases. RADIUS has enjoyed massive vendor support from almost all the key players. However, it suffers from the lack of encryption capability to ensure that data transmission sessions are secured. So this may require explicit encryption methods included in the remote access policy (e.g. use of IPSec).

The other policy options must address shredding, degaussing, sanitization, responsible e-waste, recycling and re-writing by appropriate tools, physical asset destruction, etc.

1.1. ICT Assets Disposal Techniques

ICT assets at the end-of-useful life span usually have data left on the hard disk drives or storage media which is a source of data confidentiality vulnerability. To ensure that the user data does not end up with unauthorized entities, SMEs can use utilities such as HDDerase, a freeware which complies with the

[3] RADIUS facilitates multiple remote access users via the same authentication database with common service management.

National Institute for Standards & Technology [5] standard.

Hughes & Coughlin [6] posit that deletion of file pointers is a faster way to re-write data, as actual over-writing is a much slower process. Normal computer usage has in-built OS mechanism to recycle and "unerase", that are meant to prevent accidental data sanitization. In essence, these protective measures for data also in turn create data confidentiality vulnerabilities susceptible to recovery by unauthorized entities.

Garfinkel & Shelat [7] extensively studied the security concerns of hard disk drive disposal, for instance. They found out that 74% of the drives studied had recoverable data on them; 17% had fully functional operating systems (OSs) that required no efforts to re-use them; 36% of those drives had been reformatted, but still had recoverable data.

Before asset disposal, SMEs ought to ensure complete data eradication beyond recovery. Many companies have 2-to-3 years of use for their PCs, laptops, or office equipment, after which they are retired. These assets often find their way into the cyber-market and the data on them are usually recoverable; unless great care had been taken to erase them securely.

1.1.1. Data Sanitization

Hughes & Coughlin [6], classified data sanitization into 4 vulnerability levels, namely:

i. Files deletion (including drive formatting) – as the weakest erasure at the highest vulnerability level;
ii. Block or sector erasure – as over-written by external software, at the medium vulnerability level; susceptible to malware vulnerability if due care is not taken;
iii. Normal secure erasure – as per NIST 800-88, at the low vulnerability level; a positive ease-of-use data destroy and command, tantamount to "electronic data shredding"; and
iv. Enhanced secure erasure – at the lowest vulnerability level.

It must be noted that the software utilities used for data sanitization are themselves susceptible (or vulnerable) to malware and require constant updates to ensure effectiveness and security [6].

1.1.2. Physical Asset Destruction

Physical asset destruction carried out securely can ensure data confidentiality. Disk drives must be reformatted or overwritten to by special software utility to render the data unrecoverable. Shredding of physical ICT assets to render the assets unrecognizable under ethical guidance may be one secure mode of asset disposal. Shredding here could be either paper, which could be recycled or hardware, which could be scraps for recycling.

For instance, destruction of hard disk drives (HDD) by broken into minute pieces could be effective. Physical assets that are likely to be vulnerable to SMEs include HDD, magnetic tapes, optical disk media, USB drives, private branch exchanges (PBXs), PDAs, Smartphone, Fax machines, print-outs, etc.

1.1.3. Degaussing

Degaussing is the process that employs high intensity electromagnetic fields to the media in order to erase any data stored permanently. This ensures that no data recovery tools would be able to salvage the erased data. It also ensures that the track and motor magnets of the disk drives are erased beyond recovery. Degaussing the data storage media prior to asset disposal could mitigate the risks of information assets being exposed to unsuspecting entities.

1.2. Assets Disposal Regulation

There are lots of regulation and compliance requirements governing the use of data, its storage and retention, and its disposal. Common regulations include the Health Information Portability and Accountability Act [8], Personal Information Protection and Electronic Documents Act [9], Gramm-Leach-Bliley Act [10], Sarbanes-Oxley Act [11], the European Union Data Protection Directive [12], NIST 800-88 [5], Payment Card Industry Data Security Standard [13], etc.

Besides the generic compliance requirements most of these regulations have punitive measures, including fines and/or imprisonment, upon breaches or lapses.

1.3. Key Issues

ICT asset disposal is of great importance to organizations, especially service providers, consultants, manufacturers, and even politicians. Asset disposal is a key concern in ICT since any lapses could compromise the confidentiality property; be it of the corporate entity or of its customers.

The issue is, if the disposal process is not carried out properly, it could make the organization vulnerable to various security threats, such as data confidentiality breaches, governance, and risk and compliance lapses. How then do SMEs ensure that the end-of-useful-life assets they disposed of would not create security challenges for them? In 2003, a major Canadian bank discarded only two computers which had customers' account numbers and balances that found their way to the used computers market [7]. In another development, a senior corporate executive in USA sold his black berry phone on e-Bay for pittance of $15, only to realize that it had very sensitive corporate information [14].

There are two main issues at stake; data confidentiality and associated cyber-risks of e-waste aspects of the problem. The wider environmental concerns are left with the green ICT proponents to tackle.

This paper evaluates the possible vulnerabilities of ICT asset disposal policies and the associated impact on SMEs. The evaluation of vulnerabilities resulting from indiscriminate ICT assets disposal involves limited historical data sets and imprecision. This creates a form of uncertainty and methods employing fuzzy set theory become handy. This study used Fuzzy Cognitive Maps (FCMs) to evaluate the relationships between the policies and vulnerabilities that confront SMEs in developing economies. The FCM approach analyzed the policies (as concepts) using expert's opinion and basic fuzzy matrices to capture the latent knowledge inherent in detecting cyber-security vulnerabilities. By employing fuzzy matrices and directed graphs tools the correlation between the various asset disposal policies and vulnerabilities were established.

The motivation is that typical SMEs (especially from developing economies) don't have access to sophisticated methodologies or techniques to resolve problems. So this simple FCM approach comes handy as no computer programming is required, nor any elaborate budget.

SMEs were surveyed in developing economies on their asset disposal and destruction policies. The perceived correlations were analyzed using FCM to ascertain if any cyber-security vulnerabilities from a particular policy have implications on others.

1.4. Outline

This introductory section dealt with the background to vulnerabilities due to asset disposal policies or the lack of it, which confront SMEs in developing economies. An overview of some asset disposal techniques and issues has been presented.

The methodological approach adopted is highlighted and a couple of issues are raised that beg for answers. The remaining sections deal with some related works using fuzzy cognitive maps (FCMs) on cyber-security related problems. Highlights on data confidentiality as a cyber-security policy framework and a few compromises due to e-waste are raised. Fuzzy cognitive mapping as an approach is also discussed, with an overview presentation on fuzzy α-cut concepts.

Section 4 presents the empirical analysis and findings with the use of fuzzy matrices to evaluate the vulnerabilities on the policies.

Section 5 discusses the implications arising out of asset disposal policies vis-à-vis vulnerabilities. Conclusions are drawn and an idea for further research work is offered.

2. METHODOLOGY

This study is a subset of the cyber-security vulnerabilities on SMEs in developing economies. Cognizant of the complexities and uncertainties in cyber-security metrics, the study set off with extensive literature review and designed a survey questionnaire philosophy which was submitted to five (5) cyber-security practitioners for review and comments. Based on their comments and advice, a pre-test survey was designed and administered to these experts, again for critique. The actual full scale survey was then launched and administered using LimeSurvey Online

(**www.limesurvey.com**) facilities. This approach was adopted in order to target most SMEs in Ghana and Nigeria; and in view of the challenges associated with physically distributing questionnaires in the case-study countries. *To ensure credible results, a cookie was set-up in the online survey program to prevent repeated participation.*

The study administered objective-based questionnaire to security functionaries and chief-level (C-level) officers of about 500 SMEs in Ghana and Nigeria. Email messages were sent out to the target population with a preamble and a hypertext link to the online survey website. ICT-based SMEs, financial organizations and government agencies were targeted, and were selected by a simple random sampling. For instance, the lists of Ghana ISPs Association and professional IT experts in Ghana and Nigeria were used.

2.1. Research Methods

Typical research methods involve drawing conclusions, or making inferences about something that has not been observed or measured on the basis of those parameters that have been observed or measured. Most cyber-security endeavors lack historical data or it is difficult to measure security posture metrics of a live system. So by inferential statistics, for example, one can generalize from a sample to a population of interest from which the sample was taken.

To use data to generalize findings, into areas for which there are no data, or to predict an outcome based on a limited data set, requires different techniques and analytical methods. For this paper, fuzzy cognitive map (FCM) framework was used to evaluate the vulnerabilities culminating from effects of asset disposal and data destruction policies based on the empirical data collected.

The model represents relationships between cyber-security policy vulnerabilities, the threats emanating when vulnerabilities are exploited, and the resulting implications on SMEs.

3. FCM & CYBER-SECURITY PROBLEM

James Tiller [15] asserts that every security initiative has inherent security policies and their importance. These policies must regulate access to authorized entities and resources. They must spell out the security posture by providing the guidance, and expectations of all stakeholders as well as the measures to utilize the systems.

In view of that, this paper underscores that importance by measuring the cyber-security posture of SMEs through the physical asset disposal, e-waste disposal, regulation and compliance, Acceptable Internet Use and remote access policies. The climax is when all these policies are actually signed off by all employees (or stakeholders). "Cyber-security policies are inarguably the core point of any successful security program within an organization" [15].

The criticality and uniqueness of asset disposal policies cannot be over-emphasized; probably, after an embarrassing event, which is also associated with a high cost.

3.1. Data Confidentiality

Universally, the classical cyber-security triad of confidentiality, integrity and availability (CIA) form the basic building blocks of any good cyber-security initiative. This is also in line with Lee's [16] cyber-security policy types.

In this paper, the discussion shall be restricted to the property of confidentiality in relation to asset disposal vulnerabilities. Lee's [16] definition of confidentiality policy is herewith adopted:

> "A confidentiality policy typically states that only authorized users are to be permitted to observe sensitive data, and that all unauthorized users are to be prohibited from such observation." [16]

Cyber-security *vulnerabilities are* flaws or weaknesses that could be exploited to violate computing systems or the information they contain [17]. Vulnerabilities enable threats to be realized. ITU-T. Rec. X.805 [17] categorizes vulnerabilities into four (4), namely:

i. Threat Model vulnerabilities – which originate from the difficulty of foreseeing possible future threats (e.g. failing to realize that non-existence of policies could be detrimental to the firm;
ii. Operation and Configuration vulnerabilities – which originate from improper usage of options in implementations or weak deployment policies (e.g. not enforcing use of encryption in a Wi-Fi network or not shredding sensitive print outs);
iii. Design and Specification vulnerabilities – which come from errors or oversights in the design of a

system or protocol that make it inherently vulnerable; and

iv. Implementation vulnerabilities – which are introduced by errors during system or protocol implementation.

The first two vulnerability groups are of interest to this study.

Data confidentiality vulnerability exists when information and/or ICT assets can be accessed, viewed or read by unauthorized individuals, entities or processes. The vulnerabilities may be exploited either on physical assets (e.g. stolen laptops; password on stick-on under keyboards; datasheet print-out; company financial report, etc.) or electronic assets (e.g. unencrypted files on hard drives; electronic copy of data sheets; product strategy or algorithm, etc.).

Cyber-risk is the likelihood of the occurrence or realization of a threat, with the possibility to adversely impact on business. Mitigation techniques are enshrined in the cyber-security policy framework. Typically, the threats and associated agents may change with time, whereas the vulnerabilities usually remain unchanged, unless they are addressed. For instance, SMEs who dispose of paper-based reports or sales accounts print-out without shredding them may stand the risk of losing sensitive corporate information.

Today, advances in technologies facilitate some employees working from home, the field users or sales force traveling, and the remote users accessing network resources from afar, implying the company has a lot of data out there, outside of their premises. Also, if knowledge workers or telecommuters could connect to the corporate network via any Wi-Fi or Internet café, the dangers of being compromised or infected by a malware remain high.

3.2. E-Waste Issues

The term "e-waste" is not clearly defined. Loosely, it is the informal name for electronic devices or assets reaching their end-of-useful-life span. Typical definition encompasses almost all consumer electronic products that are disposed or discarded. For the purpose of this discussion, the scope is limited to electronic resources or assets used for computing and information technology and services; e.g. laptops, hard disk drives, routers, access points, PDAs, PBXs, etc.

Quite apart from the environmental hazards that e-waste disposal may pose; there are also adverse health implications and cyber-security risks. This study is limited to the risks associated with data confidentiality breaches.

For instance, some researchers uncovered that a hard disk drive discarded at the dumping grounds in Accra, Ghana, which was sold at about US$25 contained confidential and sensitive information involving US government [14] [18].

Yet, other studies also discovered that some discarded assets had "intimate details of people's lives" [14, 18], files containing credit card details, bank account transactions and related personal information of the original asset owners.

Warner [14] recounted the correlation between e-waste disposal and the rise of cyber-crime in Ghana. He had discovered enormous amount of information about the original owners, including personal emails, residential addresses and sensitive files. The adverse impact of e-waste vulnerabilities with exposure to sensitive, top secret government, public and private information leaves much to be desired. Warner [14] also narrated how someone from Ghana had attempted to blackmail a US Congressman, Robert Wexler (D-Florida), with some information retrieved from the latter's end-of-useful-life hard disk drive that was sold at the dumping site in Accra. These and many more are the likely risks that asset disposal can pose to many SMEs, especially if no proper guidance is followed.

3.3 Fuzzy Cognitive Map (FCM)

Fuzzy Cognitive Map (FCM) is a signed directed graph with concepts like policies, events, etc., as nodes or vertices and causalities as edges or arcs. FCMs are used for the abstraction of real world problems, knowledge representation and computational inference, by representing the key constructs as concepts or nodes, and linked with concurrently active causal relations [19] [20]. Its basic framework uses vector-matrix operations to infer causative fuzzy concepts relations.

The concepts take fuzzy numbers from the unit interval [0, 1]. The causal relations between concepts are represented by the signed directed edges or links, which are indications of the relational impact or influence. The FCM process is used for human inference or approximate reasoning.

The utility of fuzzy sets expressed in the membership functions, make fuzzy set theory suitable for uncertainty metrics and most importantly gives meaning to the representation and interpretation of vague concepts in simple human reasoning [20]. FCM is simple, works well with expert's opinion, and it's able to handle unsupervised data to unearth the latent characteristics or correlation of variables. According to W. Kandasamy et al [20], FCM theory is solidly grounded when there are more experts' opinions. This facilitates the application of combined FCM using those experts' opinions. That notwithstanding, Kandasamy et al. [20] assert that the key disadvantage is when there exist conflicting opinions, the combined FCM could be sum to zero, in which case the experts' opinions would have been rendered worthless.

Another disadvantage with FCM is the encoding nature of expert's opinion or biases which could render the model inaccurate. This issue is mitigated by deriving this study's expert's opinion partially from the dataset.

In spite of its simplicity, this FCM approach can be applied to almost any techno-economic endeavor which require assessment of cause-and-effect analysis.

Siraj, A. et al. [21] used FCM to model a decision support system that utilized causal knowledge for intelligent intrusion detection system (IIDS). This was an innovative model where fuzzy rule-base was applied, just as in a similar risk assessment study by Smith & Eloff [22]. This study however, employs simple FCM modeling with matrix operations.

FCM was used for expert judgment elicitation and then innovatively transformed into a fuzzy inference system that was used to predict the discount rate for a venture capital valuation of firms [23].

The alpha-cut (α-cut) concept finds applications in engineering and science, as it facilitates the execution of fuzzy rules and intersection of fuzzy sets [24] [1]. This is an important facility that controls the execution of fuzzy rules as well as the intersection of multiple fuzzy sets.

3.3.1. The Concept of Alpha-cut sets (α-cut)

Let $\mathbf{A}$ be a fuzzy set in the universe of discourse, $\mathbf{X}$. Let α be a number belonging to the fuzzy unit interval [0, 1]. Then α-cut of $\mathbf{A}$, denoted by $\mathbf{A}_\alpha$, is a crisp set with all elements of $\mathbf{A}$ with membership function values in $\mathbf{A}$ greater than or equal to α; i.e. $\mathbf{A}_\alpha = \{x : \mathbf{A}(x) \geq \alpha\}$ or $\mathbf{A}_\alpha = \{x : \mu_{\mathbf{A}}(x) \geq \alpha\}$. A strong α-cut is defined as $\mathbf{A}_{\alpha+} = \{x : \mathbf{A}(x) > \alpha\}$. If α = 1.0, then the crisp set α-cut is called the CORE set of the fuzzy set $\mathbf{A}$. For ease of statistical inference and interpretation, a nested set of quartile α-cut is defined, such that $nested\ \mathbf{A}_\alpha = \{x : \mathbf{A}(x) \to \alpha \geq \alpha_i\}; \forall i = 1,2,3,4,5$ or α receives the values 1, 0.75, 0.50, 0.25, 0. When α = 0, the α-cut set is called the SUPPORT set of the fuzzy set $\mathbf{A}$. For α values 0.75, 0.50, 0.25, the sets are defined as the upper quartile set, mid-quartile set and the lower quartile set, respectively.

4. Empirical Analysis and Results

The Table 1 depicts the empirical data collected from the survey of SMEs in two developing economies. The data is part of a larger dataset on cyber-security vulnerabilities. It consists of 89 sampled respondents on policies on information asset disposal, Internet use and remote access.

TABLE I
Data Disposal Policies & Vulnerabilities

	Physical Disposal Policy	E-Waste Disposal Policy	Regulation & Compliance Policy	Acceptable Use Policy	Duly Signed Policy	Remote Access Policy
Low risk	37	25	24	34	17	37
	0.42	0.28	0.27	0.38	0.19	0.42
Moderate risk	34	27	27	37	41	35
	0.38	0.30	0.29	0.42	0.46	0.39
High risk	18	37	38	18	31	17
	0.20	0.42	0.44	0.20	0.35	0.19

The top lines for each category contain the actual counts or frequency of the 89 respondents in the survey. The data

depict the levels of vulnerability, by the fuzzy tuples {low-risk, moderate-risk, high-risk}, in respect of perceived impact of each construct or policy. For example, high risk vulnerability is seen as that which could potentially allow a threat agent to compromise a mission-critical asset. The bottom lines depict the fuzzified values for each construct. Thus, three vectors (or matrices) are derived from the data table.

The normalization of the data is as follows. The normalized values are given by the equation,

$$x_n = a + \frac{(x_i - A)(b-a)}{(B-A)}$$

Where, x_i is the data to be normalized; a is the minimum normalized scale value (here $a=0$ is chosen); b is the maximum normalized scale value (here $b=1$ is chosen); A is the minimum possible value in the data set (here $A=0$); B is the maximum possible value in the data set (here $B=89$). Note that, the values of a and b are in accordance with fuzzy set theory, such that the membership values map onto the (unit interval) set [0 1].

A fuzzy relationship between two or more sets is an expression of association, interrelationship, interconnection, or interaction amongst the sets [24]. Accordingly, there is a degree of presence (or belief about the existence) or absence (or non-existence) of such relations [25]. That degree of presence in the relationship $\mathbf{R}$ between two constructs $\mathbf{A}$ and $\mathbf{B}$, is given by $\mathbf{R(A,B)}$ or $\mu_R \in [0,1]$ such that μ_R (a, b) ∈ [0, 1]. In applying the principles for analysis, the empirical data is fuzzified or normalized in view of perceived "belief" in the existence of some relations amongst the constructs.

Also, in order to ensure that any relationship existing between any constructs were not due to pure chance, the Chi-square statistic tests is applied on the data.

The results for significance of 0.05, at degrees of freedom (DF) of 10, were as follows:

- Pearson's Chi-square, λ^2 = 35.071; p-value = 0.000121
- Yates' Chi-square = 30.999; Yates' p-value = 0.000587

The critical value at the significance of 0.05 is 18.307. Since $\lambda^2 \geq 18.307$, it is inferred that any relationships between the variables are not due to chance.

In order for the product of the two matrices to be defined, the number of columns in the 1st matrix must be equal to the number of rows in the 2nd matrix. Now, let $\mathbf{Y}_{low} = \{0.42 \quad 0.28 \quad 0.27 \quad 0.38 \quad 0.19 \quad 0.42\}$ be a fuzzy set of low-risk vulnerable parameters; $\mathbf{Y}_{\text{mod}} = \{0.38 \quad 0.30 \quad 0.29 \quad 0.42 \quad 0.46 \quad 0.39\}$ be a fuzzy set of moderate-risk vulnerable parameters; and $\mathbf{Y}_{high} = \{0.20 \quad 0.42 \quad 0.44 \quad 0.20 \quad 0.35 \quad 0.19\}$ be a fuzzy set of high-risk vulnerable parameters. [0.1]

Note that, the augmentation matrices are permuted to facilitate meaningful aggregation of the vulnerability rankings – for which the FCM as a tool, has aggregation functionality [19] [20]. Kandasamy et al. [20] posits that all matrices associated with an FCM are always square matrices of dimension which is equal to the total number of distinct concepts or events used by the experts, and with diagonal elements as zero.

The fuzzy matrix relation R ($\mathbf{Y}_{low}$, $\mathbf{Y}_{\text{mod}}$) is given as:

$$\begin{bmatrix} 0.42 \\ 0.28 \\ 0.27 \\ 0.38 \\ 0.19 \\ 0.42 \end{bmatrix} \begin{bmatrix} 0.38 & 0.30 & 0.29 & 0.42 & 0.46 & 0.39 \end{bmatrix} = \begin{bmatrix} 0.16 & 0.13 & 0.12 & 0.18 & 0.19 & 0.16 \\ 0.11 & 0.08 & 0.08 & 0.12 & 0.13 & 0.11 \\ 0.10 & 0.08 & 0.08 & 0.11 & 0.12 & 0.11 \\ 0.14 & 0.11 & 0.11 & 0.16 & 0.17 & 0.15 \\ 0.07 & 0.06 & 0.06 & 0.08 & 0.09 & 0.07 \\ 0.16 & 0.13 & 0.12 & 0.18 & 0.19 & 0.16 \end{bmatrix} \quad [0.2]$$

Similarly, the fuzzy matrix relation R ($\mathbf{Y}_{low}$, $\mathbf{Y}_{high}$) is given as (note that of R ($\mathbf{Y}_{\text{mod}}$, $\mathbf{Y}_{high}$) is also computed, but not shown here):

$$\begin{bmatrix} 0.42 \\ 0.28 \\ 0.27 \\ 0.38 \\ 0.19 \\ 0.42 \end{bmatrix} \begin{bmatrix} 0.20 & 0.42 & 0.44 & 0.20 & 0.35 & 0.19 \end{bmatrix} = \begin{bmatrix} 0.08 & 0.18 & 0.18 & 0.08 & 0.15 & 0.08 \\ 0.06 & 0.12 & 0.12 & 0.06 & 0.10 & 0.05 \\ 0.05 & 0.11 & 0.12 & 0.05 & 0.09 & 0.05 \\ 0.08 & 0.16 & 0.17 & 0.08 & 0.13 & 0.07 \\ 0.04 & 0.08 & 0.08 & 0.04 & 0.07 & 0.04 \\ 0.08 & 0.18 & 0.18 & 0.08 & 0.15 & 0.08 \end{bmatrix} \quad [0.3]$$

The matrix $\mathbf{E}_{ixj} = \{e_{ij}\}$, where e_{ij} are the weights of the directed edge $\mathbf{C}_i\mathbf{C}_j$. $\mathbf{E}_{ixj}$ is called adjacent matrix of the FCM or connection matrix of the FCM.

For a finite number k of FCMs, there exist a combined FCM which produces the joint effect of all the FCMs put together. Let $\mathbf{E}_i (i = 1,2,.....,k)$ be the connection matrices of the FCMs with nodes $P_1, P_2, ...P_n$, then the combined FCM is given by adding all the connection matrices:

$$\mathbf{E} = \mathbf{E}_1 + \mathbf{E}_2 + ... + \mathbf{E}_k \quad [0.4]$$

So the combined connection matrix is given by

$$\begin{bmatrix} 0.32 & 0.46 & 0.47 & 0.34 & 0.47 & 0.32 \\ 0.22 & 0.33 & 0.34 & 0.23 & 0.33 & 0.22 \\ 0.21 & 0.32 & 0.32 & 0.23 & 0.32 & 0.21 \\ 0.30 & 0.45 & 0.46 & 0.32 & 0.45 & 0.30 \\ 0.20 & 0.33 & 0.34 & 0.21 & 0.31 & 0.20 \\ 0.32 & 0.47 & 0.48 & 0.34 & 0.48 & 0.32 \end{bmatrix}$$

transformed into

$$\begin{bmatrix} 0.0 & 0.46 & 0.47 & 0.34 & 0.47 & 0.32 \\ 0.22 & 0.0 & 0.34 & 0.23 & 0.33 & 0.22 \\ 0.21 & 0.32 & 0.0 & 0.23 & 0.32 & 0.21 \\ 0.30 & 0.45 & 0.46 & 0.0 & 0.45 & 0.30 \\ 0.20 & 0.33 & 0.34 & 0.21 & 0.0 & 0.20 \\ 0.32 & 0.47 & 0.48 & 0.34 & 0.48 & 0.0 \end{bmatrix}$$

For practical purposes and in accordance with Kandasamy et al [20], the diagonal elements or the self-feedbacks at the edges are all zeroed.

Theoretically, in using the expert's opinion, if an increase in one concept (or policy) leads to an increase in another concept, then the value 1 is assigned. Otherwise, if the effect is negative or decreasing, -1 is assigned. For concepts which have no relation or causative effect on each other, the value 0 is assigned.

Kandasamy, W. et al [20] referred to the Fuzzy Cognitive Map (FCM) nodes as fuzzy nodes and assigned the set {-1, 0, 1} to the edge weights or causalities. The concept nodes are used to represent processes, events, values, norms or policies.

To build the asset disposal policy model the following 6 fuzzy nodes of FCM are used:

- P_1 - physical asset disposal policy (e.g. hardware, use of shredder, hard disk drive, etc.)
- P_2 - electronic waste (e-waste) disposal policy (e.g. software, data sheets, hardware, storage media, applications, or intellectual property (IP), etc.)
- P_3 - regulation & compliance policy (e.g. regulation, compliance, asset custodians, data disruption processes, etc.)
- P_4 - acceptable Internet use policy (e.g. do's & don't's of computer usage, websites to visit and not to visit, system updates, etc.)
- P_5 - duly signed employee policy (e.g. all employees are required to sign off on the ICT policies upon engagement in the organization)
- P_6 - remote access policy (e.g. guidance on Intranet or Extranet interconnections, Wi-Fi connections, café usage, etc.)

Using directed graphs (digraphs) to represent the aggregated fuzzy relations of $\mathbf{Y}_{low}$, $\mathbf{Y}_{\text{mod}}$ and $\mathbf{Y}_{high}$. The resulting FCM map or directed graph is shown in Figure 1 below:

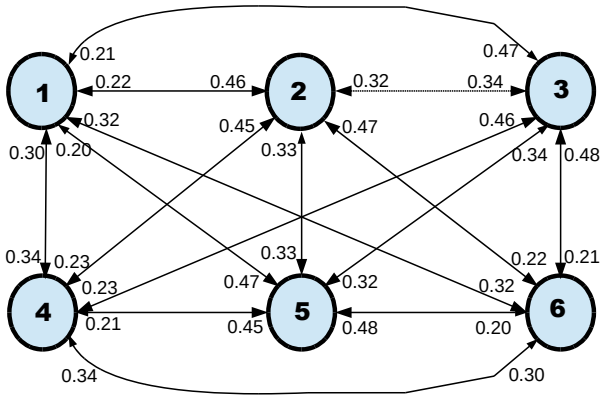

Fig. 1. original FCM map

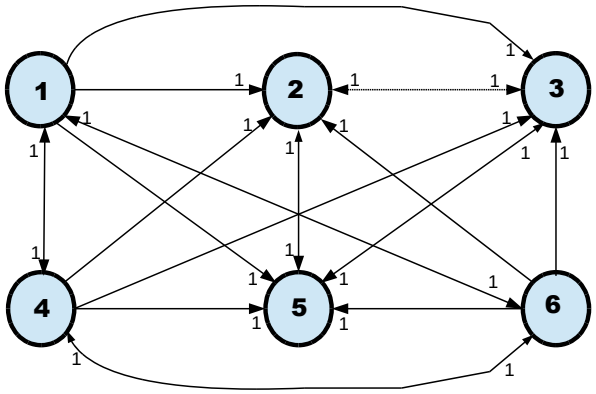

Fig. 2. FCM with alpha at 0.25

By choosing the lower percentile α –cut, α = 0.25, the resulting FCM map or directed graph is given in Figure 2 above.

Deducing from figure 2 above an expert's opinion is created, a 6x6 causal connection matrix, $\mathbf{E}_{6x6}$, representing the asset disposal policy model using FCM.

That is, $\mathbf{E}_{6x6} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$

Since matrix multiplication involves both addition and multiplication, the max-min principle (or operation) for fuzzy matrices were used. In many cases, the algebraic addition "+" is replaced with "max" operation; i.e. instead of (0.5 + 0.7) = 1.2, max (0.5, 0.7) = 0.7 is obtained. Similarly, the algebraic multiplication "x" is replaced with "min" operation; i.e. (0.8 x 0.9) = 0.72, min (0.8, 0.9) = 0.8 is obtained.

A vector $\mathbf{A} = \{a_1, a_2, ...a_n\} \; \forall \; a_i \in [0,1]$ is known as the instantaneous state vector, denoting the ON-OFF states of the nodes at any given instant; e.g. $a_i = 0 \Rightarrow a_i$ is OFF and $a_i = 1 \Rightarrow a_i$ is ON. Suppose $\mathbf{C} = \{c_1, c_2, ...c_n\}$ is an initial state vector passed through the dynamic system $\mathbf{E}$, then $\mathbf{CE} = (c_1^{'}, c_2^{'}, ...c_n^{'})$. Upon thresholding and updating the vector, suppose the resultant vector is $\mathbf{D} = (d_1, d_2, ...d_n)$ such that $\mathbf{CE} = (c_1^{'}, c_2^{'}, ...c_n^{'}) \mapsto (d_1, d_2, ...d_n)$, where the symbol "↦" implies the resultant vector has been thresholded or non-linearly transformed and updated after each pass.

Irrespective of the FCM matrix dimension, the system settles down to a temporal associative memory (TAM) limit cycle or fixed equilibrium point which is an indication of the hidden pattern of the system. This fixed point inference is a summary of the joint causal effects of all the interacting fuzzy concepts [20].

Now, let the starting input vector be $\mathbf{C}_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$, representing the physical asset disposal policy. The state vector $\mathbf{C}_1$ is repeatedly passed through the FCM connection matrix $\mathbf{E}_{6x6}$ thresholding and simultaneously updating the result after each pass. Thus,

$$\mathbf{C}_1\mathbf{E}_{6x6} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \mapsto \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} = \mathbf{C}_2 \quad [0.5]$$

$$\mathbf{C}_2\mathbf{E}_{6x6} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \mapsto \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} = \mathbf{C}_3 = \mathbf{C}_2$$

This indicates that the prevalence of physical asset disposal threats (or vulnerabilities) results in risks due to regulation and compliance, e-waste and remote use policies. Also, the resultant vector indicates (from the latent patterns) that similar vulnerabilities could emanate from the acceptable use and unsigned policies effects.

Similarly, using the acceptable use policy input vector $\mathbf{D}_1 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$, then

$$\mathbf{D}_1\mathbf{E}_{6x6} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 1 \end{bmatrix} \mapsto \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} = \mathbf{D}_2 \quad [0.7]$$

$$\mathbf{D}_1\mathbf{E}_{6x6} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \mapsto \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} = \mathbf{D}_3 = \mathbf{D}_2 \quad [0.8]$$

Here, the resultant vector indicates that there exist interacting effects of e-waste disposal, regulation &

compliance, unsigned and remote use policies, as well as physical asset disposal.

5.0. DISCUSSION AND CONCLUSIONS

The empirical analysis and findings have established that data confidentiality vulnerabilities resulting from ICT asset disposal policies have implications on each other. It was shown, for example, that vulnerabilities presented by physical asset disposal policy, such as indiscriminate hard disk disposal or the lack of shredder, had adverse implications on e-waste and regulations and compliance policies. Indeed, SMEs ought to have elaborate policies in place to deal with asset disposal threats.

The asset disposal policies are meant to:

- reduce any incidental disclosure of confidential information or breach of data confidentiality;
- create awareness of assets disposal procedures, asset classification and handling;
- encourage and enforce compliance with regulatory requirements.

The policies governing these procedures or processes must be scrutinized and judiciously enforced. Because of the vulnerabilities inherent in the asset disposal processes, there are snowball effects as weakness in one has the potential to affect the others. In essence, vulnerabilities in one policy can cause other policies to be susceptible to threats.

From the empirical data, overall 81% of SMEs were unaware of the policies (if existed) and as well, stakeholders had not signed off the policies. Also, it was found out that, 58% of SMEs do not have shredders, nor any physical asset disposal policies; that, 72% of SMEs do not have any e-waste policy, neither is due care taken in discarding end-of-useful-life assets.

Interestingly, 73% SMEs used third party asset disposal contractors without any due diligence nor special recourse to the third party's procedures.

Using the FCM approach, the correlations amongst the various policies were established. It must be noted that, though the matrix products $\mathbf{AB} \neq \mathbf{BA}$, in the event of a different expert opinion, say $\mathbf{F}_{ij}$ as the causal connection matrix, it has been ascertained that the results still show some correlations amongst most of the policy constructs. This is an indication of the transparency of the FCM approach, and that there exists causal correlations amongst the policies.

Though a breach or compromise of information asset confidentiality can have serious repercussions or consequences on the SMEs, the extent of impact depends on the sensitivity and asset value involved. The total impact or risk to the SME is not only financial liabilities, but also, morale, business output, credibility, investor & customer confidence, corporate image, legal actions, etc.

The policies put in place are only effective if all stakeholders are duly informed of the tenets of those policies, which will in turn enhance enforcement, hence assuring the confidentiality security property.

Throughout this paper, it has been shown that first, SMEs ought to have appropriate asset disposal policies in place. Then, these policies ought to be shared and informed amongst all stakeholders who must duly sign off as a matter of responsibility. The use of FCM to evaluate vulnerabilities is innovative but simple risk assessment, such that most SMEs should be able to carry out.

The simple FCM approach used for this study could be enhanced by eliciting more experts' opinions. Each expert opinion can form a causal connection matrix. By standardizing the size of the matrices, the opinions can be aggregated to enrich this approach and refine the study further. Also, fuzzy similarity measures can be computed with relative importance of the experts taking into consideration. Certainly, this can magnify the extent of correlation amongst the policies and provide quality knowledge to assist SMEs.

REFERENCES

[1] E. Cox, The Fuzzy Systems Handbook: A Practioner's Guide to Building, Using & Maintaining Fuzzy Systems, Academic Press, Inc., 1994.

[2] Anderson, R.& Moore, "The Economics of Information Security," *Science*, pp. 610-613, 2006.

[3] Allison, I. & C. Strangwick, "Privacy Through Security, Policy & Practice in an SME," in *Computer Security, Privacy & Politics: Current Issues, Challenges & Solutions*, IRM Press, 2008.

[4] Ahonen, P. et al., "Threats & Vulnerabilities," in *Data Centric Systems & Apllications*, Berlin, Springer, 2010.

[5] NIST 800-88, *Special Publication 800-88: Guidelines for Media Sanitization*, National Institute for Standards & Technology, 2006.

[6] Hughes, G. & T. Coughlin, "Secure Erase of Computer Disk Data," UCSD, 2007.

[7] Garfinkel, S. & A. Shelat, "Remembrance of Data Passed: A Study of Disk Sanitization," *IEEE Security & Privacy*, 2003.

[8] HIPAA - 164.310(d)(2)(i)&(ii), *Health Information Portability and Accountability Act*, US Dept. of Health & Human Services (DHHS), 1996.

[9] PIPEDA, *Personal Information Protection & Electronic Documents Act*, Canada SC, 2000.

[10] GLB, *Gramm-Leach-Bliley Act*, US Congress, 1999.

[11] SarbOx, *Sarbanes-Oxley Act*, US Congress, 2002.

[12] EU 2006/24/EC, *EU Data Protection Directive*, EU, 2006.

[13] PCI-DSS, *Payment Card Industry Data Security Standard*, PCI Council, 2006.

[14] J. Warner, "Understanding Cyber-crime in Ghana: a view from below," *International Journal of Cyber Criminology*, vol. 5, 2011.

[15] J. S. Tiller, "Reporting Security Breaches," in *Information Security Management Handbook*, Boca Raton, CRC Press, 2003.

[16] S. Lee, Security Policies, Principles & Mechanisms, 1999.

[17] ITU-T, "Internation Telecommunications Union (ITU) - Telecoms Standards Recommendation X.805," 2005.

[18] S. Abugri, "Ghana: Internet Criminals Cashing in on e-Waste," *New Africa magazine*, 2011.

[19] B. Kosko, Neural networks & Fuzzy Systems: A Dynamical Systems Approach to Machine Intelligence, Englewood Cliffs, NJ: Prentice Hall, 1992.

[20] Kandasamy, W., Florentin Smarandache & K. Ilanthenral, Elementary Fuzzy Matrix Theory & Fuzzy Models for Social Scientists, Automaton, 2008.

[21] Siraj, Anbareen, Susan Bridges & Rayford Vaughn, "Fuzzy Cognitive Maps for Decision Support in an Intelligent Intrusion Detection System," *IEEEXplore*, 2001.

[22] Smith, E. & J. Eloff, "Cognitive Fuzzy Modeling for Enhanced Risk Assessment in Health Care Institution," *IEEE Intelligent systems & their Applications* , pp. 69-75, 2000.

[23] Heydebreck, P. et al., F2C - An Innovative Approach to Use FCM for the Valuation of High-Technology Ventures, IBIMA Publishing, 2011.

[24] B. M. Ayyub, Elicitation of Expert Opinions for Uncertainty & Risks, CRC Press LLC, 2001.

[25] P. Dadone, *Introduction to Fuzzy Sets*, 1995 ed., vol. 83, J. Mendel, Ed., Proceedings of IEEE, 2000.

[26] Kapurubandara, M. & R. Lawson, "Barriers to adopting ICT & e-Commerce with SMEs in Developing Countries: An Exploratory Study on Sri Lanka," 2006.