INFORMATION TECHNOLOGY SECURITY METRICS

CHARLES OCHIENG' OGUK
coguk@rongovarsity.ac.ke, ogukcharles@gmail.com.
RONGO UNIVERSITY

ABSTRACT

It is a common management principle that one can only manage and improve what one can measure. Studies indicate that information technology security management could be improved if appropriate security metrics which are based on elements of information technology security are used. The objectives of this study were: to identify the major elements of information technology security, and to develop suitable information technology security metric's model based on major elements for universities in Kenya. Methodology involved a review of secondary publications to ascertain the major information technology security. Ten percent of universities in Kenya were sampled for data collection. Purposive sampling was conducted for data collection using questionnaire and an interview schedule. In each sampled university, 13 operation areas related to information systems were considered, giving a total of 91 resepondents. Data was collected from the team leader of each operation area, then analysed using SPSS, where regression model in Tobin's Q equation was adopted. The regression analysis helped to generate coefficients that constituted security metrics' model and prototype. In conclusion, while the level of implementation of IT security elements was found to contribute to the metrics, information security policy was found to contributes as twice. Therefore, it is recommended that the developed IT security metrics model should be used together with the security policy for better information systems security management.

Keywords: IT security metrics, IT security elements, metrics models, metrics dashboard, merics algorithms, goal question metrics and security mesaurement scaling.

INTRODUCTION

Background to the study

For improved management of information systems' security, Jonsson and Pirzadeh (2011) posited that there is need to incorporate elements of IT security in determination of security status in an organization. Sekeres and Bevans (2016) studied the information technology security breaches in the university based in California and the possible factors which could have contributed to the reported breaching of the information systems' security. Along the elements of IT security, the study noted that flat computer network, with little segmentations and inadequate firewall configurations was associated with vulnerabilities that made the attack successful. The information systems' security lapse was attributed to the ease of attack on the systems. Since the

technical staff admitted lack of user-groups, segmentations and required levels of firewall configuration, adoption of check points for security status was recommended to provide proactive approach to security management, (Bevans 2016). In the study, information security metrics emerged as a required approach for better and proactive information security management.

Stojmenovic and Wen (2014) noted that systems attack for a university based in North Dakota could have easily been reduced if basic level information security metrics systems were in place to alert the systems administrators of areas associated with vulnerabilities. The study asserted that since university information security coverers wide areas with multiple elements, use of information technology security metrics to give a close picture of information technology status related to the major elements could be an asset for information technology security management.

According to Gritzalis, Kandias, Stavrou and Mitrou (2014), information systems for some universities in Texas were victims of malicious systems attack that compromised the security of critical databases for students and administration. The study reaffirmed that in most cases of breaches of information systems' security, the colleges' administrations admitted that the situation could have been avoided through basic assessment of information security vulnerabilities and security status checks prior to the attack. It is against this backlash of proactive information security management that poses emphasis on the need for information technology security metrics, based on network security and access control, as a tool for better management of information technology security within universities.
Even though the use of passwords had been adopted for controlling access to information systems in universities in the United Kingdom, Howe (2015) noted that administrators could not make early detection of a possibility of students using administrators' password to gain unauthorized access and manipulate examination databases. Since the security levels of databases bearing examination files were not clear, the study explained that improvements made through investing on data security could not be quantified either. This highlights the requirement of security metrics related to data security for better management of data security in universities.

Further, in South Africa, Jaffer, Ng'ambi and Czerniewicz (2007) elucidated that since weak information security practices, low levels of implementing physical security controls around IT facilities, inadequate data security provision, non-implemented information security policies, little network security and uncontrolled access to the university systems are attributed to information systems' security breaches, ways of measuring security status along the highlighted areas ought to be adopted to make security management in universities easier.

Analyzing security breaches for computerized systems in Nigerian universities, Nweze (2010) pin pointed inadequate adoption and implementation of IT security policies, lack of physical barriers, porous network and little data security practices as possible contributing factors to

information security breaches. However, the study highlighted inadequate ways of monitoring information security levels along the mentioned lines of system security and recommended the need for IT security metrics for better management of IT security within the universities.

Weak policies for controlling access to the computer information system, little controlled physical access to computer facilities, unsecure examination databases and risky practices around the use of passwords were associated with systems vulnerabilities within universities in Uganda, (Tibenderana & Ogao 2008). The study suggested adoption of information technology security metrics as a possible effective way to improve information systems' management within the universities. It's arguable that such metrics allow proactive monitoring and detection of vulnerabilities along the major elements of IT security, that if strengthened would timely reduce the vulnerabilities, could make IT security management more effective.

In Kenya, Mang'ira and Kitoi (2011) attributed loss of physical computer devices, vandalism, and theft and fiber optics line cuts to inadequate IT security metrics that show the levels of physical security implementation in universities in Kenya. It argued that while availability of inventories, signage that identifies critical computer assets and areas traversed by data lines within the university is necessary, a status indicator approach relating the required number of signage and other physical security practices against the available number already installed, is necessary for managing IT security within the universities. In support of this view, Okibo and Ochiche (2014) indicated that for access control to information systems in universities in Kenya, standard elements of access control should be established, and then compared with the already existing access control mechanisms, to help establish information security status within the universities. This comparison not only gives picture of the levels of implementation of the security interventions for information systems, but also portrays the additional efforts that need to be undertaken to improve IT security. Ndung'u (2015) study on enterprise resource management - ERP, revealed that ERP associated systems security challenges within universities in Kenya could be attributed to lack of security monitoring tools as part of information systems security management.

While the foregoing studies independently stressed the need for security metrics along the given elements of IT security, the studies converge to the point that there are significant benefits for using IT security metrics, as it helps in proactive interventions for improving IT security management within universities

Statement of the Problem

The application of suitable metrics that highlight IT security status will improve management of IT security within universities in Kenya, (Bichanga & Obara 2014). Stojmenovic and Wen (2014) found that IT security metrics derived from major elements of IT security has statistically significant relationship with effective management of IT security.

On the contrary, the most of the current IT security metrics used in universities in Kenya are not based on major elements of IT security; hence they could be unreliable, Mang'ira and Kitoi (2011). While proactive management of IT security is recommended, if the use of unreliable IT security metrics is not addressed; confidentiality, integrity and availability (CIA) of information asset may continue to be compromised within the universities in Kenya.

Objectives

i. to identify the major elements of information technology security,
ii. to develop suitable information technology security metric's model based on major elements for universities in Kenya.

Significance of the study

A research on information technology security metrics approach based on major IT security elements, had not received much academic focus within the universities in Kenya, despite several studies' affirmation of positive relationship between the metrics and effective management of IT security. Since measurement and management go hand in hand, the developed model will provide a platform for continuous security monitoring that facilitates proactive management of IT security within the universities.

Scope

The research was conducted to identify the application of major elements of IT security in managing IT security within universities in Kenya and apply the elements in developing a suitable IT security metrics' model. Statistical analysis mainly regression was employed and the resultant metrics' model presented in an online hosted dash-board with color codes indicating different status of the universities' IT security. The research was conducted between August 2016 and September 2017.

Assumption of the study

The researcher went into this study with an assumption that all universities in Kenya have attained appreciable levels of computerization, that the networked computerized systems are currently used for academics and administrative functions, and that the dependence on computerized systems within universities will continue even in future. This was a suitable environment for this kind of study. Indeed, the research found that all the universities had adopted appreciable levels of computerization in their operations, which made the research feasible.

LITERATURE REVIEW

Information systems security estimation in Universities

In attempts to determine information technology security status, most approaches that have been adopted in different universities in Kenya reflect dispersion from the expectation. The expectation, according to Jonsson and Pirzadeh (2011), requires the application of performance levels of the elements of IT security towards formulating credible IT security metrics. Kitheka (2013) noted that some universities in Kenya rely on the users' personal feelings, not based on any element of IT security, to gauge the security status of their information systems. Other institutions gauge IT security status through the number of onslaughts, the number and types of security tools and appliances deployed as the only way of determining Information Technology security levels in the university. The study showed that some universities do not apply any approach to establish their IT security levels.

These approaches could be a wide digression from IT security metrics' expectation. Jonsson and Pirzadeh (2011) demonstrated the need to incorporate elements of IT security in determination of security status in an organization. In view of the foregoing studies, this research assessed the use of major elements of information systems' security in universities in Kenya, and applied associated statistical approaches in developing an information technology security model which is based on security elements of information technology. This approach could provide the required means of gauging IT security metrics within universities in Kenya to facilitate better management of IT security.

In Kenya, Kitheka (2013) criticized the current reliance on personal feelings to estimate IT security status within universities, and recommended the use of approaches based on IT security elements as suitable. Ndung'u (2015) revealed that the daily ERP systems security attacks within universities in Kenya could be attributed to lack of security monitoring tools, and pointed to suitable metrics as a necessary part of effective information systems security management. Mang'ira and Kitoi (2011) attributed loss of physical computer devices, vandalism, and theft and fiber optics line cuts to inadequate IT security metrics in universities in Kenya. Due to lack of adequate management visibility for IT security management programs, some executives get reluctant to invest further in the programs, as the returns on IT security investments cannot be easily determined. The IT security model developed may help in continuous IT security monitoring that facilitates management visibility. The model has provision for every major IT security element and this approach may assist universities' managements to review returns associated with investment on specific elements of IT security, thus facilitating confident investment on IT security, among the executives.

Building Information Technology Security Metrics

While everything can be measured with certainty, for the measurement to be comprehensive, one should be limited to a few key areas at a time and use a methodical approach that's more likely to yield required measurements of state, (Veseli, 2011)). To effectively determine the information technology security status within the universities, Peláez, (2010) suggests that an in-depth analysis on IT security elements should be conducted, and the key IT security elements should be used to derive security metrics associated with information technology. The metrics can help determine the prevailing security situation in a university. This approach is supported as a reliable means for creating a metrics' model for information technology security, (Mitnick & Simon, 2011). This indicates that the first step to developing IT security metrics' model is the identification of major elements of IT security, then collecting data related to the performance of these elements in the given institution, and finally applying necessary statistical methodologies to create the metrics' model.

The Elements of information technology security

There are many information technology security elements, but which fall under broad areas of technology, processes and people. According to Casey (2011), information security elements emanating from the three broad categories of; technology, processes and people could be classified further into major and minor IT security elements. The study agreed with a review of Martins, Eloff and Park (2001) which showed the major elements of IT to include: security policies, physical security, network security, data security, and access control. Since the elements are highly useful contributors to IT security status, they should be explored further for IT security metrics within universities.

This study, therefore, has analyzed information on the levels of implementation of the elements of information technology security within the universities, to come up with a model for information technology security. According to Makori (2013), implementation of IT security along the major elements of information technology security directly facilitates secure operations for the universities' academic and administrative functions, which rely on automated information systems. On this note, Veseli (2011) demonstrated that the effective management of IT security appliances at the elementary levels helped executives in improving information systems security as well as quantifying returns on IT security investment among Norwegian University. From the foregoing studies, the major elements of IT security include: security policy, physical security, network security, data security and access control. Jonsson and Pirzadeh (2011) argued that since performance and implementation levels of the major elements determine the IT security levels, there could be a relationship between the elements and IT security status of a given entity. Similarly, Ismail and Zainab (2011) demonstrated a direct relationship between elements of data security and the status of IT security within Australian libraries.

IT security metric's Color - Codes Scheme

Thomas *et al*. (2015) asserted that there's no better self communicating metaphor for creating the awareness state of mind than by the use color code scheme. Many information systems end up in bad situations since majority of those in charge do not see the danger or threat in advance before it becomes a serious problem (MacLean, 2012). This calls for the need for easily observed techniques to assist in constantly assessing information systems security situation. Information systems security situational awareness is the ability to scan the systems environment and sense security challenges and opportunities, with minimal interference caused to the normal operation of the system (Furnell, Bryant & Phippen 2007).

Color codes of IT security situation awareness could provide a clear and easy to understand explanation on the prevailing IT security situation in an organization. The concept of color code for evaluating security situation awareness was first developed by Jeff Cooper during the Second World War. Colonel Jeff Cooper's security situation analysis and demonstration using color codes was successfully applied to create an awareness system that associated levels of security risks to specific colors, (Angelini & Santucci 2015). According to Lenders, Tanner and Blarer (2015), by understanding how data collected from the IT security elements can be processed to indicate levels of danger; a color code system can be formulated to communicate the evaluated security situation in an organization.

Color codes scheme has been successfully applied in the field of information technology to show the levels security status and implementation levels of the elements of IT security. Angelini and Santucci (2015) demonstrated that a visual cyber situational awareness creates proper proactive security management technique for critical systems' infrastructures. It argued that cyber management space security for an organization could be improved when color codes are used to show the security status of the systems at any given time. Lenders, Tanner and Blarer (2015) supported this argument through further demonstrating gaining an edge in cyberspace security management through the application of an advanced situational awareness color-code scheme.

Similarly, Thomas *et al*. (2015) showed that there could be substantive reduction in access control vulnerabilities through the use of interactive color code annotations that provide earlier warnings to IT security experts. Furnell, Bryant and Phippen (2007) assessed the IT security perceptions of personal internet users and concluded that the majority would feel safer when browsing through URLs shaded green.

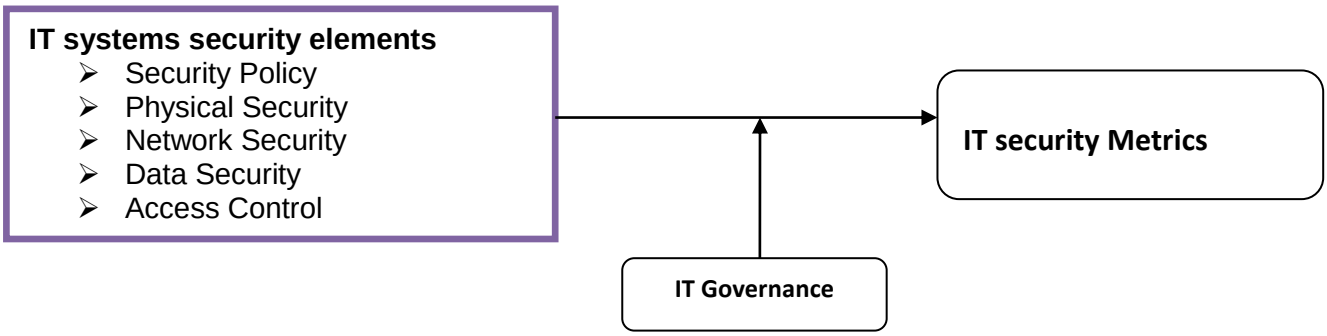
IT Security Metric's Dashboard

ICT staff members make so much IT security observations from their daily operations in different organizations. Some of the observed elements could contribute tremendously in improving ICT security if presented before management for consideration. However, according to Beas and Salanova (2006), most ICT personnel hardly express and present the observations in a manner that the executive can understand and consume towards bettering IT security. This

implies that once the observations related to IT security have been made, they need to be recorded and displayed in a format that the organizations' management and the general stakeholders can understand and consume easily.

In information and communication technology, a dashboard is a graphic user interface that, operates like an automobile's display, which organizes and presents information to the driver about mileage, speed, fuel levels, transmission and other information related to the machine in a way that is easy to read and understand. Dashboards have been applied in a number of fields, including information technology, to help present information more effectively than when using long descriptive narrations. The use of dashboards has helped to establish accountability across various project activities, automate performance reporting processes, provide methodological support based on given pre-defined algorithms, and to enable business consequence modeling for real-time reporting of performance levels, (Haubner & Petermann 1986).

Conceptual framework



The IT securirty Metrics' Model

According to Martins, Eloff, and Park (2001), Mitnick and Simon (2011) & Luambano and Nawe (2004), the implementation and performance levels of IT security elements are directly related to IT security status / metrics. The two features of the elements (implementation and performance levels) were used to quantify IT security metrics within universities. The study used descriptive values of central tendencies mainly the mean, as the average performance of the elements. Regression analysis helped for the relationship between the variables. Respondent's opinions with regards to the elements were quantified using a Likert scale. Regression model in Tobin's Q equation was used as:

$Q_M = \beta_0 + \beta_1 A1 + \beta_2 A2 + \beta_3 A3 + \beta_4 A4 + \beta_5 A5$: Tobin's equation.
$Q_M = \beta_0 + \beta_1 SP + \beta_2 PS + \beta_3 NS + \beta_4 DS + \beta_5 AC$ conceptualized equation
Whereby β_1, β_2, β_3 and β_4 and β_5 are Tobin's coefficients for the dependent variables while β_0 is Tobin's constant for the model.

Q_M = Tobin's Q for IT security metrics as the dependent unit. In this particular case, the independent variables are: SP = IT Security Policy. PS = Physical Security, NS = Network Security, DS - Data Security and AC=Access Control. Coefficients of the independent variables in the model above weree obtained through regression analysis of data in Statistical Package for Social Sciences (SPSS version 20.0).

RESEARCH METHODOLOGY

Secondary publications were reviewed to ascertain the major information technology security elements and questionnaire based survey conducted to seek the extent of application of the elements within the universities. Ten percent of the universities was sampled randomly and further, purposive sampling was employed for data collection targeting IT personnel only. Data was analysed using SPSS, where the mean scores for the various elements' contents were calculated and expressed as percentage. The approach employed for ascertaining the major IT security elements considered in the management of IT security was the adoption of well designed questionnaire. The target population for this research was 910 respondents resulting from the seventy (70) universities in Kenya according to CUE in the year 2015; Mukhwana, Kande and Too (2017). Team leaders of various categories of information system users and IT administrators formed the target for data collection.

For the purposes of this study, ten percent (of 910 respondent from the 70 universities = 91 respondents) was sampled. The reliance on sample size equivallent to ten percent of a population to provide fair base for analysis is supported by (Mugenda & Mugenda, 1999); (Rubin & Babbie 2012) & (Kothari 2003). The 7 universities sample was constituted by samples under public and private university categories. Further, purposive sampling was used to obtain response from employees . Since not every staff member in the entire university work force deals with information systems whose work involved information systems. Consequntly, users and administrators of IT systems were considered to be richer in information needed for the study, especially, in IT security experience and data desired by the researcher.

The IT Security Metrics' Model development

From the above review, regression analysis model in Tobin's Q equation was conducted to relate the IT security elements and the metrics as:

$Q_M = \beta_0 + \beta_1 SP + \beta_2 PS + \beta_3 NS + \beta_4 DS + \beta_5 AC + E$: Tobin's equation, according to Villalonga (2004), whereby β_1, β_2, β_3 and β_4 and β_5 are Tobin's coefficients for the dependent variables while β_0 is Tobin's constant for the model.
Q_M = Tobin's Q for IT security metrics' scale as the dependent unit. In this particular case, the independent variables are: SP = IT Security Policy. PS = Physical Security, NS = Network Security, DS - Data Security and AC=Access Control. Coefficients of the independent variables in the model above were obtained through regression analysis of data in Statistical Package for Social Sciences (SPSS version 20.0) and the resultant equation became the algorithm used.

Algorithm for implementation the IT Security model

The programming languages used were: Hyper Text Markup Language (HTML), Cascading Style Sheets (CSS), JavaScript and Hypertext Preprocessor (PHP). The applications were applied on the Chart and graph codes download as the major sourceFor every element, the percentage score is also shown on a graph which is color-coded to help the user know in which zone they are in relation to the security element as the key below. However, contributions of every element to the overall IT security metrics are conducted according to the algorithms' model:

$Q_M = 1.9 + 1.6\ SP + 0.8\ PS + 0.8\ NS + 0.8\ DS + 0.8\ AC$

OR

$Q_M = 1.9 + 0.8\ (2\ SP + PS + NS + DS + AC)$

The maximum metric's value equals 6.7, approximated metrically to 7.0, while the lowest metrics' value equals 1.9, approximated metrically to 2.0.

Metrics' presentation in color-code

According to Trethowen, Anslow and Welch (2015), the measurements' outputs should be related to colour codes for better visualization. The idea for better visualization is further supported by (Kruger and Kearney2006). The measuremesnt forn the above metric's model should be categorized into three, depending on the magnitude, and then mapped into corresponding colour codes associated with the different security status as shown below. Red implies severe security status that needs immediate attention, and it takes measurement values from 2.0 - 4.0. Yellow means inseure environment that needs considerarion for improvement and takes values form 4.1 - 6.0, while Green means a safe computing environment that needs to be maintained and taakes values from 6.1 - 7.0 as shown below;

Table 4.32: Metrics' presentation in color-code

2.1	3.1	4.1	5.1	6.1	7.0
Severe security status *(Needs immediate attention)*		Insecure *(needs improvement)*		Safe (Needs maintenance)	

The following were used to achieve different tasks

Hyper Text Markup Language (HTML) was used to make the web-based application. Lebel (2007) showed that the tool is suitable for developing and implementing web-based applications as it was effectively implemented in the U.S. patent application. Cascading Style Sheets (CSS) is another tool that was used to customize the look and feel of the metrics' application. This is supported by Lie and Bos (2005), which demonstrated the effectiveness of Cascading style sheets in designing the web. JavaScript was used to create the chart that enhances visualization. Gesmann and Castillo (2011) showed that visualization can be greatly enhanced using the Google visualization API. Hypertext Preprocessor (PHP) assisted in the creation of sessions, passing values to different pages to the final tally as well as to do calculation on the web pages that gives results. Similarly, Nixon (2012) analysis found that PHP as a programming language is effective for creating dynamic websites.

DATA ANALYSIS AND FINDINGS OF THE STUDY

Table 4.1: Regression analysis of the relationship between IT security elements and Metrics

Model elements	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Standard error	Std. Error		
(Constant)	1.904	0.539		3.533	0.003
IT security policy	1.62	1.84	0.791	0.880	0.023
Physical Security	0.80	0.53	0.391	1.509	0.030
Network Security	0.808	0.879	0.471	0.919	0.035
Data Security	0.796	0.986	0.398	0.807	0.046
Access Control	0.788	0.661	0.325	1.192	0.046

Completing the model by inserting the factors associated with the constant value and other elements for IT security, which are ($\beta_{0=}$ 1.904, β_1 = 1.62, β_2 = 0.80, β_3 = 0.88, β_4 = 0.796 and β_5 = 0.788) with respective p – values less than 0.05, the final equation become;

Q_M = 1.904 + 1.62 SP + 0.800 PS + 0.808 NS + 0.796 DS + 0.788 AC and this defined the mode for IT security metrics.

This model is interpreted as: the coefficients for all the elements of IT security are significant because its p-values are smaller than 0.05. Therefore, for every unit increase in every major IT security element, a significant increase in IT security metrics' value is predicted. Holding all other IT security elements' variables constant, the increase in IT security metrics associated with a unit increase of the element under consideration equals the coefficient value of the element under consideration. As posited by Jonsson and Pirzadeh (2011) & Simon (2011), the model shows that the constant value which could be contributed by other IT security factors that are not considered in this study, as well as all the minor elements of IT security in the model.

The researcher reviewed the metrics' model above and noted that when the coefficient factors are rounded off to one decimal place, the equation becomes;
$Q_M = 1.9 + 1.6\ SP + 0.8\ PS + 0.8\ NS + 0.8\ DS + 0.8\ AC$
Therefore, $Q_M = 1.9 + 0.8\ (2\ SP + PS + NS + DS + AC)$
Thus, this yielded a unique model coefficient ratio of (2: 1) was found in this study. That is, the coefficient associated with IT security policy is twice as any other element in the model. The above model was implemented in computer coding and mounted online through the URL (http://41.89.203.228/oguk).

Program Code for the prototype

```
<html>
<?php
session_start();
$_SESSION['policy'];
$_SESSION['physical'];
$_SESSION['network'];
$_SESSION['access'];
$_SESSION['data'];

$policy=$_SESSION['policy'];
$physical=$_SESSION['physical'];
$network=$_SESSION['network'];
$access=$_SESSION['access'];
$data=$_SESSION['data'];
$q6=(1.9
+((1.6*$policy)/100)+((0.8*$physical)/100)+((0.8*$network)/100)+((0.8*$data)/100)+((0.8*$ac
cess)/100));
?>
<style type="text/css">
<!--
```

```
.style1 {
	font-family: Verdana, Arial, Helvetica, sans-serif;
	font-weight: bold;
}
.style3 {
	font-family: Georgia, "Times New Roman", Times, serif;
	font-weight: bold;
	font-size: 14px;
	color: #006633;
}
-->
</style>

<head>
<title></title>

</head>
<body>

<div style="width:800px;height:800px;-webkit-border-radius: 20px;-moz-border-radius: 20px;border-radius: 20px;background-color:#FFFFFF;-webkit-box-shadow: #76B36F 2px 2px 2px;-moz-box-shadow: #76B36F 2px 2px 2px; box-shadow: #76B36F 2px 2px 2px; margin-right: auto; margin-left: auto; border:1px solid #033803; padding: 20px; ">
 <div align="center">
  <p><span class="style1">Summary of scores per item:</span>
    <!-- Styles -->
   </p>
  <p>
    <style>
#chartdiv {
	width	: 100%;
	height	: 400px;
}

    </style>

    <!-- Resources -->
    <script src="https://www.amcharts.com/lib/3/amcharts.js"></script>
    <script src="https://www.amcharts.com/lib/3/gauge.js"></script>
    <script src="https://www.amcharts.com/lib/3/plugins/export/export.min.js"></script>
```

```
   </p>
 </div>

<!-- Styles -->
<style>
#chartdiv1 {
        width           : 100%;
        height          : 200px;
        font-size       : 11px;
}
</style>

<!-- Resources -->
<script src="https://www.amcharts.com/lib/3/amcharts.js"></script>
<script src="https://www.amcharts.com/lib/3/serial.js"></script>
<script src="https://www.amcharts.com/lib/3/plugins/export/export.min.js"></script>
<link rel="stylesheet" href="https://www.amcharts.com/lib/3/plugins/export/export.css"
type="text/css" media="all" />
<script src="https://www.amcharts.com/lib/3/themes/light.js"></script>

<!-- Chart code -->
<script>
var chart = AmCharts.makeChart( "chartdiv1", {
  "type": "serial",
  "theme": "light",
  "dataProvider": [ {
    "area": "Policy",
    "values": <?php echo $policy; ?>
  }, {
    "area": "Physical",
    "values": <?php echo $physical; ?>
  }, {
    "area": "Network",
    "values": <?php echo $network; ?>
  }, {
    "area": "Access",
    "values": <?php echo $access; ?>
  }, {
    "area": "Data",
    "values": <?php echo $data; ?>
```

```
  },{
   "area": " ",
   "values": 0
  } ],
  "valueAxes": [ {
   "gridColor": "#FFFFFF",
   "gridAlpha": 0.2,
   "dashLength": 0
  } ],
  "gridAboveGraphs": true,
  "startDuration": 1,
  "graphs": [ {
   "balloonText": "[[category]]: <b>[[value]]</b>",
   "fillAlphas": 0.8,
   "lineAlpha": 0.2,
   "type": "column",
   "valueField": "values"
  } ],
  "chartCursor": {
   "categoryBalloonEnabled": false,
   "cursorAlpha": 0,
   "zoomable": false
  },
  "categoryField": "area",
  "categoryAxis": {
   "gridPosition": "start",
   "gridAlpha": 0,
   "tickPosition": "start",
   "tickLength": 20
  },
  "export": {
   "enabled": true
  }

} );
</script>
<table width=100%>
<tr>
<td width="80%">
<!-- HTML -->
```

```
<div id="chartdiv1"></div>
  <link       rel="stylesheet"       href="https://www.amcharts.com/lib/3/plugins/export/export.css"
type="text/css" media="all" />
  <div align="center">
    <p>
      <script src="https://www.amcharts.com/lib/3/themes/light.js"></script>

      <!-- Chart code -->
      <script>
var gaugeChart = AmCharts.makeChart( "chartdiv", {
  "type": "gauge",
  "theme": "light",
  "axes": [ {
    "axisThickness": 2,
    "axisAlpha": 0.2,
    "tickAlpha": 0.2,
    "valueInterval": 0.5,
    "bands": [ {
      "color": "#cc4748",
      "endValue": 4.1,
      "startValue": 1.9
    }, {
      "color": "#fdd400",
      "endValue": 6.1,
      "startValue": 4.1
    }, {
      "color": "#228B22",
      "endValue": 7.1,
      "innerRadius": "95%",
      "startValue": 6.1
    } ],
    "bottomText": "0",
    "bottomTextYOffset": -0.5,
    "endValue": 7.0
  } ],
  "arrows": [ {} ],
  "export": {
    "enabled": true
  }
} );
```

```
setInterval( randomValue, 2000 );

// set random value
function randomValue() {
  var value = <?php echo $q6; ?>;
  if ( gaugeChart ) {
    if ( gaugeChart.arrows ) {
      if ( gaugeChart.arrows[ 0 ] ) {
        if ( gaugeChart.arrows[ 0 ].setValue ) {
          gaugeChart.arrows[ 0 ].setValue( value );
          gaugeChart.axes[ 0 ].setBottomText( value + " " );
        }
      }
    }
  }
}
  </script>

    </p>
    <p><span class="style1">Overal analysis of results </span>
    </p>
  </div>
  <div id="chartdiv"></div>
<p>The score on the overall security is:<span class="style3"> <?php  echo $q6; ?> </span></p>

<p  align="right"><a  href="m.php"><img  src="img/index.jpg"  width="117"  height="37"
></a></p>
</div>
</td>
<td width="20%">
<table>
  <tr>
  <td colspan="2"> KEY</td>
  </tr>
  <tr bgcolor="red">
  <td>1.9-4.0</td>
   <td>Severe security</td>
  </tr>
  <tr bgcolor="yellow">
```

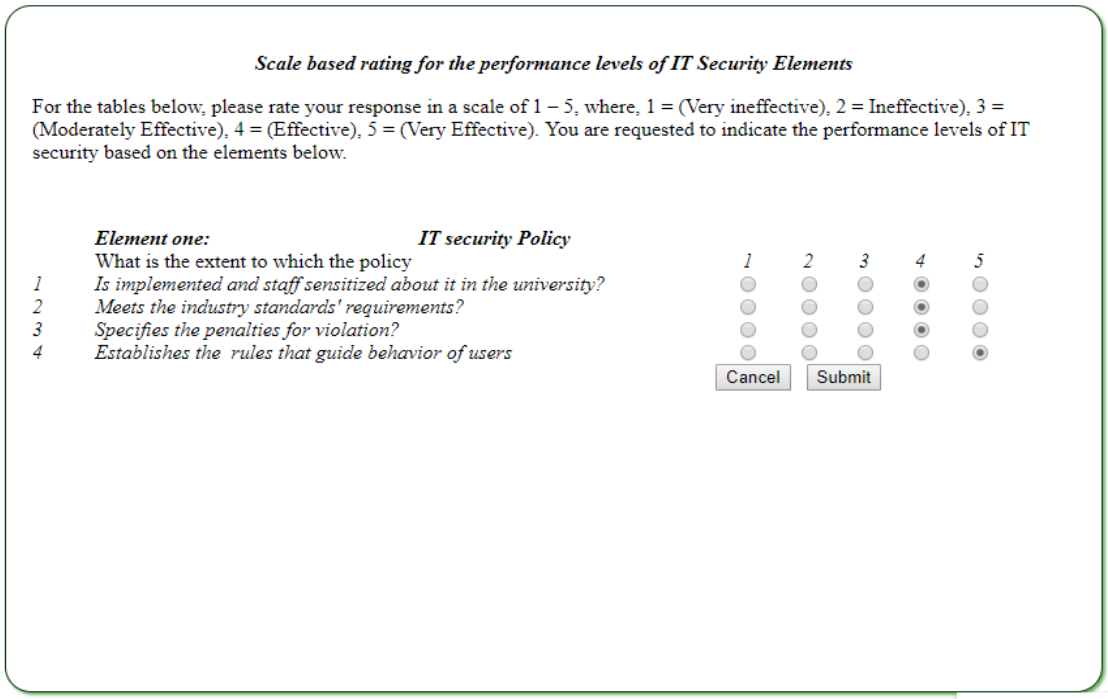
```
 <td>4.1-6.0</td>
  <td >Insecure</td>
 </tr>
 <tr bgcolor="green">
 <td>Above 6.0</td>
  <td>Safe</td>
 </tr>
 </table>
</td>
</tr>
</table>


</body>
</html>
```

The online IT security metrics Model dashboard

When one clicks (http://41.89.203.228/oguk), the dash board appears as shown below, when one clicks on the "start button"

The first element of IT security, (IT security policy) is evaluated as follows and submitted



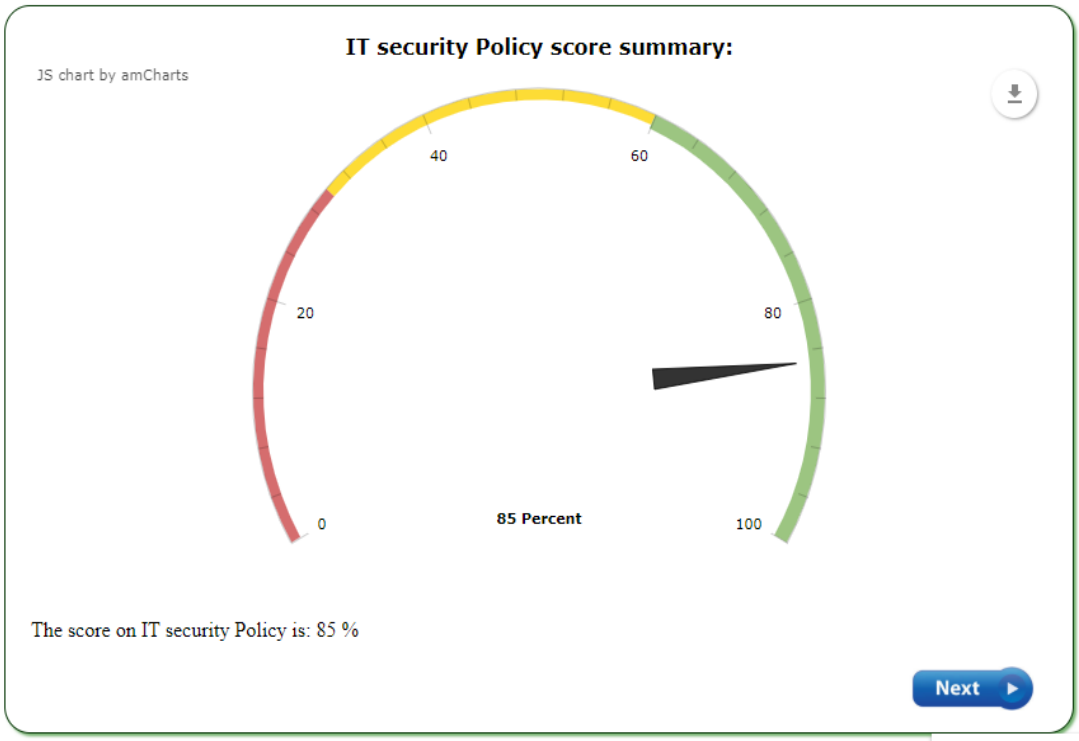
Scale based rating for the performance levels of IT Security Elements

For the tables below, please rate your response in a scale of 1 – 5, where, 1 = (Very ineffective), 2 = Ineffective), 3 = (Moderately Effective), 4 = (Effective), 5 = (Very Effective). You are requested to indicate the performance levels of IT security based on the elements below.

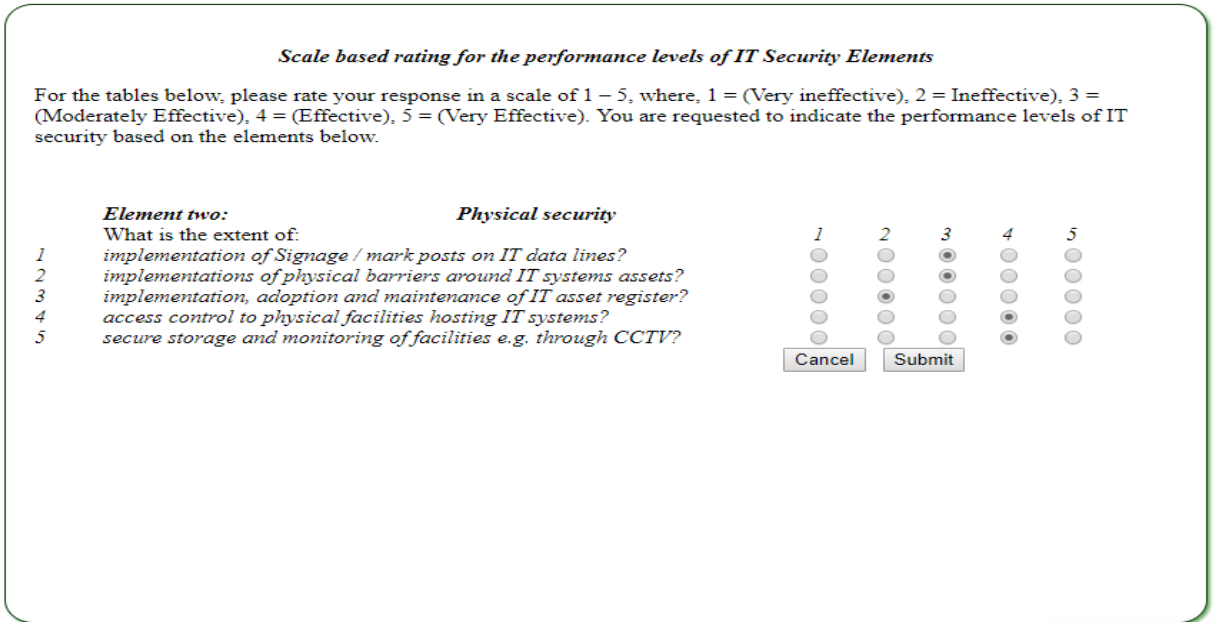
	Element one:	***IT security Policy***				
	What is the extent to which the policy	*1*	*2*	*3*	*4*	*5*
1	*Is implemented and staff sensitized about it in the university?*	○	○	○	◉	○
2	*Meets the industry standards' requirements?*	○	○	○	◉	○
3	*Specifies the penalties for violation?*	○	○	○	◉	○
4	*Establishes the rules that guide behavior of users*	○	○	○	○	◉

Cancel Submit

The dashboard loads after clicking the “submit button”



The second element of IT security, (Physical security) is evaluated as follows



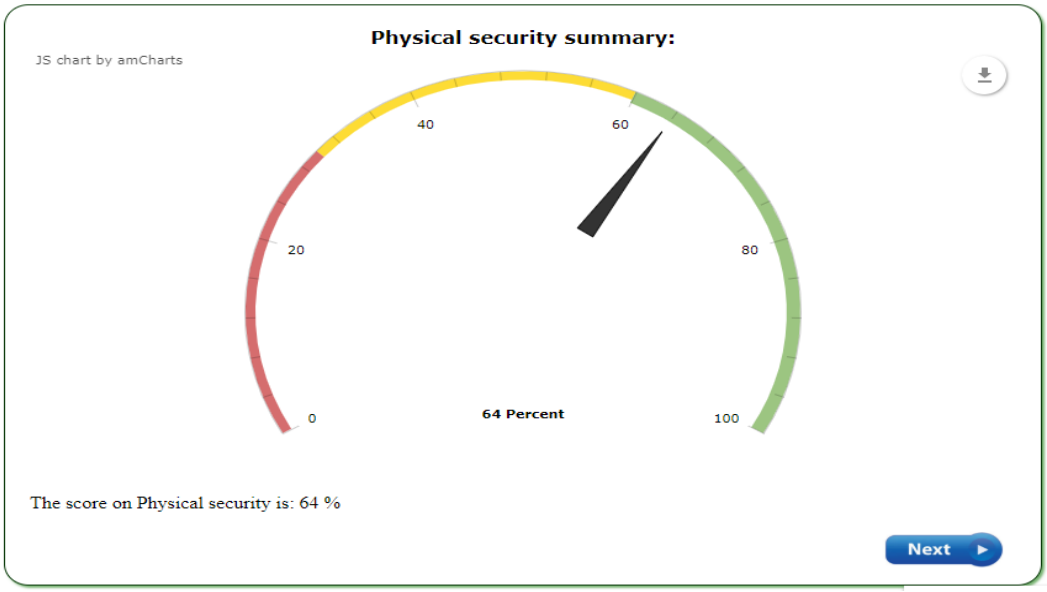
Scale based rating for the performance levels of IT Security Elements

For the tables below, please rate your response in a scale of 1 – 5, where, 1 = (Very ineffective), 2 = Ineffective), 3 = (Moderately Effective), 4 = (Effective), 5 = (Very Effective). You are requested to indicate the performance levels of IT security based on the elements below.

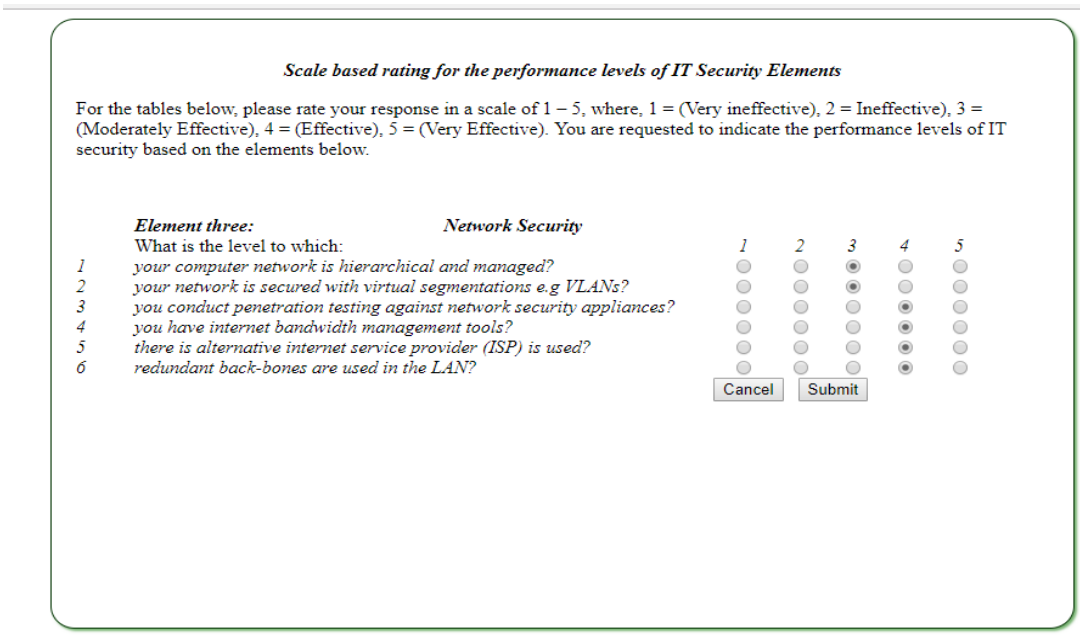
	Element two: What is the extent of:	***Physical security***	1	2	3	4	5
1	*implementation of Signage / mark posts on IT data lines?*		○	○	◉	○	○
2	*implementations of physical barriers around IT systems assets?*		○	○	◉	○	○
3	*implementation, adoption and maintenance of IT asset register?*		○	◉	○	○	○
4	*access control to physical facilities hosting IT systems?*		○	○	○	◉	○
5	*secure storage and monitoring of facilities e.g. through CCTV?*		○	○	○	◉	○

Cancel Submit

The dashboards the loads…..



The thord element of IT security, (network security) is evaluated as follows and submitted



Scale based rating for the performance levels of IT Security Elements

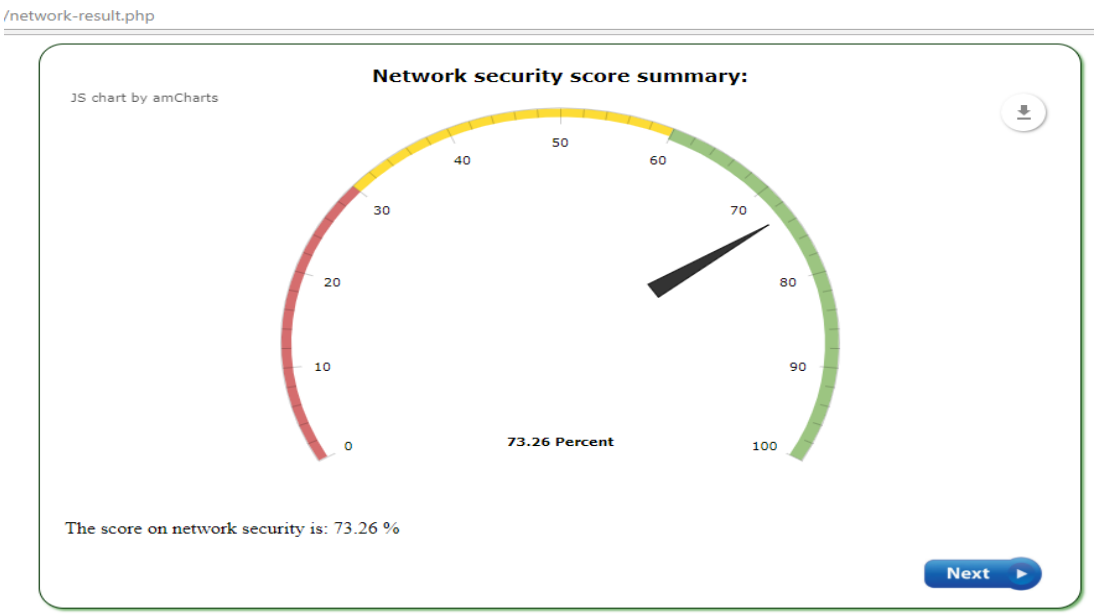
For the tables below, please rate your response in a scale of 1 – 5, where, 1 = (Very ineffective), 2 = Ineffective), 3 = (Moderately Effective), 4 = (Effective), 5 = (Very Effective). You are requested to indicate the performance levels of IT security based on the elements below.

Element three: ***Network Security***

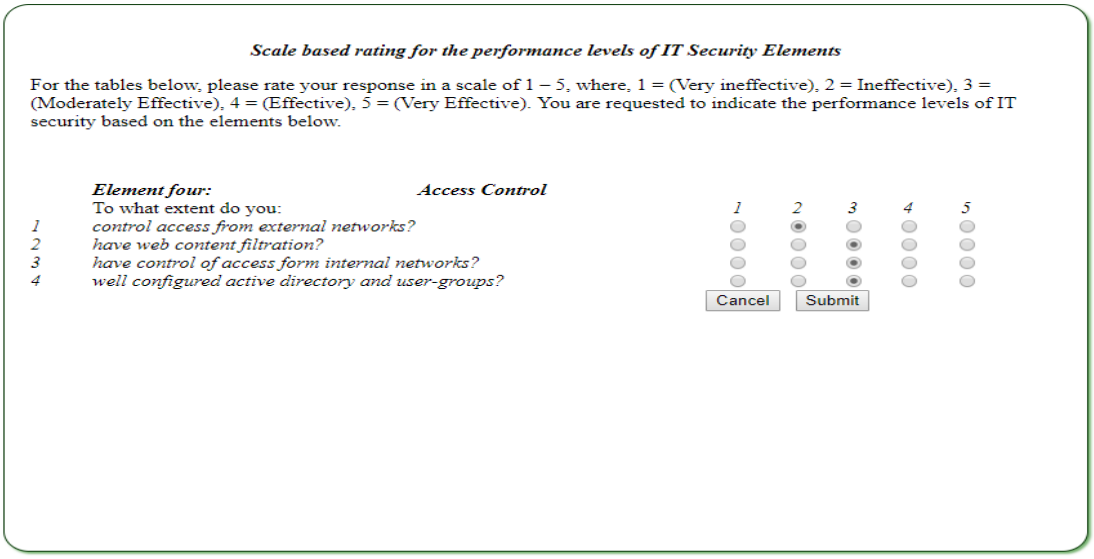
	What is the level to which:	1	2	3	4	5
1	*your computer network is hierarchical and managed?*	○	○	◉	○	○
2	*your network is secured with virtual segmentations e.g VLANs?*	○	○	◉	○	○
3	*you conduct penetration testing against network security appliances?*	○	○	○	◉	○
4	*you have internet bandwidth management tools?*	○	○	○	◉	○
5	*there is alternative internet service provider (ISP) is used?*	○	○	○	◉	○
6	*redundant back-bones are used in the LAN?*	○	○	○	◉	○

Cancel Submit

The dashboard loads…



The forth element of IT security, (access control) is evaluated as follows and submitted



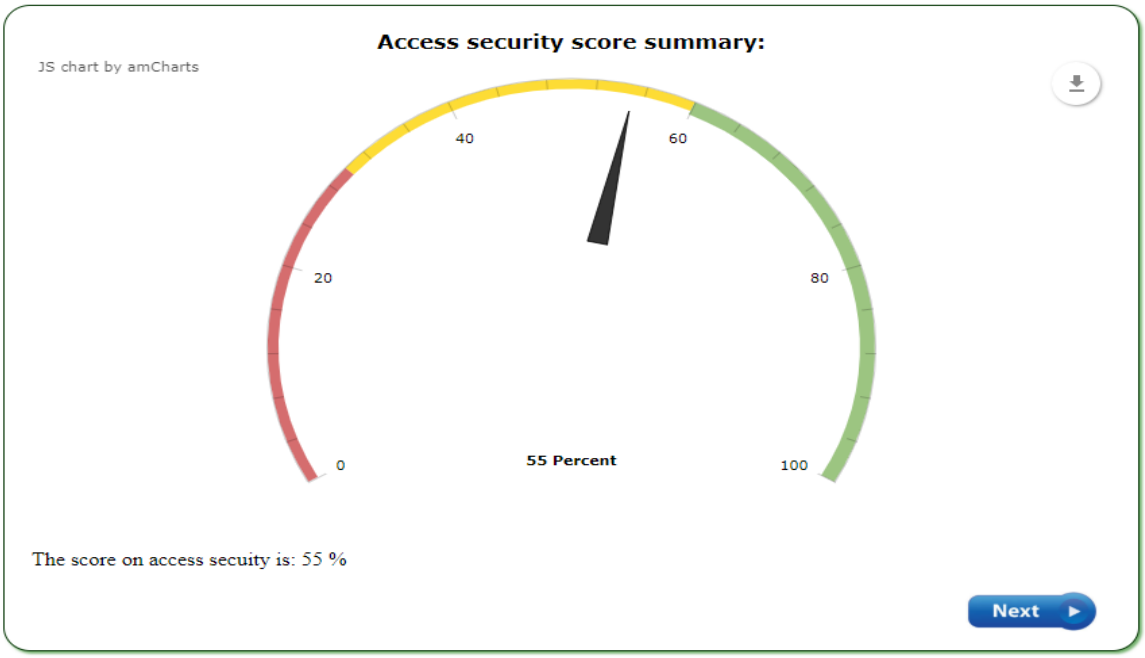
Scale based rating for the performance levels of IT Security Elements

For the tables below, please rate your response in a scale of 1 – 5, where, 1 = (Very ineffective), 2 = Ineffective), 3 = (Moderately Effective), 4 = (Effective), 5 = (Very Effective). You are requested to indicate the performance levels of IT security based on the elements below.

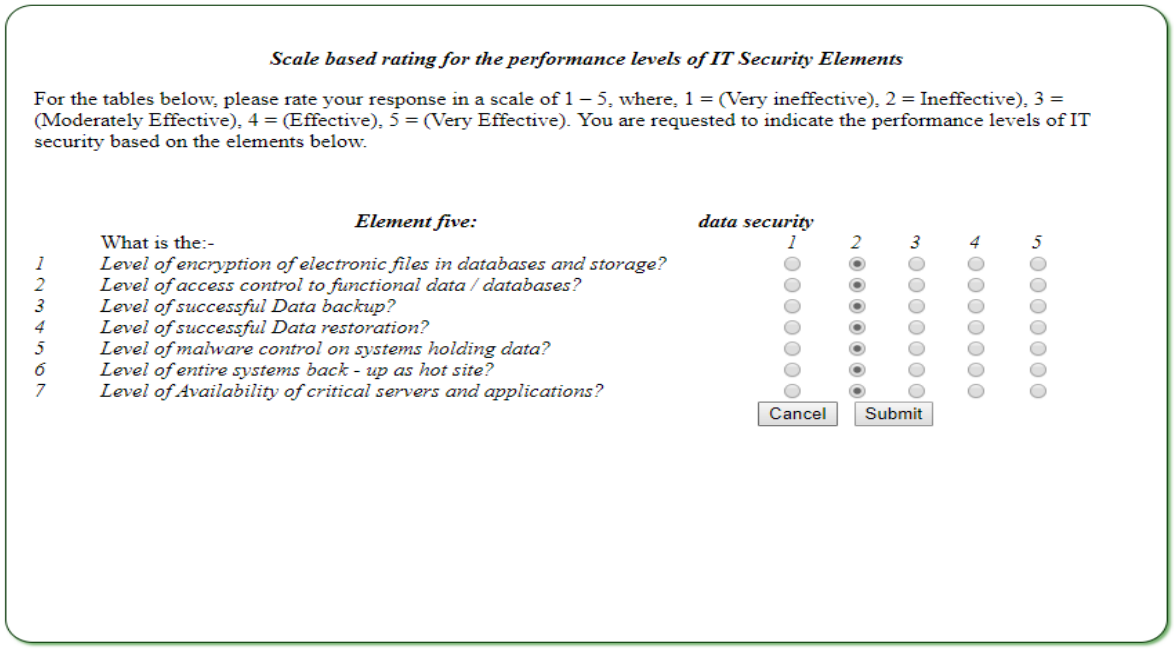
	Element four: ***Access Control*** To what extent do you:	*1*	*2*	*3*	*4*	*5*
1	*control access from external networks?*	○	◉	○	○	○
2	*have web content filtration?*	○	○	◉	○	○
3	*have control of access form internal networks?*	○	○	◉	○	○
4	*well configured active directory and user-groups?*	○	○	◉	○	○

Cancel Submit

The dashboard then loads……..



The fifth element of IT security, (data security) is evaluated as follows and submitted



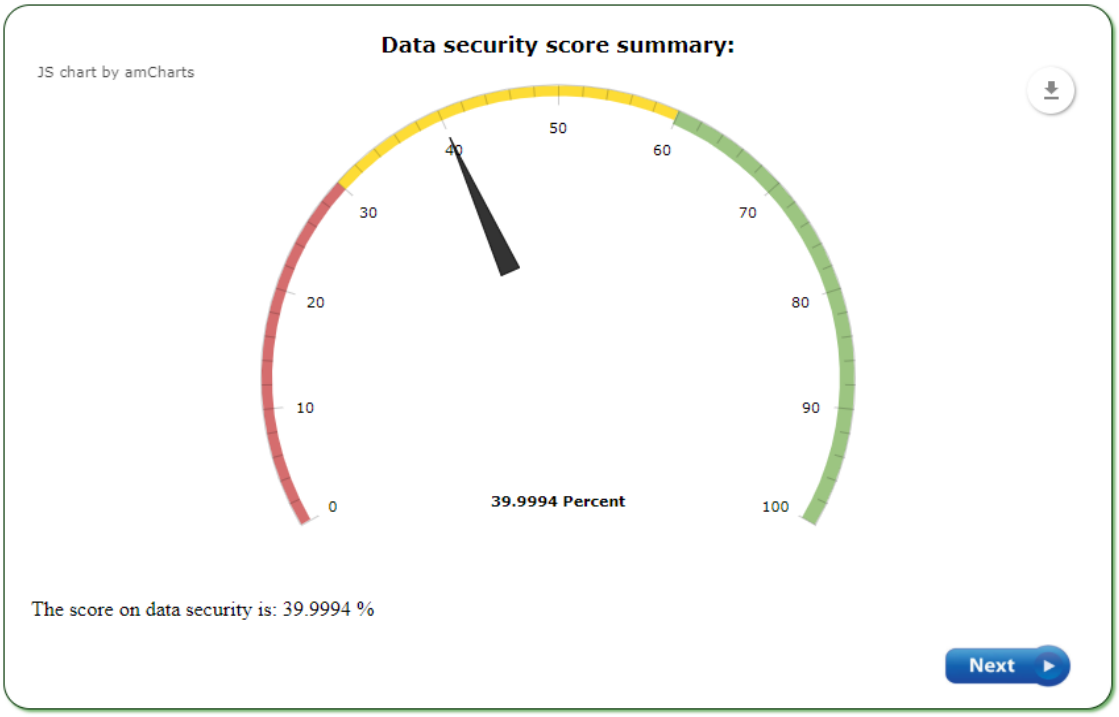
Scale based rating for the performance levels of IT Security Elements

For the tables below, please rate your response in a scale of 1 – 5, where, 1 = (Very ineffective), 2 = Ineffective), 3 = (Moderately Effective), 4 = (Effective), 5 = (Very Effective). You are requested to indicate the performance levels of IT security based on the elements below.

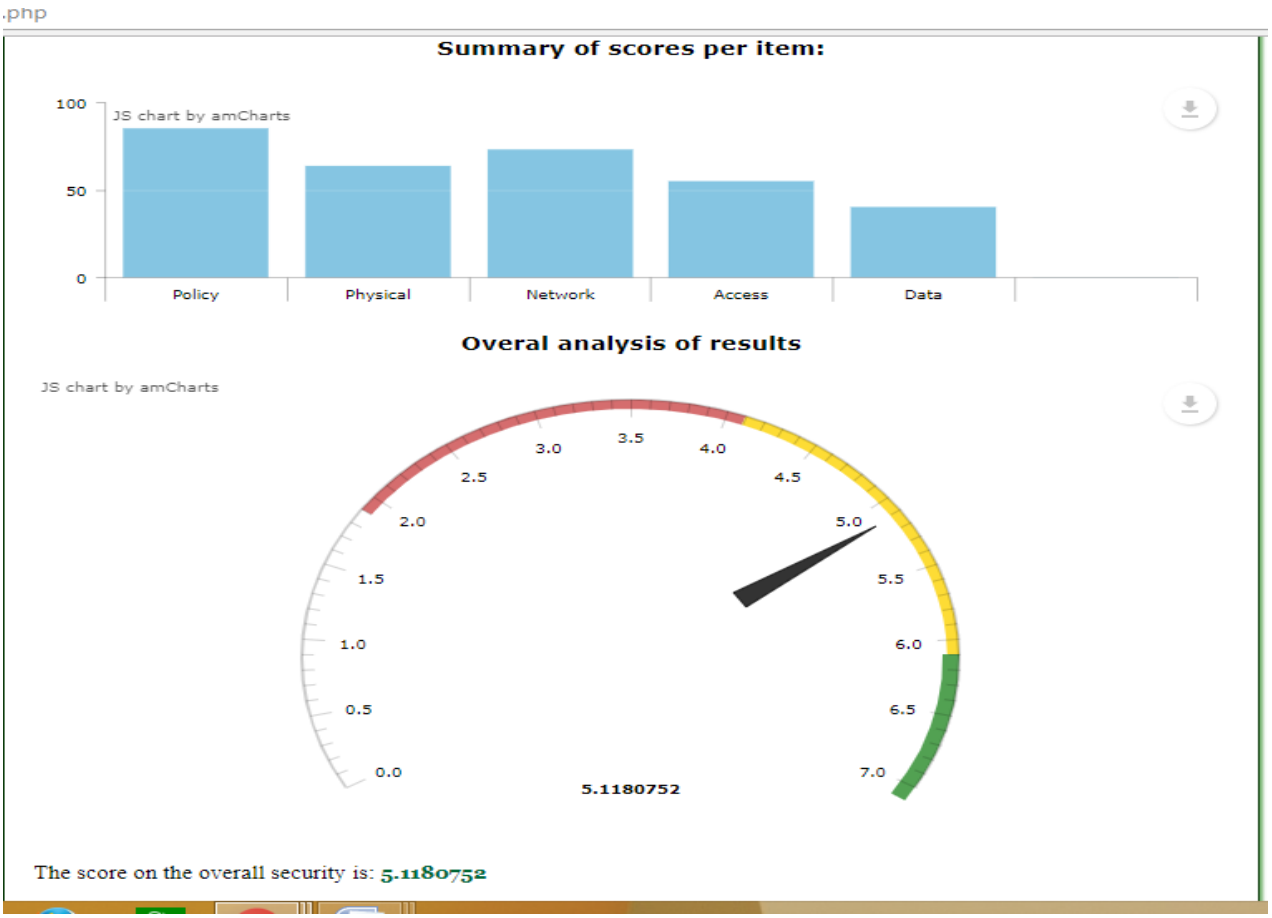
	Element five:	***data security***				
	What is the:-	*1*	*2*	*3*	*4*	*5*
1	*Level of encryption of electronic files in databases and storage?*	○	◉	○	○	○
2	*Level of access control to functional data / databases?*	○	◉	○	○	○
3	*Level of successful Data backup?*	○	◉	○	○	○
4	*Level of successful Data restoration?*	○	◉	○	○	○
5	*Level of malware control on systems holding data?*	○	◉	○	○	○
6	*Level of entire systems back - up as hot site?*	○	◉	○	○	○
7	*Level of Availability of critical servers and applications?*	○	◉	○	○	○

Cancel Submit

The dashboard then loads……..



The overall assessment result for the IT security loads. This summarizes the implementation levels and thus measure the status of IT security based on the scores for all the elements in a given university. The overall metrics' value must fall between 1.9 (min) and 6.7 (max).



SUMMARY, CONCLUSION AND RECOMMENDATIONS

Summary and conclusion:

For objective three, the suitable IT security metric's model based on major IT security elements for universities in Kenya was found to be $Q_M = 1.904 + 1.62\ SP + 0.800\ PS + 0.808\ NS + 0.796\ DS + 0.788\ AC + E$ and this defined the model for IT security metrics. This model was interpreted that for a unit increase in every major IT security element, a significant increase in IT security metrics' value is predicted. Holding all other IT security elements' variables constant, the increase in IT security metrics associated with a unit increase of the element under consideration equals the coefficient value of the element under consideration. The simplified form of the model –

$Q_M = 1.9 + 0.8\ (2\ SP + PS + NS + DS + AC) + E$ yielded a unique model coefficient ratio of (2: 1). That is, the coefficient associated with IT security policy is twice as any other element in the model. This means IT security policy takes a cornerstone value in managing IT security.

Recommendations

IT security officers in universities should single out each major IT security element and properly implement it for better systems' security management. IT security policy should be given much higher priority as it is the cornerstone for IT security management. IT managers could improve the status of IT security in their various institutions by implementing IT security appliances along the major IT security elements. Further, it is recommended that universities management should apply the IT security metrics' model, not only for gauging the IT security status, but also for determining the returns on investment (ROI) in IT security appliances within the universities.

REFERENCES

Angelini, M., & Santucci, G. (2015). Visual cyber situational awareness for critical infrastructures. In *Proceedings of the 8th International Symposium on Visual Information Communication and Interaction* (pp. 83-92). ACM.

Bichanga, O. W., & Obara, O. B. (2014). Challenges Facing Information Systems Security Management in Higher Learning Institutions: A Case Study of the Catholic University of Eastern Africa-Kenya. *International Journal of Management Excellence*, *3*(1), 336-349.

Beas, M. I., & Salanova, M. (2006). Self-efficacy beliefs, computer training and psychological

Bevans, B. (2016). Categorizing Blog Spam.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press.

Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. *Computers & Security*, *26*(5), 410-417.

Gesmann, M., & de Castillo, D. (2011). Using the Google visualisation API with R. *The R Journal*, *3*(2), 40-44.

Gritzalis, D., Kandias, M., Stavrou, V., & Mitrou, L. (2014). History of information: the case of privacy and security in social media. In *Proc. of the History of Information Conference* (pp. 283-310).

Haubner, G., Petermann, H., & Zobl, H. (1986). *U.S. Patent No. 4,630,043*. Washington, DC: U.S. Patent and Trademark Office.

Howe, E. D. (2015). Mormonism unvailed (p. 252). Utah Lighthouse Ministry.

Ismail, R., & Zainab, A. N. (2013). Information systems security in special and public libraries: an assessment of status. *arXiv preprint arXiv:1301.5386*.

Jaffer, S., Ng'ambi, D., & Czerniewicz, L. (2007). The role of ICTs in higher education in South Africa: One strategy for addressing teaching and learning challenges. *International journal of Education and Development using ICT*, *3*(4).

Jonsson, E., & Pirzadeh, L. (2011). A framework for security metrics based on operational system attributes. In 2011 Third International Workshop on Security Measurements and Metrics (pp. 58-65). IEEE.

Kitheka, P. M. (2013). Information Security Management Systems In Public Universities In Kenya: A Gap Analysis between Common Practices and Industry Best Practices (Doctoral dissertation, University of Nairobi).

Kothari, C. R. (2003). Research Methodology–Methods & Techniques, Wishawa Prakashan, New Delhi. *Ali SS, Models in Consumer Buying Behaviour, Deep & Deep Publications*.

Lebel, P. (2007). *U.S. Patent Application No. 11/212,790*.

Lenders, V., Tanner, A., & Blarer, A. (2015). Gaining an edge in cyberspace with advanced situational awareness. *IEEE Security & Privacy*, *13*(2), 65-74.

Lie, H. W., & Bos, B. (2005). *Cascading style sheets: designing for the Web*. Addison-Wesley Professional.

MacLean, R. (2012). Dangerous environments. *Environmental Quality Management*, *21*(3), 109-116.

Makori, E. (2013). Adoption of radio frequency identification technology in university libraries: A Kenyan perspective. *The Electronic Library*, *31*(2), 208-216.

Mang'ira, R., & Andrew, K. (2014). Towards establishment of a full-fledged disaster management department for Moi University libraries.

Martins, A., Eloff, J. H. P., & Park, A. (2001). Measuring information security. In *Proceedings of Workshop on Information Security–System Rating and Ranking*.

Mitnick, K. D., & Simon, W. L. (2011). *The art of deception: Controlling the human element of security*. John Wiley & Sons.

Mugenda, O. &Mugenda A.(2003). *Research methods: quantitative and qualitative approaches*.

Mukhwana, E. J., Kande, A., & Too, J. (2017). Transforming University Education in Africa: Lessons from Kenya. *African Journal of Rural Development*, *2*(3), 341-352.

Ndung'u, P. W., & Kyalo, J. K. (2015). An evaluation of enterprise resource planning systems implementation experiences for selected Public Universities in Kenya.

Nixon, K. C. (2012). Winclada (BETA) ver. 0.9. 9. *Published by the author*.

Nweze, C. M. (2010). The use of ICT in Nigerian universities: A case study of Obafemi Awolowo University, Ile-Ife.

Okibo, B. W., & Ochiche, O. B. (2014). Challenges Facing Information Systems Security Management in Higher Learning Institutions: A Case Study of the

Catholic University of Eastern Africa-Kenya. *International Journal of Management Excellence*, *3*(1), 336-349.

Peláez, M. H. S. (2010). Measuring effectiveness in Information Security Controls. *SANS Institute InfoSec Reading Room, http://www. sans. org/reading_room/whitepa pers/basics/measuring-effectivenessinformation-security-controls_33398*.

Rubin, A., & Babbie, E. R. (2012). *Brooks/Cole Empowerment Series: Essential research methods for social work*. Cengage Learning.

Sekeres, M. A., & Bolwell, B. J. (2016). Will cancer patients be the next victims of the data privacy debate. *FoxNews. com. Accessed April*, *19*.

Stojmenovic, I., & Wen, S. (2014). The fog computing paradigm: Scenarios and security issues. In *Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on* (pp. 1-8). IEEE.

Tibenderana, P. K., & Ogao, P. J. (2008). Acceptance and use of electronic library services in Ugandan universities. In *Proceedings of the 8th ACM/IEEE-CS joint conference on Digital l ibraries* (pp. 323-332). ACM.

Thomas, T., Chu, B., Lipford, H., Smith, J., & Murphy-Hill, E. (2015). A study of interactive code annotation for access control vulnerabilities. In *Visual Languages and Human-Centric Computing (VL/HCC), 2015 IEEE Symposium on* (pp. 73-77). IEEE.

Trethowen, L., Anslow, C., Marshall, S., & Welch, I. (2015). VisRAID: Visualizing Remote Access for Intrusion Detection. In *Australasian Conference on Information Security and Privacy* (pp. 289-306). Springer International Publishing.

Veseli, I. (2011). *Measuring the Effectiveness of Information Security Awareness Program* (Master's thesis).

Villalonga (2004). Intangible resources, Tobin's q, and sustainability of performance differences. *Journal of Economic Behavior & Organization*, *54*(2), 205-230.