Concordia University College of Alberta

Master of Information Systems Security Management (MISSM) Program

7128 Ada Boulevard, Edmonton, AB

Canada T5B 4E4

An Internet ccTLD Security Governance Framework

by

PEREZ, Luis

A research paper submitted in partial fulfillment of the requirements for the degree of

Master of Information Systems Security Management

Date: August 2009

Research advisors:

Dr. Dale Lindskog, Assistant Professor, MISSM

Ron Ruhl, Director and Assistant Professor, MISSM

Dr. Pavol Zavarsky, Director of Research and Associate Professor, MISSM

An Internet ccTLD Security Governance Framework

by

PEREZ, Luis

Research advisors:

Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Dale Lindskog, Associate Professor, MISSM

Reviews Committee:

Dale Lindskog, Assistant Professor, MISSM
Ron Ruhl, Assistant Professor, MISSM
Pavol Zavarsky, Associate Professor, MISSM

The author acknowledges the significant contributions to the work by Academic Advisors and Review Committee Members and gives the right to Concordia Univeristy College to reproduce the work for the Concordia Library, Concordia Websites and Concordia MISSM classes.

An Internet ccTLD Security Governance Framework

By Luis Perez
Pavol Zavarsky (research advisor)
Ron Ruhl (research advisor)
Dale Lindskog (research advisor)
Department of Information Systems Security Management
Concordia University College of Alberta
7128 Ada Boulevard, Edmonton, AB T5B 4E4, Canada
lperez@csa.concordia.ab.ca

Abstract

We propose an Internet ccTLD (country code Top Level Domain) Security Governance Framework and a maturity index for measuring the level of Security Governance within the ccTLD registrars. This basic conceptual structure will permit to assess risk management and maturity/effectiveness across ccTLD registrars and track progress in effective security governance of the Internet. The aim of this paper is to provide the initial approach for a multidimensional risk-based index for the ISG on the ccTLD level containing strategic, managerial, and operational components. Local domain registrars of every country, governments, and international organizations will benefit with this index that will permit assessing, benchmarking, comparing, and making improvements in the ISG of particular ccTLD.

Keywords: *Framework, Internet Security Governance, country code Top Level Domain, Maturity Level.*

1. INTRODUCTION

Internet Security Governance is a topic that has been increasingly discussed [1], [2], [3], [4] to deal with security governance of the Internet. The need for this specific topic – Internet Security Governance – as a subset of Internet Governance, is important to create regulations and mechanisms to administer the security of the Internet and generate the best climate and conditions for the cyber security of the network.

The issues related to Internet Security Governance are broad, and involve infrastructure, security per se, stability, privacy, national sovereignty (country domain names, for example), etc. These issues have potentially wide-ranging social, economic and national security implications and are linked to economic development and poverty reduction as seen in many studies [1], [2], [3].

Governance is a key component of information security and what constitutes good governance is a critical and important question.

Information Security Governance deals with the protection of online confidentiality, availability and integrity throughout the life cycle of the information. The benefits of good ISG are not just a reduction in risk or a reduction in the impact should something go wrong, but also can improve reputation, confidence and trust from others with whom registrars, interact.

There are many generic definitions of Internet governance notably [4], and in spite of a non-existent accepted definition of IT governance, some authors have provided a definition based on a consolidation of literature [5].

There is considerable agreement about certain broad features of what constitutes “good IT governance”. Furthermore, there have been some attempts to define ISG [14]. However, there is not an accepted and shared definition of ISG in previous research that creates a general consensus.

The definition we use for Internet Security Governance is crucial for the Internet ccTLD Security Governance framework and the maturity index we propose. For the clarity of scope and intent of this current study we use the following definition:

“ISG is the application of principles, norms, rules, best practices, security policies, decision making procedures, processes and structures, and laws used to manage Internet Security problems. This involves having the adequate resources, allocating resources, controlling, coordinating activities, creating awareness, training and

education, sponsoring of organizations to address Internet Security, and monitoring and auditing processes. At the same time, it has mechanisms for measurement of effectiveness of governance by examining whether or not objectives were achieved." It is this 'measure of effectiveness' that this research wishes to justify. This working definition reinforces the concept of inclusiveness of Governments, the private sector and civil society in the mechanisms of ISG. In addition, three dimensions are used for the framework for defining ISG, and contain strategic, managerial, and operational components. This paper provides an initial approach for a multidimensional risk-based index for the ISG on the ccTLD level containing strategic, managerial, and operational components.

With ISG, we must address two problems:

1. Selecting attributes that reflect the ISG aspects for each dimension of interest and,

2. Finding appropriate ways to amalgamate these attributes so that we can measure overall Internet Security Governance.

According to ISM3 Consortium [15], there are three levels of Security Management:

- Strategic (direct and provide), which deals with broad goals, coordination and provision of resources;
- Tactical (implement and optimize), which deals with the design and implementation of the Information Security management system, specific goals and management of resources;
- Operational (execute and report), which deals with achieving defined goals by means of technical processes.

The generic goals of an Information Security Management system are:

- Prevent and mitigate incidents that could jeopardize the registrar objectives;
- Risk reduction;
- Trust.

The proposed framework facilitates the understanding of this multidimensional risk-based index for the Internet ccTLD Security Governance.

To establish the state and coverage of current risk management systems in the registrars, we do this using a Capability Matrix type of evaluation. The capability Maturity Model – Risk Management (CMM-RM) is basically an extension of the Capability Maturity Model Integration (CMMI) process used by the Software Engineering Institute (SEI) [17]. CMMI is a process improvement approach that provides organizations with the essential elements of effective processes. The Maturity Matrix of the ISG is organized into five stages of ISG maturity, which maps the three components and stages of the framework and each level representing a higher evolutionary stage within each component. This Maturity Matrix maps the different stages against the capability dimensions of the registrars and measures risk management maturity/effectiveness across the registrars.

2. ISG Maturity Framework for registrars

The risk-based ISG Maturity Framework contains strategic, managerial, and operational components. Each component defines the fundamental dimensions and guidelines of this multidimensional maturity model for registrars.

The three dimensions of Internet Security Governance corresponding to the framework are:

- Strategic: helping to achieve ISG objectives and goals
  - Vision, leadership, resource allocation, sponsorship, institutional quality

- Managerial: controlling the process to achieve ISG objectives and goals
  - Accountability, security management, security policies and best practices, awareness and training

- Operational: executing, monitoring, reporting and achieving defined goals of ISG
  - Monitoring, assessing, compliance, auditing, benchmarking

2.1 ccTLD registrar's ISG Strategic Components

Strategic Internet Security Governance is basically the process of proactively addressing where the registrar is going and how it intends to get there to achieve a plan for the governance of the Internet security. Its purpose is to increase the possibility that the registrar will accomplish its purpose and make effective use of its available resources. There is a successive process which typically includes creating a vision for where the registrar should

be in the future, analyzing the levels of maturity of ISG, determining where the registrar is at today, and then developing operational plans for closing the gap over time. The intended outcome is to make the goal of achieving a desired level of maturity of ISG by effectively managing the risk of the network through robust risk management and ISG processes. There are two parts of the process, creating the vision and the strategic plan with the sponsorship and commitment of the registrar leadership to protect information security.

2.1.1 Creating the Vision

The first action is to create a vision of what the registrars should accomplish for ISG and how the future will be different as a result. Before one can set out in a direction, they need to understand where they wish to end up. In strategic planning this definition of destination may be called by several names including the vision or the organizational purpose. It specifically addresses the questions of what good the registrar is to create in the world, whom is the intended receiver of this good is (stakeholders), and the comparable value of achieving that good for those people [6].

2.1.2 Creating the Strategic Plan

The second step in the process is creating the strategic plan for ISG. The strategic plan defines, in operational terms, how the registrar will achieve the vision defined in the first step. This vision is held against the current reality of where the registrar sits today. Operational objectives, goals, strategies, tactics, programs, and activities are set to actually achieve that change in the future. In other words, all the strategic planning activities are about operations and are dependent upon, and directed by the vision and until the vision is defined, there is no way to judge the soundness or expectation of success of any of the strategies for ISG.

The vision is above the operational planning and must come first. It then guides all the further planning activities with the commitment from the board and highest leadership to protect information assets. In practice, the planning activities arrange the use of assets and operations to be utilized in achieving the vision [6].

Leadership is a fundamental and critical constituent of the strategic components and organizations like Internet Corporation for Assigned Names and Numbers (ICANN), World Group on Internet Governance (WGIG), and World Summit on the information Society (WSIS) play an important role in the policies and regulations that govern the security of the Internet.

2.2. ccTLD ISG Managerial Components

This area controls the operation to achieve the objectives and goals and deals with accountability and security management of the ISG. Many components of national and international legislations need to be considered for Internet security, such as security policies, certification, accreditation, security assessments, planning risk assessments, awareness and training, ethical conduct, configuration planning, and configuration management.

Contrary to the popular belief, that security of the Internet is a technical issue, even the best attempts to buy software-based security solutions and build security into the security of the Network and operational systems encounter considerable scepticism and opposition since the problem is mainly organizational, cultural, human behaviour, governance, and not technical. Effective security governance in today's interconnected environment requires integrating legal, managerial, operational, and technical considerations.

2.2.1 Security Management

This category deals with an Internet security framework plan program management that includes awareness, education and training, ethical conduct, security policies, procedures, standards, and guidelines, which are keys to the implementation of a consistent information security program. A continuous program to promote, implement and encourage information security awareness and education should be in place in all the organizations involved. As in COBIT 4.1, DS7, Deliver and Support, Educate and train users [8], and important ingredient of governance is awareness and training.

Awareness, motivation, and compliance are the accepted, expected cultural norm. Security awareness and targeted training are conducted routinely and consistently as part of the user security management program. Security at the country level is essential to maintaining citizens' trust in the continued use of current and future technologies. Governments want to ensure that the country is a 'secure' place to be online and so is keen that people are aware of the associated security threats. Good information security backed up by good governance is viewed as being increasingly important to the success and stability of the country as a whole. The main purpose of awareness is to educate people and change their behaviour.

At the same time, the highest standards of ethical conduct are essential to the success of the concerned organizations to create a trusting environment for governance and management of Internet security, woven

into the very culture and fabric of organizational behaviours and actions.

2.2.2 Accountability

It is essential here to determine who is responsible and accountable for what with clear definitions of the functions and roles and built upon that delegation should be clean and clear. Clean and clear accountability and defining the roles of the different actors are clearly delineated. Each side has a separate, important, and unique role to play in fulfilling the objectives of Internet Security to create good governance. Unclear role definition is often the cause of friction, overlapping jurisdiction, and uncertainty on the authority to act. A RACI Chart [7] could be used to clarify roles and responsibilities in the organization. A RACI chart indicates which role(s) is responsible, accountable, consulted and informed for each key activity—defined as a group of management practices supporting the chart's associated Risk Information Security process.

Leaders are accountable and responsible with respect to the Internet security governance for the registrars, for their stakeholders, for the communities they serve (including the Internet community), and for the protection of critical national infrastructures as well as economic and national security interests. They perceptibly take part in the registrar's organization security governance program and support this work with adequate financial resources, effective management, risk-based policies, and annual evaluations.

2.3 ccTLD Operational Components

This part deals with monitoring, assessing, incident response, compliance, auditing and essentially involves management of incidents, business continuity, system and information integrity. ISG has achievable, measurable objectives that are integrated into strategic, managerial, and operational plans, and are implemented with effective controls and metrics. Reviews and audits of plans identify security problems and deficiencies, requirements for the continuity of operations, and measure progress against plans of action and milestones.

Senior leaders measure this work against defined performance parameters and monitoring, assessing, and compliance are key elements. Acting unified, conforming to certain accepted standards and having the ability to reasonably ensure conformity and adherence to organization policies, plans, procedures, laws, regulations, and contracts are fundamental to a sound ISG program.

Security has achievable, measurable objectives that are integrated into strategic and operational plans, and implemented with effective controls and metrics. Assessments, incident management, and audits help identify security weaknesses and deficiencies, requirements for the continuity of operations, and measure progress against benchmarks already established. Monitoring of the awareness, for example, can be accomplished through yearly audits for compliance with ISO 27001 [9].

3. Creating the index.

There is not a set of metrics universally accepted or embraced as "useful" for the Internet ccTLD Security Governance in the three multi-dimensions of the framework. Related difficulties exist in other fields, where intangible attributes such as health or safety, for example, are difficult to characterize and measure. In each circumstance, the attributes being measured are usually some amalgamation of characteristics, each of which reflects an aspect of the whole. The trouble rests not only in finding an appropriate measure but also in understanding how the whole is constituted from its parts. Furthermore, the measures are often drawn from what is easy or available to measure, not from what is most adequate.

For the three multi-dimensions of this ISG framework for ccTLD registrars, pertinent objective data are difficult to acquire and even where objective measures are available, they provide only imperfect substitutes for real life conditions. However, for the purpose of measuring, evaluating and estimating the effectiveness of the sub components of the ISG maturity framework, the following metrics for the three multi-dimensions are useful:

1. Strategic: measuring quality of Internet security governance in the respective registrar and the allocation of resources are important indicators of the degree of accountability of the registrars. Money (in US$) allocated for Internet Security as a percentage of Internet Governance budget is an important metric in the strategic dimension. The allocation of money for security purposes not only represents resource allocation per se, but also the degree of commitment, leadership, sponsorship, institutional quality the registrar has.

2. Operational: different levels of activities of multiple threats (phishing, spam, DoS attacks, etc.) require different metrics. In case of phishing related to ccTLD, I choose phishing activity within a country domain, more specifically, "Phishing Domains per 10,000".

This is a ratio of the number of domain names used for phishing in a TLD to the number of registered domain names in that TLD. This metric is a way of revealing whether a TLD has a higher or lower incidence of phishing relative to others [11]. Many of the domains used for phishing are registered exclusively for phishing and domain tasting allows a domain registrant to register a domain and return it within 5 days without incurring any financial liability. This practice is feared to be misused in phishing and has been heavily debated in the Internet community and there are talks about ending it due to its misuse [13].

Although we use different measurements in different situations, all measurements have something in common: some aspect of best practices, for example, is assigned a descriptor to allow comparison. In our case, I want to compare the ISG of one registrar (country) with another, or to one used as a benchmark.

"Measurement is the process by which numbers or symbols are assigned to attributes of entities in the real world in such a way as to describe them according to clearly-defined rules" [12]. A measurement mapping is therefore, a function associating an element in its real-world domain with a quantitative or qualitative element in its mathematical-world range. This mapping preserves relationships for a given attribute, so that what happens in the real world is reflected in what happens in the mathematical world.

The explanation for the maturity process of the ISG is the following: to reach any particular level of ISG, all the preceding stages in each of the dimensions must be true. For example, to reach level 2, all statements in stages 1 of the 3 components of the framework must be true; and if all stages 2 statements are true we move on to level 3 and so on. As soon as we find one statement in a stage that is untrue, we slip back to the previous level of ISG and this is the current "level of maturity of the ISG for the ccTLD registrar" i.e. all statements at a particular stage have to be true in order to achieve that level. Level 5 should be the aspiration that most registrars (countries) should aspire and all statements in stage 4 of each dimension must be true to achieve this level. In summary, the possible levels for the ISG are from 1 to 5.

Each level of maturity of the Internet Security Governance for the registrars is described in detail.

1. Level 1– Initial or started

This level has no strategic vision, leadership, and resource allocation for ISG. The domain registrar has not yet established its key policies, practices, or control framework for ISG. Absence of compliance, assessing, monitoring, and auditing. Achievement of the registrar's objectives for ISG depends on isolated efforts. This level represents the initial state of the maturity of the ISG in the three dimensions: strategic, managerial, and operational.

2. Level 2 – Controlled or repeatable

Some initial stages in the three dimensions of ISG. Control framework is in place to provide a stable environment and to ensure that control practices for ISG are repeatable and sustainable. Key processes for ISG defined and instituted and statutory requirements are met. Management is aware but control weakness remains. Successfully repeating previously mastered tasks, to avoid recurrent failures brings a registrar to Level 2.

3. Level 3 – Implemented and integrated

This level is divided in two: Implemented represents taking measures to ensure the implementation of the procedures and best practices across the entire registrar through communication and promotion of ISG. Processes are formally defined, documented and integrated into a standard process that is understood and followed. Information is used to produce guidelines and to provide valuable support to operational managers. In the integrated level, it goes a step further with quality by creating processes, establishing activities to measure, and monitoring risks to ISG, and high standard procedures for improving ISG.

4. Level 4 – Managed

It uses the information developed in the previous levels to balance competing objectives of effectiveness, efficiency and accountability of ISG in the three dimensions. It focuses on the process controls in place to measure quality and information to make informed decisions is available and used in a way that facilitates management choices. Detailed measures of the management processes are collected and used to identify and improve issues with ISG. The measured data enables to assess the success of the adjustments made and a managed process for these continuous improvements helps to establish and maintain a high performing registry.

5. Level 5 – Optimized

The focus is on continuous improvement and optimizing existing processes for ISG. The registry at this level will be equipped to proactively address the strengths and weaknesses of ISG issues in the different dimensions and instead of correcting defects as they occur, quality efforts will focus on prevention and will also anticipate root case scenarios. This level is the premier level of optimization.

The following figure depicts graphically the risk-based ISG maturity framework containing strategic, managerial, and operational elements and maps these components to the corresponding ISG maturity level according to the resulting combination in the different dimensions. We can also call it the Maturity Matrix of the ISG. This matrix uses different "stages of excellence" and maps these against the different Internet ccTLD Security Governance Levels. Level 5 should be the aspiration of all registrars.

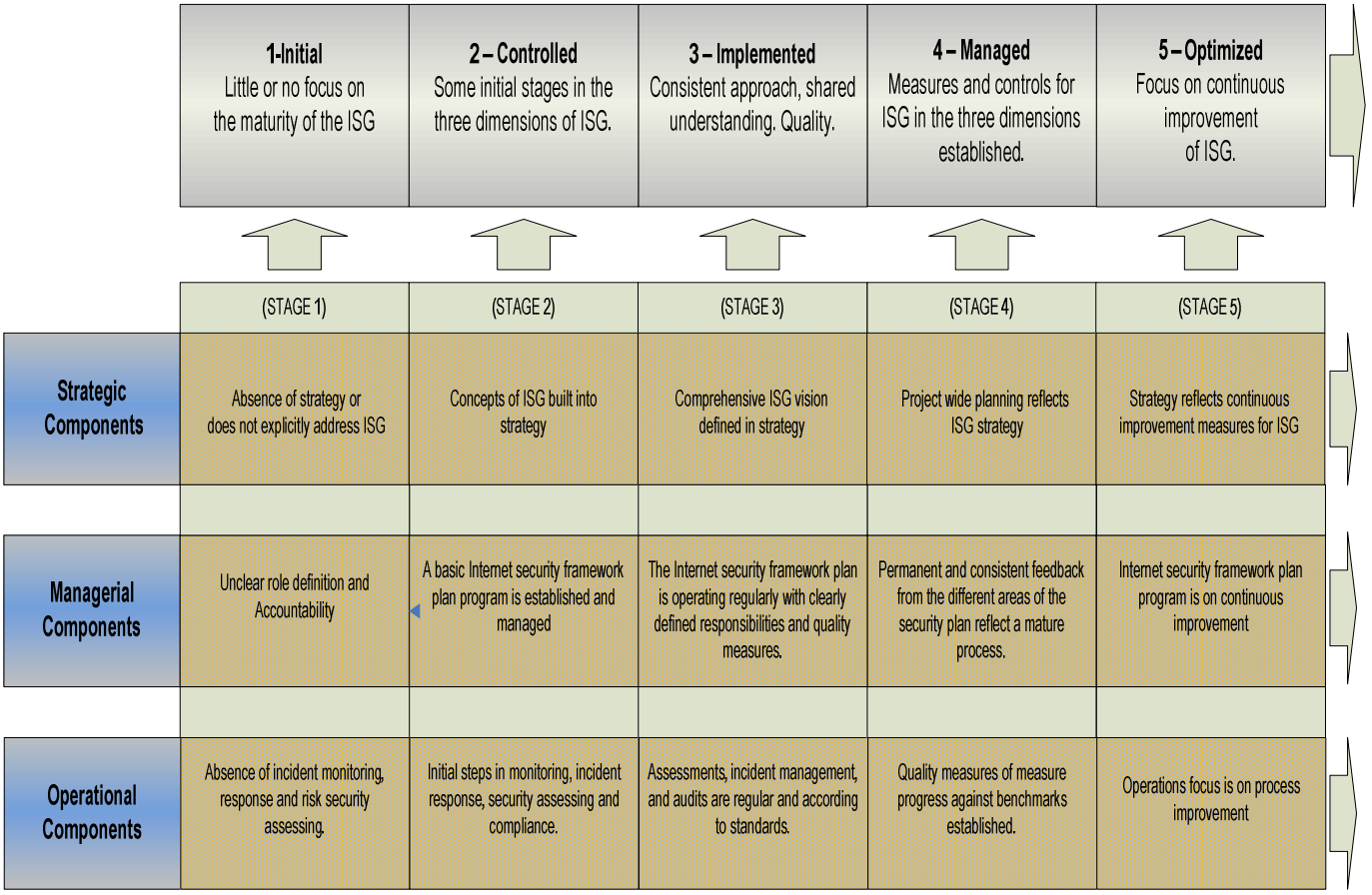

Fig 1. Maturity Matrix of the Internet Security Governance

Each of the aforementioned maturity levels for each dimension is assigned a number from 1 to 5 and the lowest of the 3 dimension values is the final Internet Security Governance value. For example, if the registrar is in stage 5 (strategic), stage 5 in managerial, and stage 4 in operational, the current level of maturity of the ISG is 4. All statements at a particular stage have to be true in order to achieve that level. Level 5 should be the aspiration of all registrars and the adequate implementation of a good ISG risk management process can get registrars to Level 5. In addition, the three components need to be aligned to have a consistent measure.

The different "stages of excellence" of the matrix are mapped against the various Internet ccTLD Security Governance Levels.The following figure shows the results of the the different Internet ccTLD Security Governance Levels of the three combined dimensions.

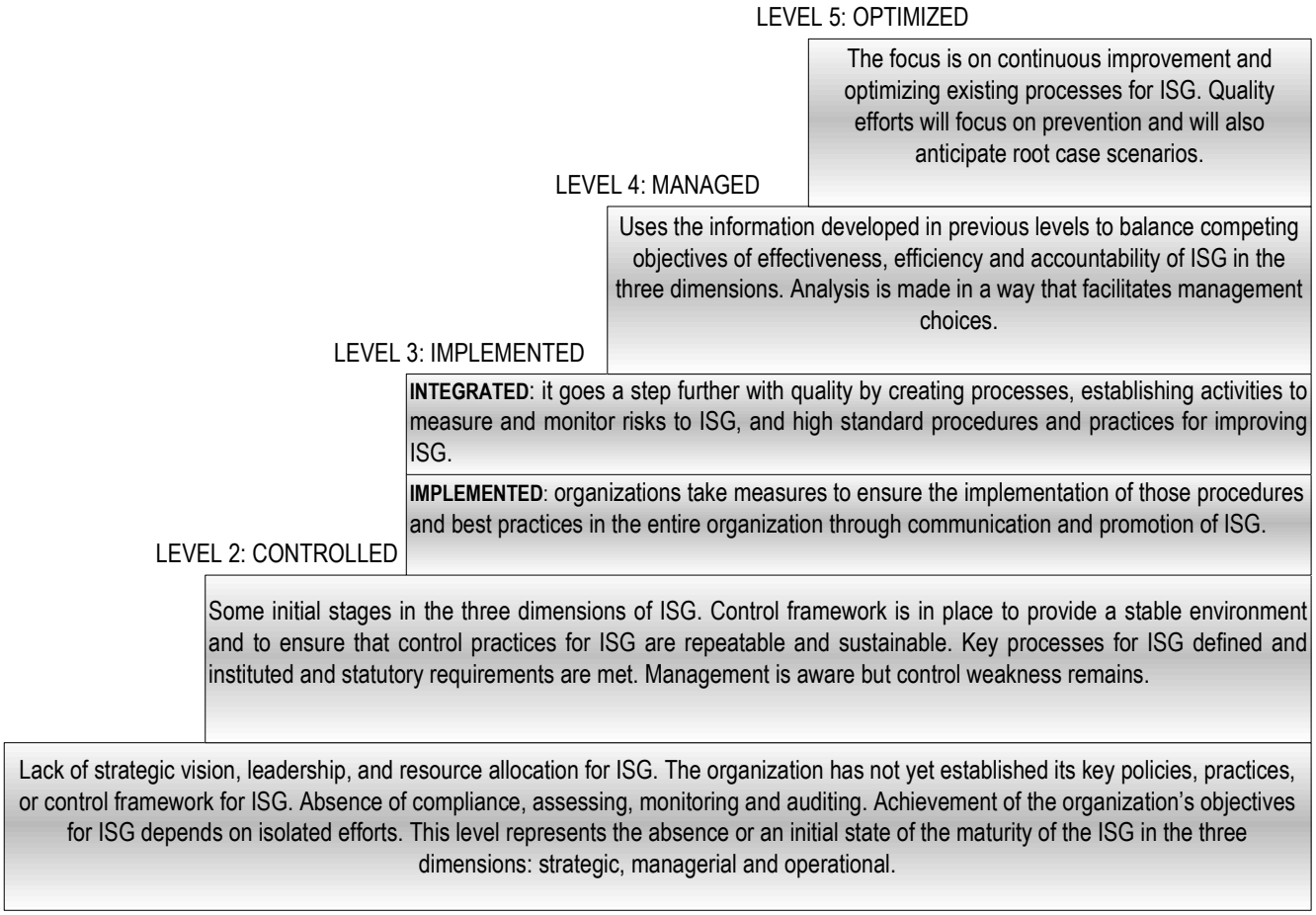

Fig 2. Graphic of the different Internet ccTLD Security Governance Levels.

4. METHODOLOGY

We need metrics to measure the effectiveness of the sub components of the ISG maturity framework in each of the dimensions. In the operational dimension – a subset of the whole risk-based framework – we can have many indicators: phishing related to ccTLD, spam, spyware, etc. Since we are testing part of the framework of this multidimensional risk-based index for the ISG on the ccTLD, we use the metric from the new Global Phishing Survey released by the Anti-Phishing Working Group (APWG) [11], "Phishing Domains per 10,000". This metric compares the number of established phishing domains to the total number of registered domain names in that TLD. The criteria for selecting countries in table 2 were according to the level of phishing activity, more specifically, Phishing Domains per 10,000 and then assigning a Maturity level rating according to the ranges given in Table 1. In addition to that, the domain registration policies were assigned a number according to the level of strictness of policies and procedures to get a TLD: very strict=5; the least strict=1.

Range of score: phish per 10,000 domains 2H2008	Maturity Level rating from 1 to 5 (operational component)	Domain Registration Policies. Strictness of policies and procedures: 5 very strict; 1 least strict (managerial component)
From 0.0 to 1.5	5	5
From 1.6 to 2.5	4	4
From 2.6 to 3.5	3	3
From 3.6 to 5.0	2	2
Greater than 5.0	1	1

Table 1. Phishing scores ranges and corresponding Maturity Level ratings for operational sub component and level of strictness of policies and procedures.

A paper, where domain registration policies (managerial) are correlated with the level of phishing (operational) activity within its country domain is [14]. This could give a feeling of déjà vu, but the objectives are different.

4.1 Data sources

The data in columns 1 to 5 in the Table 2 related to phishing statistics were sourced from the APWG [11]. The metric "Phishing Domains per 10,000" was selected and represents the ratio of the number of domain names used for phishing in a TLD to the number of registered domain names in that TLD and is a method of showing whether a TLD has a higher or lower prevalence of phishing comparative to others. The data in column 7, domain registration rules, were sourced from [16].

The criteria for selecting the data were a minimum of 25 phishing domains and 30,000 domain names in registry. The phishing attacks and average uptimes were not considered. At the same time, data other than that related to ccTLD were not considered.

4.2 Data analysis

Considering the data in Table 1, a decrease in the score of phishing is often associated as an increase of the ISG of a registar in the operational dimension – but this assumption is not always valid; the three dimensions of the framework related to the ccTLD need to be considered. This means that the phishing score is only part of the picture and is affected by the other two dimensions: strategic and managerial. Anti-phishing policies, best practices, and mitigation programs by domain name registrars and registries can have a significant and positive effect. At the same time, adequate resource allocation (money, technical, human) and sponsorship can influence the final level of the ISG maturity.
In most countries, there is a correlation between the "phishing per 10,000 domains" and the strictness of policies and procedures in that country, showing that weak (or strong) anti-abuse policies and procedures can have a tremendous impact on the level of security of the Internet.

There are some interesting cases, like Venezuela (.VE). "In late 2008, the .VE registry was taken advantage of by phishers who registered .VE domains to mount attacks against eBay and PayPal, supported by fast-flux hosting.
NIC.VE provides services under a combined registry/registrar model, and works under a branch of the Venezuelan government. The phishers began with a probing set of attacks in July. NIC.VE's policy required it to seek various authorizations before acting, and as a result phishing remediation times measured in weeks. There was also a shift in how the registry was managed within the government, exacerbating the situation. The phishers realized they had found a reliable and weakly defended source of domains [11]". This helped NIC.VE put new policy and procedures in place, which allowed it to make prompt domain suspensions. This efficacious response drove the phishers away, and the attacks dropped. Something similar happened with Hong Kong (.HK) in the past with high phishing scores also attributed to the Rock Phish Gang who systematically abused weakness in the .HK registry anti-phishing capabilities and the phishing score dropped dramatically due to the implementation of anti-phishing best practices within their domain.

Chile, with a high phishing score, is the result of a weak strictness of policies and procedures. A good example is the website www.gooogle.cl with 3 "o" instead of 2 (typosquatting, or URL hijacking), which is considered perfectly legal and considered "a business with great vision" by some. This contrasts with the good level of governance in other areas, though.
An interesting case is Tokelau (TK), with a population of less than 1,500 people and 1,880.000 domains in registry that has added more than 10% to its GDP (Gross Domestic Product) through registrations of domain names under its top-level domain and has very weak strictness of policies and procedures.

Another interesting case is China that has strict policies and also restrictions for registering domain names like limiting the content of those that spread pornography, obscenity, gambling, violence, homicide, terror or instigate crimes; rumors, disturb public order or disrupt social stability, instigate hostility or discrimination between different nationalities, or disrupt the national solidarity. More details in [16].

A decrease in phishing score is often interpreted as an increase in security and better governance – but this assumption is not always valid. What is often measured does not necessarily and accurately indicate the registrar's overall security (or quality of ISG). This is part of the story, and management must take a wide variety of evaluations to capture the overall picture of ISG and the three components (strategic, managerial and operational) must be correctly aligned to have a consistent and good level of ISG for the registrars.

Table 2. Phishing related to ccTLD and corresponding stage (Operational component); strictness of registration rules.
Minimun 25 phishing domains and 30,000 domain names in registry

TLD	TLD Location	Unique Domain Names Used for Phishing 2H2008	Domains in Registry in Dec-08	Score: Phish per 10,000 domains 1H2008	Maturity Level Rating (1 to 5)	Domain Registration Rules (1:weak; to 5:strong)
cn	China	499	13,572,326	0.4	5.0	5.0
de	Germany	834	12,402,383	0.7	5.0	5.0
tk	Tokelau	132	1,880,000	0.7	5.0	2.0
ws	Samoa	40	544, 000	0.7	5.0	4.0
ar	Argentina	149	1,826,634	0.8	5.0	5.0
eu	European Union	234	2,988,269	0.8	5.0	5.0
se	Sweden	71	834,886	0.9	5.0	5.0
ch	Switzerland	110	1,244,567	0.9	5.0	4.0
dk	Denmark	107	965,816	1.1	5.0	5.0
nl	Netherlands	338	3,191,127	1.1	5.0	4.0
nz	New Zealand	37	348,769	1.1	5.0	4.0
no	Norway	50	412,839	1.2	5.0	5.0
pt	Portugal	34	275,972	1.2	5.0	5.0
uk	United Kingdom	886	7,310,000	1.2	5.0	4.0
it	Italy	214	1,622,938	1.3	5.0	5.0
at	Austria	116	799,562	1.5	5.0	3.0
us	United States	216	1,434,301	1.5	5.0	4.0
za	South Africa	66	437,000	1.5	5.0	4.0
fi	Finland	31	198,000	1.6	4.0	5.0
hu	Hungary	69	400,000	1.7	4.0	4.0
br	Brazil	273	1,535,117	1.8	4.0	4.0
sk	Slovakia	31	172,500	1.8	4.0	5.0
tr	Turkey	33	180,065	1.8	4.0	5.0
au	Australia	250	1,286,439	1.9	4.0	4.0
ca	Canada	212	1,136,411	1.9	4.0	5.0
in	India	105	501,155	2.1	4.0	2.0
cz	Czech Republic	111	506,258	2.2	4.0	5.0
hk	Hong Kong	38	173,651	2.2	4.0	5.0
pl	Poland	303	1,350,138	2.2	4.0	2.0
es	Spain	253	1,082,757	2.3	4.0	4.0
jp	Japan	242	1,062,731	2.3	4.0	4.0
il	Israel	38	139,243	2.7	3.0	3.0
lt	Lithuania	25	94,000	2.7	3.0	2.0
sg	Singapore	31	114,549	2.7	3.0	4.0
ua	Ukraine	107	397,051	2.7	3.0	4.0
be	Belgium	240	859,474	2.8	3.0	2.0
gr	Greece	71	250,000	2.8	3.0	3.0
ir	Iran	29	102,800	2.8	3.0	4.0
mx	Mexico	80	277,652	2.9	3.0	4.0
my	Malaysia	25	80,786	3.1	3.0	4.0
fr	France	430	1,289,599	3.3	3.0	4.0
tw	Taiwan	144	406,669	3.5	3.0	2.0
ru	Russian Fed.	676	1,860,179	3.6	2.0	2.0
vn	Vietnam	37	92,992	4.0	2.0	2.0
kr	Korea	413	983,626	4.2	2.0	4.0
cl	Chile	116	232,897	5.0	2.0	3.0
ro	Romania	188	310,114	6.1	1.0	4.0
su	Soviet Union	76	85,119	8.9	1.0	2.0
bz	Belize	55	43,377	12.7	1.0	2.0
th	Thailand	88	39,880	22.1	1.0	4.0
ve	Venezuela	1,504	82,500	182,3	1.0	2.0

4.3 Discussion

A limitation of this index is the difficulty in precisely measuring Internet ccTLD Security Governance due to the difficulty not only in finding an appropriate measure but also understanding how the whole is formed from its parts. Furthermore, the measures are often drawn from what is available or easy to measure and not from what is most adequate. In addition, its intangible and subjective nature makes it difficult to define and measure abstract attributes in the different dimensions and hence has complicated the development of these metrics. No suggested set of metrics is universally accepted or embraced as applicable or "useful", and no framework let registrars answer their vast variety of questions about the governance of the Internet security. Attributes being measured are usually some combination of characteristics, which are often subjective in nature and reflect a restricted aspect of the whole. The difficulty rests not only in finding a suitable measure but also in understanding how the whole is constituted from its parts.

The dynamic nature of the Internet imposes an additional factor to consider in measuring a variety of data, system, and network characteristics and then combining them to see changes at different levels, so that registrars need to recognize and understand emergent behaviours.

5. CONCLUSIONS

It is necessary for ISG to be recognized as a multidisciplinary management task at the highest level of leadership and reinforcing the concept of inclusiveness of Governments, the private sector and civil society in the mechanisms of ISG.

The proposed framework and index should help reflect the evolving process of Internet Security Governance for the registrars and serve as a benchmark for best practices in effective ISG. Determining what policies, laws, regulations to promote trust as a consequence of adequate ISG within a registrar is a challenging proposition.

This research is an invitation to future studies in the ever changing ISG scenario and further research is needed to gain better understanding of the multiple factors that affect the Internet ccTLD Security Governance.

6. REFERENCES

[1] Adel M. Abdellatif, Good Governance and Its Relationship to Democracy & Economic Development. Regional Bureau for Arab States, UNDP, Ministry of Justice Republic of Korea, May 2003.

[2] Suchitra Punyaratabandhu, Commitment to good governance, development, and poverty reduction: methodological issues in the evaluation of progress at national and local levels. National Institute of Development Administration Bangkok, Thailand, 2004.

[3] Larry Diamond, Democracy, Development and Good Governance: The Inseparable Links, Hoover Institution, Stanford University at the Maiden Annual Democracy and Governance (Kronti ne Akwamu) Lecture of the Ghana Center for Democratic Development (CDD-Ghana) British Council Hall, Accra, Ghana, March 1, 2005.

[4] John Mathiason, Internet Governance Project, Internet Governance Wars, Episode II: the Realists Strike Back R., July 3, 2006.

[5] Mårten Simonsson and Pontus Johnson, Ph.D, Defining IT Governance – A Consolidation Of Literature, Department of Industrial Information and Control Systems, Royal Institute of Technology (KTH), Osquldas väg 12, 7tr S-100 44 Stockholm, Sweden, 2005.

[6] Eric Craymer, Strategic Planning with Policy Governance: The Board's Role. http://www.policygovpartners.com.

[7] Royston Morgan, How to Do RACI Charting and Analysis: A Practical Guide, December 7, 2008.

[8] "COBIT 4.1", IT Governance Institute, ISBN 1-933284-72-2, USA, 2007.

[9] International Organization for Standardization (ISO), ISO/IEC 27001:2005, http://www.iso.org/iso/catalogue_detail?csnumber=42103

[10] European Network and Information Security Agency (ENISA), Information security awareness initiatives: Current practice and the measurement of success, July 2007.

[11] Greg Aaron and Rod Rasmussen, Global Phishing Survey: Trends and Domain Name Use in 2H2008, May 2009.

[12] N. Fenton and S.L. Pfleeger, Software metrics: A rigorous and Practical Approach, 2nd ed., PWS Publishing, 1996.

[13] D. Kevin McGrath, Minaxi Gupta, Behind Phishing: An Examination of Phisher Modi Operandi, Computer Science Department, Indiana University, Bloomington, IN, U.S.A., 2008.

[14] Michael B. Hyacintho, Internet Security Governance: Comparative Analysis of Country Code Top Level Domain (ccTLD) Administration, Concordia University College of Alberta, December 2008.

[15] "ISM3", Information Security management Maturity Model, The ISM3 Consortium, ISBN 978-84-613-0541-4, Spain, 2009.

[16] Domain Registration Rules, International Domain Rules, http://www.101domain.com/rules.html.

[17] CMMI for Services, Version 1.2, CMMI Product Team, Software Engineering Institute, Carnegie Mellon University, 2009.