Global network security: a vulnerability assessment of seven popular outsourcing countries

MIDDLETON, Ray, DAY, David and LALLIE, Harjinder Singh

Global Network Security

A Vulnerability Assessment of Seven Popular Outsourcing Countries

Raymond Middleton [#1], David J. Day [*2], Harjinder Singh Lallie [%3]

[#]*Glosec Consulting, Derby, DE55 1BH, UK*

[1]ray.middleton@gmail.com

[*]*Sheffield Hallam University, Sheffield, S1 1WB, UK*

[2]d.day@shu.ac.uk; Corresponding Author

[%]*International Digital Laboratory (WMG), University of Warwick, Coventry, CV4 7AL, UK*

[3]h.s.lallie@warwick.ac.uk

***Abstract*—With increasingly more businesses engaging in offshore outsourcing, organisations need to be made aware of the global differences in network security, before entrusting a nation with sensitive information. In July 2011, Syn and Nackrst1 explored this topic by analysing seven countries from a wide spectrum across the globe for network security vulnerabilities. The countries selected were China, the United Kingdom, Germany, Russia, India, Mexico and Romania. Their method utilises Nmap and Nessus to probe and test for network vulnerabilities from each respective nation, in order to collect quantitative data for national vulnerability volumes. The Vulnerability statistics collected are of four categories; High, Medium, Low and Open Ports. This paper extends Syn and Nackrst1's work by constructing a more detailed analysis of their results, showing the number of real-world vulnerabilities per nation; the differences between national levels of network security, the ratios of vulnerabilities/IP address; and vulnerability summary rankings. Multiple causal factors are also looked at to quantify the reasoning behind the varying levels of vulnerabilities per nation. This paper concludes that each nation has millions of vulnerabilities of varying amounts, and therefore, each nation differs in network security levels. Mexico and India exhibited the most worrying statistics, with the highest number of high level vulnerabilities/IP address ratio.**

Ultimately, this paper highlights the vulnerability levels that organisations are faced with when engaging in foreign and domestic outsourcing.

Keywords—network; network security; information security; global; vulnerability; outsourcing; Nmap; Nessus; infrastructure

I. INTRODUCTION

With globalisation so prevalent in business today, it is easier for companies to outsource various business processes to foreign organisations. This allows businesses to better focus their core competencies, to be more cost efficient, and to gain technology external to the organisation [1]. Any business process can be outsourced including, call centres, accounting, finance, HR, logistics, and data centres [2], as well as payroll, internal audits, administration and tax compliance [3]. In 2008, the world Business Process Outsourcing (BPO) market was valued at £228 Billion, with India and China holding 44.8% and 25.8% respectively [4]. Blokdijk [5] states that companies are increasingly looking to offshore outsourcing providers for IT solutions, resulting in the IT sector dominating the outsourcing market with a 28% market share. The Information Technology Outsourcing (ITO) market has grown, and continues to grow year-on-year. In 2007, IT outsourcing commanded a worldwide market growth rate of 10.2% [6]. The uptake on cloud services such as, Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Desktop as a Service (DaaS) has contributed greatly to these rising statistics. According to IDC [7], spending on IT cloud services is growing at five times the rate of traditional, on-premises IT, with projected spending on cloud services looking to triple by 2012. Gartner [8] suggests that the global cloud computing market is expected to reach $150 billion by 2014. In the same vein, a recent forecast by Forrester Research [9] predicts that the market size for worldwide cloud services is expected to top more than $240 billion by 2020. But by businesses engaging so heavily in cloud, and therefore outsourcing, so much internal control is given away to other companies, some of whom are located on the other side of the globe. In doing this, businesses are entrusting foreign organisations, and as such, the network security standards of foreign countries, with the confidentiality, integrity and availability of their information. However, organisations have little to no way of knowing what levels of network security specific countries adhere to. With malicious attacks growing in numbers due to readily available tools [10] and vulnerability numbers increasing year-on-year [11]; [12], organisations should be able to identify whether the country being outsourced to is prone to vulnerabilities, and whether the country being outsourced to is more or less vulnerable than their own. This poses the question; does network security differ around the world?

To address this question, data collected by Syn and Nackrst1, will be used for the basis of this research topic. The data will be analysed to expose the varying differences (if any) between national levels of network security vulnerabilities. Statistical data of this nature is not readily available, and there is a distinct lack of academic research into this field of study. Major Information Security vendors such as Trend Micro, IBM, Symantec, and CSI go to great lengths each year to document information security levels and trends in extreme detail. Regardless, every year the compiled reports neglect to

identify simple parameters such as, whether the servers of one country have more or less vulnerabilities than that of another. The lack of information and research in this area should be a concern. Varying nation's network infrastructure security levels should be a fundamental consideration for any organisation engaging in BPO/ITO.

The remainder of this paper will be constructed as follows. Section two will explain the method used by Syn and Nackrst1 to obtain the vulnerability data. This will include the rationale for country and IP address selection, along with the applications used for reconnaissance and vulnerability scanning. Section three will provide results and analysis via real-world vulnerability statistics, expressed holistically, and in ratio format. The differences in vulnerability levels between countries will also be compared. In section four we discuss possible causal factors which indicate why the statistical differences between nations were recorded. Finally, in section five, we offer our conclusions.

II. METHODOLOGY

A. Country Selection

The countries selected by Syn and Nackrst1 for vulnerability data collection are as follows:-

- India
- China
- Mexico
- Romania
- Russia
- Germany
- United Kingdom

According to Syn and Nackrst1 [13] country selection was based upon multiple factors. These factors are as follows:

- A varying selection of top outsourcing countries.
- Countries that are most affected by cybercrime.
- Countries that produce the most malware.
- Countries that host the most malicious files.
- Gross National Income.
- Diverse range of cultures.
- Political situation of a nation.

B. IP Address Sample Size

The IP data for each chosen country was downloaded from www.countryipblocks.net in Classless Inter-Domain Routing (CIDR) format. Because of the national differences in IP address allocation, an unbiased method that allowed for percentile data gathering was used. 0.001% of the total IP addresses from each country were identified for availability, i.e. actively being used. 10% (0.0001% of the total IP addresses) of this sum were tested for application vulnerabilities. By utilising this method, a manageable sample size was attained. Table I lists the IP population and sample sizes for each nation.

TABLE I. IP POPULATION AND SAMPLE SIZES

Country	IP Address Population and Sample Sizes		
	Total IP addresses	***Required***	***10%***
China	293,819,478	2939	294
UK	121,532,029	1216	122
Germany	113,924,178	1139	114
Russia	37,202,457	372	37
India	30,467,289	305	31
Mexico	27,906,188	279	28
Romania	10,729,892	107	11

a. Final IP Numbers, Source: Syn and Nackrst1. (2011)

Syn and Nackrst1 ensured that the experiment was conducted within a controlled environment, and with strict parameters as to who had access to the data. To preserve the authenticity and integrity of the data, the data was stored in Encrypted File System (EFS) databases. The databases were then stored on removable media encrypted with TrueCrypt. All authors who contributed to the paper used encrypted email to ensure any post-experiment data was secure.

C. Five Stage Host Discovery and Selection Process

1. Obtain network list for a specific country
2. Networks are separated by their CIDR prefix
3. Networks are selected from each prefix group at random and then probed for active IP addresses via the port scanning tool NMAP [14].
4. All alive IP addresses are pooled and mixed together
5. 10% of all active IP addresses from the required pool are chosen for vulnerability testing. Each IP address is selected at random to ensure unbiased results.

The network vulnerability scanner Nessus [15] was used to scan the IP addresses for vulnerabilities. Nessus organises the vulnerabilities for any given IP address into five categories; total vulnerabilities; high level vulnerabilities; medium level vulnerabilities; low level vulnerabilities and open ports [16]. Nessus maps all vulnerabilities with a Common Vulnerability Scoring System (CVSS) equal to or greater than 7 into a "High" severity, 4 to 6.9 into a "Medium" severity and lower than 4 into a "Low" severity [17]. The same five categories have been used for this study.

III. RESULTS

The results gathered via the method detailed in section two show four key pieces of information. Firstly, the total vulnerabilities for a specific country is shown. Secondly, the amount of each vulnerability type found in the total IP addresses for a given country is expressed as a percentage (rounded to the nearest %). Thirdly, country vulnerabilities are expressed in millions after reverse engineering the percentile method used to collect the data. Fourthly, the vulnerability to IP ratio for each of the five vulnerability categories is stated.

A. China

Vuln. Type	National Vulnerability Statistics for China		
	Total/Percentage	*In Millions*	*Vuln. to IP Ratio*
Total	2,887	2,887m	10:1
High	49 (2%)	49m	1:6
Medium	142 (5%)	142m	1:2
Low	2084 (72%)	2,084m	7:1
Open Ports	612 (21%)	612m	2:1

b. National Vulnerability Statistics for China

B. United Kingdom

Vuln. Type	National Vulnerability Statistics for the UK		
	Total/Percentage	*In Millions*	*Vuln. to IP Ratio*
Total	3,407	3,407m	28:1
High	63 (2%)	63m	1:2
Medium	385 (11%)	385m	3:1
Low	2303 (68%)	2,303m	19:1
Open Ports	656 (19%)	656m	5:1

c. National Vulnerability Statistics for the United Kingdom

C. Germany

Vuln. Type	National Vulnerability Statistics for Germany		
	Total/Percentage	*In Millions*	*Vuln. to IP Ratio*
Total	2,466	2,466m	22:1
High	62 (3%)	62m	1:2
Medium	296 (12%)	296m	3:1
Low	1658 (67%)	1,658m	15:1
Open Ports	450 (18%)	450m	4:1

d. National Vulnerability Statistics for Germany

D. Russia

Vuln. Type	National Vulnerability Statistics for Russia		
	Total/Percentage	*In Millions*	*Vuln. to IP Ratio*
Total	579	579m	16:1
High	11 (2%)	11m	1:3
Medium	40 (7%)	40m	1:1
Low	417 (72%)	417m	11:1
Open Ports	111 (19%)	111m	3:1

e. National Vulnerability Statistics for Russia

E. India

Vuln. Type	National Vulnerability Statistics for India		
	Total/Percentage	*In Millions*	*Vuln. to IP Ratio*
Total	753	753m	24:1
High	24 (3%)	24m	3:4
Medium	84 (11%)	84m	3:1
Low	470 (63%)	470m	15:1
Open Ports	175 (23%)	175m	6:1

f. National Vulnerability Statistics for India

F. Mexico

Vuln. Type	National Vulnerability Statistics for Mexico		
	Total/Percentage	*In Millions*	*Vuln. to IP Ratio*
Total	709	709m	25:1
High	29 (4%)	29m	1:1
Medium	75 (11%)	75m	3:1
Low	467 (66%)	467m	17:1
Open Ports	138 (19%)	138m	5:1

g. National Vulnerability Statistics for Mexico

G. Romania

Vuln. Type	National Vulnerability Statistics for Romania		
	Total/Percentage	*In Millions*	*Vuln. to IP Ratio*
Total	310	310m	28:1
High	6 (2%)	6m	1:2
Medium	58 (19%)	58m	5:1
Low	196 (63%)	196m	18:1
Open Ports	50 (16%)	50m	5:1

h. National Vulnerability Statistics for Romania

H. Country Comparisons

Four facts become apparent when analysing the results of the survey. The first, every country has vulnerabilities in all categories (which we would expect). The second, the amount of vulnerabilities varies between all countries. The third, when extrapolating the sample size to the IP population size, the amount of vulnerabilities each country is susceptible to, is in the millions. The fourth, whilst China's sample size was the largest of all countries tested, it consistently had the least amount of vulnerabilities per IP address in every vulnerability category; Russia (mid table sample size) exhibited similar tendencies, consistently having the second lowest amounts of vulnerabilities per IP address.

A distinct pattern can be observed when overlaying the plotted line data for all countries vulnerability to IP ratio categories (Fig. 1).

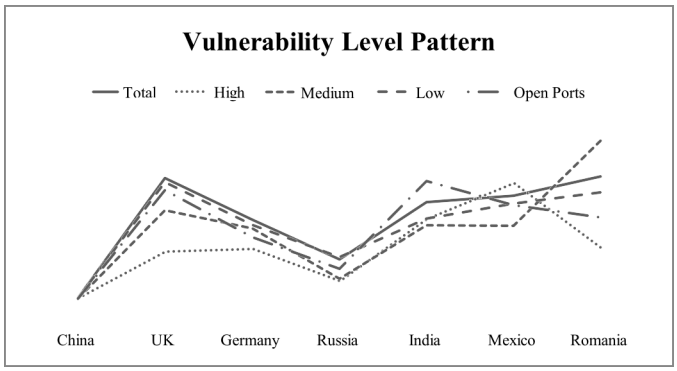

Figure 1. Country Vulnerability Comparisons

IV. CAUSAL FACTORS

Using a cause and effect analysis, four key areas of possible global influence have been identified: People, Political, Economic and IT Governance (Fig. 3.).

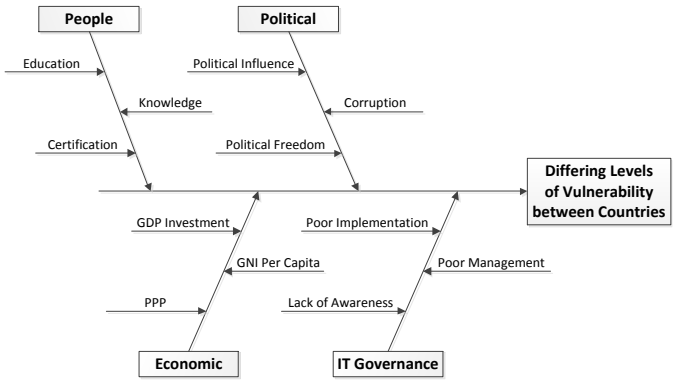

Figure 3. Cause and Effect Analysis

A. People

The Human development Index (HDI) ranks countries based upon a summary measure of human development [18]. HDI has been used to gauge the overall levels of education, certification and knowledge for a particular country (Fig. 4.).

Comparing the results from the HDI to the vulnerability volumes, does not lead to a direct correlation. China, the UK and Germany show a similar score (0.849 – 0.885), as do Russia, Mexico and Romania (0.719 – 0.767). A similar pattern cannot be observed in the vulnerability results. India scores the lowest on human development. This does not correlate with a similar pattern in the vulnerability data.

B. Political

To analyse whether or not political influence, political freedom and corruption share relationships with the vulnerability volumes found in this study, data was extracted from two sources. Firstly, Freedom House ranks every country in the world by political rights and civil liberties and assigns it a value. It also provides three classes of status, free, partly free, or not free [19]. Secondly, the Corruption Perception Index (CPI) ranks countries based upon their documented levels of corruption (the lower the ranking, the more corrupt). The Freedom House ranking scheme for political rights and civil liberties scores countries using a method that is inverse to the rest of the results shown in this study (i.e. the higher the score, the least politically free). These figures have been inverted to facilitate analysis. For example, the number seven is now the number one and vice versa, with the number four staying the same. This will not affect the accuracy of the results.

The Freedom House political rights and civil liberties scores show that China and Russia have less political rights and civil liberties than the other countries. Freedom House also states that China and Russia are not politically free.

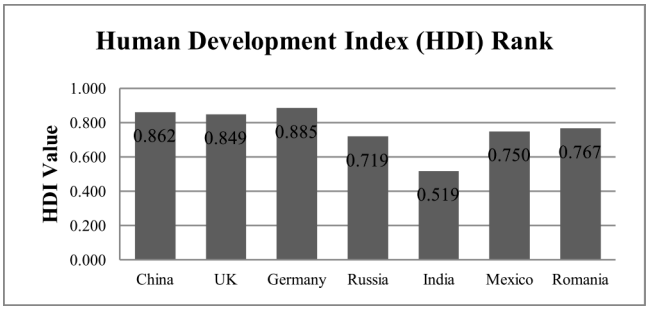

Figure 4. Human Development Index Rank

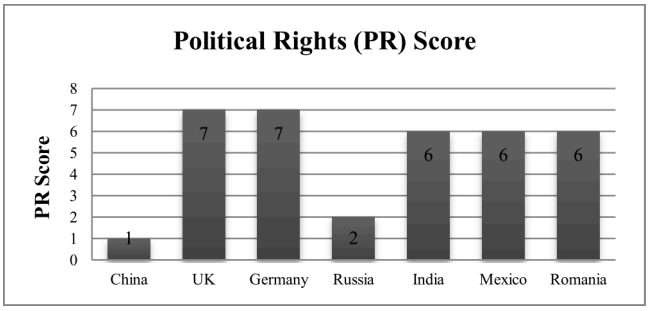

Figure 5. Political Rights Score

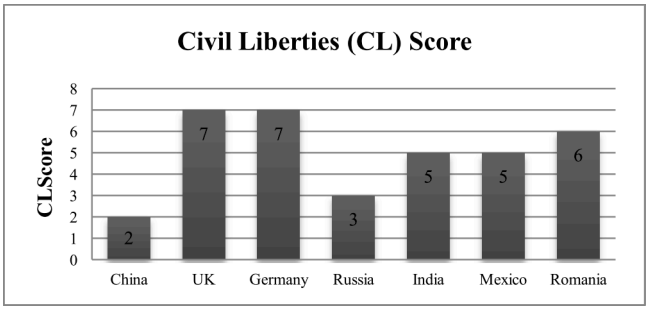

Figure 6. Civil Liberties

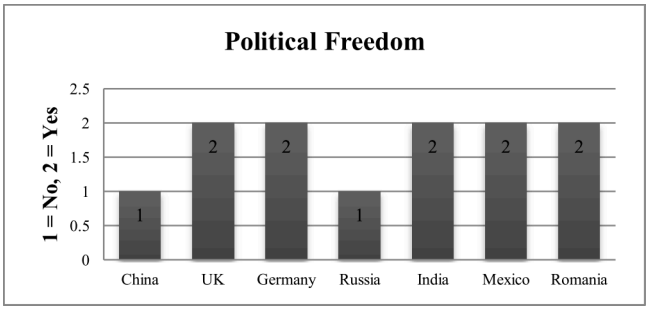

Figure 7. Political Freedom

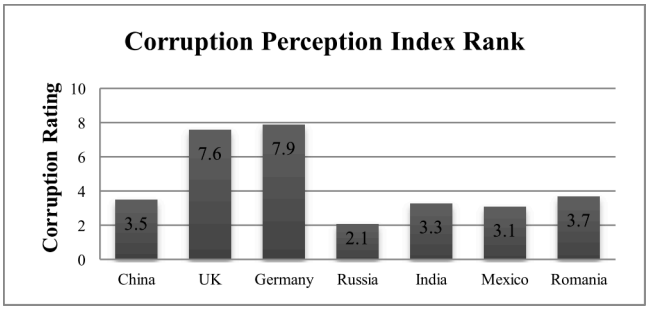

Figure 8. Corruption Perception Index Rank

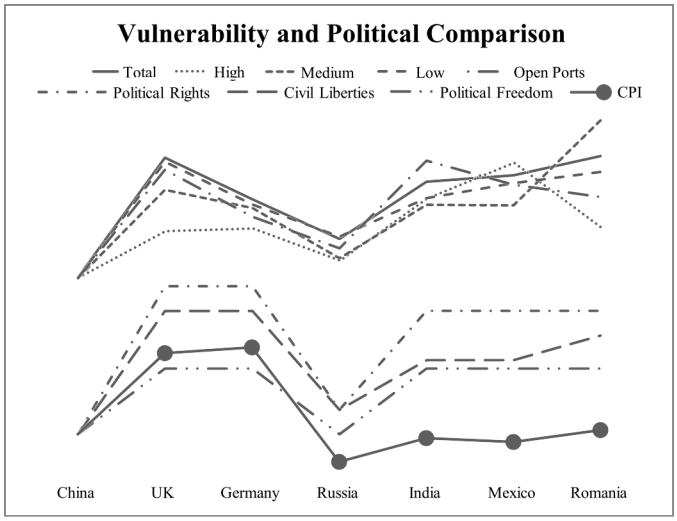

Figure 9. Vulnerability and Political Pattern Comparison

One trend that was similar throughout all of the vulnerability results was that China and Russia consistently scored lower in every category. This same trend is apparent in all political figures, 5 – 8. As established earlier, a clear pattern had emerged throughout the all categories of vulnerabilities. Fig. 9 shows a comparison of the patterns from the vulnerability and political results.

C. Economic

Gross Domestic Product (GDP) gauges the health of a country's economy. GDP is the total amount of goods and services produced in a single year [20]. Gross national Income (GNI) per capita, measures the average annual income of a single person per nation. Purchasing Power Parity (PPP) adjusts GNI per capita to compensate for the cost of living [19]. These factors have been looked at to determine any relationships with the vulnerability results (Fig. 10 and 11). Both GDP and GNI per capita do not share any similarities with the vulnerability results. The GDP statistics highlight strong annual growth for both China and India. This is not reflected on any of the vulnerability charts; in fact, neither country shares a single commonality. GNI per capita is low for both China and Russia and high for the UK and Germany. However, for the same vulnerability pattern to emerge, India, Mexico and Romania would also have to be high. Instead they dip lower than Russia which is inconsistent with the vulnerability data.

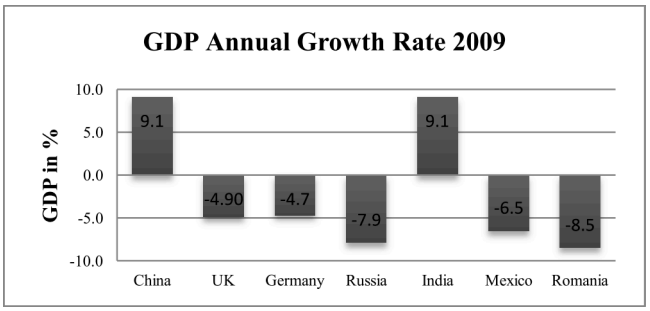

Figure 10. GDP Annual Growth Rate 2009

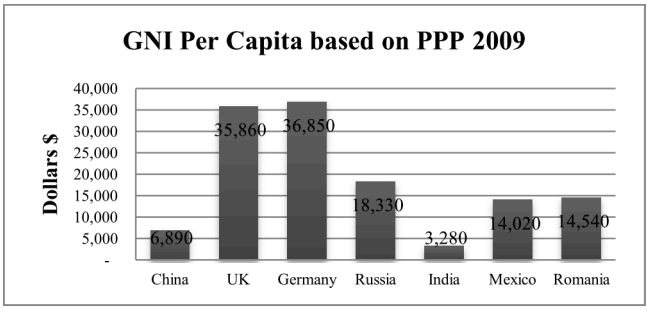

Figure 11. GNI Per Capita based on PPP 2009

D. IT Governance

PricewaterhouseCoopers [22] emphasise key facts regarding Asia, South America and Europe vis-á-vis information security. Asia is set to lead the world in information security through constant investment regardless of the economic climate. Vigorous security strategies which focus heavily on client requirement and data protection are being pursued, with far more emphasis on strengthening governance, risk and compliance capabilities than any other continent in the world. Europe on the other hand trails other regions in most areas of information security. Europe has the lowest responding figures to protecting sensitive customer information, Instead, placing a higher priority on the economic climate and the short-term impacts it has on information security. Showing a far more conflicted focus, South America is most likely to drop security initiatives or cut security budgets for other non-related business areas, ultimately highlighting financial caution. These key statements from PricewaterhouseCoopers are certainly reflected in the findings from this study. The results indicate that China is the most secure of the countries tested for vulnerabilities. Mexico, Romania, Germany and the United Kingdom all indicate high amounts of vulnerabilities, which is also reflected in PricewaterhouseCoopers findings. Nevertheless, this does not account for Russia or India. Parts of Russia lie within Europe; however, they have the second lowest amounts of vulnerabilities. India is part of Asia, yet has the second highest amounts of vulnerabilities. These two statements go against the findings from PricewaterhouseCoopers.

V. Conclusion

This research specifically looked at four levels of vulnerability (high, medium, low and open ports) pertaining to seven of the main IT outsourcing nations. The purpose of this was to identify the reality that organisations are faced with when outsourcing to foreign entities. With globalisation easing the restrictions placed upon international business, more and more organisations are looking to offload business operations via BPO and ITO to other countries. However, all countries exhibit millions of vulnerabilities, vulnerabilities that can be exploited in minutes. Historically, malicious attacks upon networks and network devices were sparse. The orchestration of an attack was complex, time consuming and took a great deal of skill and knowledge. Today, penetrating a valuable system is made easy using tools that are readily

available on the Internet [23]. Within hours, and with little to no knowledge, malicious individuals with limited technical understanding can be exploiting vulnerabilities within systems that carry sensitive information. India is the most popular BPO destination in the world, commanding 37-45% market share, yet three out of every four IP addresses on average is susceptible to a high level vulnerability. Mexico is a popular outsourcing destination for the United States. However, on average, every IP address in Mexico has the potential to carry a high level vulnerability. Businesses also outsource to other organisations within the same country. A UK business outsourcing domestically must take into consideration that a UK IP address can carry three medium level vulnerabilities. These statistics indicate that information may not be safe. It is questionable how companies partaking in any form of outsourcing can ensure that the confidentiality, integrity and availability of sensitive information remains preserved.

The results show that countries have varying amounts of vulnerabilities in all categories, high, medium, low and open ports. Table 2 ranks each country in the order of most amounts of vulnerabilities per IP address for each vulnerability category.

Four areas have been looked at to determine the root cause of the differing amounts of vulnerabilities between countries. Two possible theories emerged from the root cause analysis. Firstly, IT Governance, showed similarities between the regional levels of IT governance and the differing levels of vulnerability across the world. For example, PricewaterhouseCoopers [22] identified that Asia has focused their resources on achieving the highest levels of information security maturity, and the results from this study indicate that China and Russia (Eastern Russia also resides in Asia) are the most secure in terms of vulnerabilities. These facts corroborate with PricewaterhouseCoopers. However, the results show that India has some of the worst high level vulnerabilities which contradict this theory. Secondly, a recognised pattern between a country's political freedom and its vulnerability volumes was found in this study. China hides most of its infrastructure behind firewalls designed to block the outside getting in, and severely limit the inside getting out [24]. Russia on the other hand devotes extensive government resources to manipulating the internet through controlling the infrastructure it resides on [25]. This could explain why both countries exhibit far less vulnerabilities than that of the other politically free countries. It is pertinent to note that the conclusions presented in this paper are only a contributing cause to the varying vulnerability levels exhibited between countries. Further, their presence is neither necessary, nor sufficient, to negatively affect the potential for vulnerability issues within businesses offering outsourcing. Thus, it could be argued that considering the reputation and infrastructure (technical or otherwise) of the outsourcing provider under analysis, should be deemed paramount.

TABLE 2. COUNTRY VULNERABILITY RANKINGS

No.	*Country*	*High Vuln/IP*
1	Mexico	1:1 (1.04)
2	India	3:4 (0.77)
3	Romania	1:2 (0.55)
4	Germany	1:2 (0.54)
5	UK	1:2 (0.52)
6	Russia	1:3 (0.30)
7	China	1:6 (0.17)

No.	*Country*	*Med Vuln/IP*
1	Romania	5:1 (5.27)
2	UK	3:1 (3.16)
3	India	3:1 (2.71)
4	Mexico	3:1 (2.68)
5	Germany	3:1 (2.60)
6	Russia	1:1 (1.08)
7	China	1:2 (0.48)

No.	*Country*	*Low Vuln/IP*
1	UK	19:1 (18.88)
2	Romania	18:1 (17.82)
3	Mexico	17:1 (16.68)
4	India	15:1 (15.16)
5	Germany	15:1 (14.54)
6	Russia	11:1 (11.27)
7	China	7:1 (7.09)

No.	*Country*	*Open Port/IP*
1	India	6:1 (5.65)
2	UK	5:1 (5.38)
3	Mexico	5:1 (4.93)
4	Romania	5:1 (4.55)
5	Germany	4:1 (3.95)
6	Russia	3:1 (3.00)
7	China	2:1 (2.08)

VI. FUTURE WORK

Repeating this study yearly for all 195 countries would allow trend analysis for each country's vulnerability volumes. Each country's vulnerabilities could also be tested by taking the same sample size from each country, and cross-referenced with the percentile method results.

VII. LIMITATIONS AND CONSTRAINTS

A honeypot is designed to lure potential attackers away from critical infrastructure and to gather information about attacks and the malicious individuals [26]. A honeypot can contain any number of vulnerabilities depending on how it is configured. The method used to gather data from specific countries in this survey does not attempt to identify honeypots from legitimate network devices. Therefore, this may or may not have had an impact on the final results for each country.

REFERENCES

[1] M. Schniederjans, A. Schniederjans and D. Schniederjans. *Outsourcing and Insourcing in an International Context.* USA: M.E. Sharpe, 2005, pp. 25-28

[2] J. Halvey and B. Melby. *Business Process Outsourcing: Process, Strategies, and Contracts*. USA: John Wiley & Sons, 2007, pp. 134

[3] V. Sople. *Business Process Outsourcing, A Supply Chain of Expertises*. New Delhi: PHI, 2009, pp. 40

[4] Businessweek. "World's Outsourcing Market Worth $373 Billion." Internet: http://www.businessweek.com/globalbiz/content/sep2009/Gb20090925_476872.htm [July. 15, 2011].

[5] G. Blokdijk, *Outsourcing 100 Success Secrets: 100 Most Asked Questions: The Missing IT, Business Process, Call Center, HR-Outsourcing to India, China and More Guide*. Australia: Emereo Publishing, 2008, pp. 172-173

[6] S. Leimeister, *IT Outsourcing Governance: Client Types and Their Management Strategies.Germany: Gabler Verlag, 2010, pp. 1*

[7] IDC. “IT Cloud Services Forecast – 2008, 2012: A Key Driver of New Growth.” Internet: http://blogs.idc.com/ie/?p=224 [July. 29, 2011].

[8] Gartner. “Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010.” Internet: http://www.gartner.com/it/page.jsp?id=1389313 [Aug. 2, 2011].

[9] Forrester Research. “Sizing the Cloud – Understanding And Quantifying The Future Of Cloud Computing.” Internet: http://www.forrester.com/rb/Research/sizing_cloud/q/id/58161/t/2 [Sept. 5, 2011]

[10] Symantec. “Norton Cybercrime Report: The Human Impact.” Internet: http://us.norton.com/theme.jsp?themeid=cybercrime_report [July. 29, 2011].

[11] Symantec. “Symantec Internet Security Threat Report: Trends for 2010.” Internet: https://www4.symantec.com/mktginfo/downloads/21182883_GA_REPORT_ISTR_Main-Report_04-11_HI-RES.pdf [July. 25, 2011].

[12] IBM. “IBM X-Force 2010 Trend & Risk Report.” Internet: https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-spsm-tiv-sec-wp&S_PKG=IBM-X-Force-2010-Trend-Risk-Report [July. 26, 2011].

[13] Syn and Nackrst1. “IT Outsourcing Vulnerabilities.” Internet: http://outsourcingvulnerabilities.wordpress.com [July. 5, 2011].

[14] Nmap. “Free Security Scanner For Network Exploration & Security Audits.” Internet: http://nmap.org [July. 10, 2011]

[15] Nessus. “Tenable Network Security.” Internet: http://www.tenable.com/products/nessus [July. 10, 2011]

[16] Nessus. “Nessus 4.4 User Guide.” Internet: http://www.nessus.org/documentation/nessus_4.4_user_guide.pdf [Sept. 14, 2011]

[17] R. Gula and M. Arboi. “Performing PCI DSS and OWASP Web Application Audits with Nessus.” Internet: http://www.nessus.org/sites/drupal.dmz.tenablesecurity.com/files/uploads/documents/whitepapers/nesssus-web-based-auditing_0.pdf [Sept. 14, 2011].

[18] United Nations Development Programme. “The Human Development Index (HDI).” Internet: Available from: http://hdr.undp.org/en/statistics/hdi/ [July.27.2011].

[19] Freedom House. “Introduction.” Internet: http://www.freedomhouse.org/template.cfm?page=351&ana_page=362&year=2010 [July. 26, 2011].

[20] M. Parkin, M. Powell and K. Matthews. *Economics*. UK: Pearson Education Limited, 2008, pp. 470

[21] C. Hill. *International Business – Competing in the Global Marketplace*. USA: McGraw-Hill, 2010, pp. 57-59

[22] PricewaterhouseCoopers. “Global State of Information Security Survey 2011.” Internet: http://www.pwc.com/gx/en/information-security-survey/pdf/giss-2011-survey-report.pdf [July. 25, 2011].

[23] L. Spitzner. Honeypots: tracking hackers. USA: Pearson Education, 2003, pp. 15

[24] R. Clayton, S. Murdoch and R. Watson. “Ignoring the Great Firewall of China.” In *Proc. Privacy Enhancing Technologies: 6th International Workshop*, 2006, pp. 20-35

[25] Freedom House. “Country Report, Russia 2011.” Internet: http://www.freedomhouse.org/template.cfm?page=22&year=2011&country=8119 [July. 26, 2011]

[26] M. Whitman and H. Mattord. *Principles of Information Security.* USA: Cengage Learning, 2011, pp. 325