PERCEPTION OF COMMUNICATION NETWORK FRAUD DYNAMICS BY NETWORK ADMINISTRATORS AND STAKEHOLDERS

I.F.C. Onah[a], **H.C. Inyiama**[b]

Department of Computer Engineering, Enugu State University of Science & Technology, Enugu, Nigeria.

[a] *(Email: ikonah@yahoo.co.uk)*
[b]Present address: Department of Electronics and Computer Engineering, Nnamdi Azikiwe University, Awka, Anambra State.

Abstract

The massive growth of electronic commerce represent a new set of vulnerabilities aimed at the distortion, disruption, and destruction of the global and national information infrastructures, and are indeed significant threats to the integrity of networked systems. This paper investigates the perception of communication network fraud dynamics by network administrators and stakeholders. In considering the implications of the varied nature of the potential targets, the paper identifies the view to develop effective intelligence analysis methodologies for network fraud detection and prevention by network administrators and stakeholders. The paper further notes that organizations are fighting an increasingly complex battle for higher stakeholders, and thus require a greater, enterprise-wide understanding of the threats they face, across all operations and in all territories. In order to establish the appropriateness of the audience, this paper presents an analysis of the interview randomly administered. Informed opinion about the perception index of network administrators and stakeholders is analyzed.

Keywords: fraud dynamics, perception index, quantitative analysis

1. Introduction

As societies become more dependent upon linked communication and information systems the possibility that these systems will be compromised or disrupted becomes more salient, and the resulting consequences more serious. In spite of some well-publicized and extremely costly incidents of vulnerabilities, there remains a remarkable level of complacency on the part of administrators and stakeholders [1]. Results from the annual Computer Security Institute and United States Federal Bureau of Investigation (FBI) Annual Survey have revealed considerable reluctance to report problems. In 1999, for example, only 32 per cent of those who suffered serious attacks reported the intrusions to law enforcement [2]. While this almost doubled from the 17 percent figure of the three preceding years, it was still a remarkably low percentage; and actually dropped back to 25 percent in the Department of Trade and Industrys Information Security Breaches 2000 survey [3]. The report suggested that up to 60 percent of connected businesses in the UK, the United States, and

parts of Africa might have been the victims of cyber crime within the last two years. However, two-thirds of the companies interviewed noted that nothing had changed since the intrusions, while 30 percent did not see protection of business information to be a priority.

The risks inherent in information systems is changing as fast as new technologies are brought online. The multitude of systems and methodologies in place duplicate effort, reinforce divisional structures and are unable to share and cross-reference information. These create barriers to financial crime management and hinder the successful detection of todays organized criminal. They drive up operational costs and total cost of ownership through duplication of effort, inefficient processes and multiple support and maintenance costs.

It is worthy of note that this "democratization of high technology" has been accompanied by a new form of individual empowerment. The positive side of this is the growth of computer literacy; the negative is the emergence of the hacker/cracker sub-culture. Hackers/crackers are occasionally vulnerable to recruitment by criminal or terrorist organizations and "there is a real danger that a Global Dictator could emerge and begin to make a deadly and perverted use of" the national and global information infrastructures [4]. But rather than exploding a bomb in front of a government office or corporate headquarters, however, the weapon of choice will be a computer program that will do far more damage and affect far more lives.

In this dispensation, skilled individuals or groups residing anywhere within the Global Information Infrastructures (GII) can develop new potential information warfare weapons. This advent of computer warfare has the potential to significantly change the balance of power in a world increasingly dependent on sophisticated technologies. This will give nations that would never consider themselves players in the arena of global power strategies a new place in a different kind of world. In such a world of Information Warfare, technological capability, rather than the size of kinetic weapons arsenals or standing armies, is the primary factor in determining the balance of power. Any sort of malicious operation against a network may lead to wide-ranging unintended effects [1].

2. 1.0 Review of related Works

One person with a computer, a modem and the requisite knowledge and skills has the capacity to wreak considerable havoc. The "I love you" virus, for example, caused an estimated $6.7 billion in damages in the first 5 days [5]. The costs were so diffused among business, government, and educational institutions as well as individual computer users. The potential targets are so diverse, covering local, regional, national or transnational boundaries. Among the dimensions that could all too easily be compromised are:

- Public disclosures about classified information that could compromise national security.
- Denial of service attacks which cause enormous backlogs in communications and interfere with transactions in both business and government.
- Attacks on information, called information tampering, which can affect the implementation of missions of government agencies and departments or businesses.
- Breaches of security in financial transactions (e-commerce) by criminals, terrorists, unhappy customers or bored teenagers.
- Damage or disruption to National Infrastructures - communications, transportation, power grids, etc. which could have enormous cultural and economical consequences.
- Distribution of memes - self-propagating or actively contagious viruses which affect the content of existing information.

> Cyber-space is a wonderful domain for the propagation of "memetic viruses" [1].

The nature of fraud is changing dynamically because todays criminals:

- attack globally, not locally
- are organized and systematic, not random and opportunistic
- infiltrate systems rather than people or places
- erode profits through persistent high volume attacks

Today, the multitude of systems and methodologies in place create barriers that put the business at risk in several key areas:

- increased exposure to unpredictable financial losses
- increased risk of exposure to sanctions
- escalating operational costs
- reduced productivity of investigative resources

The problem of fraud detection is to discover dishonest intention of the customer, which clearly cannot be directly observed. The intentions of the customers are reflected in the transaction behaviour and thus in the observed transaction data. Gathering normal transaction data is relatively easy as this mode dominates the population. But collecting fraudulent transaction data is more problematic because it is relatively rare. Data collection involving human labour is expensive. The processing and storing of data is also subject to restrictions due to legislation on privacy of data.

3. Methodology

The study was conducted in Enugu metropolis, capital of Enugu State of Nigeria. The selection of the study area was influenced by the sufficient availability of network resources, and vibrant individuals knowledgeable on the concept, universality and potential danger of network related frauds. Opinions of stakeholders and data communication operators were gathered from both Primary and Secondary sources. Primary data were gathered from the field through the use of questionnaires, observations, discussions and interviews while secondary data were gathered from secondary sources such as books, journals and internet sources; among others. The types of primary data collected include characteristics of stakeholders and operators in Enugu, network fraud dynamics, fraud detection techniques in place, changing patterns of fraudsters, in the study area, among others. Examples of secondary data collected include age distribution, educational qualifications, and assessment of levels of respondents, among others.

Two surveys were undertaken during the primary data collection. The first and main survey spanned a period of one week while the second survey lasted for a period of four days. The second survey was to gather additional data as well as mop up all the gaps identified during the first survey. In all, a total of 150 questionnaires were distributed and 50 individuals were interviewed during the field surveys. The multi-stage sampling technique [6] was used to collect individual data using both stratified and simple random sampling methods. The individuals in the metropolis were grouped into two main strata (network operators and stakeholders) which exhibit definite characteristics such as age and educational levels (Tables 2 and 3). The simple random sampling method was then used to select individuals from each stratum. The reason for the use of the simple random sampling method was that every element or stakeholder had an equal chance of being selected from the population [7]. Chi-Square distribution is adopted to test the viability and reliability of the hypotheses formulated in the study.

Please tick (√) to one which is applicable to you.

1. Sex: (a) Male ( ) (b) Female ( )
2. Age: (a) 25 - 30 ( ) (b) 31 - 35 ( ) (c) 36 - 40 ( ) (d) Above 40 ( )
3. Religion: (a) Christian ( ) (b) Moslem ( ) (c) Traditional ( )
4. Marital Status: (a) Single ( ) (b) Married ( )
5. Qualification: (a) WASC/GCE ( ) (b) NCE/OND ( ) (c) HND/B.Sc ( ) (d) M.Sc/MBA/PhD ( ) (e) Professional Cert. ( )

Table 1: Sample Questionnaire.

S/N	Test Questions	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
6.	The existence of computer network related frauds is real.					
7.	Fraudsters in networked systems are constantly changing their tactics to avoid detection.					
8.	Every subscriber of an online service is a potential fraudster.					
9.	Security and privacy of network systems should be the concern of government at all levels.					
10.	Adoption and implementation of efficient fraud detection and analysis systems will curb the nefarious attitude of fraudsters.					

11. Do you browse the Internet? Yes ( ) or No ( )
12. Have you ever engaged in any form of online business transactions? Yes ( ) or No ( )
13. Are you aware that information resources maintained in computer network infrastructures are plagued by various network frauds? Yes ( ) or No ( )
14. Have you ever participated in any seminar, training or workshop on online commerce? Yes ( ) or No ( )
15. Any other comments please state below.

.....
.....
.....

3.1. Screening Questions

4. Analysis of the Perception Index

Quantitative method was used to process and analyze raw data for the purpose of gathering informed opinion about communication network fraud.

4.1. Questionnaire analysis

In our research problem, answer options are classified into five mutually-exclusive categories namely: Strongly Agree, Agree, Neutral, Disagree, and Strongly Disagree. The dependent variable – Quest/Rank – is classified into the various research questions. With this information, the frequency distribution of answer options for 90 questionnaire respondents was designed.

4.1.1. Collating respondents returns

Respondents returns are arranged in a frequency distribution to present the data in a more manageable and comprehensible form.

Table 2: Age distribution of respondents.

Age of Respondents	No. of Respondents	Percentages
25-30	10	11.11%
31-35	26	28.89%
36-40	34	37.78%
Above 40	20	22.22%
Total	**90**	**100**

Table 3: Age distribution of respondents.

Qualification of Respondents	No. of Respondents	Percentages
WASC/GCE	06	6.67%
NCE/OND	12	13.33%
HND/B.Sc	30	33.33%
M.Sc/MBA/PhD	15	16.67%
Professional Cert.	27	30.00%
Total	**90**	**100**

The ages of the respondents are shown in Table 2.

The analysis in the table above indicates that the respondents are vibrant, matured individuals who understand the impact of fraud in organizations and businesses.

The educational qualifications of the respondents are shown in Table 3.

The above analysis indicates that the respondents have adequate and relevant educational qualification to understand the concept and universality of the research topic.

4.1.2. Evaluation Procedures

Statistical inference is drawn from data presented by the frequency distributions (Tables 4, 6 and 8) so that one can use the findings from this sample population to generalize on perception of operators and stakeholders.

STEP 1: Set up the Hypothesis - some testable belief or opinion which aims to test statistically the more likely of two possibilities. Two hypotheses for the statistical testing are:

a) Null Hypothesis, designated as H_0, in which there is no assumption of contradiction between the supposed mean and the sample mean and any difference can be ascribed solely to random factors.
b) Alternative Hypothesis, designated as H_1, in which there are differences between two or more measures, for example, the sample mean and the population mean.

It is likely that the information gleaned from a sample data taken to test some Hypothesis (e.g., the sample (population) mean or standard deviation) does not completely support the Hypothesis due to either the original Hypothesis being wrong or the sample being slightly unrepresentative (which virtually all samples will be to a greater or lesser extent).

The process of testing the probability that observed differences are due to chance in order to accept or reject the Hypothesis is referred to as a test of significance. The difference "not due to chance" values are termed statistically significant values. The difference "due to chance" values are known as statistically nonsignificant values [8].

When the value of a given difference between two or more measures falls into the nonsignificant difference region, the null Hypothesis is said to have been retained. But when the difference falls into the significant difference region, the null Hypothesis is said to have been rejected.

Both tails of the distribution of sample means (H_0 and H_1) shall be used and this is thus called a two tail test of significance. The null Hypothesis is symbolized by H_0 and the alternative hypotheses are symbolized by H_1, H_2, H_3, etc. The null Hypothesis is the one which is tested. If H_0 is accepted, H_1 is rejected whilst if H_0 is found to be false, H_1 is accepted.

Our two tail test is stated as follows:

H_0: $f_0 = f_e$ - Mean of A = Mean of B
H_1: $f_0 > f_e$ - Mean of A $\neq$ Mean of B

The null Hypothesis is seen as the logical opposite of the alternate Hypothesis. So, where the null is rejected the alternative is automatically accepted through logical implication.

The following three hypotheses are formulated for the purpose of the test:

Test of Hypothesis 1

H_0: The existence of computer network frauds is real.
H_1: The existence of computer network frauds is not real.

Test of Hypothesis 2

H_0: Adoption and implementation of efficient fraud detection and analysis systems will curb the nefarious attitude of fraudsters.
H_1: Adoption and implementation of efficient fraud detection and analysis systems will not curb the nefarious attitude of fraudsters.

Test of Hypothesis 3

H_0: Efficient, dynamic and adaptive fraud detection techniques will give service operators a competitive edge in terms of customer care and retention, marketing and revenue assurance.
H_1: Efficient, dynamic and adaptive fraud detection techniques will not give service operators a competitive edge in terms of customer care and retention, marketing and revenue assurance.

STEP 2: Sampling Statistic

A number of statistical operations can be performed on a set of data depending on the

research parameters. Some of them include the regression analysis, the Chi-square, Correlation analysis, the students t-test and z-test, the f-test, the significance of percentages, the standard error of percentages, the standard deviation, the probability test, and the Wilcoxon [8] two-sample test, etc.

Being quantitative data, the Chi-Square test of independence will be used in this analysis. The reason for the choice of Chi-Square, symbolized by X^2, as the statistical measure is that X^2 has a theoretical sampling distribution which permits us to address research problems involving frequencies where the variables have been classified into two or more mutually exclusive categories. The X^2 is most often used in evaluating research data reported in frequencies, such as proportions and percentages. It is one of the best statistical methods available for us for comparing observed frequencies against expected frequencies [8].

This is quite unlike proportion statistics where there are only two categories, for classifying observations such as yes – no, agree – disagree, etc. The sampling statistic for testing the feasibility of the null Hypothesis under the Chi-Square is defined by the formula:

$$X^2 = \sum (f_o - f_e)^2 / f_e \qquad (1)$$

where f_o = Observed frequencies in a category (Generated from sample data); f_e = Expected frequencies in the same category (provided by population parameters); $\sum$ = Sum this ratio over all columns and rows.

The sampling distribution of the Chi-square is a function of the associated degrees of freedom (df). In Chi-square, the df is based on the number of categories symbolized by K. For example, to rate five colours of a sample textile, the variable is Colour and it is divided into five categories of different colours ($K = 5$). Thus the df under this condition is $K - 1 = 5 - 1 = 4$. The Critical values for Chi-Square for various significance levels are presented in a Chi-Square table.

STEP 3: State the significance level and define the rejection region(s) as appropriate.

Significance level must be chosen before the test is carried out, and it is a critical factor in deciding whether to accept or reject a Hypothesis. This is why the term 'Significance testing' is commonly used instead of Hypothesis testing. It cannot be said with 100% certainty that a difference is significant since samples and random factors are being handled. Accordingly, various levels of significance are chosen, most commonly 5% or 1%, and thus the result of a particular test might be expressed as follows:

'The difference between the sample mean and the hypothetical population mean is significant at the 5% level'.

Or,

'There is a 95% confidence that the difference between the sample mean and the population mean is not due to chance factors.'

The score for a two tailed test at the 5% level is 1.96.

The significance level is set at .05, two tailed. The above three hypotheses will be tested at 5% level of significance with $(r - 1)(c - 1)$ degree of freedom. If x^2 calculated is greater than x^2 tabulated, the null Hypothesis (H_0) is rejected; else the null Hypothesis is accepted.

A total of 100 questionnaires were randomly distributed to the respondents out of which 90 were returned with responses.

STEP 4: Compute sample statistics and draw conclusions based on your findings.

The expected frequencies for each cell were determined and the general X^2 formula was then applied.

4.1.3. Test of Hypothesis 1

H_0: The existence of computer network frauds is real.

H_1: The existence of computer network frauds is not real.

The data collected based on these hypotheses are presented in table 4. The numbers in each cell of the table without bracket are observed frequencies, while those in brackets are the expected frequencies.

Table 4: The Existence of data communication frauds is real and constitutes a major problem to the data communications industry.

Quest/ Rank	Strongly agree	Agree	Neutral	Disagree	Strongly Dis-agree	Row total (R_i)
1	40(40)	35(40)	15(10)	0(0)	0(0)	90
2	40(40)	45(40)	5(10)	0(0)	0(0)	90
Column Total (C_j)	**80**	**80**	**20**	**0**	**0**	**180**

Table 5: Contingency table for Test of Hypothesis 1.

CELL	$\mathbf{F_0}$	$\mathbf{F_E}$	$\mathbf{F_0 - F_E}$	$\mathbf{F_0 - F_E}^2$	$\mathbf{F_0 - F_E^2/F_E}$
$A: r_1c_1$	40	40	0	0	0
$B: r_1c_2$	35	40	-5	25	0.625
$C: r_1c_3$	15	10	5	25	2.5
$D: r_1c_4$	0	0	0	0	0
$E: r_1c_5$	0	0	0	0	0
$F: r_2c_1$	40	40	0	0	0
$G: r_2c_2$	45	40	5	25	0.625
$H: r_2c_3$	5	10	-5	25	2.5
$I: r_2c_4$	0	0	0	0	0
$J: r_2c_5$	0	0	0	0	0
					$\sum X^2 = 6.250$

Table 6: The adoption and implementation of good strategies will curb the activities of fraudsters.

Quest/ Rank	Strongly agree	Agree	Neutral	Disagree	Strongly Dis-agree	Row total (R_i)
3	38(39)	44(40)	5 (6)	3 (3)	0 (2)	90
4	40(39)	36(40)	7 (6)	3 (3)	4 (2)	90
Column Total (C_j)	**78**	**80**	**12**	**6**	**4**	**180**

Table 7: Contingency table for Test of Hypothesis 1.

CELL	$\mathbf{F_0}$	$\mathbf{F_E}$	$\mathbf{F_0 - F_E}$	$\mathbf{F_0 - F_E}^2$	$\mathbf{F_0 - F_E^2/F_E}$
$A: r_1c_1$	38	39	-1	1	0.02564
$B: r_1c_2$	44	40	4	16	0.4
$C: r_1c_3$	5	6	-1	1	0.16667
$D: r_1c_4$	3	3	0	0	0
$E: r_1c_5$	0	2	-2	4	2
$F: r_2c_1$	40	39	1	1	0.02564
$G: r_2c_2$	36	40	-4	16	0.4
$H: r_2c_3$	7	6	1	1	0.16667
$I: r_2c_4$	3	3	0	0	0
$J: r_2c_5$	4	2	2	4	2
					$\sum X^2 = 5.185$

Expected frequencies are obtained thus:

$$\begin{aligned} e_{11} &= (90*80)/180 = 40 \\ e_{12} &= (90*80)/180 = 35 \\ e_{13} &= (90*20)/180 = 10 \\ e_{14} &= (90*0)/180 = 0 \\ e_{15} &= (90*0)/180 = 0, \text{ etc} \end{aligned}$$

Designing a 10-cell contingency table:

Where r = number of rows, c = number of columns

X^2cal = 0 + 0.6250 + 2.5 + 0 + 0 + 0 + 0.6250 + 2.5 + 0 + 0 = 6.250

$$\begin{aligned} df &= (r-1)(r-2) \\ &= (2-1)(5-1) \\ &= 1*4 \\ &= 4 \end{aligned}$$

With 4 df, the critical X^2 value required for significance at .05 significance level is 9.488 (from table).

That is, X^2 (tabulated) = $X^2(r-1)(c.1)$; $0.05 = X^2$ df,$0.05 = 9.488$

Conclusion: If the computed Chi-Square value exceeds the tabled critical Chi-Square value at a specified level of significance, then the null Hypothesis is rejected. In other words, there is justification for the claim that computer network frauds exists. Since X^2 calculated (i.e. 6.250) is less than X^2 tabulated (i.e. 9.488), H_0 is accepted and it is concluded that the existence of computer network frauds is real.

4.1.4. Test of Hypothesis 2

H_0: Adoption and implementation of efficient fraud detection and analysis systems will curb the nefarious attitude of fraudsters.

H_1: Adoption and implementation of efficient fraud detection and analysis systems will not curb the nefarious attitude of fraudsters.

The data collected based on these hypotheses are presented in table 6:

Expected frequencies are obtained thus:

$$\begin{aligned} e_{11} &= (90*78)/180 = 39 \\ e_{12} &= (90*80)/180 = 40 \\ e_{13} &= (90*12)/180 = 6 \\ e_{14} &= (90*6)/180 = 3 \\ e_{15} &= (90*4)/180 = 2, \text{ etc} \end{aligned}$$

Designing a 10-cell contingency table:

Where r = number of rows, c = number of columns

X^2cal = 0.02564 + 0.4 + 0.16667 + 0 + 20 +

Table 8: Fraud detection and prevention will reduce revenue leakages.

Quest/ Rank	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree	Row total (R_i)
5	43(41)	35(37)	7 (8)	3 (2)	2 (2)	90
6	40(41)	38(37)	9 (8)	1 (2)	2 (2)	90
7	40(41)	38(37)	8(8)	2 (2)	2 (2)	90
Column Total (C_j)	**123**	**111**	**24**	**6**	**6**	**270**

$$0.02564 + 0.4 + 0.16667 + 0 + 2 = 5.185$$

$$\begin{aligned} df &= (r-1)(r-2) \\ &= (2-1)(5-1) \\ &= 1*4 \\ &= 4 \end{aligned}$$

With 4 df, the critical X^2 value required for significance at .05 significance level is 9.488 (from table).

Conclusion: Since X^2 calculated (i.e. 5.185) is less than X^2 tabulated (i.e. 9.488), H_0 is accepted and it is then concluded that the adoption and implementation of efficient fraud detection and analysis systems will curb the nefarious attitude of fraudsters.

4.1.5. Test of Hypothesis 3

H_0: Efficient, dynamic and adaptive fraud detection techniques will give service operators a competitive edge in terms of customer care and retention, marketing and revenue assurance.

H_1: Efficient, dynamic and adaptive fraud detection techniques will not give service operators a competitive edge in terms of customer care and retention, marketing and revenue assurance.

The data collected based on these hypotheses are presented in table 8:

Table 9: Contingency table for Test of Hypothesis 2.

CELL	F_0	F_E	$F_0 - F_E$	$F_0 - F_E{}^2$	$F_0 - F_E^2/F_E$
$A: r_1c_1$	43	41	2	4	0.09756
$B: r_1c_2$	35	37	-2	4	0.108108
$C: r_1c_3$	7	8	-1	1	0.125
$D: r_1c_4$	3	2	1	1	0.5
$E: r_1c_5$	2	2	0	0	0
$F: r_2c_1$	40	41	-1	1	0.02439
$G: r_2c_2$	38	37	1	1	0.027027
$H: r_2c_3$	9	8	1	1	0.125
$I: r_2c_4$	1	2	-1	1	0.5
$J: r_2c_5$	2	2	0	0	0
$K: r_3c_1$	40	41	-1	1	0.02439
$L: r_3c_2$	38	37	1	1	0.027027
$M: r_3c_3$	8	8	0	0	0
$N: r_3c_4$	2	2	0	0	0
$O: r_3c_5$	2	2	0	0	0
					$\sum X^2 = 1.559$

Expected frequencies are obtained thus:

$$\begin{aligned} e_{11} &= (90*123)/270 = 41 \\ e_{12} &= (90*111)/270 = 37 \\ e_{13} &= (90*24)/270 = 8 \\ e_{14} &= (90*6)/270 = 2 \\ e_{15} &= (90*6)/270 = 2 \\ e_{21} &= (90*123)/270 = 41 \\ e_{22} &= (90*111)/270 = 37 \\ e_{23} &= (90*24)/270 = 8 \\ e_{24} &= (90*6)/270 = 2 \\ e_{25} &= (90*6)/270 = 2 \end{aligned}$$

And so on.

Designing the 15-cell contingency table:

Where r = number of rows, c = number of columns

$X^2\text{cal} = 0.09756 + 0.108108 + 0.125 + 0.5 + 0 + 0.02439 + 0.027027 + 0.125 + 0.5 + 0 + 0.02439 + 0.027027 + 0 + 0 + 0 + 0 = 1.559$

$$\begin{aligned} df &= (r-1)(r-2) \\ &= (3-1)(5-1) \\ &= 2*4 \\ &= 8 \end{aligned}$$

With 8 df, the critical X^2 value required for significance at .05 significance level is 15.507 (from table).

Conclusion: Since X^2 calculated (i.e. 1.559) is less than X^2 tabulated (i.e. 15.507), H_0 is accepted and it is concluded that efficient, dynamic and adaptive fraud detection techniques will give service operators a competi-

tive edge in terms of customer care and retention, marketing and revenue assurance.

5. Concluding Remarks

The message is simple – as organized crime continues to grow, organizations must get smarter and more efficient at stopping criminals in their tracks. Firstly, significantly improved positive detection of organized money laundering and financial crime attacks delivers:

- reduced financial losses
- reduced risk of exposure to sanctions
- increased reputation protection

Secondly, reduced operational costs of both human and technological resources can be maximized, as duplication of effort is eradicated. Institutions who have already started on the journey of an enterprise approach report substantial improvements, including:

- 98% improvements in the speed of completion for first level investigations
- 200% increases in the accuracy of detection rates

The adoption and implementation of efficient fraud detection and analysis systems will curb the nefarious attitude of fraudsters, and delivers the information and intelligence for you to take command and control of your defenses across all products, channels and regions. It will also help deliver an early warning system to help you quickly understand the magnitude of an attack and the crucial information needed to make informed operational decisions that protect your business.

References

1. Robert, C. Seacord and Allen, D. Householder. *A Structured Approach to Classifying Security Vulnerabilities*, Technical Note, CMU/SEI-2005-TN-003, January 2005, URL: http://www.sei.cmu.edu/reports/pdf/05tn-003.pdf.

2. Jerry Scott. *2004 CSI/FBI Annual Survey*, URL: tjscott.net/policy/csifbi2004.pdf, 2004

3. John Doody, David Hodges. Information Security Breaches 2000 Survey. Presentation to the *First International Common Criteria Conference*, Baltimore, UK IT Security, Evaluation and Certification Scheme, 23 May 2000.

4. Inyiama, H. C. *Computer Applications and Information Technology*, The Dynamic Informer, Enugu, 2000, pp 108.

5. Michael Erbschloe. *Love Bug Damage Costs Rise to 6.7 Billion.* May 9, 2000, URL: http://www.businesseconomic.com/cei/-press.index.html

6. Michael Erbschloe. *Guide To Disaster Recovery.* 2003, URL: www.cert.org/archive/html/Analysis10a.html

7. Oppenheim, A. N. *Questionnaire Design, Interviewing and Attitude Measurement*, Wellington House, London, 1992.

8. Ikponmwosa Owie. *Fundamentals of Statistics in Education and the Social Sciences*, United City Publishing Company, Benin City, Third print, 1996.