International Journal on Advances in Engineering Technology and Science
Volume: 2, Issue: 1, January-February 2016, e-ISSN: 2455-3131

Economical Improvements by Analysing & Enhancing Cyber Security in Small and Medium-Sized Business (SMBs)

Rajeshbhai Kadchha[1], Nitin Chikani[2], Shrey Shah[3]

Atmiya Institute of Science and Technology, Rajkot, Gujarat, India

[1]rajesh.kadchha@gmail.com, [2]nitinchikani5@gmail.com, [3]shrey.shah.mca@gmail.com

Abstract— **The objective of this paper is to investigate and enhance the safety aspects of net service delivery to small and medium-sized businesses (SMBs), and also the policy and restrictive implications of cyber-security within the 'fragmented' structural surroundings in an exceedingly developing economy. The ever present interconnectivity provides the first passage for exploiting vulnerabilities on a widespread basis; Medium Enterprises (SMB) sector is crucial in terms of economic process in developing economies. The ever present net permeates each aspect of human endeavour, not solely to the technologically developed countries, however additionally more and more current in developing countries. Whereas some argue that the pace of the expansion of the computer network ought to continue while not governmental restrictions, others, from another point of view , argue that these connectivity's ought to be actively regulated through domestic and international laws. The latter thinks that non-regulation of the computer network may have a grave cyber-security issue which is probably going to inhibit this growth and development gains. This analysis analyzed the assorted policies and frameworks in respect of secured interconnectivity, adherence to governance, risk and compliance problems in an exceedingly best-practice fashion. Inferential analysis reveals that there is a unit some cyber-security implications on SMB in an exceedingly fragmented policy and restrictive surroundings. The findings area unit mentioned and taken to produce highlights of those policy and restrictive challenges.**

Keywords— **Cyber Security, Data Collection Methodology, SMB (small and medium-sized SMB), Null Hypothesis, Alternative Hypothesis.**

I. INTRODUCTION

Motivation for locating out cyber-security policy and restrictive implications on SMB in developing economies was galvanized by the ever present interconnectivity, and also the sensitive nature of knowledge and transactions carried across these networks. The primary decade of the twenty first century has witnessed huge and unprecedented growth within the info & technology (ICT) sector of the worldwide economy, making a virtual marketplace. This growth necessitated several reforms world-wide. To understand the complete advantages of the digital revolution, users should trust that sensitive info is secured, commerce isn't compromised, and also the infrastructure isn't infiltrated.

The underlying technology was fictitious within the latter 1/2 the nineteenth century, as well as Babbage's analytical engine and therefore the telegraph. Data communication became economical for widespread adoption once the invention of the private laptop. Claude Elwood Shannon, a Bell Labs scientist, is attributable for having ordered out the foundations of medical care in his pioneering 1948 article, A Mathematical Theory of Communication.[13] The digital revolution regenerate technology that antecedently was analog into a digital format. By doing this, it became doable to form copies that were just like the initial. In digital communications, for instance, continuance hardware was ready to amplify the digital signal and pass it on with no loss of knowledge within the signal. Of equal importance to the revolution was the power to simply move the digital info between media, and to access or distribute it remotely.

A serious landmark within the revolution was the transition from analog to digital recorded music. within the Eighties, the digital format of optical compact discs supplanted analog formats, like vinyl records and container tapes, because the in style medium of alternative.[14]

Underlying the digital revolution was the event of the digital computer, the private laptop, and notably the silicon chip with its steady increasing performance (as delineated by Moore's law), that enabled technology to be embedded into an enormous varies of objects from cameras to private music players. Equally necessary was the event of transmission technologies as well as laptop networking, the net and digital broadcasting. 3G phones, whose social penetration grew exponentially within the 2000s, conjointly compete a awfully massive role within the digital revolution as they at the same time offer present recreation, communications, and on-line property.

Whereas there are Brobdingnagian edges to society from the digital revolution, particularly in terms of the accessibility of knowledge, there is variety of considerations. enlarged powers of communication and knowledge sharing, accumulated capabilities for existing technologies, and therefore the advent of recent technology brought with it

several potential opportunities for exploitation. The digital revolution helped commence a replacement age of mass police investigation, generating a variety of recent civil and human rights problems. Responsibleness of data became a difficulty as information may simply be replicated, however not simply verified. The digital revolution created it doable to store and track facts, articles, statistics, still as trivia till now impracticable.

From the attitude of the scholar, an outsized a part of human history is thought through physical objects from the past that are found or preserved, notably in written documents. Digital records are straightforward to make however conjointly straightforward to delete and modify. Changes in storage formats will build recovery of information troublesome or close to not possible, as will the storage of knowledge on obsolete media that replica instrumentality is unobtainable, and even distinguishing what such information is and whether or not it's of interest is close to not possible if it's not simply legible, or if there's an outsized variety of such files to spot. Info passed as authentic analysis or study should be scrutinized and verified. With such huge proliferation of knowledge it became doable to jot down a piece of writing citing whole false sources, conjointly supported false sources.

These issues are more combined by the employment of digital rights management and different copy bar technologies that, being designed to solely permit the information to be browse on specific machines, would build future information recovery not possible. Apparently, the traveler Golden Record, that is meant to be browse by AN intelligent extraterrestrial (perhaps an appropriate parallel to a person's from the distant future), is recorded in analog instead of digital format specifically for simple interpretation and analysis.

The SMB sector is crucial to attaining future and property economic process. They produce employment to numerous sectors of the economy and are forefront within the adoption of technology. Whereas exploitation of ICTs is crucial to putting together the economy, a myriad of cyber-security challenges confront SMB, that are each technological and human-centric in nature.

"Cyber-security policy has to begin from a transparent and through empirical observation grounded understanding of the character of the issues before potential solutions are often devised." [1]

The ubiquitous net permeates each aspect of human endeavour, not solely to the technologically developed countries, however conjointly more and rifer in developing countries. Whereas some argue that the pace of the expansion of the Internet ought to continue while not governmental restrictions, others, from another perspective, argue that these interconnectivities ought to be actively regulated through domestic and international laws. The latter thinks that non-regulation of the Internet may have grave cyber-security considerations which are probably going to inhibit this growth and development gains.

In this study we tend to conduct a survey and followed-up with interviews of some strategic stakeholders. Existing policies were reviewed with the read to spot some cyber-security challenges try SMB. Their answers were analysed and people represent the findings of this paper.

In this paper, we tend to discuss the analysis question and methodology, followed by the review of connected works in cyber-security, significantly its impact on SMB, its policy and regulation, its implications, and neutral perceptions. We tend to provide a summary of the SMB contribution to the African country economy, the market scenario and also the technologies used for net service delivery in Ghana. We tend to then gift the empirical information collected and its analysis. We tend to conclude with a discussion of the results and supply many recommendations on the method forward and any analysis work.

Key Issues & Statistical Analysis with Hypothesis

This analysis sets dead set investigate on the protection aspects of web service delivery to SMB, specifically, and its associated policy and regulative implications during a fragmented regime.

This is premised on the actual fact that threats to cyber-security emanate from a pair of main sources: particularly, direct cyber-attacks from the cyber-criminals and therefore the interconnected network-of-networks. "When infrastructures square measure interconnected, new vulnerabilities would possibly arise from the common links, failures would possibly propagate through the various systems, intrusion and disruption in one provoke surprising threats to others." It's this interconnection wherever the ICTs play a significant role which is that the import of this paper.

A growing variety of corporations area unit embrace 'disruptive' technologies. They're investment in social media, mobile devices, cloud computing and massive information to have interaction with customers in new ways that and gather insights for developing and promoting new offerings additional effectively. They're additionally changed of integrity forces with organizations in adjacent industries.

But capitalizing on these technologies is tough, given the speed at that they're progressing. It's only too straightforward to urge on the 'wrong side' and find yourself as a casualty, not a pioneer. Several corporations also are unsure concerning a way to use the info they collect. And finding sensible allies is turning into noticeably more durable as additional and additional companies collaborate.

The transformation of the geographical point has different implications. Most corporations can have to be compelled to offer digital tools for coaching those who don't pursue ancient career ways. They'll even have to adopt a additional democratic management vogue to draw in 'digital natives' and use executives WHO area unit extremely skilful at grouping and managing groups.

Organizations have to be compelled to accommodate ever additional laws and rules that impact mission important processes. They have to join forces cross border and cross-domain so as to satisfy client demand. Economic process keeps gaining pace and technological innovation ne'er stops.

Change is here associate degreed growing at an exponential rate. Modification all told types of ways that, progressive, turbulent and transformational, inevitable and unpredictable. With increasing complexness modification becomes additional and additional unpredictable.

In any domain the economic worsening has affected countries and organizations worldwide. They have to try and do additional with less. Prices area unit rising and revenues area unit decreasing. Increasing potency and effectiveness is important.

We reside in associate degree forever on, forever connected society, with instant gratification and short attention spans. Web and social media have formed client expectations. Customers currently demand a private approach, immediate response, 24hours*7days and thru the channels of their selection.

Organizations area unit presently unequipped to face these challenges. Their processes cause unacceptable error rates, low productivity, and client disengagement and worker unskillfulness. Technology is suboptimal and hand tied in bequest applications. Optimization can now not serve. What organizations would like could be a technological and method paradigm shift towards true progress.

You may be acquainted with the catalogs or internet site of TigerDirect, the merchandiser that slugs it out with a number of internet sites providing discounted technical school merchandise to shoppers. However you'll not apprehend that Systemax, the parent company of TigerDirect is Systemax, a 65-year recent NYSE-listed international company that's seeing its industrial reseller SMB grows quicker than the other phase of its SMB. In step with Adam Shaffer, govt vp of commerce at Systemax, the corporate has over five hundred departing salespeople in thirteen regions in addition as technical results in support over a hundred customers.

Indeed, last month the corporate rented out associate degree intimate very little venue called Miami Marlins Park to attach customers with several of tech's biggest vendors. The event, called the TigerDirect Innovation IT Conference and accumulation was hosted by Shark Tank's Kevin O'Leary. Before the event, Systemax's Shaffer shared what TigerDirect sees as four of the key IT problems for little SMB in 2015:

Cloud computing has sturdy allure--affordable computing capability, storage and apps offered on-demand and to everybody in a company. SMB get solely the capability they have and receive dynamic updates with stripped installation problem. However, the cloud additionally comes with several questions: what is the right cloud structure? Ought to we tend to host off-premise? Ought to we tend to host our own cloud? Ought to we tend to invest within the infrastructure? However will we begin off? In several cases, a cloud answer could also be cheaper, however there are a unit issues concerning management and security. There can even be questions on migrating across competitive ecosystems, like Microsoft workplace and Google apps.

Since most people solely wish to accommodate one Smartphone at a time, these devices ushered within the era of BYOD. Language no to non-public devices will be a productivity buster which will be powerful to enforce. However, there is a unit still several problems with that several tiny SMB area unit wrestling. These embody ensuring that a phone or pill is not a simple access purpose to disrupting the network whereas keeping workers information safe and separate. There can even be restrictive issues in sectors like money and health.

Once, the roles of devices were clearly defined--the desktop for stationary productivity and additional rigorous process tasks, laptops for mobile productivity, and Smartphone for unsettled property. However, the doorway of latest operative systems like ions and Chrome OS in addition as a slew of hybrids and convertibles from completely different corporations have created selecting the correct instrumentality plenty additional difficult; this issue is in fact conflated thereupon of BYOD. Tiny SMB will currently faucet into inexpensive Chrome books in addition as Windows notebooks and even reasonable two-in-ones which will work as a laptop computer or pill.

It appears that each day we tend to hear concerning information breaches at massive corporations like Target, Home Depot, JP Morgan Chase and, last and infamously, Sony footage. The bread and butter of antivirus remains vital, however even tiny SMBs should be troubled with the integrity of client information. There are unit myriad choices within the marketplace which will facilitate with this.

According to Shaffer, the key in determinant the correct answer is listening fastidiously to client desires. The method begins with a telephone call or internet site lead and evolves to account managers WHO act as quarterbacks to usher in the suitable resources to service customers, as well as consultants from several of their seller partners. Whereas there could also be several queries around wherever tiny SMB it'll enter 2015, it appears clear that there are a unit additional selections than ever to best match a tiny low SMB's desires.

The issue is “how square measure these interconnectivities regulated, a number of that square measure cross-border originated?” Since the de-regulation of the telecommunication setting in Republic of Ghana, what has been the impact of cyber-security policy and regulation on SMB? Over a decade when the de-regulation, what square measure the security-related challenges with web service delivery?

Are there any impacts and inhibitions to growth of the SMB thanks to multiple inter-connectedness and its cyber-security implications? That stakeholders square measure to

blame for vulnerability incidents, and the way square measure incidents handled?

This searching analysis can take a look at if cross-border provisioning and repair supplier sort have any effects on cyber-security. Cross-border ICT-enabled services square measure same to be services provided from one country to a different over the web, telecommunications and information networks. Here cyber-security implications see challenges related to service provision, risk, protection, trust, incident handling, standards and solutions, etc.

The null hypothesis is:

H0: there are not any cyber-security implications on SMB during a fragmented policy and regulative setting.

The alternative hypothesis is:

H1: there square measure cyber-security implications on SMB during a fragmented policy and regulative setting.

Note that, H0 and H1 square measure reciprocally exclusive.

Methodology

In this analysis, we've got adopted the subsequent definitions of SMB. SMB with but 10 staff as a small Enterprise, between 10 and fifty as tiny Enterprises, and between fifty to 2 hundred and fifty staff as Medium-sized enterprises. This definition is per alternative similar studies and forms the premise for choosing SMB for the study.

Methods of obtaining primary data include: observations, questionnaires, interviews, conversations, written exchanges electronically and in letter from between you and respondents

You should additionally collect secondary information made inside and regarding the organizations being studied. This information can are collected and used for functions apart from those of your project, therefore the challenge is for you to sift, choose and kind the information in ways in which match your analysis aims. Sources of secondary information generally comprise: reports and accounts of the topic organizations, publications place out by them, together with message material, reports regarding them written by SMB analysts and alternative lecturers, general net information (with appropriate caution in choosing respected sources)

You can get applied math information from a large kind of public and personal sources, though your selections are easier to validate and justify if they're from giant international organizations like the globe Bank or the Organization for Economic Cooperation and Development (OECD).

In terms of knowledge analysis, you'll be able to analyze primary and secondary information by drawing on established analytical tools. Totally different analytical tools could also be used for various analysis methodologies. As an example, as qualitative analysis principally involves matter analysis of orally communicated information, analytical tools could also be drawn from discursive strategies, together with narrative analysis, to review speech within the recorded text. Subtle information analysis code like Nvivo-9 could also be used for explicit qualitative information analysis functions like cryptography and thematic analysis.

Statistical analysis in each qualitative and quantitative analysis could draw on a variety of elementary and advanced tools to check relationships between variables. Choice of appropriate applied math tools depends on the quality of the relationships between variables that square measure being tested, though in your project elementary applied math tools can sometimes do for information analysis.

Larger datasets, as an example of monetary information, square measure typically analyzed with code programs like SPSS (Statistical Package for Social Sciences) which will apply each elementary (F and t-tests, ANOVA) and advanced (multivariate multivariate analysis, forecasting) applied math tools.

Drawing on a variety of applied math techniques will increase the sophistication of findings in your project, wherever elect techniques ought to directly take a look at such hypotheses.

We reviewed existing policies and frameworks, with the read to spot some challenges as a results of fragmentation, and additionally to spot cyber-security vulnerabilities grappling SMB in several countries. The study administered associate degree objective-based structured form to security functionaries and chief-level (C-level) officers of 320 SMB in African country. Mistreatment face-to-face surveys, we have a tendency to targeted ICT-based SMB, money organizations and government agencies that were selected by an easy sampling. Supported the respondents, some stakeholders were known for more strategic level interviews. Especially, we have a tendency to interviewed strategic stakeholders like the Ministry of Communications (MoC), National Communications Authority (NCA), African country ISPs Association (GISPA), African country Investment Fund for Electronic Communications (GIFEC), etc.

Already some results are obtained through analysis of those new offered knowledge. Among these, the 2002, 2003, and 2004 editions of the report on little and Medium Enterprises in Japan offer an intensive analysis supported the SFE. they need known and processed numerous basic facts regarding little SMB funding that antecedently had for the most part gone unquantified: as an example, the extent to that interest rates applied to a company receiver take issue counting on the scale and capital adequacy magnitude relation of the receiver, what sorts of firms square measure providing collateral or credit guarantees, then forth. additionally, responding to the growing interest within the squeeze drawback and also the ever-changing relationships between banks and their company customers, the SME white papers analyze the disposition attitudes of main banks vis-a-vis numerous company customers; as an example, whether or not the bank rejected letter of invitation for an extra loan, whether

or not the bank raised or tried to boost the charge per unit, whether or not the bank demanded extra collateral, then forth.

However, most of the analyses conducted for the white papers target the crosswise dimension of the knowledge collected in every survey year and no try has been created to utilize them as panel data. At a similar time, economists in Japan and plenty of different countries try to work out the state of little SMB funding and bank behavior supported a huge range of hypotheses. For them, knowledge collected through the SFE square measure very helpful to check these planned hypotheses. Indeed, supported these knowledge, many studies, with the exception of those for the white papers, are conducted. I introduce 2 such works one by Hosono, Sawada, and Watanabe (2004) and another by Uesugi (2004) below.

Hosono, Sawada, and Watanabe (2004) examine the characteristics of firms that manage to get loans from different banks and stay viable even once their main bank rejects their request for a loan.

When a monetary crisis happens, it raises issues over important adverse impacts to firms. The grave issues regarding the negative impact on native firms in Ezo caused by the collapse of Ezo Takushoku Bank in 1997 square measure still contemporary in our recollections. The information collected within the SFEs, however, show that some 2 hundredth of the SMB whose loan requests had been rejected by their main bank between 1999 and 2001 were ready to get loans from different lenders. The study shows what it takes for an organization that has been spurned by its main bank to be picked up by another.

First, the authors emphasize the importance of firms doing SMB with quite one bank throughout traditional times and keeping those banks enlightened of one's monetary and management conditions. This, the authors say, is a form of "insurance," that firms secure loans elsewhere if their main bank refuses to lend. It's been recognized, somewhat critically, that in Japan even little SMB handle many various banks whereas most of their yank counterparts handle just one or 2. However given the above-described purpose created by the 3 researchers, it appears quite rational for an organization to handle many various banks.

Second, they denote that the more serious the status of the most bank that has refused to lend, the bigger the possibility for the abandoned SME to be picked up by another bank. Suppose there square measure 2 firms whose monetary conditions square measure equal which Company A's loan request has been turned down by Associate in Nursing undercapitalized main bank and Company B's by a sound bank. In line with Hosono et al. (2004), Company A includes a bigger likelihood to get a loan from another establishment as a result of there's a bigger likelihood that refusal of the loan request stems from the poor status of the investor instead of the receiver. This means the status of the initial disposition bank is a symbol to different banks in creating credit choices on potential receiver firms.

Uesugi (2004) expands the scope of the investigation to shed light-weight not solely on bank loans however additionally on trade credit wide provided through company goods transactions... Uesugi investigates the relationships between trade credit and bank loans supported the SFE knowledge. Previous studies assume that suppliers of trade credit have a plus over banks, each in creating credit choices and taking acceptable actions in an exceedingly timely manner. Through day-after-day SMB transactions, human non-financial firm's square measure ready to get a reasonably correct image of the monetary and SMB conditions of every receiver company. This allows human firms to evaluate the borrowers' credit risk additional accurately. Also, they're ready to build a comparatively correct judgment on the inventories command by receiver firms and, if necessary, eliminate them in an exceedingly timely manner. The chart below shows however human companies' attitudes in trade credit modification in response to changes within the credit risk of borrowers.

Their answers were analyzed and people represent the findings during this paper. We have a tendency to shall take a look at the null hypothesis by subjecting it to some style of empirical scrutiny to see if it's supported or refuted by the info collected from the sector. It should be noted that literature review was performed to spot the progressive of the discussions and also the main challenges; which fashioned the premise for the planning of the empirical study.

II. Effect of Cyber-Security on SMB

The SMB sector is crucial to attaining long run and property economic process [2][3]. ICTs have well-tried to be important in up the potency and increasing the market reach of SMB still as in establishing new ways in which for SMB to get and create the foremost effective use of SMB info.

Literature reveals that there are "... opportunities that ICT provides for SMB in developing countries..." [4][5] Emphasized that service suppliers have recognized the necessity of SMB to security and have created acceptable SMB models with safety features. Some give a full vary of security solutions and technologies services. Posit that SMB face numerous cyber-security challenges as a result of interconnections that expose SMB to hacking and alternative malwares. Even once SMB procure security solutions, they're then exposed to body and alternative operational overheads.

A poorly secured network is "potentially the weakest link" [6][7][8] within the cyber-security chain. As an example, malware in associate degree noncurrent network will become a botnet through that alternative systems may be attacked. They aforementioned that ISPs are typically not proactive in characteristic and removing botnets seeable of the value implications. They continued that true causes SMB to under-invest. Developed a model of dependent risk of cyber-security breach across corporations, and finished that this dependent risk ends up in under-investment.

III. CYBER-SECURITY IMPLICATIONS

Virtually any component of Net is in danger, and also the degree of interconnection of these parts will create it tough to work out the extent of the protection measures required. [9][10] Posit that "it's terribly tough to get knowledge regarding truth value of a security incident (single loss expectancy (SLE))." generally, corporations don't track security incidents; they specialize in fixing the matter instead of assessing the incident value. Effects of botnets are anticipated to grow as networks become a lot of powerful and high-speed interconnectivities become inevitable. Though, newer technologies with new powerful defenses is also introduced, [11] posits that, cyber-security researchers assume that the present state of affairs is, primarily, because of adverse effects of interconnectivities. Future researches ought to specialize in reducing uncertainties and up on the standard of vulnerability mensuration.

The companies during this prime tier—whom we have a tendency to sit down with as security leaders—understand that they're up against differing kinds of cyberthreats. There primarily square measure four styles of attacks, every of that incorporates a totally different motive. It's useful to think about these as storm waves, moving around your SMB. At any given time, it's not possible to understand that wave can hit and what sort of harm it'll bring.

The first and oldest wave is nuisance hacking, during which there's very little material impact to the corporate. A classic example is hackers defacing your company's web site. A lot of serious and widespread is that the second wave, that is hacking for gain.

As SMB has migrated to the digital world, criminals have, too. What has emerged could be a subtle criminal scheme that has matured to the purpose that it functions very like any SMB—management structure, internal control, off shoring, and so on. This sort of hacking currently goes on the far side blindly stealing client MasterCard info or worker passwords. As an example, hackers would possibly target a company's money operate so as to get its statement before it's publically discharged. With such advance information, they will profit by exploit or merchandising stock.

Protecting the SMB from crime is one factor, however firms conjointly should worry a few new sort of risk—the advanced persistent threat. If you think that the term appears like it's out of a spy motion picture, you're shortly off. This sort of hacking is preponderantly concerning stealing belongings and generally is related to state-sponsored undercover work. The motives transcend gain. Consultants could quibble concerning the specifics of this sort of attack and whether or not it perpetually has concerned use of advanced techniques; however this can be a heavy and growing threat. It's not a real understatement to mention that what's in danger isn't solely your belongings however probably national security.

The high-profile Stuxnet worm case demonstrates however specialized and complicated these attacks is. The Stuxnet worm that was discovered in 2010 was designed to infiltrate industrial management systems, like those who manage water or power plants. However it wasn't Associate in nursing infrastructure system that was hit; hackers infiltrated and doubtless sabotaged the Iranian systems that manage metal. Because the chilling details emerge, what's noteworthy is that the attack was planned (and the worm developed and placed) as several as four years before the incident.

This foresight echoes a trend we've got seen in our work with firms like defense contractors. Once they announce plans to accumulate another company, perpetrators follow the potential acquisition. Their hope is to engraft malicious software package on the systems of the acquisition target so once the SMB ultimately square measure integrated, hackers can have access to the parent company's systems—even if it suggests that biding time for eighteen to twenty four months or longer.

And it's not solely specialized industries like defense that square measure in danger for advanced persistent threats. We've got seen tidy activity within the money services and technology industries. In some cases, the perpetrators infiltrate a bank or service supplier so as to induce access to the organization's customers' systems.

Finally, there's another sort of threat that's on the rise: hacktivism. Wiki Leaks directly involves mind, but, for the non-public sector, think about this because the digital corresponding to Occupy Wall Street. The goal of perpetrators is to alter or produce a public perception of your complete. As an example, hackers would possibly acquire sensitive info and disclose it to the general public.

New threats emanate as entities get interconnected. Attacks occur inside and across national boundaries; with cross-border nature of cyber-security creating it tough for stakeholders to unilaterally securitize (ref. Copenhagen School) nascent cyber-threats. It becomes apparently necessary for nation-states to shield their interests by operating along. [12] Emphasizes that similar policy ways accustomed foster regional integration in different sectors may be adopted for Net. Per cross-border threats will emanate from entities, be they firms or state agencies, against one another from any a part of the globe.

IV. THE DATA

The results are presented in the following table:

The variables being analyzed here area unit nominal categorical knowledge, wherever there's no inherent order to the classes. For nominal categorical variables, the mean, median and variance statistics aren't substantive. The freelance variables area unit the Service supplier kind and VSAT Facilities; the remainder area unit dependent variables.

Survey Data - Cyber-security & SMEs: Policy & Regulatory Implications

Item	Variables	Observations	Value Label/Value	Value Label/Value	Value Label/Value	Value Label/Value	Value Label/Value	Value Label/Value
			Yes	No				
1	Internet Usage	150	120	30				
			Daily	Once a week	Once a month			
2	Frequency of Usage	150	89	25	15	21		
			Local ISP	Foreign ISP	Self-Provided			
3	Service Provider Type	150	126	7	1	16		
			Yes	No				
4	VSAT Facilities	150	6	123	21			
			Very often	Often	Seldom	Never		
5	Online Transaction	148	17	62	42	11	16	
			Yes	No	Don't Know			
6	Security Standards	149	39	11	80	19		
			Yes	No				
7	Security Solutions	150	75	53	22			
			Adequate	Somewhat	Inadequate			
8	Internet Protection	150	23	49	23	55		
			Yes	No				
9	Internet Risk	149	46	75	28			
			Yes	No	Not Sure			
10	Data Loss	150	40	37	56	17		
			Reported & dealt with	Under reported, just cover-up	Not reported,at all			
11	Incident Handling	150	60	42	29	19		
			My Company	NCA	The Ministry	National Security	Not Sure	
12	Stakeholder Responsibility	150	69	6	7	2	44	22
			Contact Type(SLA)	Security Policy	Track record	Vulnerability Procedures	None of the above	
13	Service Provider Trust	191	6	52	14	69	50	
			Yes	No	Not Sure			
14	Risk Perception	150	44	26	57	23		

V. Description of Procedure for Data Collection

The analysis engaged a team of undergraduates from the University of Republic of Ghana, Legion, to administer the survey. Victimization face-to-face surveys, we tend to targeted ICT-based SMB, monetary organizations and government agencies, which were selected by a straightforward sampling. We tend to invite their views on key cyber-security connected problems.

The study administered associate objective-based structured form to security functionaries and chief-level (C-level) officers of 320 SMB in Republic of Ghana. one hundred fifty respondents (46.9%) were received; of those a hundred and twenty (37.5%) used net for SMB functions and were enclosed within the analysis. we tend to had strategic neutral interviews with the Ministry of Communications (MoC), Republic of Ghana Investment Fund for Electronic Communications (GIFEC), Republic of Ghana ISPs Association (GISPA), National Communications Authority (NCA), etc.

We organized and understood unstructured information, ensuing from the interviews. We first, sorted meaningful text segments, or created tags. Then we tend to regrouped similar text segments or created classes. These were employed in either affirming identified results from the survey or employed in explaining the explanation behind those results.

VI. Data Limitations & Problems

The analysis had some challenges together with "missing" values ensuing from non-responses to sure queries. There have been instances once respondents had to run a second form since the primary one had been misplaced. There have been alternative challenges related to obtaining interviews with key stakeholders, particularly the government sector stakeholders.

VII. Empirical Results

This section outlines initial areas of action to assist the stakeholders deliver the goods an additional coherent policy and regulative framework towards secured interconnectivities. It doesn't gift typical policy pointers per se; instead it articulates some issues that require to be factored into a viable policy framework for cyber-security solutions. This section structured the precise findings and choices for action beneath some key objectives:

- To assess the provision and use of cyber-security standards and solutions by SMB in Ghana;
- To estimate the extent of security breaches, its occurrences, and whether or not or not the breaches square measure reported;
- To estimate the perception of cyber-security in African country by SMB;
- To estimate the extent of involvement of cross-border (and/or) SMB presence suppliers in Ghana; and
- To assess the neutral responsibility for making certain cyber-security.

VIII. Conclusion & Discussion

Generally, this analysis is a trial to handle one or additional of the subsequent problems with a given phase of the SMB population in Ghana:

- Are there cyber-security implications on SMB in developing economies during a fragmented policy and regulative environment?
- How are these interconnectivities regulated, a number of that is cross-border originated?
- What has been the impact of cyber-security policy and regulation on SMB?
- What are the challenges of web service delivery on SMB in respect of security, governance, risk and compliance?
- What are the enablers and inhibitors to growth of the trade thanks to multiple link and its cyber-security implications?

In view of the broad scope of cyber-security policy and regulation, drawing general conclusions is also inappropriate. However, we have a tendency to shall comment in brief on some specific options of the analysis that are quite hanging. Cross-border and SMB presence suppliers represent concerning five-hitter of the SMB we have a tendency to survey. Security standards and best practices don't seem to be adhered to; security solutions don't seem to be adequate; web and systems protection don't seem to be adequate; averagely, concerning thirty fifth SMB perceived web service delivery in Republic of Ghana as risky, unsecured and susceptible to cyber attacks.

We can infer that governance, risk and compliance problems need the policy-makers pressing attention. Obviously, there are some cyber-security implications on SMB as results of fragmented policy and regulation. These might not are necessitated by the cross-border and SMB presence suppliers. We have a tendency to so reject the null hypothesis and deduce that there are some cyber-security implications on SMB during a fragmented policy and regulative atmosphere of a developing economy.

Though, this study was from tutorial analysis perspective, the teachings drawn might assist policy-makers weigh

numerous regulative reform proposals cyber-security trends, and think about ways in which during which the present regulative regime may well be optimized.

We commend the on-going policy initiatives on information protection; however would recommendation the incorporation of specific clauses to handle the totality of cyber-security dimensions as per the ITU-T Recommendation X.805. We have a tendency to additionally suggest the institution of foregone conclusion to cater for cyber-disaster preparation and recovery programs. In essence policy manufacturers ought to endeavor to consolidate existing policies or frameworks in favor of a coherent policy that will expressly address cyber-security vulnerabilities with SMB in mind, and to position the SMB to vie within the cyber-market. There's additionally the requirement to suitably manage the "cross-border" and "commercial presence" suppliers to make sure adequacy of cyber-security solutions, implementations and compliance.

We suggest that stakeholders be incentivized to report incidents, and to take a position in cyber-security solutions. We have a tendency to additionally suggest that policy manufacturers ought to examine thoroughly the impacts and inhibitions to growth thanks to multiple inter-connectedness and its cyber-security implications. Obviously, this demand more analysis works into examining the impact of cyber-security vulnerabilities with SMB.

Since cyber-security threats are not any longer perceived as chiefly technological in nature, however additionally human central, awareness programs and dissemination of information on user behavior may well be useful to SMB. Finally, arguably cyber-security may well be perceived as "public good", and from that perspective, governments ought to give leadership, with public-private-partnerships being cast.

REFERENCES

[1] Bauer & van Eeten. (2009). Cyber-security: Stakeholders incentives, externalities & policy options.

[2] Baldwin, J. et al. (2002). The Trend to Smaller producers in Manufacturing in Canada & US. Center for Economic Studies, US Census Bureau.

[3] Lange, T. et al. (2000). SMB & Barriers to Skills Development: A Scottish Perspective. 24 (1), 5-11.

[4] Heeks & Duncombe. (2001). Technology Planning in ICT: A Handbook for Enterprenuers in Developing Countries. University of Manchester, UK.

[5] Kolodgy, C. et al. (2002). Meeting the Grwoing Security Needs of Small & Medium sized Enterprises: SMB Security Solutions. IDC.

[6] Allison & Strangwick. (2008). Privacy Through Security, Policy & Practice in an SMB. In R. Subramanian, Computer Security, Privacy & Politics: Current Issues, Challenges & Solutions. IRM Press.

[7] Anderson & Moore. (2006). Information Security Economics - and Beyond. Science , 610-613.

[8] Bauer, M. (1996). The Narrative Interview - comments on a technique for qualitative data collection. London School of Economics & Politics.

[9] ITU. (2005). A Comparative Analysis of Cyber-security Initiatives Worldwide. International Telecommunications Union (ITU).

[10] Sonnenreich, W. et al. (2006, February). Return on Security Investment (ROSI) - A Practical Quantitative Model. 38 (1).

[11] Hammock, M. (2010, June). A Review of the Economics of Information Security Literature. Social Sciences Research Network (SSRN) .

[12] Thomas, N. (2009). Cyber Security in East Asia: Governing Anarchy. Asian Security , 5 (1), 3-23.

[13] Shannon, Claude E.; Weaver, Warren (1963). The mathematical theory of communication (4. print. ed.). Urbana: University of Illinois Press. p. 144. ISBN 0252725484

[14] "The Digital Revolution Ahead for the Audio Industry," SMB Week. New York, March 16, 1981, p. 40D.