International Journal of Management and Commerce Innovations ISSN 2348-7585 (Online)
Vol. 7, Issue 1, pp: (814-825), Month: April 2019 - September 2019, Available at: www.researchpublish.com

ASSESSING SECURITY METRICS IN CORPORATE SECURITY MANAGEMENT IN AFRICA TODAY

[1]Dr. Mary Ragui, PhD, [2]Muhumed A Sheikh, [3]Amon Nyansera Nyakundi, [4]Denis Kimathi Kairemia

KENYATTA UNIVERSITY

Abstract: **Security metrics relevance in business management has exploded in recent times due to the increase in the role of security in organizations in the face of global security challenges, cut-throat competition and the concomitant rise in budgetary allocations to the function. The security metrics however, are challenged for a number of reasons including its relative age, nature of the function and perception of the same. A number of theories have been postulated to justify the need for security metrics as well as postulate analysis tools and they include the Argumentation Theory, the Gordon-Loeb Model and the Critical Infrastructure/Key Resource Protection Theory. Correctness and effectiveness, leading vs lagging indicators, organizational security objectives, quantitative and qualitative properties and measurement of small vs huge dimensions are key aspects in the field that must be carefully considered in the development of security metrics and have been discussed in this paper. The biggest challenges in the field include what measure, how to measure, how to report and the problem of outliers in data. These challenges can however be overcome through careful consideration of the aspects to arrive at correct and highly effective security metrics.**

Keywords: **Africa, Security, Management, Metrics, Measurements, Models, organizational, Corporate, Effectiveness, Efficiency.**

I. INTRODUCTION

Until something can be measured and expressed in numbers, then our knowledge in that field is insufficient according to Lord Kelvin a 19th century eminent physicist. Management's ability to run something is a function of sufficient knowledge of it. The import of the so often cited Lord Kelvin quote is that all aspects of a corporations' business must be understood well enough to be measured and expressed in figures to assure informed decision making on the part of the management for business continuity. Corporate security management finds itself in this rubric.

In the last few decades, and even more intensely in the wake of the 9/11 attack and a series of other targeted terror attacks thereafter, corporate security has found itself in the limelight credit to the increased security threats to corporations and other organizations as well as the broadening of the mandate in the corporation. The September 11, 2001 made it crystal clear that global terrorism posed a present and credible threat that was no longer vague and/or unlikely (Sennewald, 2003). Sennewald went further to contend that these unfortunate developments had elevated corporate security to a key function in managing a corporation's going concern. This, then, led to increased budgetary allocations for security in absolute as well as relative terms. Security like other functional departments in an organization, must sufficiently articulate its issues albeit in the face of more sceptics.

The demand for more transparency and accountability coupled with the need for improved justification and prioritization of security investments, suitable alignment between security and the general organizational mission, goals, objectives, perfect effectiveness and efficacy of the security programmes is giving prominence to the rise on security metrics. The cost to every endeavor or programme in capital expenditure and running costs as well as the cost of detriment to the core business of the organization vis a vis the direct and indirect benefits of any organizational undertaking coupled with the opportunity costs of investing resources in a given way weighs into the determination of the efficacy of that undertaking and ultimately its prioritization among other business needs for cash and cash equivalents.

Security metrics are a system of related dimensions compared against a standard to enable quantification of the degree of freedom from possibility of suffering damage or loss as a result of a security incident (Payne, 2006). Like in physical sciences, security metrics are also founded on numerical reckoning and practicable methods for measuring some quality connected to it. The numerical reckoning is based on the analysis of sometimes objective or subjective human interpretations. The objectivity or subjectivity of human interpretations of the premises of any given security metrics speaks to its reliability and ultimately the trust and confidence level that can be laid on the outcome.

II. THEORETICAL REVIEW

The growth of corporate security from simple ingress control to a momentous corporate function in organizations over the last few decades and the concomitant rise in budgetary needs and allocations has led to the need to ensure maximum value for money invested in the related programmes. Maximizing value for money in any undertaking is about ensuring efficiency and effectiveness. The evaluation of effectiveness can only be done on the basis of numerical figures for it to be intelligible. Consequently, researchers, academicians and practitioners in the field have postulated theories to address the issue of measurability of corporate security management related outcomes for evaluation against investment. This paper will evaluate a few of them in the subsequent paragraphs.

A. Argumentation Theory

The argumentation theory postulated by Yasasin and Schryen of the University of Regensburg is a development of a 20th century British philosopher Stephen Toulmin's Argumentation model. The theory states that for an assertion on security management outcomes to be merited, it must at the very least satisfy three of the Toulmin's model criteria points. The security management makes a claim, evidence is adduced in support of the claim then justification is presented. In doing so, the claim, the evidence and the warrant criteria is met and therefore can be used in evaluation (Emrah, 2015).

Developing a claim with regard to security management outcomes could involve just mentioning what would be considered as the benefits emanating from a certain strategy or investment in security management. This claim or assertion must then be proven by providing evidence as to the actual change in status of something when related to a given point in time in the past. The claimant or the security manager must also establish warrant. They must show that the change in outcome or status claimed is actually as a result of security. Establishing the three ground rules will align the measurements against the requirements of the Argumentation theory.

B. The Gordon-Loeb Model

This model was postulated by Lawrence Gordon and Martin Loeb of the University of Maryland in the United States. The model states that investment in security does not usually lead to profits but rather prevents further losses. Therefore, in determining the rate of return on security investment, a business decision maker must compare the cost of protecting some form of asset with the potential loss in case the asset is stolen, lost, damaged or corrupted (Gordon, 2016). In essence, security benefits will not reflect in an organization's profit and loss account as income because it does not directly lead to cash inflows into the business but rather prevent outflows or maintain current inflows. At times, rarely though, an investment in security leads to increased business for the organization but even then, that increase cannot be factored on a profit and loss account as an income with the head, 'security'.

To employ the model, the concerned party must process knowledge in three key parameters; the worth of the assets at risk, how much the assets are at risk and the probability of an attack on the assets being successful or vulnerability of the assets (Giuseppe, 2017). Those factors considered together in the model present the medium loss to the corporation if no security investment is made to address the risks abound. The worth of a given asset must not be the capital cost but also the loss in business should that given asset be unavailable for employment at normal rates. The worth of the asset at risk is in determined by multiplying the worth of the given asset to the exposure factor.

The model is based on three assumptions; that organizational assets are inherently vulnerable to attacks denoted by the expression v ($0 \leq v \leq 1$), this presents the assumption that assets are vulnerable to attacks under current conditions, that a breach in asset security represents a potential loss and can be expressed in monetary terms and that investment in security will reduce the impact of the expected loss based on the effectiveness of the investment (Gordon, 2016). The reduction in the expected impact on the asset and the organization upon an attempted or successful attack is considered the benefit of security in this model.

C. Critical Infrastructure/Key Resource Protection Theory

This theory hypothesizes that the probability of intent in threat as a component of threat can be influenced by security activities that deter possible attacks by patching up vulnerabilities and consequences of possible attacks and as such, deterrence efforts can be quantified (Taquechel, 2018). The theory intimates that logical programmes can be used to asses and determine numerical values to exploitation susceptibility that can in turn be used to develop security metrics.

Critical infrastructure protection theory offers the chance to discuss risk related phenomena in developing security metrics. Including risk in the evaluation of security system performance metrics further presents the opportunity to consider adaptive adversary initiatives as a likely moderator variable influencing the nexus between intermediate and end-state corporate security outcomes. Adaptive adversary considerations as well as deterrence quantifications are vital in generating worthwhile security performance metrics.

Conversely, the perception of the effects of an adversary adapting intent upon erection of threat reduction measures must be captured in a logical framework to come up with threat reduction security metrics. If a perceived adversary had targeted a given asset that has immense value or could cause immeasurable financial adversity to the firm if targeted, and security measures successfully divert their intention to a less valuable asset, then that should find a place in the metric development logical framework (Anderson, 2011).

III. ASPECTS OF SECURITY MEASUREMENT

Security measurement is an exhausting problem to a point it was added to the Hard Problem List in 2006 by the INFOSEC Research Council (Bellovin, 2006). Governments as well as industry leaders in security and communication have made efforts to quantify security and justify security budgets. The endeavors can be summarized in a number of aspects. The highlighted aspects help identify possible pitfalls in the area or security metrics as well as other pertinent concerns in the field. The issues are discussed hereafter.

A. Correctness and Effectiveness

Correctness signifies the assurance level that a security system put in place has been appropriately implemented, that is the mechanism does exactly what it was intended to do. Effectiveness on the other hand, denotes the ability of the system to have fidelity to the objectives of the programme. Correctness can be evaluated both in construction and in operation all in respect to the environment but the emphasis should be on how well it shows the behavior anticipated of it. Evaluation of effectiveness involves ascertaining the ability of all the components of the system to work synergistically to withstand attacks, consequence of possible vulnerabilities be they discoverable or known (Microsoft Corporation, 2007). A programmes fidelity to the pre-set objectives and the assurance that the system has been implemented as was anticipated or planned are phenomena that can differ with change in perception.

In practice, most security measurements in this aspect are done qualitatively, through logical reasoning rather than quantitatively through the measurement of machines or software. Outcomes are therefore made of simplified assumptions. These forms of abstractions and simplifications often dissociates the evaluation from the actual operational use. Even though correctness can be emphasized, for significantly huge systems, the confidence level in the evaluation criteria cannot be assured because of the involvement of the human biases. Standardized procedures as well as training in conformance as well as automation where possible are useful in heightening the assurance level and replicability of the evaluation outcomes. The training must be repeated often enough as refresher courses.

B. Leading vs Lagging Indicators

Security metrics may potentially be generated from leading, coincidental or lagging indicators of the state of a security system. Leading and lagging indicators are observable conditions before or after the occurrence of a security incident respectively, while the coincidental indicators are concurrent with the security incident. If any indicator is miscategorized, the interpretation and the subsequent reaction could be calamitous. Another challenge is usually the post-occurrence indicators taking unduly long to signal so. The lagging indicators must have a short latency period so that the response post-occurrence is timely and guided. Where it's not possible to achieve short latency lagging indicators, the latency must be recognized and preparations made to handle the intrinsic delay and the associated shortcomings. Failure to achieve short latency lagging indicators or recognize the lag, appreciate and plan accordingly will be detrimental in the response.

At times, security incident statistics may be hard to categorize as either of the three categories. For instance, what might be perceived as leading indicators could be an elaborate intrusion measure or just surveillance and possible reductions in

incident counts post a major incident could signify either a reduction in adverse activities or a compromised security system. Similarly, an increase in security incidents around a major occurrence which could be viewed as coincidental could in theory be leading or lagging if the security mechanisms are hyper vigilant post an attack or a distraction from the major incident.

Experience in the security system deepens the practitioners understanding of its weaknesses and related vulnerabilities, especially post a security breach. This deepened understanding helps correctly categorize the indicators which enables better, timely and more efficient response besides the identification of good preparatory measures for possible future attempts. However, while experience improves these evaluations, no metric exists that can measure the state of security at any one given instance in absolute terms (Torgerson, 2007). In other words, the state of security is almost always relative to other factors and mostly the environment. What would, in theory, deny ingress to a technologically challenged attacker will not deny entry to one who is technologically savvier. The state of security or the security level is therefore, usually expressed relative to a given environment or threat as the metrics are subject to those intervening factors.

C. Organizational Security Objectives

Different organizations exist for varying reasons, have different asset portfolios, dissimilar exposures and face diverse threats. Accordingly, different organizations' security objectives are rarely alike. Besides considerations like the role of the organization in the society and threat to the assets, there exists practical considerations that may influence an organization's approach to security and ultimately its security objectives. For instance, most organizations cannot possibly secure all assets on its charge to the highest possible degree because of financial constraints and therefore prioritization based on asset sensitivity and criticality becomes necessary and this influences the security objectives.

With security objectives varying so widely, it is only logical that the metrics that are appropriate for the different organizations be as different for effectiveness and relevance. This is because, security is dependent on risk and policy from an organizational perspective. This implies that security metrics that can be used across organizations with similar effectiveness are hard to establish. Different security objectives as a result of differences in other areas of different organizations infer metrics cannot be universal for all organizations in the lower levels of security management.

Even though security objectives are unique to various organizations, often, similarities in high level security objectives exist and are at times termed as best practices. Some steps, such as standard security outlines of structural security necessities and norms, can be engaged to standardize mutual cliques of principal necessities needed by analogous organizations and permit reuse of engineered solutions. Nevertheless, at best they comprise only a mutual subset of the whole picture and may focus principally on technical metrics.

D. Quantitative and Qualitative Properties

Security systems have some desirable properties including; scalability, complexity and usability which can only be expressed in general terms. The distinction between quantitative and qualitative security metrics can be obscured in security systems that exhibit those desirable properties (Henning, 2001). While quantitative metrics outrightly give figures to represent the security level, qualitative metrics are assessed, ranked and assigned numeric values that can then be used in calculations. At times, the numeric difference in security rankings assigned arbitrarily by evaluators may not have any particular significance. The absence of particular significance more often than not is an indication of the absence of reliability in those measurements.

Quantitative security values may also at times be weighted and combined to derive composite values. Such combinations however, can lead to a lack of diversity, this can be evident in cases where different vulnerabilities with differing characteristics end up receiving the same score. This happens despite the vulnerabilities having different severity levels. Amalgamation of different quantitative and qualitative measurements in developing security metrics may lead to dilution of critical logical values or the introduction of errors in the calculation as a result of wrongful evaluations or erosion of important outliers.

E. Measurement of Small vs Huge Dimensions

Anecdotal evidence in existing security literature tends to show an indirect correlation between success of security measurement and the size and complexity of the measurements. This phenomenon has been attributed to larger systems having greater functionality and are much more complex in general. As a general rule, the number of possible interactions increases with the square of the number of components increase. The greater the functionality, the greater the need for

evaluation and scrutiny. Given the number of interactions in a security system increases at the square of the number of components added in that system, a system with many components has very many interactions, all of which must be evaluated.

Two security systems that could be adjudged secure when evaluated individually can be connected together resulting in a composite system that is less secure than the individual components in what is known as the composability problem. In the absence of sound security metrics that can be used to evaluate the security of composed systems made of composable components with computed properties, the high latency and outlay in assessing large systems can be expected to endure and limit the ability to perform cross-system comparisons in security.

IV. QUALITIES OF GOOD SECURITY METRICS

Numerous studies have identified a number of qualities that define a good security metric. So as to effectively serve the required purpose, security metrics must conform to a number of principles that make them standard and unambiguous. Different security domains raging from physical security through information security have identified somewhat different characteristics for discernibly good metrics. However, the general standards are similar and are identified in subsequent paragraphs. However, as stated earlier, the term standard should not be understood to imply the same metric procedures for all organizations but rather, they should meet a given set of benchmarks.

Identified and selected metrics must measure and communicate information that is not only relevant but also context specific to the field and environment they are intended for. The metrics must also be meaningful to the target audience in both content and presentation (Jelen, 2000). The essence of security metrics is to portray the value of security in any context to any organization. To achieve this, the metrics must be relevant to the specific context of that organization besides being understandable and meaningful. Therefore, presentation is also as important as ensuring relevance and accuracy as ineffective presentation negates all other qualities of the metrics.

The value of metrics should be within the value of their costs. Required measures should be attainable easily enough, such that any potential inefficiencies in data collection does not lead to pulling of resources meant for subsequent steps in the measurement process or from other functions of the corporation (Jelen, 2000). The evaluation of a security system or programme is what is expressed in metrics. The evaluation process which includes collection of measurements and analysis should not cost so much so that it eats into other budgetary provisions. The design should be such that the measurements can be collected, analysed and presented cost-effectively enough so as not to interfere with other cost heads. Cost-effectiveness also encourages routine metrics analysis as there are few opportunity costs.

The rate at which targets of measurement change must be considered in determining the frequency and timeliness of measurements so that they are appropriately in conformance. Doing this will ensure that the latency of metrics does not defeat the intended purpose. Achieving this makes it possible for even third parties to track changes informing the metrics outcomes (Chapin, 2005). Often are times the measurement targets change. In designing the metric system, this must be considered so that the measurements are taken whenever such targets change. This will inform whether the effectiveness is maintained or if there are logical changes that can be implemented to improve either the effectiveness or efficiency of the system.

Useful metrics should ideally be objective and sufficiently measurable. This, in essence therefore, means that they must be derived from accurate and consistent numerical values. This ensures that qualitative assessments are avoided as much as possible because more often than not, they will be affected by bias. The obtained metrics must be subsequently analysed and then be expressed unambiguously and using readily understood units of measure (Herrmann, 2007). Where qualitative data must be used, there should be developed guidelines on the evaluation and assigning of levels and values to the assessed states. Training could also play a key role in attaining reliability and consistency in evaluation and placement in an ordinal scale.

Organizations must ensure that formal procedures are put in place to define the measurement of the metrics constituents. This formality, ensures that the metrics can be reproduced consistently by different evaluators under similar circumstances. Obtaining a high degree of reproducibility ensures reliability of the data and the metrics themselves and can be used to inform other organizational stakeholders (Jaquith, 2007). The importance of high reliability of data obtained for security metrics or any other data for that matter cannot be overemphasized and so are the need for measures to ensure reproducibility of data. This ensures that data can be verified by someone using similar procedures.

While some security phenomenon can render themselves for measurement readily, meaning that its inherently easier to collect and quantify, and simplicity and high precision are considered key merits in identifying reliable measures, other data must not be overlooked. It is advisable to use statistical methods to reduce uncertainty surrounding presumably less tangible data rather than eliminating entirely. Complexity in collection of some measurements compared to the ease of others should not be allowed to justify overlooking them. This would cause inaccuracies while simple statistical methods could address the complexities inherent in the measurement collection, analysis and presentation.

Possible practical problems and challenges.

Security metrics implementation is faced by a number of practical challenges, most of which are as a result of the nature of the function itself and others due to the relatively young age of security as a corporate function having developed from the more archaic 'watchman' function of security.

What to Measure. Often are times, security managers are faulted for allegedly presenting information to the senior management that is non-informative to support strategic decision making (Hubbard, 2007). This is mostly as a result of a widely recognized security management concern of presenting easily measurable and reportable information rather than what is actually meaningful strategically. The complexity of the acquisition of metrics for a function that does not ordinarily lead to a direct increase in profit in absolute terms is sufficiently acknowledged and appreciated in the security circles. This, however, makes it hard to justify investment in the face of sceptics.

For security information to be meaningful and correctly support decision-making it must be put into context and co-related with something else. It is therefore vital that relevant metrics are obtained, and used to demonstrate correlations and trends. These forms of metrics expressed to show trends and correlations enable logical presentation of dynamics involved in the security management. This however, cannot be achieved if the right metrics are not used either because they are complex for other reasons.

How to measure. It is generally desirable that metrics conform to the ideal characteristics postulated in the earlier section. However, in practice, these metrics fall short of the preferred qualities as a result of two easily discernible issues. First, in many organizations, qualitative measures are preferred over other forms of measures and therefore decisions are based on inefficient measurement processes and subjective information. Second, quantitative security metrics obtained are often misapplied or inappropriately put into context minimizing their information potential.

It is generally important to appreciate what different measurements types can be used to address a given issue and not another. For illustration, Boolean value styled metrics can be used to establish presence of controls but they cannot efficiently put across how they are performing. This therefore makes the information uninformative to decision-makers with regard to how they are performing and how they can be improved in that case (Axelrod, 2008). Put differently, some measurements can be used to express the existence of barriers but are not able to tell of their effectiveness. For example, a metric can express the number of access control points in a security system but without having a measure of how may false positives and false negatives are rendered in a given period such information about number of gadgets only is insufficient to support decision-making.

Existence of outliers in measurement data. Some outliers can be obscured even in seemingly statistically sound metrics creating pitfalls. For instance, it is statistically sound to average the performance of a myriad of controls in a given building or college, but in there may lie one that is tragically ineffective but that could be obscured by above average performance of the other controls it is evaluated cumulatively with. This could lead to catastrophic security failures despite the entire system seemingly achieving set performance targets on average (Boyer, 2007).

How to report. Security information reporting is generally afflicted by three major problems. First, when qualitatively obtained security information is presented in numerical form, which most certainly obscures the true level of its assurance as well as its foundation. Secondly, measures tend to be presented in isolation without context or baseline for comparison and therefore fail to show any form of correlation which ultimately results in the value of the information being limited in meaning. Thirdly, oversimplification of lower level measures can turn the information to mere 'traffic lights' making it lose its inherent and desirable qualities (Mimoso, 2009).

In essence, the first two problems highlighted in the preceding paragraph are as result of measurements design and development. To address the two issues, it is imperative that the questions they seek to address as well as the presentation format be developed well in advance and used as template. The third problem arises from security professionals not having established procedures to present lower-level measures rolled into higher-level ones (Bartol, 2008). Security

managers should therefore develop tiered presentation models where the level of detail reduces with increasing levels and technicalities omitted where they are considered other than useful to decision making.

Senior Management Support. Active involvement as well as support of a security management metrics by senior management is very essential. Preconceptions and expectations that are mostly erroneous are more often than not to blame for failed management support. The absence of broadly accepted security metrics mapping into organizational structures models also contributes to this problem. Lack of these models leave security professionals split between presenting to senior management in too technical terms or impairing their metrics through oversimplification (Mimoso, 2009).

To address this challenge, security managers must breakdown their reporting and presentations into tiers such that all details in the lower level are not oversimplified but the higher levels are expressed in business lingo which the senior management are more likely to understand. Care must however be taken not to employ underhand measures to accomplish management support. These include exaggeration of issues and forecasts. Erroneous preconceptions must also be overcome through elaborate detailing of both measures, threats, vulnerabilities and risks that threaten business continuity.

V. MODELS OF SECURITY METRICS

In investment theory, there is one key quantity that concerns business managers and that is the ration of cost to benefit or the output per unit of input in production lines. The main reason of developing security metrics is to express the formal relationship between a security model and the business bottom-line. Security metrics define the input, output and the operational parameters of the security system or investment.

The most commonly used security metric assessment model is one looked at earlier in the paper among the theories known as the Gordon-Loeb model. The model seeks to define a security breach probability function. This model maps the probability of occurrence of a defined loss as a result of a security breach on the monetary value of a security investment. The model further seeks to cap security investment as a given fraction of the expected losses in the case of the corporation's failure to invest in the security (Willemson, 2006). However, there exists anecdotal evidence of criticism of this aspect of the model in a genre of literature on security metrics. Some extensions of the model cite the need to grow optimal investment guidelines for other forms of the breach probability function (Hausken, 2006), endogenize the prospect of a breach (Matsuura, 2008) or comprise timing decisions (Tatsumi, 2009).

All the literature on security metrics agree and it is logical that security metrics exist in a dichotomy regardless of all other measurements criteria. These are the cost of the investment in the security system and the outcome of the investment. In the subsequent paragraphs, this paper will explore two sides of the dichotomy and how their measurements can be improved or better selected to increase accuracy and reliability of information conveyed through the security metrics be it to the management or stake holders of the organization employing security.

A. Calculating Cost of Security

The cost of a security investment is what it takes for a given corporation to attain a given level of security. While security itself is an abstract concept of a latent metric defining the aggregation of protection measures in a given organization. The cost of a security system could be direct or indirect and it could also be an instant cost factored in the books of account of one year or discounted over a given period of time.

The investment in a security system is seemingly the easiest to identify and quantify in monetary terms especially in regard to direct costs. Some corporations may assume the cost as the capital cost of acquisition of a system and its installation while some assume the cost as the life-time cost of the system which includes the capital cost of purchase and installation summed together with the costs of manning staff, maintenance over the course of its useful life and the replacement. The choice of the security system cost assumption depends on the accounting system of the organization. However, it is advisable to use the life-time cost distributed over the life of the system as it gives a more logical picture of the cost.

Some security systems however, depending on environment, business type and the functionality itself may have non-negligible indirect costs. If the indirect costs of the security system are significant and are not factored in the cost, then the metrics derived will be less than accurate and should not be depended upon. Some of the indirect costs of security systems include; latencies caused by incompatibility in the system, additional resources including manpower and storage devices needed to transfer data between security zones, time lost by staff who lose or forget credentials or forget entry codes (B□hme, 2010).

In cases where security enhances confidentiality, some decision makers may make sub-optimal decisions as a result of unavailability of some confidential information that would have informed them better. This could happen because those decision makers lack the required level of clearance to access that information or they are unwilling to fulfil the required procedures to obtain the information. The opportunity costs of such decisions if they are less than optimal entirely on account of the security measures, then they should count as an indirect cost of security. These occurrences may be rare or may go unreported and therefore care must be taken to ensure when such are realized, they are used to predict the probability of similar occurrences.

Other forms of indirect costs exist and may be overlooked in some instances. Costs of litigation with regard to light trespass into neighbouring facilities as well as cameras that may be considered as invading privacy of neighbours. The cost of such litigations, resulting awards by courts or tribunals as well as the costs of adjustment of those fixtures should be charged on the security account as costs.

The cost of security transcends both fixed and variable costs and therefore should be modelled so to ensure accuracy (Bachlechner, 2012). Costs of installation, maintenance and replacement of security systems like CCTV cameras are independent of number of customers served by the business, also costs of installation of barrier bollards and installation of access control to controlled areas and therefore should be treated as fixed costs. However, costs like the wear and tear of movable barriers like bollards and turnstiles as well as cost of distributing security tokens to customers and indirect costs such as delayed business processes are dependent on the number of customers served and are therefore variable costs and should be apportioned as such.

Whenever costs of security are distributed over a number of accounting periods, it is prudent that non-linearities on account of taxes and time-dependent discounting be factored in the models. Security systems are now technology dependent more than most other functions in the business environment and as such obsoleteness of systems occurs often after short periods of time and other significant sources of uncertainties exist in the models. This has been cited by some researchers as the reason time-dependent discounting for distributed costs are not significant enough to warrant complicating security metrics models with the discounting (Brocke, 2007). However, this could lead to significant errors in the models for security systems like barriers that have useful lives of more than five years and considerable installation costs. That coupled with substantial time value of money due to high cost of credit in African countries, high taxation rates and taxation regimes volatility makes it important to factor in the time-dependent discounting and tax non-linearities without regard for complicating the metrics models.

Care must be taken to ensure that all significant costs relating to the security systems are factored in the models. The significance of a cost should not be left to the subjective judgement of a single individual as this could be affected by individual biases. Where assignment of numerical values is required from qualitative data, it is prudent that more than one individual does the assessment and the outcomes subjected to statistical modelling to reduce errors of biases that could be introduced by individual judgements.

B. Benefits of Security

The second bit of the cost to benefit ratio in the investment theory is the positive outcome of the investment, in this case the security level achieved by the investment in a security system. Just like the cost of security, its benefits are in a deterministic state. Benefits of security are even harder to measure compared to the cost, reason being the quality of protection is rarely a scaler quantity but mainly exist in discrete states that must be translated to an ordinal scale (Jaquith, 2007). The translation of the qualitative assessments into ordinal scales are subject to biases in translation. The biases could be psychological, intellectual or as a result of inadequate training and/or experience.

Part of the indirect benefits of a security investment is reduced insurance premiums as a result of the insurers considering improved security as a result of additional investment. In ideal situations, insurance premiums are based on the risk exposure. This therefore means that if an organization insures its assets against vandalism and/or theft and no measures are taken to secure that asset, the premiums will be pretty steep compared to a similar organization under similar security conditions that invest in some form of protection because there is a difference in risk. The asset secured is not necessarily the one being insured in this respect because some thefts and damages maybe be opportunistic or collateral. In this case therefore, the difference in the value of insurance premiums should count towards security metrics.

Reduction in fraudulent claims by customers and employees demanding compensation for workplace injuries because a security system installed in a premise ensures that the organization is playing its role in the duty of care as well as surveillance systems helping prove that those claims are fraudulent, then those are benefits of security. Quantifying such

improvements in monetary terms is only logical and the net positive benefit should be considered in security metrics as a benefit.

Employee productivity and safety can also be assured through some security measures. This reduces time spent away from duty stations making police reports and subsequent follow-ups, time spent in hospitals and elsewhere nursing injuries sustained in such incidences as well as employee turnover costs. Savings made in these areas are benefits of security and should be assessed as so and used in security metrics.

Security outcomes are mostly evaluated through stochastic indicators which make it infinitely hard to precisely predict future trends. The indeterminacy in this respect is as a result of possible attacker behaviours. Examples of metrics in this area include measurement of intrusion detection statistics including false positives (nuisance alarms) and false negatives (undetected intrusions).

1. Annualized Loss Expectancy

In basic terms, the benefit of security investment is to ensure a reduction of losses incurred in the absence of security. In its simplest terms, annualized loss expectancy (ALE) is obtained by multiplying single loss expectancy (SLE) being the average monetary value of a single loss event, the Annual rate of occurrence (ARO) being the number of times security related events cause the organization losses and the Exposure Factor (EF) being the percentage value erosion possible on any asset (Sennewald, 2003). This formula is however, predicated on the assumption that a number of security breaches happen in a given year to give enough data to generate SLE, ARO and the EF, this though, is unlikely.

However, in practice, security breaches happen far more randomly and sometimes rarely but when they do, the effects are catastrophic. When such occurrences are rare or there exists a threat of happening but has never actually happened, then establishing the SLE and or the ARO could turn out to be not only daunting but also impossible. To address this problem, experts could be utilized to generate such figures from knowledge and experience, but this depletes the reliability of the whole process. Other ways have been devised to address this challenge.

The benefit of security is derived by subtracting the loss distribution at a given security level attained after investing in security L_S from the loss distribution at zero investment in security L_0. However, given insecurity related losses are indeterministic since they are in a significant way dependent on the state of the world at any given time and therefore can be considered random, a probability calculus is needed to formally deal with the ambiguity of realized losses under both conditions. Therefore, it is more convenient to use moment statistics.

Moment statistics leads back to the concept of Annualized Loss Expectancy (ALEs) at a given security level attained after a given investment in security management. This is mathematically expressed as; 〖ALE (S)=E(L_S)= ∫_0^∞▒ 〖x.L_S 〗 (x) dx. The mathematical expression determines the expected losses at one given time but in order to establish the benefits of security, the difference between two moments must be determined to establish the expected benefit of security (EBS). "EBS = E(" L_0)-E(L_s)= ∫_0^∞▒ 〖x.(L_0 (x)- L_S (x))dx 〗 .

Bernoulli Loss Assumption. This concept is used to address the challenges of having to deal with continuous loss distribution functions in the absence of real data or defendable assumptions. The Bernoulli's loss assumption seeks to remedy the problem of continuous loss distribution by hypothesizing that the lost distribution function "L" can be reduced to two elements {0,λ}, such that λ>0 is a fixed loss expected when probability P_S= L_S (λ) and probability "1 - " P_S= L_S (λ). Using this, it becomes convenient to set λ=1 and rescale all monetary quantities to the unit loss. The setting of λ=1 enables a security manager to turn a loss distribution function into a Bernoulli variable with a single parameter and this simplifies the ALE expression (Loeb, 2002).

C. Return on Security Investment.

After having established the cost of the security investment and the expected benefit thereof, it is prudent to express the outcome in a manner that makes sense to people in business. This therefore means that the outcome be expressed in terms of the investment theory (Rainer, 2008). Aligning the security metrics to the investment theory produces what is termed as return on security investment (ROSI). The mathematical expression for ROSI is

〖ROSI〗_S= (〖ALE〗_S- 〖ALE〗_0-c)/c.

Where; ALE0 = Annualized Loss Expectancy at zero expenditure.

ALES = Annualized Loss Expectancy.

ROSI enables organizational management to compare security investment' efficiency regardless of the absolute scale of investment. This also facilitates comparison between heterogenous corporations or divisions. It is important to note ROSI cannot be outlined where the management makes the rational decision to refrain from investing in security. This could be because to them the risk is acceptable as is or it makes more sense being transferred through insurance.

Looking at ROSI alone could mislead someone on some occasions. In instances where very cheap measures are instituted and they mitigate risk to some extent, if compared to more expensive and definitely more comprehensive measures, the cheaper one's ROSI seems more attractive. This is because ROSI has no way of factoring in very substantial risk that may remain unmitigated by the cheap measures. The weaknesses in the cheaper system can be exploited at some time, with ease and to the detriment of the organization. It is therefore imperative that ROSI as an analytical tool be employed in context and by professionals who would be better placed to put it in the right context in view of what may turn out to be unmitigated vulnerabilities.

D. Where to Invest.

This section seeks to explore how a security manager may choose to invest a security budget optimally after it has been assigned rather than justifying security budget against non-security votes in the entire corporation. At times, when the security manager receives their allocation where such money is spent is based on gut feelings (Baryshnikov, 2012). However, it is recommendable that even such decisions be based on quantitative analysis through a model to be postulated here. Unlike in the previous sections, this area is domain specific and therefore does not have a plethora of investment models by business scholars and those in the accounting fields alike. Nevertheless, the optimal filter configuration approaches will be reviewed.

Optimal Filter Configuration

Informed decisions are aggregations of observed corporeality quantized to a discrete indicator regardless of whether they are made by humans or algorithms. Security elements like detection systems are forms of filters defined by binary classifiers. The binary classifications are determined by learned rules or heuristics to approximate decisions. Contrariwise, these decisions are anything but perfect. The imperfection poses a practical problem that can be exploited for an economic trade-off. This approach seeks to strike a balance between losses as a result of false negatives and the cost of false positives to enable a security manager determine the most efficient way of utilizing his security budget.

Assuming a is the loss to the business due to false positives by a given security filter system and b is the direct loss attributable to false negative in addition to future clean-up and lost business and that the cost of installing that given filter system be it an antivirus or access control is fixed and sunk. Then the below formula can be used to optimize outcomes and minimize the cost of decision errors.

$\beta(\alpha) = -(1-p)/p \cdot a/b$

Where: β is the false negative rate as a function of the false positive rate α.

α is the false positive rate.

p is the exogenous probability of access being malicious.

VI. CONCLUSION

Security metrics are very essential in defining security as a corporate function in the modern business environment. The nature of security itself makes it a complicated field for precise and reliable measurements. The challenges of the measurements are well documented and appreciated. However, there are ways in which the challenges can be managed in order to improve the outcomes of the security metrics and aid in decision making within the departments of security and the organizations in general.

A crucial component in eliciting a consequential metric is to aggregate the pertinent information about one's system and to align that metric with quantifiable goals and strategic objectives which rest within the bounds of a certain project or the sphere of a specific organizational structure

Security practitioners must appreciate the need for security metrics and their relevance in the industry. After which, they must acknowledge the challenges therein and their role in managing them. The qualities of good metrics identified are essential in evaluating those identified for relevance and effectiveness.

REFERENCES

[1] Anderson, M. L. (2011). Using Logic Models to Capture Complexity in Systematic Reviews. *Research Synthesis Methods*, 33-42.

[2] Axelrod, C. W. (2008). Accounting for value and uncertainty in security metrics. *Information Systems Control Journal*.

[3] Bachlechner, L. D. (2012). To invest or not to invest? Assessing the economic viability of security investments. *Workshop on Economics and Information Security.* Berli, Germany: WEIS.

[4] Bartol, N. (2008). Practical measurement framework for software assurance and information security. *Software Assurance Measurement Working Group.* Chicago: Bulding Security in th US.

[5] Baryshnikov, Y. (2012). IT security investment and Gordon{Loeb's 1=e rule. *Workshop on the Economics of Information Security.* Berlin, Germany: WEIS.

[6] Bellovin, S. (2006). On the Brittleness of Software and the Infeasibility of Security Metrics. *IEEE Security and Privacy*, Vol 4.

[7] B□hme, R. (2010). Security Metrics and. *International Computer Science Institute Journal*.

[8] Boyer, W. a. (2007). Ideal based cyber security technical metrics for control systems. *The Second International Workshop on Critical Information Infrastructures Security.* Malaga: CRITIS 2007.

[9] Brocke, J. G. (2007). Return on security investments. *Towards a methodological foundation of measurement systems.* Chicago, IL: Proc. of AMCIS.

[10] Chapin, D. A. (2005). How can security be measured? *Systems Control Journal*, 2-14.

[11] Emrah, Y. a. (2015). Requirements for IT Security Metrics- an Argumentation Theory Based Approach. *Association for Information Systems*, 5-29.

[12] Giuseppe, D. M. (2017). Big Data e Privacy by design. *Giappichelli*, 21-78.

[13] Gordon, L. a. (2016). Investing in Cybersecurity: Insights from Gordon Loeb Model. *Journal of Information Security*, 49-59.

[14] Hausken, K. (2006). Returns to information security investment: The effect of alternative information breach functions on optimal investment and sensitivity to vulnerability. *Information Systems Frontiers*, 338{349.

[15] Henning, R. (2001). Security Metrics. *Workshop on Information Security System Scoring and Ranking.* Williamsburg, Virginia: Applied Computer Security Associates.

[16] Herrmann, D. S. (2007). *Complete guide to security and privacy metrics: Measuring regulatory compliance, operational resilience, and ROI.* Boca Raton, FL: Auerbach Publications.

[17] Hubbard, D. W. (2007). *How to measure anything: Finding the value of "intangibles" in business.* Hoboken, NJ: John Wiley & Sons.

[18] Jaquith, A. (2007). *Security metrics: Replacing fear, uncertainty, and doubt.* Upper Saddle River, NJ: Addison-Wesley.

[19] Jelen, G. (2000). In National Institute of Standards and Technology and Computer System Security and Privacy Advisory Board Workshop. *SSE-CMM Security Metrics.* washington D C.

[20] Loeb, L. A. (2002). The economics of information security. *ACM Transactions on Information and System Security*, 438-457.

[21] Matsuura, K. (2008). Productivity space of information security in an extension of the Gordon-Loebs investment model. *Workshop on the Economics of Information.* Hanover, NH: Tuck School of Business, Dartmouth College.

[22] Microsoft Corporation. (2007, November 19). *Microsoft Windows Server 2003, XP Professional and XP Embedded Security Target, Version 3.0, Science Applications International Corporation, Common Criteria Testing Laboratory*. Retrieved from http://www.commoncriteriaportal.org/files/epfiles/20080303_st_vid10184-st.pdf

[23] Mimoso, M. S. (2009). Number-driven risk metrics-fundamentally broken. *Information Security Magazine*.

[24] Payne, S. C. (2006). A guide to security metrics. *SANS Institute*.

[25] Rainer, B. T. (2008). Economic security metrics. *Dependability Metrics*, 176{187.

[26] Sennewald, C. (2003). *Effective Security Management.* New York: Butterworth-Heinneman.

[27] Taquechel, E. F. (2018). Risk-Based Performance Metrics for Critical Infrastructure Protection? A Framework for Research and Analysis. *Homeland Security Affairs 14*, 1-36.

[28] Tatsumi, K. G. (2009). Optimal timing of information security investment: A real options approach. *Workshop on the Economics of Information Security (WEIS).* London, UK: University College London.

[29] Torgerson, M. (2007). Security Metrics. *12th International Command and Control Research and Technology Symposium.* Newport, Rhode Island: 12th International Command and Control Research and Technology Symposium.

[30] Willemson, J. (2006). On the Gordon & Loeb model for information security investment. *Workshop on the Economics of Information Security (WEIS).* Cambridge, UK: University of Cambridge.