Countering Security Risks at ccTLD Level and SSR

Jay Rajasekera
International University of Japan
Minamiuonuma City, JAPAN 949-7277
jrr@iuj.ac.jp

&

Suvashis Das
Nagaoka University of Technology
Nagaoka, JAPAN 940-2188

Acknowledgement:

We would like to thank Professor Yoshiki Mikami, Professor Ashu Marasinghe, and Dr. Shigeaki Kodama of Nagaoka University of Technology, Niigata, Japan and Japan Science and Technology Agency (JST) for their support for conducting this research.

Critical Factors for ccTLD Security

- How well informed about threats, the end users under a ccTLD are?
- What kind of technologies are being used by the ccTLD?
- How often maintenance and reassessment of current defense policies are done and so on…

Ref:

OECD-2009

Asia Pacific Top Level Domain Association

ICANN

ccNSO

SSR Strategic Plan for ccTLD

- Ref: ICANN-2009
- Ref:
- “Plan for Enhanced Internet **Security, Stability and Resiliency**”
- The basic role for ccTLDs is to work closely with ICANN to foster enhanced Security, Stability and Resiliency (**SSR**)

TLD Security, Stability & Resiliency Collaboration

(Security)

Objectives

- Mature Attack & Contingency Response Program
- Establish joint ISOC/ICANN tech training program
- Establish TLD exercise planning workshops
- Establish program metrics

Deliverables (milestones)

- Conduct ACRP training sessions (5 in 2009); automate planning tool by Aug 09)
- Joint technical training with ISOC plan (approve summer 09); first full program conducted fall 2009; two more by 2009)
- Conduct exercise planning workshops (initial implementation Oct 2009)
- Prototype metrics based on Resiliency Engineering Framework (fall 2009)

Key Stakeholders

- ccTLD operators
- ccNSO, regional TLD operators
- ISOC/NSRC
- ICANN staff

Resources (FY 10)

Human – 1 FTE

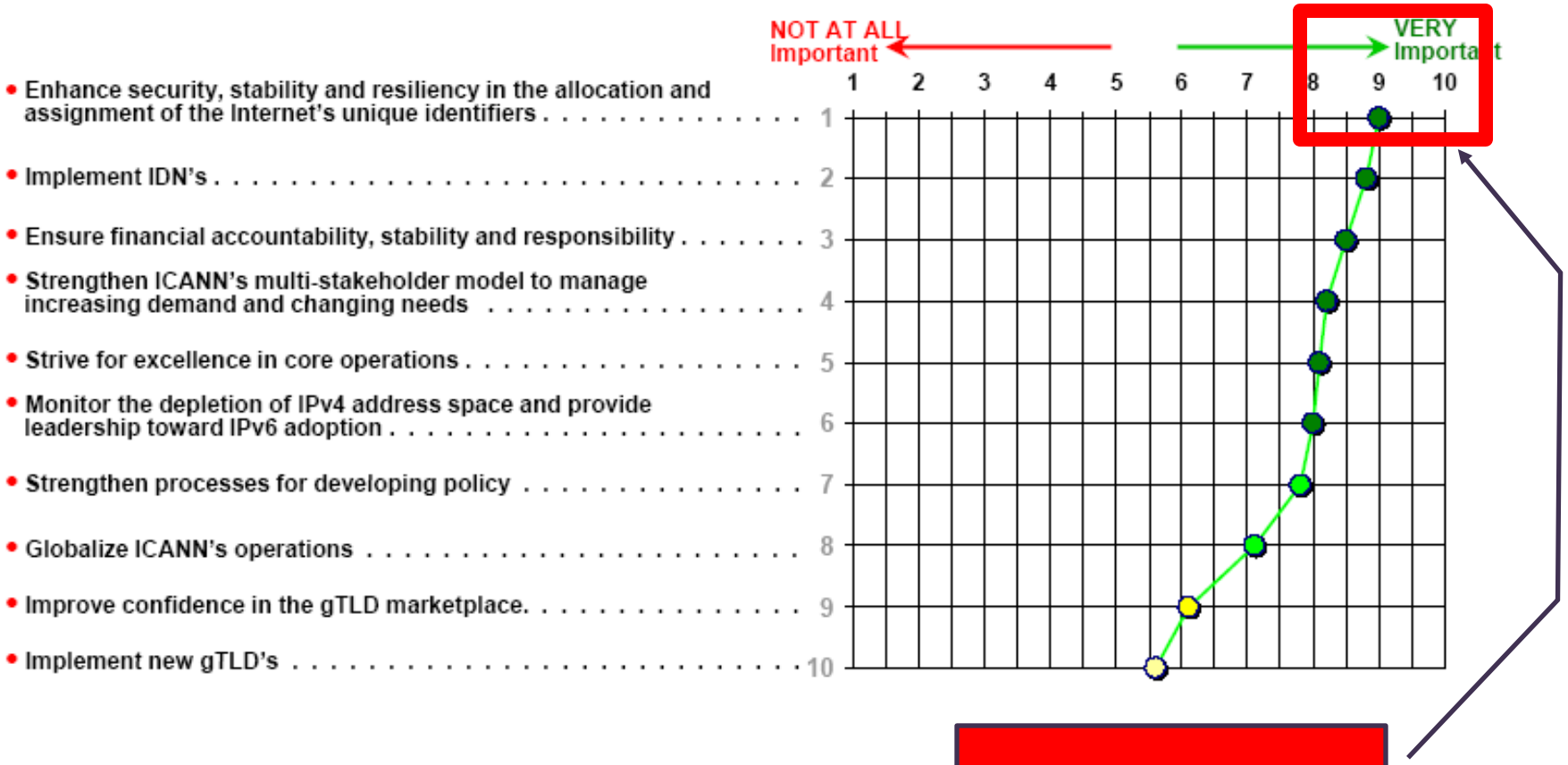
Financial – $650K for FTE, staff/travel to support; professional services for developing and conducting training programs

Ref: ICANN: PLAN FOR ENHANCING INTERNET SECURITY, STABILITY, AND RESILIENCY Approved Draft – 16 May 2009

Smith + Partners Inc.
Marketing Consultants

ATTITUDES TOWARD STRATEGIC PRIORITIES

PERCEIVED IMPORTANCE OF INDIVIDUAL PRIORITIES DEFINED IN THE 2009-2012 STRATEGIC PLAN FOR *ICANN* TO BE WORKING ON



Ref: Survey among members of the ccNSO Committee

SSR is the most important

Our Mission

Our research aims to find measures at ccTLD level that would eventually lead to an Internet with enhanced Security, Stability and Resiliency (SSR)

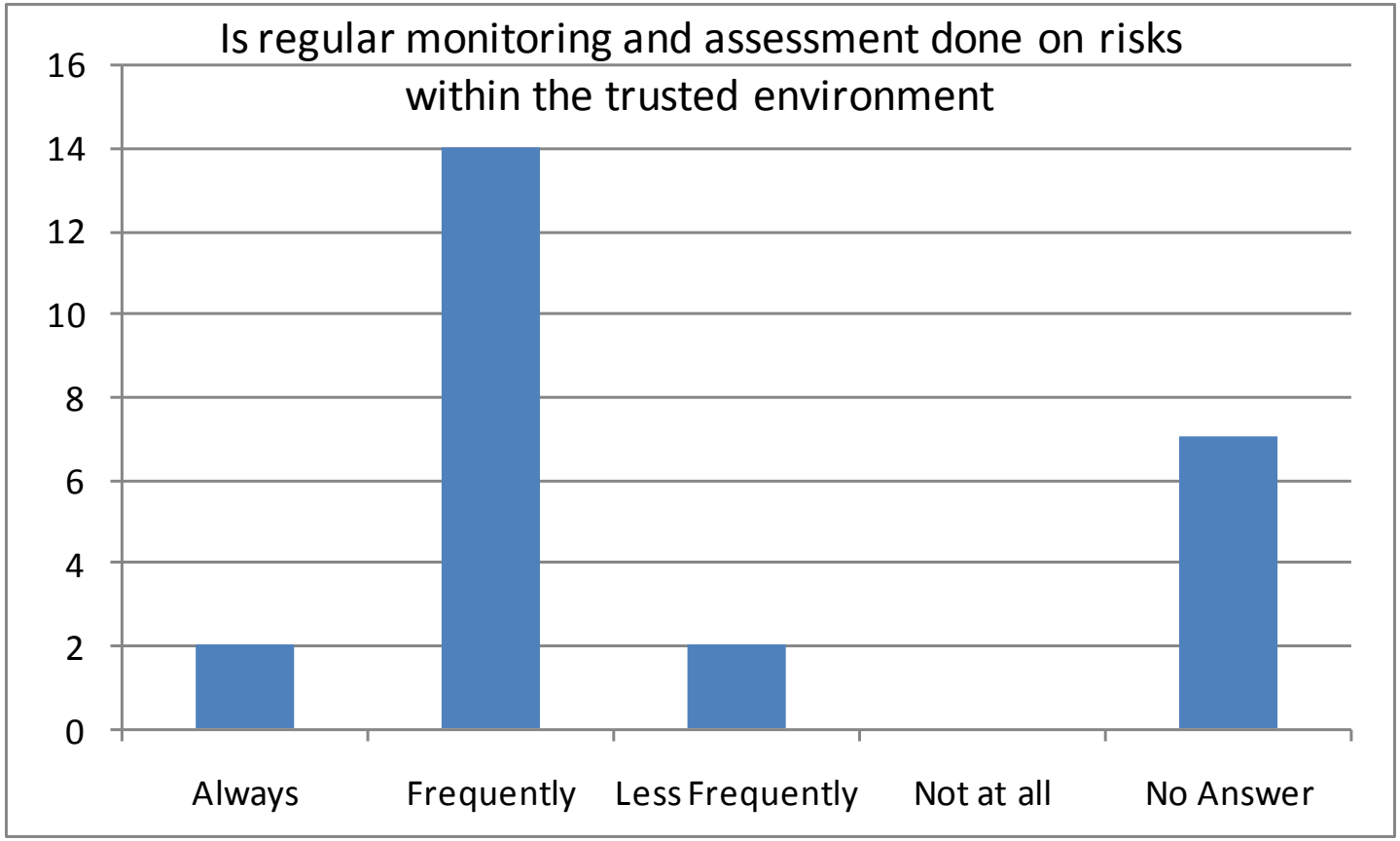
- Survey conducted at IGF 2009
- Ongoing survey involving ccTLD administrators
- Security Alert Maps

Survey Results (As of Now)

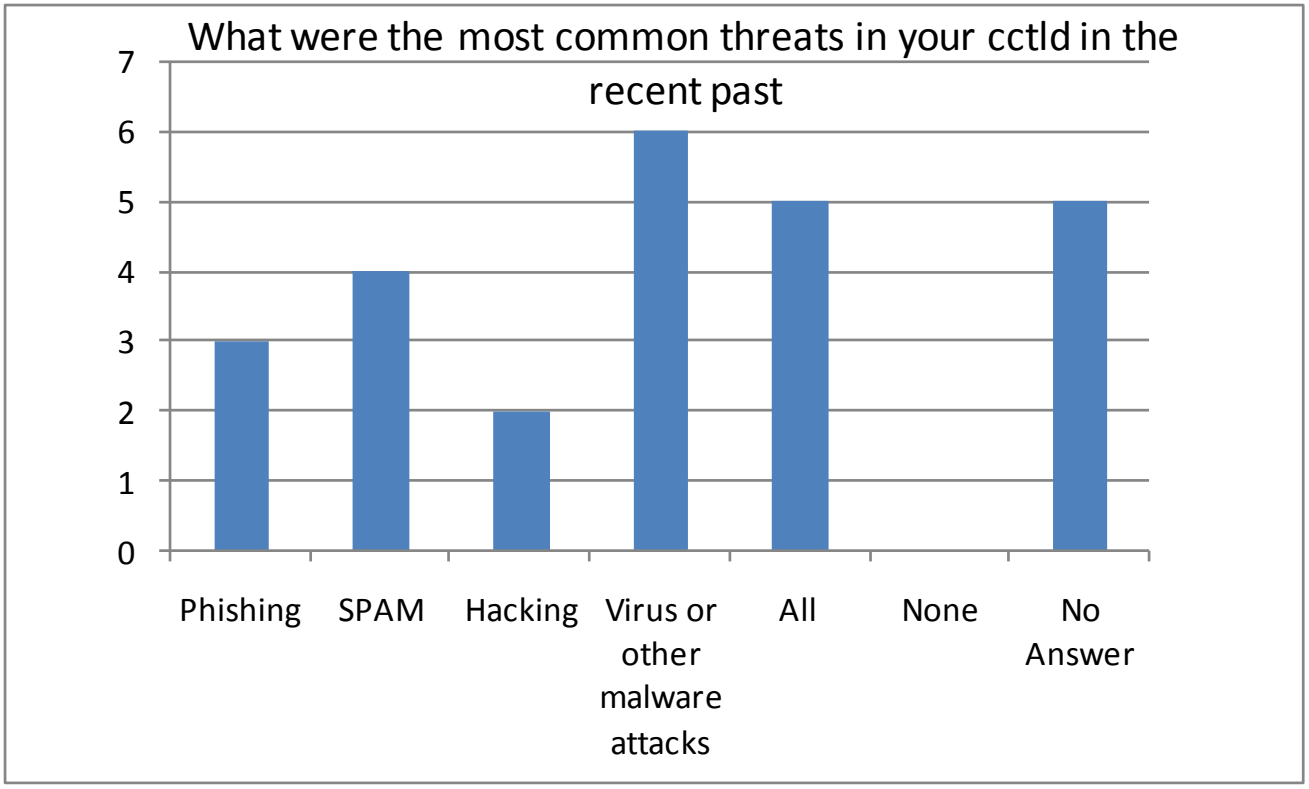
We sent around 150 questionnaires in seminars in different conference rooms related to ccTLD practices.

Out of them 25 of the questionnaires were returned to us bearing meaningful results.
We summarize it here

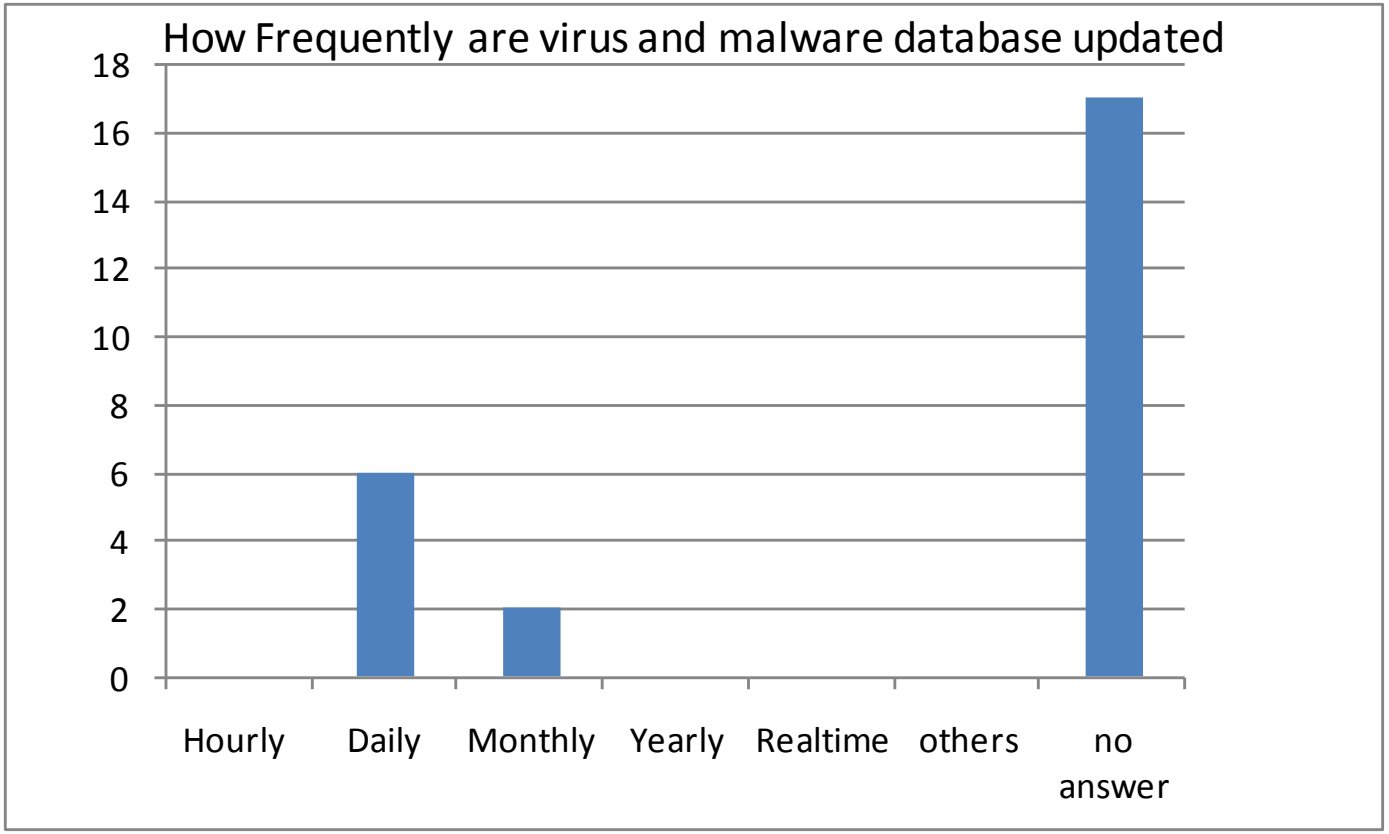
Question 1: Is regular monitoring and assessment done on risks within the trusted environment



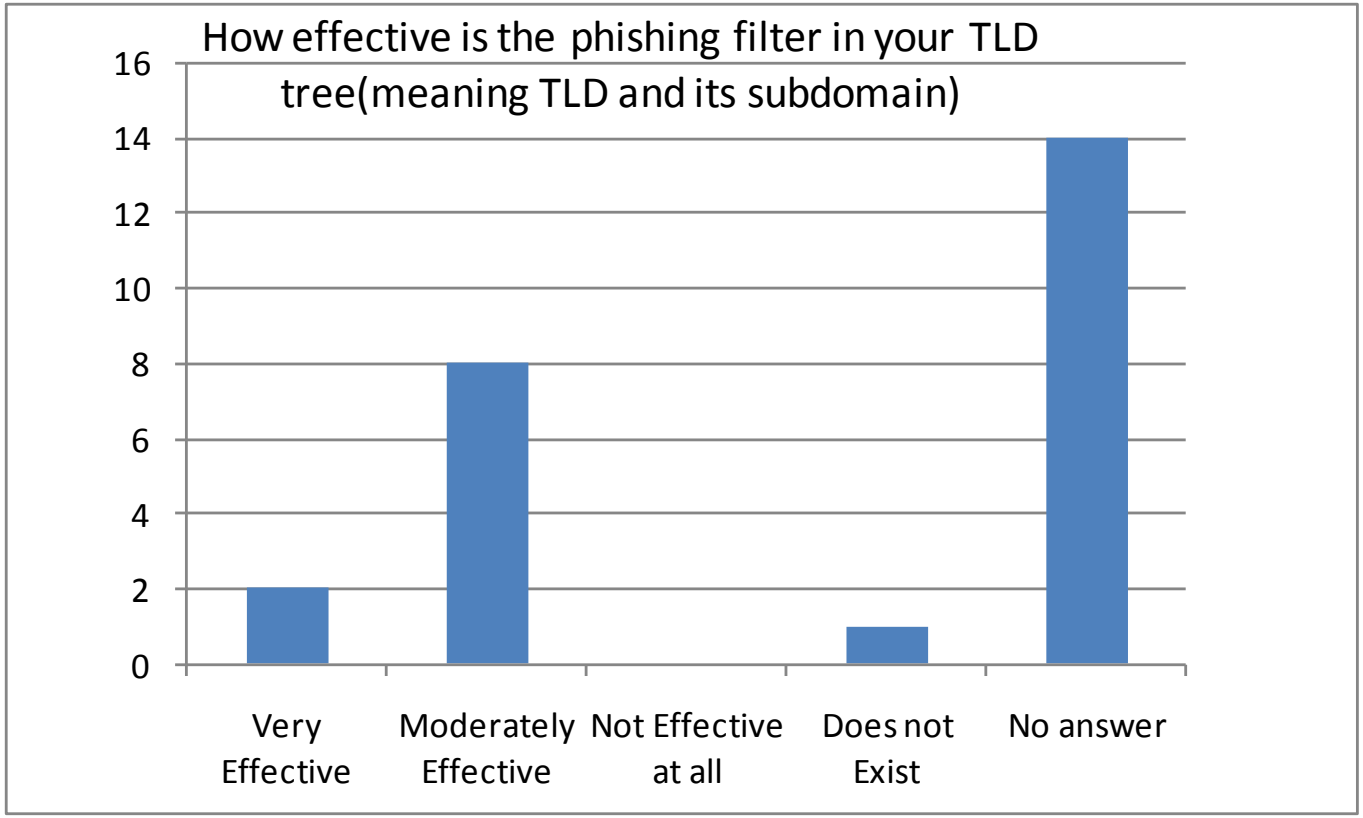
Question 2: What were the most common threats in your ccTLD in the recent past



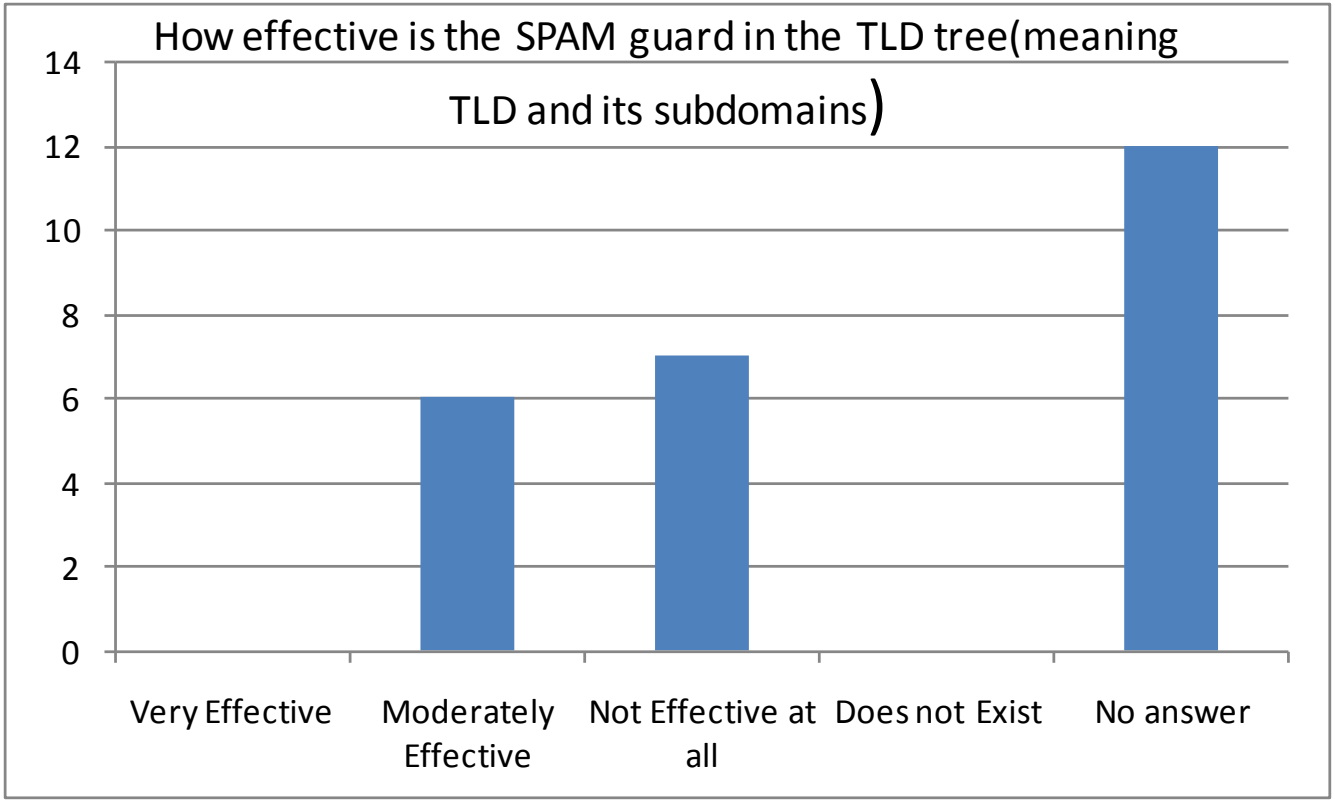
Question 3:How Frequently are virus and malware database updated



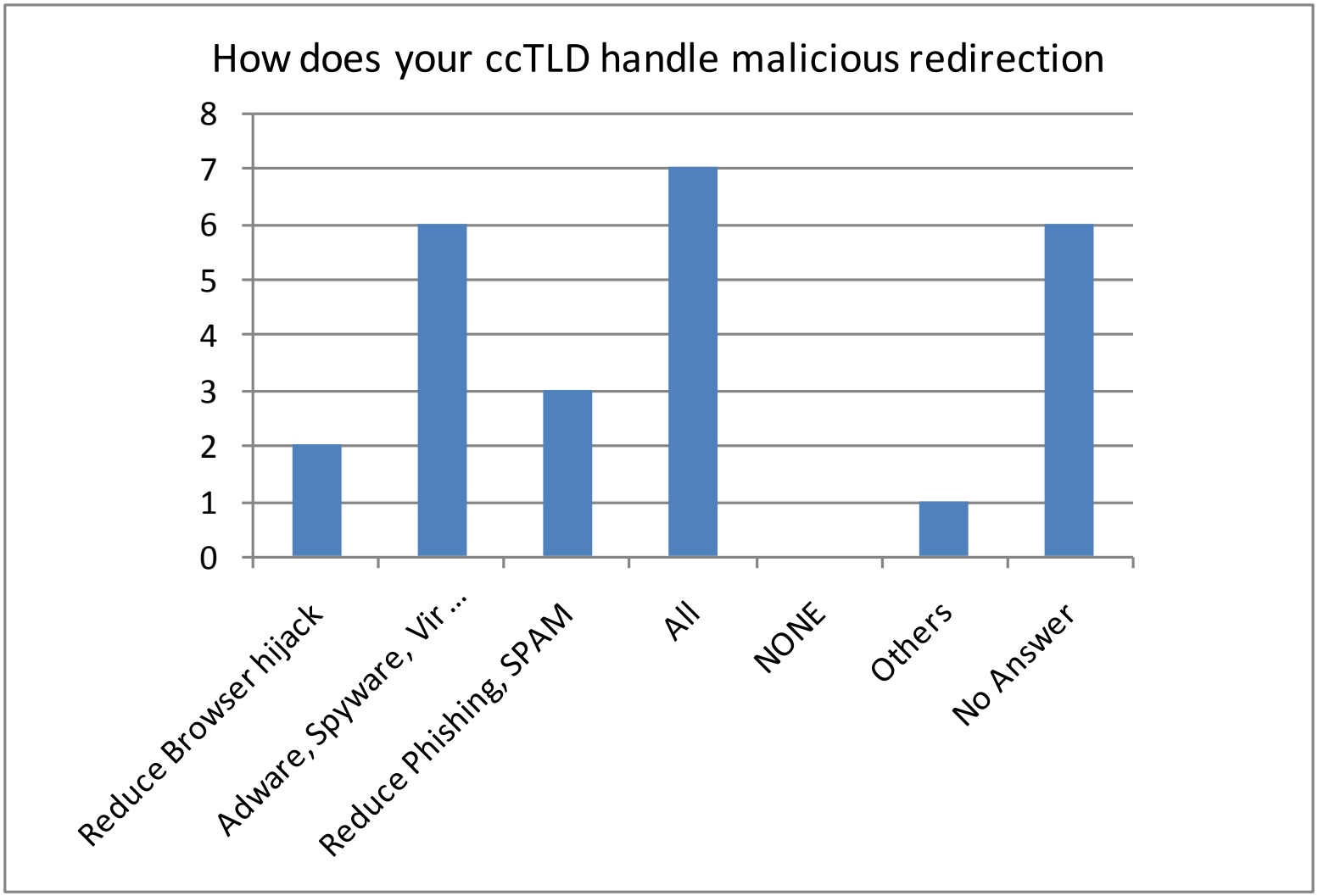
Question 4: How effective is the phishing filter in your TLD tree(meaning TLD and its sub domain)



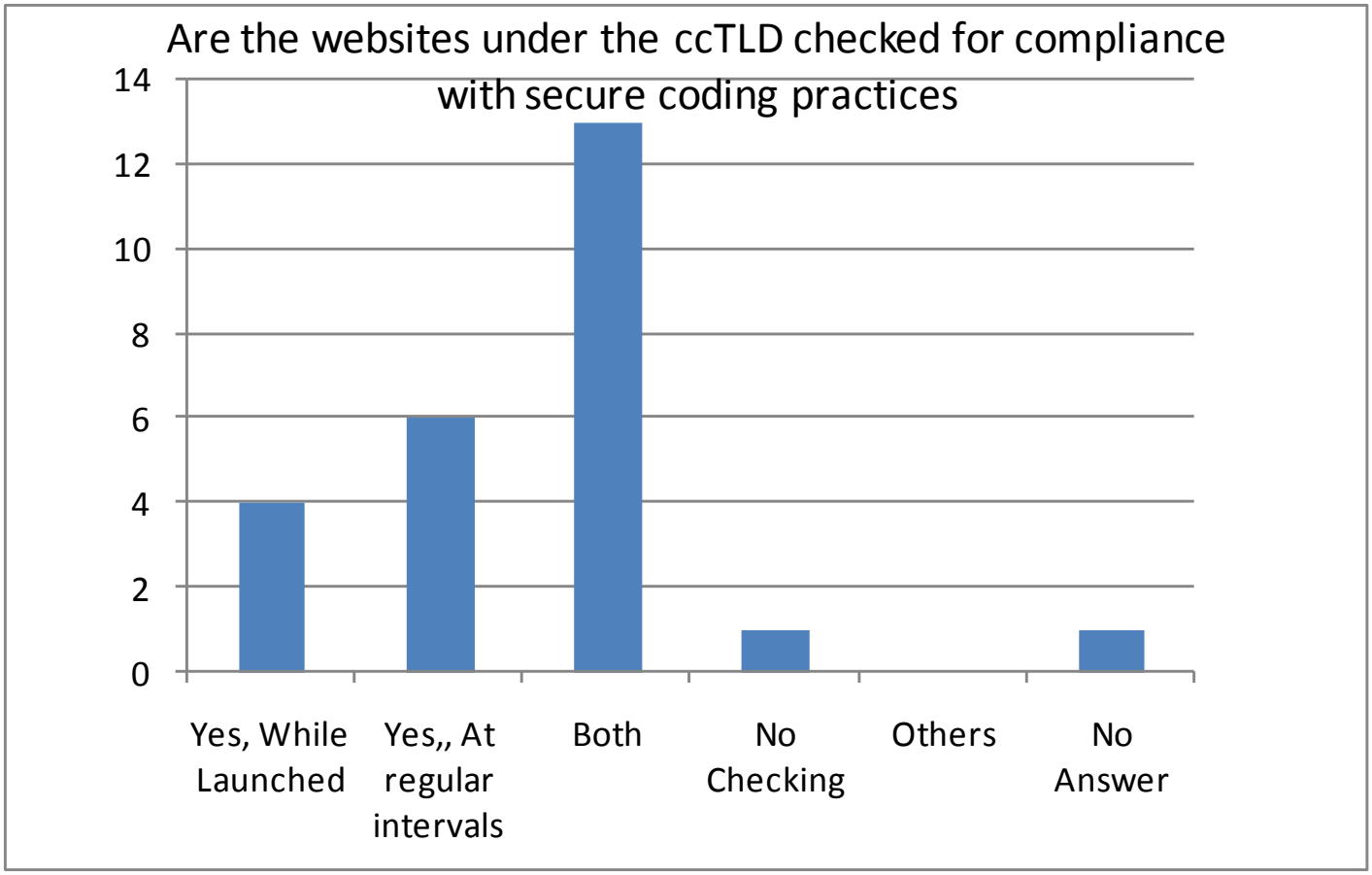
Question 5: How effective is the SPAM guard in the TLD tree(meaning TLD and its sub domains)



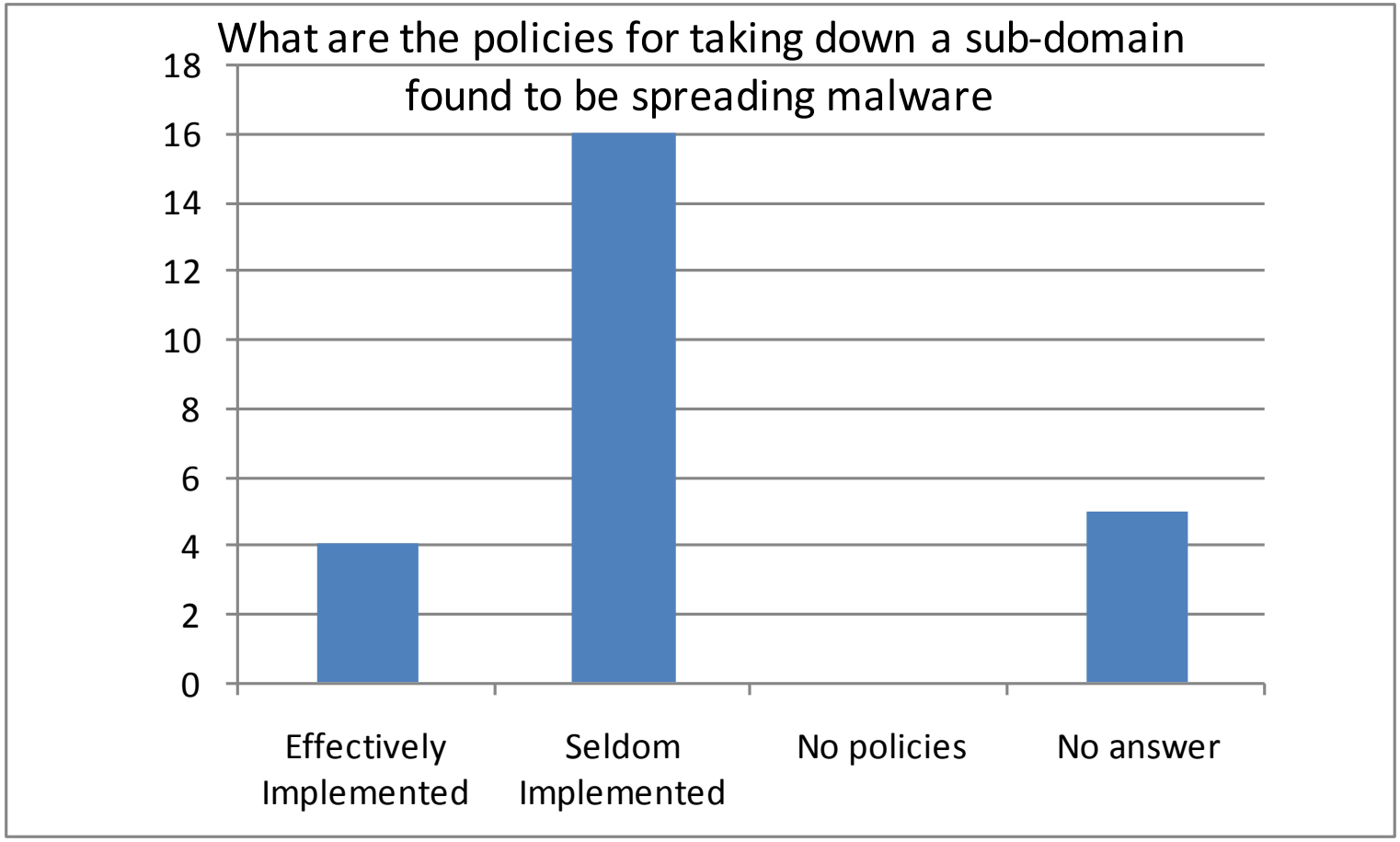
Question 6: How does your ccTLD handle malicious redirection



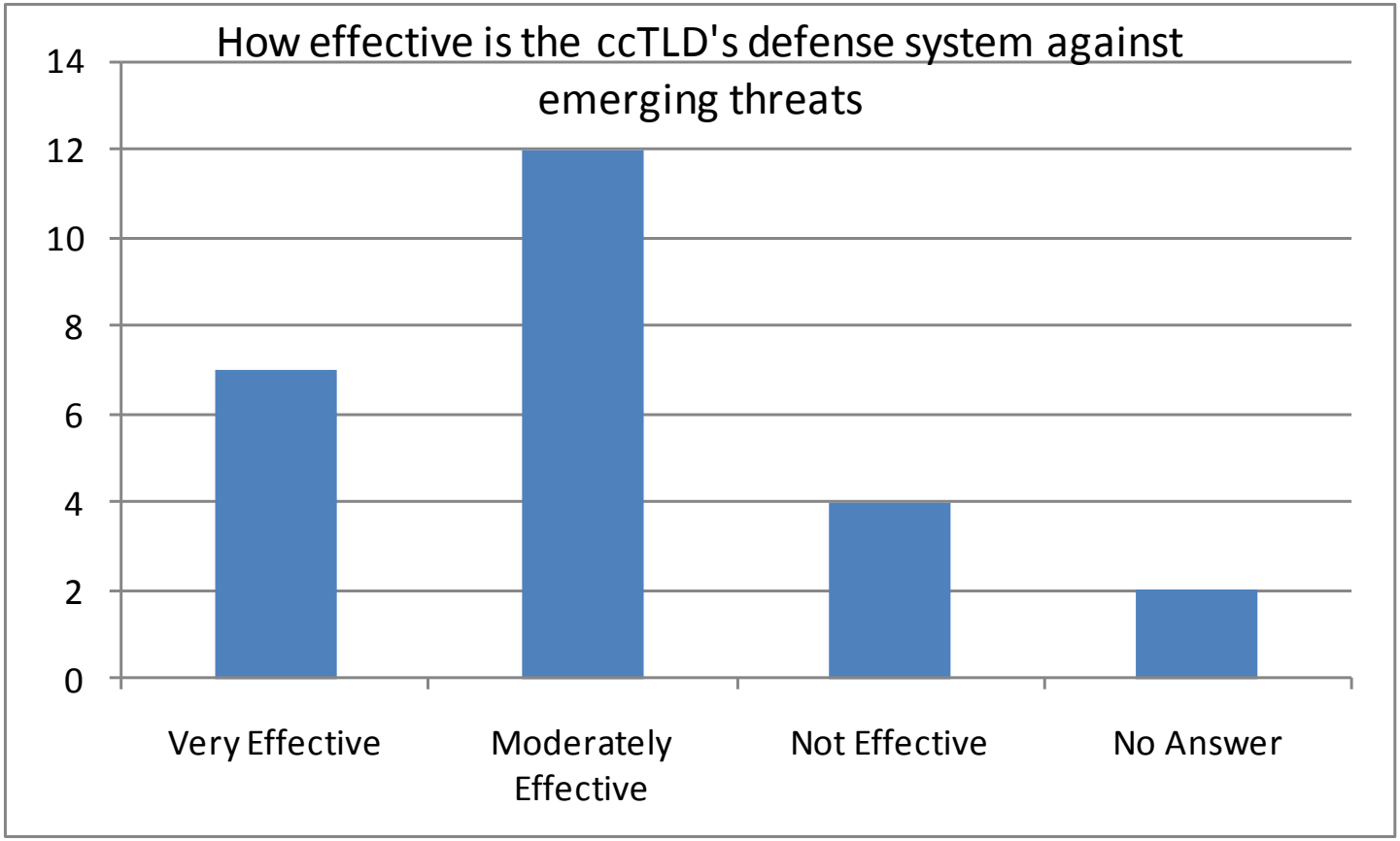
Question 7: Are the websites under the ccTLD checked for compliance with secure coding practices



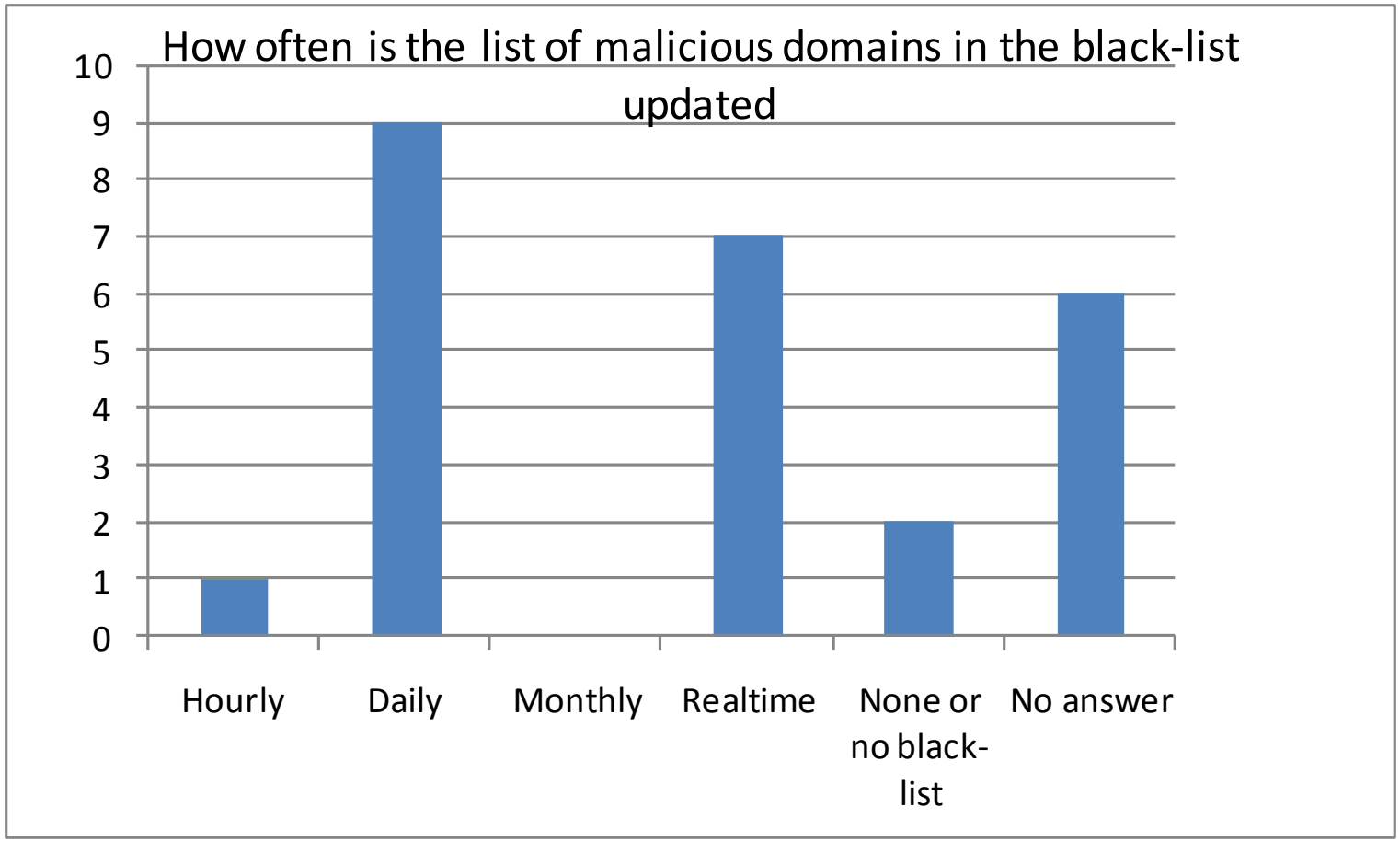
Question 8: What are the policies for taking down a sub-domain found to be spreading malware



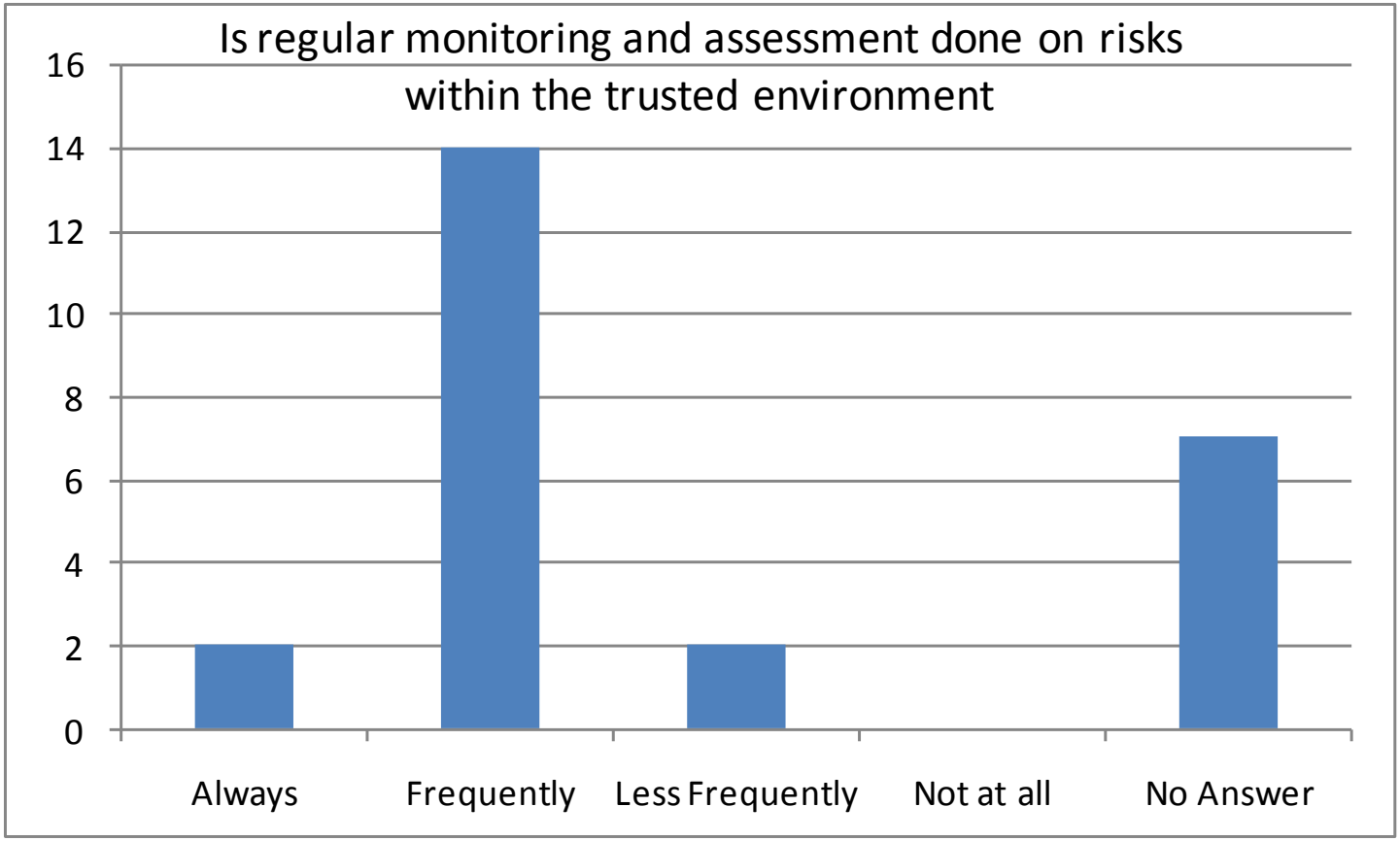
Question 9: How effective is the ccTLD's defense system against emerging threats



Question 10: How often is the list of malicious domains in the black-list updated



Question 11: Is regular monitoring and assessment done on risks within the trusted environment



Survey Analysis vs Security Alert Rankings

Here we try to comprehend the survey results by objectively looking at the Phishing and Spam alert analysis we have done earlier [Presented at GIGANET Symposium held along with IGF09 in Egypt

A snapshot of our Data Set after sorting and country-wise organizing

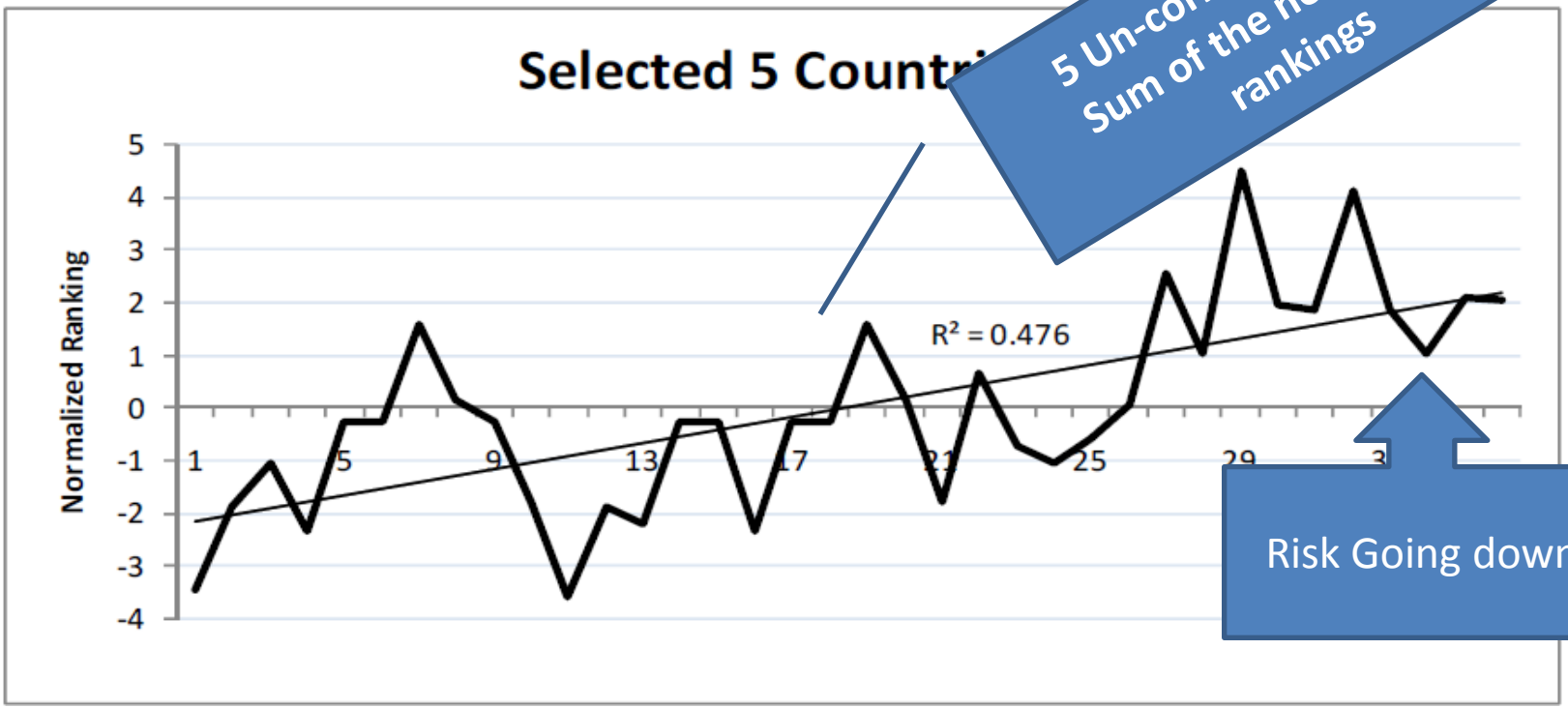
Ranking Date

	1	2	3	4	5	6	7	8	9	10
	6/2008	8/2008	9/2008	10/2008	11/2008	12/2008	1/2009	2/2009	3/2009	4/2009
US	1	1	1	1	1	1	1	1	1	1
Brazil	4	4	4	7	7	4	2	2	3	2
South Korea	11	5	5	4	4	6	11	4	5	3
Poland	3	2	2	2	2	2	6	5	4	4
Turkey	6	6	6	5	5	11	7	7	6	5
India	12	7	7	11	11	12	12	11	9	11
China	5	8	8	6	6	5	3	3	7	6
Argenina	2	3	3	3	3	3	4	6	8	7
Russia	13	11	11	12	12	13	13	8	11	8
Vietnam	14	12	12	13	13	14	14	12	12	12
Columbia	7	9	9	8	8	7	5	9	2	9
Romania	8	10	10	9	9	8	8	10	10	10
Germany	9	13	13	10	10	9	9	13	13	13
UK	10	14	14	14	14	10	10	14	14	14

Countries

Rankings

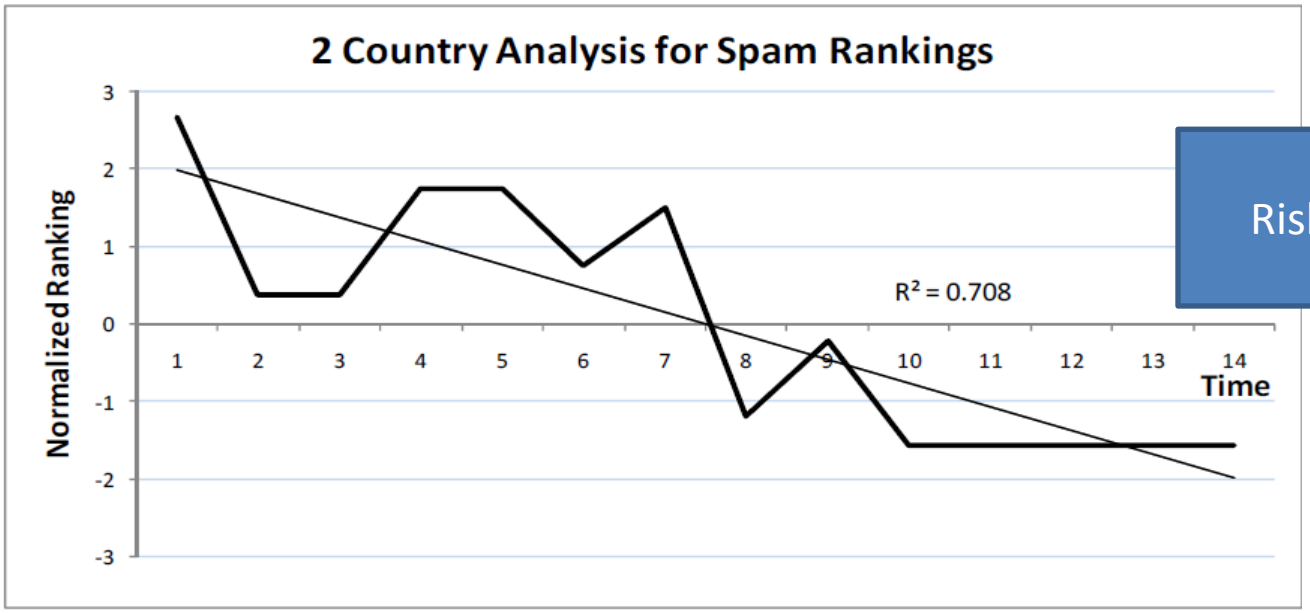
A Phishing Trend Lin



- Ranking trend graph for 5 selected countries. We can clearly observe that the
- plot is rising as time progresses. This means the countries with high rankings in the past are moving towards lower ranks meaning they are successfully reducing phishing levels in their country

Contrast this finding with Question 4 of the survey on “Phishing”

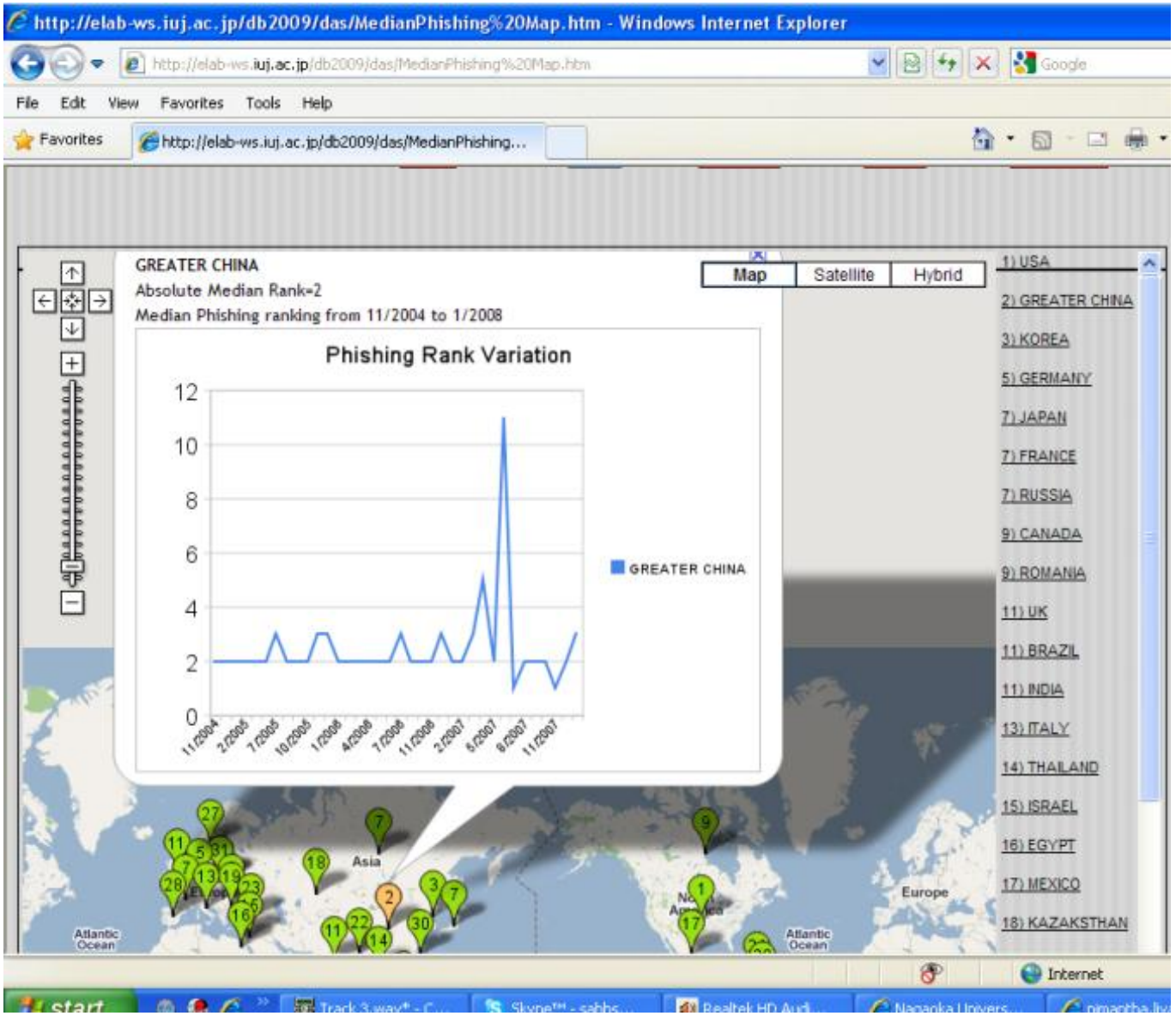
A timeline Graph



Risk Going up

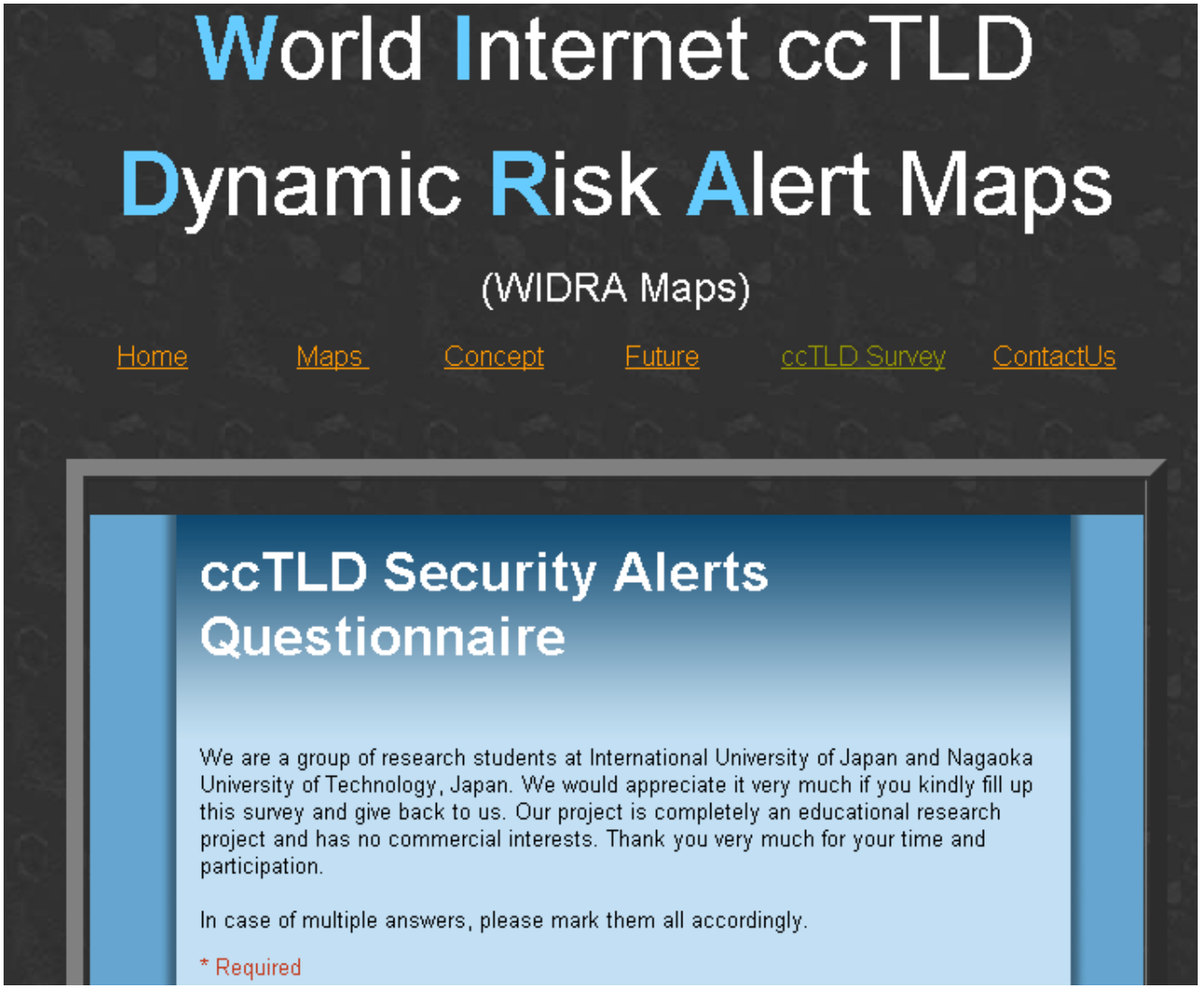
- From the graph it is evident that historical ranking has negligible impact on the future rankings and with time the countries move to higher ranks irrespective of the historical rankings.
- As we said in the introductory slides defining SPAM it is at the hands of the end user and email service providers to tackle this problem adequately.

Contrast this finding with Question 5 of the survey on “SPAM”



URL: http://elab-ws.iuj.ac.jp/cctld/index.htm

Ongoing Survey



http://elab-ws.iuj.ac.jp/cctld/ccTLDSurvey.htm

Relevance to SSR

Conclusion

IGF Survey:

- Very few people are aware about ccTLD operations and practices as the No answer field is in all answers
- Real-time updates regarding security needs to be more in practice
- Policies are there but the implementation is seldom done and thus the malicious domains are still free to abuse internet security.
- Survey results on Phishing and Spam, seem to be in agreement with the Security Alert Ranking Analysis [Presented at GIGANET Symposium held along with IGF09 in Egypt]
- Security Alerts needs to be looked carefully in three spheres: metrics, policies and implementation in SSR framework

Thank You Very Much