GSIM WORKING PAPERS

Series No. IM-2010-01

Do the Internet Security Alerts Have an Impact on Lowering ccTLD Security Risks?

Jay Rajasekera
Graduate School of International Management
International University of Japan

Suvashis Das
Department of Management and Information Systems Science
Nagaoka University of Technology

January 2010

Do the Internet Security Alerts Have an Impact on Lowering ccTLD Security Risks?

Jay Rajasekera and Suvashis Das[1]
International University of Japan
Minamiuonuma City, JAPAN 949-7277
e-mail: jrr@iuj.ac.jp

Acknowledgement:
We would like to thank Professor Yoshiki Mikami and 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.

Abstract:
Despite all the security measures to build a safely networked world there are innumerable loopholes for malicious activity. One of the countermeasures to fight such malicious activities is to issue security alerts. The purpose of this paper is to see if there is significant impact by these security alerts; to best of our knowledge, this is the first statistical study to understand such impact of Internet security alerts.

For the analysis, this paper looks at two of the most malicious security alerts, the Phishing and Spam, issued by two well-known sources. The statistical analysis concludes that for Phishing, the security alerts indeed has a significant positive impact at ccTLD[2] level. For Spam, the security alert data issued by reputed organizations is less frequent. As such, the available data is limited; and, our statistical analysis concludes that Spam is still out of control at ccTDL level. However, considering the significant positive impact on Phishing due to security alerts, it seems reasonable to suggest that the agencies issuing security alerts must be more serious and regular in publishing the rankings than at present.

---

[1] Current Address: Department of Management and Information Systems Science, Nagaoka University of Technology, Niigata, JAPAN

[2] ccTLD means country code Top Level Domain

Introduction:

In Internet governance, security plays an important role. While security is a major concern for website administrators and their customers, it is also a concern at country and ccTLD level. Of course security is a major concern for governing bodies of Internet, such as ICANN and IANA as well.

Internet security also has some major social concerns, especially when it comes to e-commerce, e-banking, social networking. Evidence shows that certain countries, such as Japan had adopted different e-business models because of the reaction of the Japanese public to security.

In order to counter the threats, ICANN, IANA, and other governing organizations continuously update the policies and conduct training or advisory sessions at various levels. The ccTLD administrators too are, in general, very much concerned about their reputation; continuous reputation as a cyber security risk is definitely not something they like to live with.

In addition, Internet security monitoring organizations such as APWG (Anti Phishing Working Group), OARC (DNS Operations, Analysis & Research Center), and US-CERT (Computer Emergency Readiness Team) constantly issue warnings. Plus, the private companies such as Mcafee, VeriSign, Symantec, Microsoft, and Cisco etc. also regularly issue the threat warnings.

It is the practice of such monitoring entities to issue security alerts; and some even do the rankings of most vulnerable domains at ccTLD level. For example Symantec issues what it calls the "MessageLabs Intelligence" report, a monthly security alert report that gives specific rankings for a number of identified security risks. Likewise APWG, issues what is called a "Phishing Attack Trends Report", a quarterly one specifically to deal with Phishing attacks, around the world. But none of the reports are very consistent. There are examples of monthly reports being suddenly changed to a yearly or quarterly report. This brings in a requirement of a consolidated and organized threat reporting and an alert system incorporating the current reporting techniques that exist.

Among some of the most common security risks for a ccTLD include, e-mail spam, denial of service (DOS), distributed denial-of-service (DDOS), Cache

poisoning, Phishing, Worms, and Botnets (Ref. Mohan). Of course new types of attacks can also occur, such as SQL Injection that was not common a few years back. Leaving this apart there are known issues of Cyber Warfare in which one country tries to initiate routing changes and use hacking techniques to stop a particular service or gain access to private network of another country's strategic and sensitive data [Ref 7]. This sometimes takes place between rival organizations as well. There needs to be some way to unravel this area of internet security risks.

The security warnings traditionally are considered a form of deterrent. For example, the US, right after the 9/11 terror attack started issuing security warnings, sometimes even identifying the source of the attack. It is believed such warnings have an impact, as analyzed in a pre-9/11 book by Gurr and Davies (Ref 6). The warnings in fact are intended to effect on the behavior of both the attacker as well as the victim. The attacker is discouraged and sometimes the attack plan completely abandoned; and the victim becomes more cautious and the damage, even attack happens, be less.

The purpose of this research that we intend to present at the Fourth Annual GIGANET Symposium is related to the effect of ccTLD related Internet security alerts on the ccTLD's behavior and effect of ccTLD's counter measures. Of course an attacker is to be blamed, first, for initiating the attack. However, in the Internet world, it is difficult to categorize an affected ccTLD as an innocent victim or as a party to the attack either. If an attacker continuously attacks a certain ccTLD, one could argue that ccTLD administration has a responsibility to find out why his or her ccTLD is being specifically targeted and take preventive measures. Lack of initiatives to taking such preventive measures could mean a lack of responsibility of ccTLD administrators.

Internet Security Warnings:

Internet security warnings or alerts are being more sought for and in demand for a somewhat organized combat against e-crime. May it be hacking, virus attacks, phishing or e-mail spam everything is being reported nowadays. Internet security has in recent years become a global issue. The emergence of distributed denial of service attacks, phishing hosts, rapidly propagating viruses, immense spread of replication capable worms are threats to secured computing across the globe.

The sources of the threats have grown in technology, sophistication and severity. Previously the virus attacks were tackled by installing antivirus, antispyware and anti-spam agents in the computers of the end user. But the increased sophistication of the hacking, phishing and spamming techniques calls for all service providers and domain hosts to come forward and make the internet environment a secure and safe one. The security aspect has now gone beyond the scope of the average end user.

To illustrate this, following is a threat growth graph for malicious code attacks from the 'Symantec Global Internet Security Threat Report 2008' [Ref. 8].

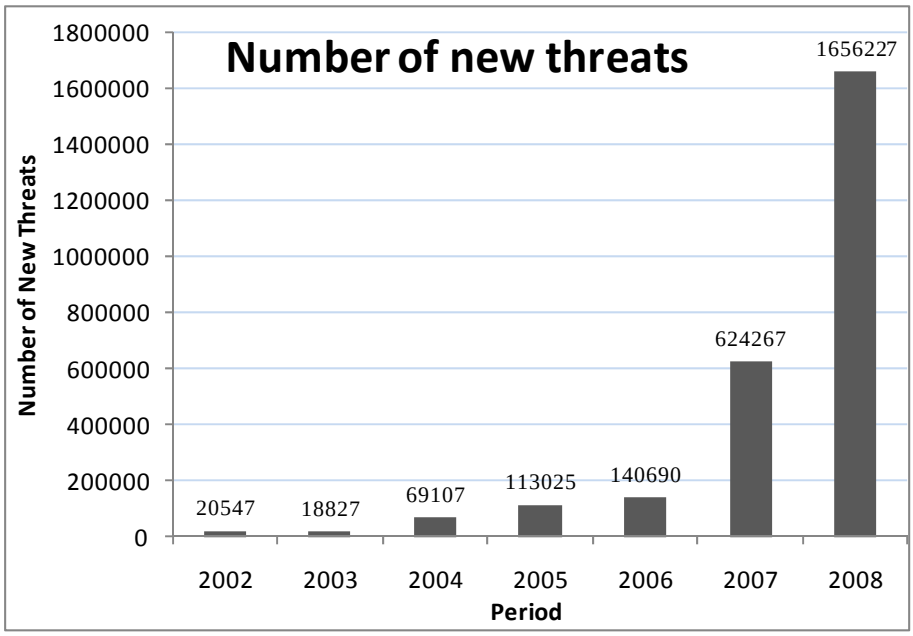

Figure 1: New Malicious Code Threats

It is clearly evident that last two years have seen exponential rise in new threats. And that has happened in spite of all high end security system being in place. So we need to figure out where we need to target the alerting and security systems. As we dig a little deeper into who needs to heed security warnings on a first priority we came to the conclusion that the ccTLDs are the ones who need to act on this. With advancement of time we have at least a handful of country wise reporting services now. The following illustration from the 'Symantec Global Internet Security Threat Report 2008' [Ref. 8] tell us about the top ten countries in terms of overall internet threats originating from a ccTLD.

2008 Rank	2007 Rank	Country	2008 Overall Percentage	2007 Overall Percentage	Malicious Code Rank	Spam Zombies Rank	Phishing Websites Host Rank	Bot Rank	Attack Origin Rank
1	1	United States	23	26	1	3	1	2	1
2	2	China	9	11	2	4	6	1	2
3	3	Germany	6	7	12	2	2	4	4
4	4	United Kingdom	5	4	4	10	5	9	3
5	8	Brazil	4	3	16	1	16	5	9
6	6	Spain	4	3	10	8	13	3	6
7	7	Italy	3	3	11	6	14	6	8
8	5	France	3	4	8	14	9	10	5
9	15	Turkey	3	2	15	5	24	8	12
10	12	Poland	3	2	23	9	8	7	17

Table 1: Some Malicious Activity Ranking

From the above table it is clearly evident that United States has been by far the biggest centre of malicious activity. Other countries in the top 10 list are China, Germany, United Kingdom, Brazil, Spain, Italy, France, Turkey and Poland. So what we require is country wise security risk data on a regular basis to collate and statistically implement them to issue meaningful alerts.

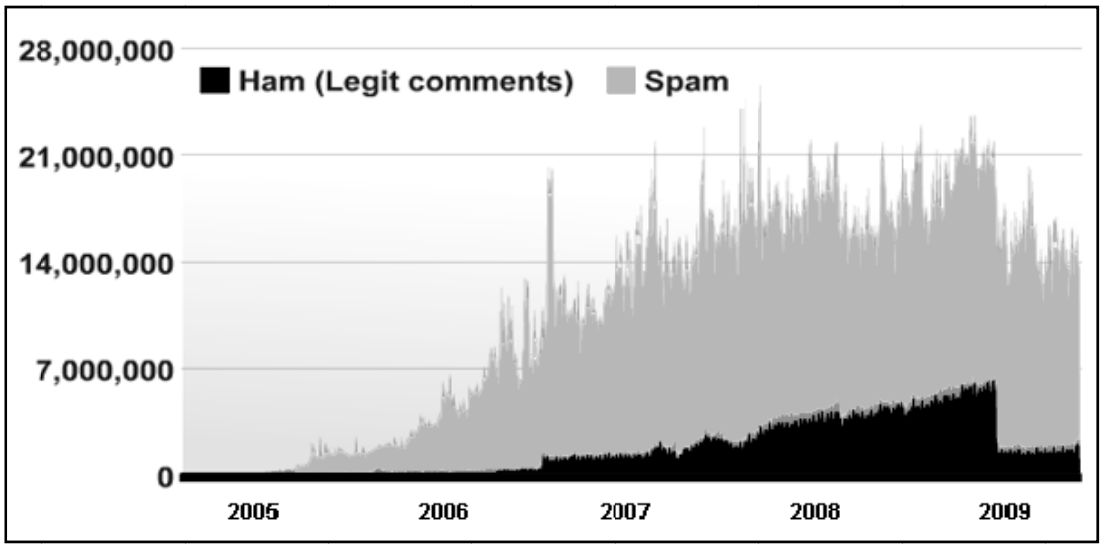

Figure 2: SPAM Timeline Live Statistics from AKISMET Stats Page

Another interesting report is available on live spam statistics. It was provided by AKISMET web site [Ref. 2]. The following graph, in Figure 2, depicts total spam in orange and in blue it depicts HAM, where the non-spam content is being delivered by e-mail. The graph timeline ranges from November 2005 to September 2009. Also live stats on this site say about the percentage of total e-mails marked as spam.

This live data says that till today the 29th of September 2009 the cumulative spam count reached 83 percent of the emails delivered worldwide. This is a significantly high percentage.

The agencies and institutions that provide us with country wise security risk information are

- Trend Micro [Ref. 9]
  - Real-time data on number of malicious URL's Blocked and number of SPAM sources found
  - Online web reputation query available
  - Gives daily, weekly and monthly data
  - Provides real-time data on the malware count
  - Global and country wise data available
  - SPAM percentage distribution across countries
- Mcafee [Ref. 10]
  - Provides virus, SPAM, malicious websites and network related reports
  - Provides country wise(TLD) threat reports
  - Provides online website checking.
- APWG [Ref. 11]
  - Provides timeline statistics of malicious websites on password theft codes and Phishing
  - Provides internet crime activities statistics
- Malware domains [Ref. 12]
  - Provides list of malicious sites and domains to be blocked
  - Provides access to complete data collected by them for the analysis
  - Data very helpful in implementing Black Hole DNS
- SANS Internet Storm Center [Ref. 13]
  - Live list of ports and source IP addresses of threats
  - We can decode the IP addresses by Whois Database and convert it to TLD information
  - Also provides current world threat level in four levels: Green, Yellow, Orange, Red in order of low to high
- SRI Malware Threat Center [Ref. 14]
  - Most Observed Malware-Related DNS Names
  - Most Aggressive Malware Attack Source and Filters
  - The data is updated real-time

- Websense [Ref. 15]
  - Provides viral statistics report
  - Provides email SPAM statistics report
- SOPHOS [Ref. 16]
  - Provides risk statistics on virus, phishing and spam attacks
- AKISMET [Ref. 17]
  - Provides live SPAM count and statistics

To the best of our knowledge after studying through the above resources, we came to the conclusion that there are no comprehensive studies on how Internet security alerts or warnings are comprehended by a concerned ccTLD. The intuitive thinking is that such alerts or warnings will have a positive effect and gradually the threat to that particular ccTLD will diminish. Lacking past studies, we, in this ongoing research, are attempting to confirm or test the validity of such hypothesis.

Risk Rankings:

Agents like APWG and Symantec has been publishing monthly reports on phishing and Spam on a monthly basis with the exception of few months where they switch to yearly reports or quarterly reports. Also internet risk data is available from Mcafee as 'Mapping the Mal-web' [Ref. 10]. But the reports from Mcafee are yearly. We wanted to analyze the ranking data over a large number of Data points. To achieve this we chose APWG reports for phishing and Symantec reports for Spam.

We started from the very first monthly report available for both phishing and spam in the two sites. We had to extract the data for top ten countries for both the risk from .pdf files provided in the sites. For spam we could collate 15 data points for analysis and for phishing we collected 36. These data were in percentage risk form i.e. if the phishing or spam percentage is 100 for the entire world then for a particular ccTLD it is the fraction that originates from that ccTLD. After we acquired the percentages we sorted them for each data point to get the rankings and then put together in one table. Below is a quick summary of phishing data plotted with the percentages. Henceforth in this paper we don't illustrate with the percentage data anymore, we use the ranking analysis.

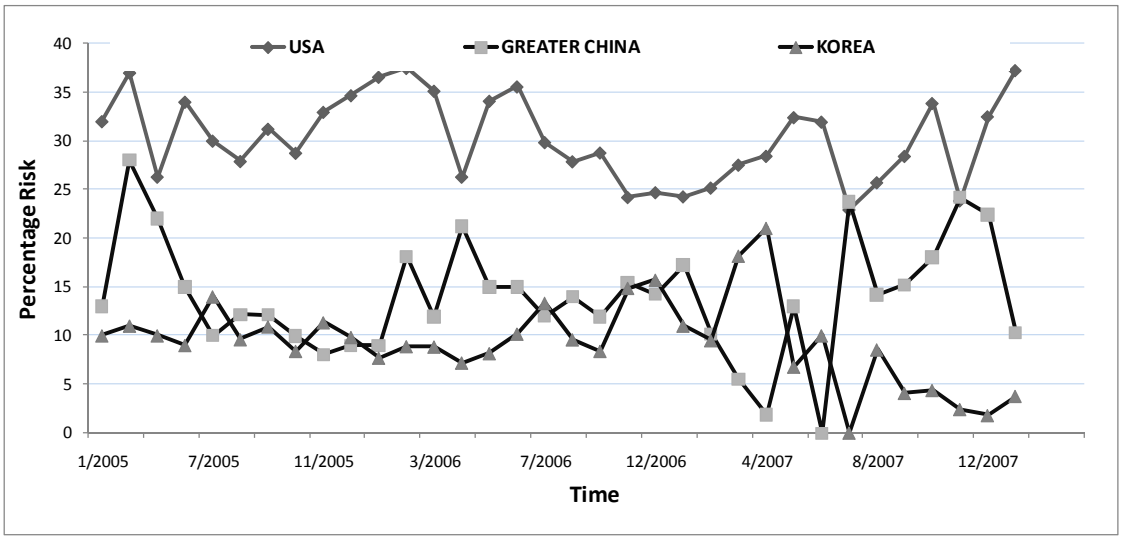

Figure 3: Three Countries With High Percentages of Phishing Activities

Our research is based on the security alert data collected, over the years, from Internet security organizations and companies mentioned earlier. In particular, we look at the ranking of security warnings on ccTLDs. For example, if a certain country (i.e. its ccTLD) is ranked high for a certain period of time, then, what kind of impact such ranking has on future ranking. Is that a positive effect? The cases where it has no impact are the ones we are testing in our research.

Impact of Security Alerts:

As stated earlier, many organizations, such as Mcafee and APWG, issue security alerts to caution the general public to be careful. They normally rank the countries based on Internet hazards such as e-mail spam, denial of service (DOS), Phishing, Spam, Worms, and as such. Such alerts can create negative impressions about a particular ccTLD. As such, it is normal to believe the concerned ccTLD administrators would take some measures to clear their name. A reasonable way to see the impact of such counter-measures at ccTLD level is to look at the historical data and see if there is any downward trend. As explained earlier, the Internet security alert data are not consistent and often needs to be dug out from several sources. We found two alerts, on Phishing and Worms had enough historical data to do a serious statistical analysis, which we will explain in detail next.

Phishing:

APWG (Ref: 11) had been producing phishing data for a long time. After

scanning through reports from Oct 2005, we were able to collects 36 periods of data extending till Jan 2008. In fact, recently, APWG's frequency of publishing the data changed to quarterly and, then, to annually. Nevertheless, the 36 data points, part of which is shown in Table 2, was good enough to make a reasonable statistical analysis.

	1	2	3	4	5	6	7	8	9	10
	10/2004	12/2004	1/2005	2/2005	4/2005	5/2005	7/2005	8/2005	9/2005	10/2005
USA	1	1	1	1	1	1	1	1	1	1
GREATER CHINA	2	2	2	2	2	2	3	2	2	2
KOREA	3	3	3	3	3	3	2	3	3	3
JAPAN	4	4	4	4	6	6	7	5	6	7
CANADA	5	9	9	7	8	8	8	9	5	6
GERMANY	6	5	5	5	5	5	6	6	4	4
BRAZIL	7	6	6	11	10	10	11	11	9	11
INDIA	8	10	11	8	11	11	12	12	11	10
UK	9	11	12	12	12	12	13	13	12	8

Table 2: Part of Phishing Alert Rankings Data (Ref: 11)

Since the scale of the data is different, the data needed to be normalized, which was done by using the formulae:

$$\mathrm{NR} = \frac{(\mathrm{OR} - \overline{\mathrm{OR}})}{\mathrm{STD}}$$

where,

NR = New Ranking

OR = Old Ranking

$\overline{\mathrm{OR}}$ = The mean value of the Old Rankings (for a given country it is the mean of the row)

STD = The standard deviation of the row values

In case STD happened to be zero for any country, we exclude it from statistical analysis as it would not indicate any effect due to historical ranking. But, the date we collected showed non-negative STDs for each of the major risk countries.

Normalized Data:	New Rankings									
	1	2	3	4	5	6	7	8	9	10
USA	-0.24254	-0.24254	-0.24254	-0.24254	-0.24254	-0.24254	-0.24254	-0.24254	-0.24254	-0.24254
GREATER CHINA	-0.29706	-0.29706	-0.29706	-0.29706	-0.29706	-0.29706	0.332008	-0.29706	-0.29706	-0.29706
KOREA	-0.29294	-0.29294	-0.29294	-0.29294	-0.29294	-0.29294	-0.79513	-0.29294	-0.29294	-0.29294
JAPAN	-1.2575	-1.2575	-1.2575	-1.2575	-0.45626	-0.45626	-0.05564	-0.85688	-0.45626	-0.05564
CANADA	-1.47918	0.159297	0.159297	-0.65994	-0.25032	-0.25032	-0.25032	0.159297	-1.47918	-1.06956
GERMANY	0.312063	-0.27921	-0.27921	-0.27921	-0.27921	-0.27921	0.312063	0.312063	-0.87049	-0.87049
BRAZIL	-1.78702	-2.28572	-2.28572	0.207793	-0.29091	-0.29091	0.207793	0.207793	-0.78961	0.20779
INDIA	-1.21122	-0.38067	0.034606	-1.21122	0.034606	0.034606	0.449884	0.449884	0.034606	-0.38067
UK	-0.46546	0.296201	0.677031	0.677031	0.677031	0.677031	1.057861	1.057861	0.677031	-0.84629

Table 3: Normalized Phishing Data

Though some countries, such as USA, remained the most risky ccTLD for phishing continuously in this table, at later periods it showed some change. Part of the normalized data is shown in Table 3.

What we are aiming at examining is the effect of the historical ranking on the future rankings. Plotting the data for UK, for example, shows the historical trend as seen in Figure 4.

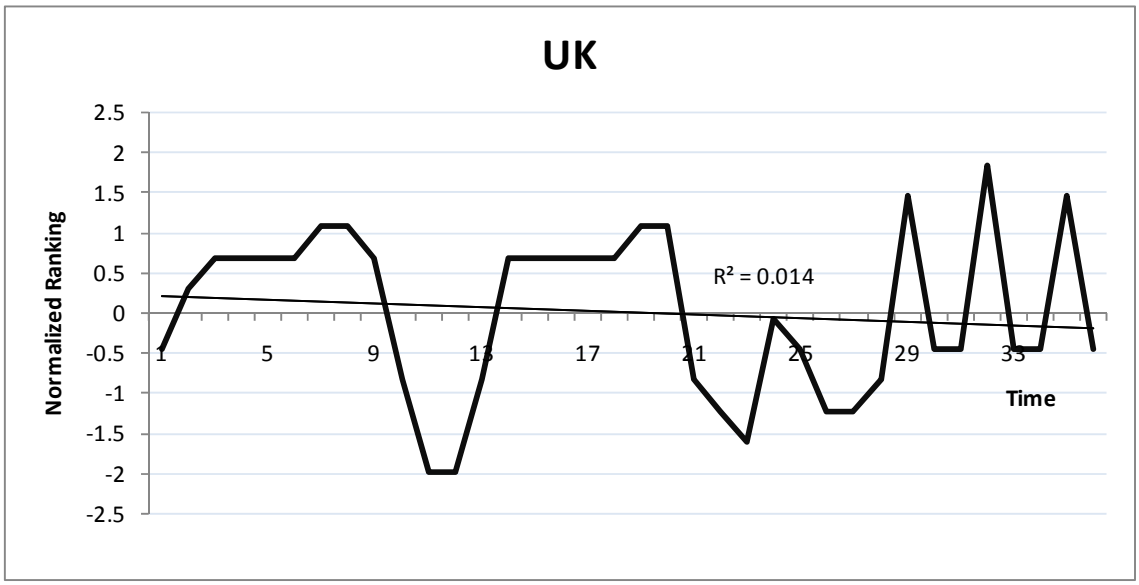

Figure 4: Phishing Ranking Trend for UK

However, a chart for a single country does not show the collective effect of historical rankings on future rankings.

While looking at collective data, one needs to be concerned about the correlations between the variables. The variance-covariance matrix for the normalized data is shown in Table 4.

	USA	GREATER	KOREA	JAPAN	CANADA	GERMANY	BRAZIL	INDIA	UK
USA	1								
GREATER CHINA	-0.21838	1							
KOREA	0.700618	-0.29789	1						
JAPAN	-0.01312	0.092826	0.228648	1					
CANADA	0.327325	0.185184	0.44535	0.438497	1				
GERMANY	0.143295	0.341252	0.249256	0.343135	0.54689	1			
BRAZIL	0.107794	0.263348	0.23503	0.615543	0.475363	0.470502	1		
INDIA	-0.28561	-0.18755	-0.00141	0.208548	0.196772	0.128756	0.076903	1	
UK	-0.10975	0.085545	0.110183	-0.21883	0.008894	0.202029	-0.09061	-0.06122	1

Table 4: Variance-covariance Matrix for Normalized Phishing Data

The covariances that are large (i.e. greater than 0.25) are marked in gray. We used the covariance value to identify correlated data. We see that USA,

Korea, Canada are highly correlated; thus we consider only USA and exclude Korea and Canada. Likewise, Greater China, Germany, and Brazil are highly correlated; thus we kept Greater China, which includes Hong Kong and Taiwan, and excluded Germany and Brazil. Also, Japan is highly correlated with Canada, Germany and Brazil; thus we consider Japan and excluded the rest.

By doing so, we ended up with five countries, USA, Greater China, Japan, India, and UK. The normalized data for those five countries, for 10 periods, are shown in Table 5.

Period	1	2	3	4	5	6	7	8	9	10
USA	-0.24254	-0.24254	-0.24254	-0.24254	-0.24254	-0.24254	-0.24254	-0.24254	-0.24254	-0.24254
GREATER CHINA	-0.29706	-0.29706	-0.29706	-0.29706	-0.29706	-0.29706	0.332008	-0.29706	-0.29706	-0.29706
JAPAN	-1.2575	-1.2575	-1.2575	-1.2575	-0.45626	-0.45626	-0.05564	-0.85688	-0.45626	-0.05564
INDIA	-1.21122	-0.38067	0.034606	-1.21122	0.034606	0.034606	0.449884	0.449884	0.034606	-0.38067
UK	-0.46546	0.296201	0.677031	0.677031	0.677031	0.677031	1.057861	1.057861	0.677031	-0.84629
5 country Totals	**-3.47378**	**-1.88156**	**-1.08546**	**-2.33129**	**-0.28422**	**-0.28422**	**1.541575**	**0.11127**	**-0.28422**	**-1.8222**

Table 5: Statistically "Independent" Normalized Phishing Rankings

The complete data set of Table 5 has 36 periods, though only 10 periods are shown. Data in each row is statistically "independent" in the sense that the covariance between any two rows is low. The last row in Table 5 shows the total normalized ranking for each period. In order to see if there is significant trend, we look at the time series plot, as shown in Figure 5.

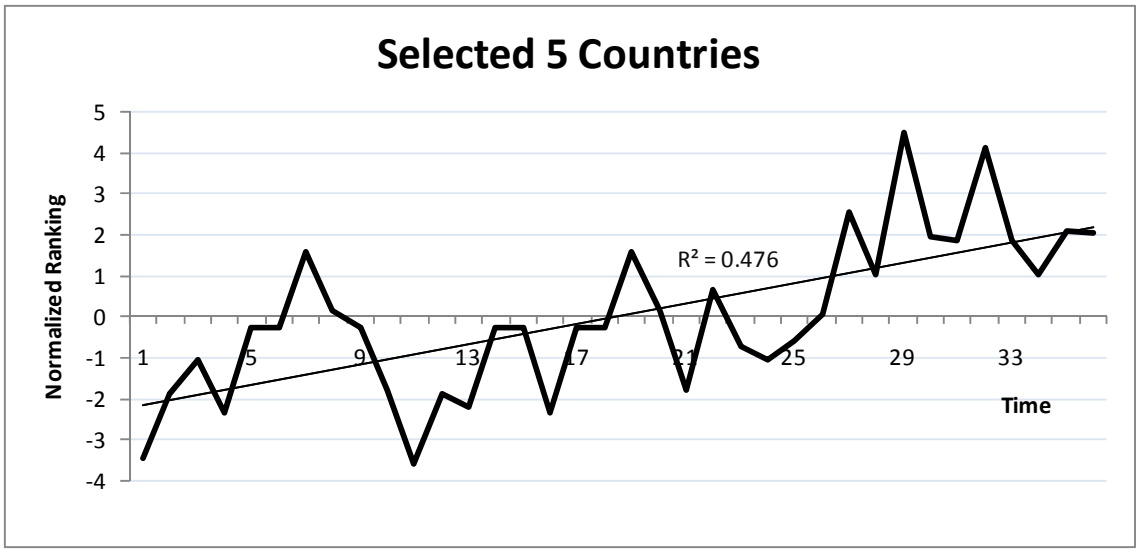

Figure 5: Phishing Ranking Trend over Time

With R^2 =0.476 and significant trend, we can conclude that for phishing alerts, there is significant impact for future rankings to get affected by past rankings. It is important to note, the higher rank, meaning the positive slope, is a sign that highly risked countries (i.e. ccTLDs with high risks of phishing activities) seem to have taken steps to suppress the phishing activities (i.e. the phishing rank going up).

Thus, statistically speaking, the phishing rankings seem to have significant impact which might have made the concerned ccTLDs taking serious effort to control the phishing activities being hosted under their ccTLD.

Spam:

Though spam has been around for many years, Symantec (Ref: 8) started producing security alert rankings, by ccTLD, since June 2008, each month. We were able to collect 14 data points, part of which is shown in Table 6.

	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

Table 6: Part of Spam Alert Rankings Data (Ref: 8)

This is not sufficiently large sample for a thorough statistical analysis; nevertheless, we analyzed the data in a way very similar to phishing case, to see any downward trend of the rank. The first thing is to remove the scaling effect between rows, which was done using the same equation

$$\mathrm{NR} = \frac{(\mathrm{OR} - \overline{\mathrm{OR}})}{\mathrm{STD}}$$

with similar definitions as before.

After normalizing and removing the highly correlated rows (i.e. rows with absolute correlation values more than 0.25), as done before, we could identify only two ccTLD's, with statistically "independent" spam rankings. Part of the

normalized data for those two countries, namely Brazil and South Korea, are shown in Table 7.

	1	2	3	4	5	6	7	8	9	10
Brazil	0.37467	0.37467	0.37467	2.12316	2.12316	0.37467	-0.791	-0.791	-0.2082	-0.791
South Ko	2.29129	0	0	-0.3819	-0.3819	0.38188	2.29129	-0.3819	0	-0.7638
	2.66596	0.37467	0.37467	1.74128	1.74128	0.75656	1.50031	-1.1729	-0.2082	-1.5547

Table 7: Statistically "Independent" Normalized Spam Rankings

The last row in Table 7 shows the total normalized ranking for each period. In order to see if there is significant trend, we look at the time series plot, as shown in Figure 6.

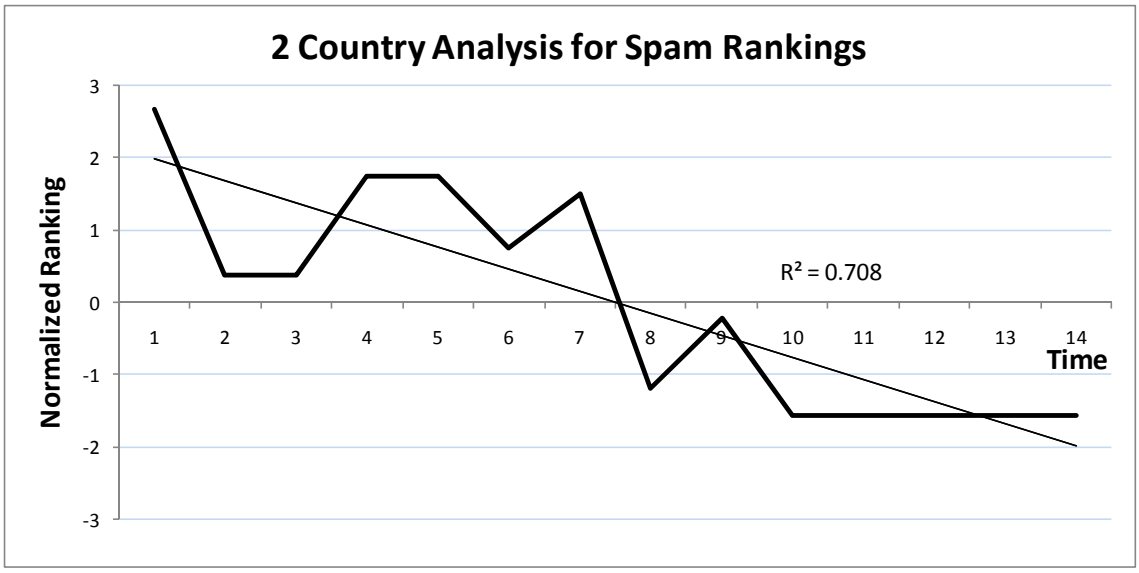

Figure 6: Spam Ranking Trend over Time

With R^2 =0.708 and significant downward trend, we can conclude that for spam, the alerts do not seem to have any impact in terms of improving the security vulnerability. This means that a high risk ccTLD could become even higher risk over time, despite a security alert -- the meaning of the negative slope is that the risk rank has gone up.

One of the countries that we selected based on the statistical reasoning, South Korea, clearly demonstrates this trend, as shown in Figure 7.

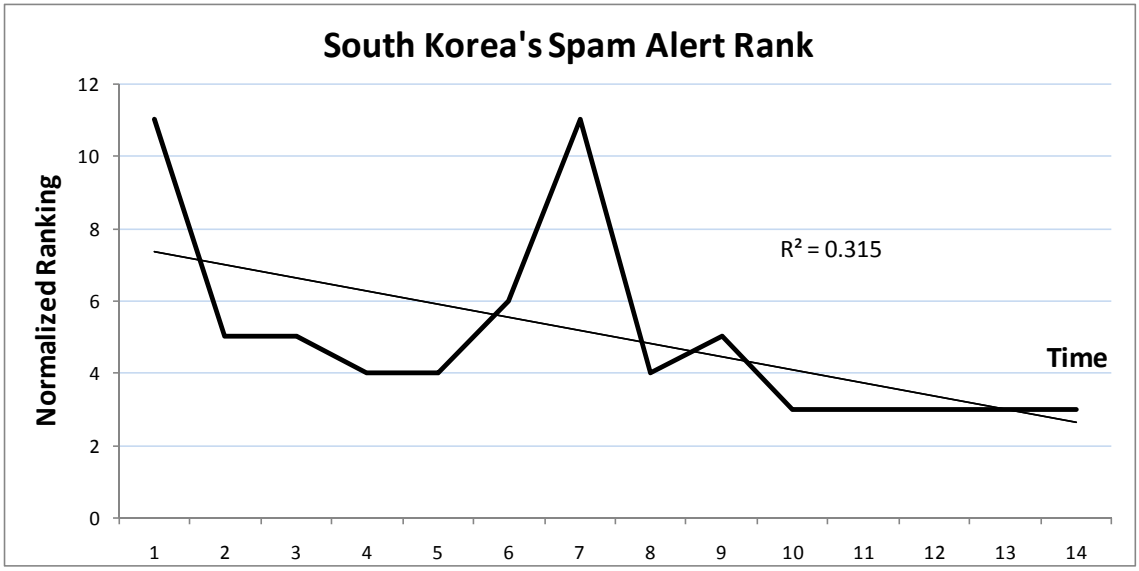

Figure 7: Despite Alerts, Spam Risk Can Get Worse

Unlike for phishing, we could not get enough data for a thorough statistical analysis for spam. But, what we could conclude with the limited data is that there is very high likelihood that spam is not completely under the control at ccTLD level.

Conclusion:

The statistical analysis concludes that for Phishing, the security alerts indeed has a significant positive impact at ccTLD level. For Spam, the security alert data issued by reputed organizations is less frequent. With limited data, our statistical analysis concludes that Spam is still out of control at ccTDL level.

To the best of our knowledge after studying through the available resources, we came to the conclusion that there had been no comprehensive statistical studies on how Internet security alerts or warnings are comprehended by a concerned ccTLD.

Considering the significant positive impact on Phishing due to security alerts, as found out by our analysis in this paper, it seems reasonable to suggest that the agencies issuing security alerts must be more serious and regular in publishing the rankings than at present.

We believe that our findings have wide appeal for ccTLD administrators and Internet governance organizations, including the organizations issuing the

security alerts. Our finding also will be important for organizations that issue Internet security related organizations.

The organizations, at present, do not publish historical data in the latest report they issue. Also, as mentioned earlier, the publishing frequencies are not always regular. We are currently experimenting with a system to automate the data collection while keeping historic data and represent the risk scenario as a mashup with Google Maps API. The experimental web link can be found at Ref: 17. A screen shot of the experimental map, designed in World Internet ccTLD Dynamic Risk Alert (WIDRA) Map website at International University of Japan, is seen in Figure 8, (WIDRA Map).

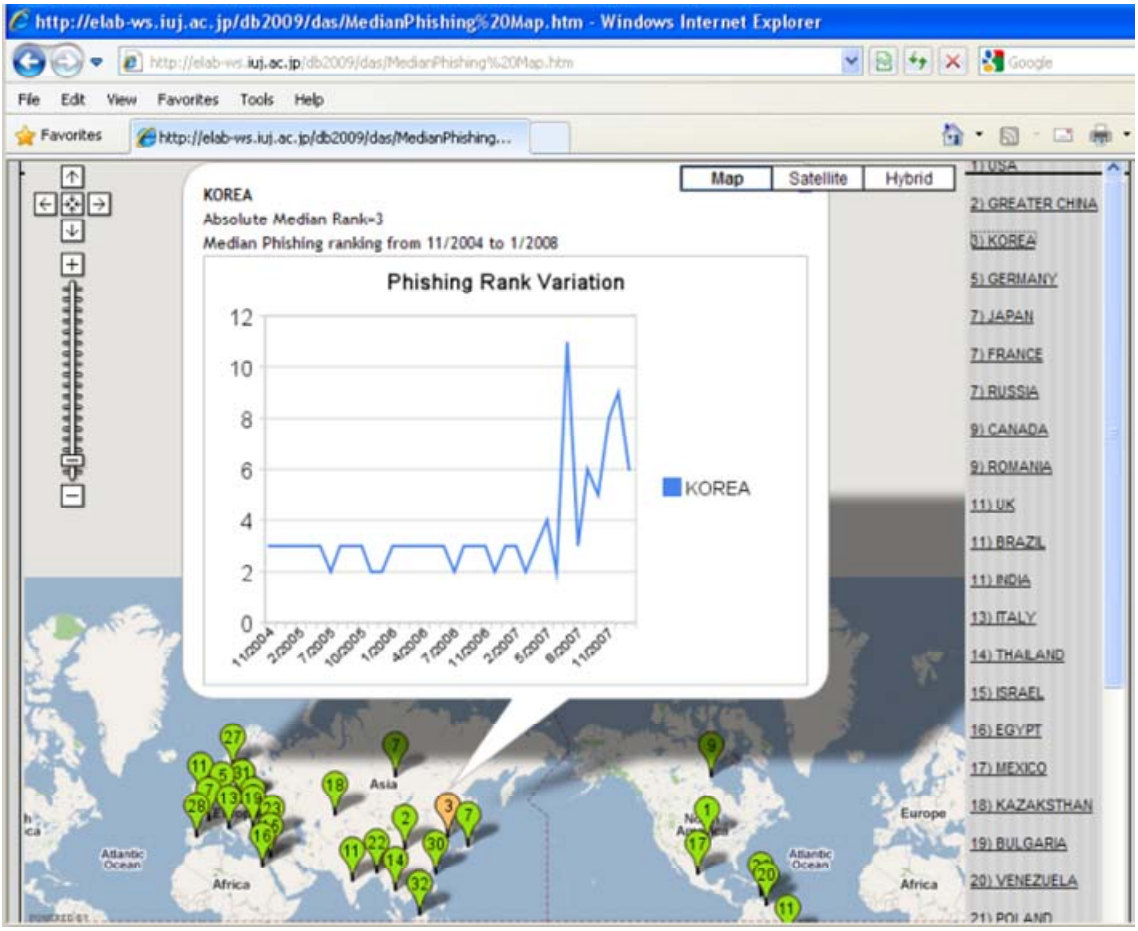

Figure 8: Experimental WIDRA Map

References:

1. Ram Mohan, “Cyber Security Outlook for TLD operators APTLD Meeting”, Manila, February 23, 2009.
2. AKISMET: http://akismet.com/stats/
3. OARC (DNS Operations, Analysis & Research Center): http://www.dns-oarc.org
4. SANS Institute (Internet Storm Center): http://isc.sans.org/
5. US-CERT (Computer Emergency Readiness Team): http://www.kb.cert.org/vuls/
6. John L. Gurr, Ted Robert Davies, “Preventive Measures: Building Risk Assessment and Crisis Early Warning Systems”, Rowman & Littlefield Publishers, Inc. (1998)
7. Emerging Cyber Threats Report for 2009 : http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf
8. Symantec Global Internet Security Threat Reports: http://eval.symantec.com/
9. Trend Micro:
   - http://itw.trendmicro.com/trend_tracker.php
   - http://itw.trendmicro.com/malware_spam_map.php
   - http://reclassify.wrs.trendmicro.com/wrsonlinequery.aspx
10. Mcafee:
    - http://www.mcafee.com/us/
    - http://www.siteadvisor.com/studies/map_malweb_mar2007.html
11. APWG: http://www.antiphishing.org/index.html
12. Malwaredomains: http://www.malwaredomains.com/wordpress/?p=508
13. SANS Internet Storm Center: http://isc.sans.org/
14. SRI Malware Threat Center: http://mtc.sri.com/
15. Websense: http://www.websense.com/content/home.aspx
16. SOPHOS : www.sophos.com/security/blog/
17. Our Experimental Web: http://elab-ws.iuj.ac.jp/db2009/das/index.htm