Towards a platform to visualize the state of South Africa’s information security

Ignus Swart
Council for Scientific and Industrial Research
Rhodes University
South Africa
ISwart@csir.co.za

Barry Irwin
Dept of Computer Science
Rhodes University
South Africa
B.irwin@ru.ac.za

Marthie Grobler
Council for Scientific and Industrial Research
University of Johannesburg
South Africa
Mgrobler1@csir.co.za

Abstract— **Attacks via the Internet infrastructure is increasingly becoming a daily occurrence and South Africa is no exception. In response, certain governments have published strategies pertaining to information security on a national level. These policies aim to ensure that critical infrastructure is protected, and that there is a move towards a greater state of information security readiness. This is also the case for South Africa where a variety of policy initiatives have started to gain momentum. While establishing strategy and policy is essential, ensuring its implementation is often difficult and dependent on the availability of resources. This is even more so in the case of information security since virtually all standardized security improvement processes start off with specifying that a proper inventory is required of all hardware, software, people and processes. While this may be possible to achieve at an organizational level, it is far more challenging on a national level. In this paper, the authors examine the possibility of making use of available data sources to achieve inventory of infrastructure on a national level and to visualize the state of a country’s information security in at least a partial manner.**

Keywords: National infrastructure, information security readiness, visualisation, big data, CVE, ISO 27001-2, security metrics

I. Introduction

Assessing the state of a nation’s cyber security is a complex and daunting task. Numerous factors contribute to the perceived assessment of readiness and often quantifying the value obtained is one of the key problems since standards are not always available or applicable. Due to the uncertain nature, complexity and active research environment found in information security, more than 1000 adopted standards have emerged [1]. Even in a single organization, defining a single metric to quantify the impact that varying people, software and systems have on cyber security is highly improbable [2].

Despite the potential complexity, the urgent need for a reliable quantification of the national security posture has spurred researchers into action to find solutions and implementations. The Cyber Readiness Index [3] is one such attempt. The index makes use of a variety of factors to assess the cyber readiness of nations. While not employing traditional information security metrics to assess information security readiness, the study adds value by allowing a comparison between countries based on common criteria.

Despite the proliferation of security standards, organizations continue to strive for compliancy since they have a strong economic incentive to do so. While a properly implemented information security standard might not prevent all attacks, it will serve to reduce the attack surface and more importantly, company liability in a variety of instances. Similarly it can be argued that governments produce policies, frameworks and legislation to protect its assets. ICT related activities currently constitute 4% of GDP and is projected to grow strongly in the coming years [4]

This paper explores the possibility of making use of commercially available datasets to construct a system that will provide an indication of the state of a nation’s information security. As a case study, South Africa will be used as an example in the sections that follow. The work conducted is in aid of exploring the South African National Cyber Security Policy [5] requirements. The potential to extend the platform to cater for other applicable ICT legislation such as the Protection of Personal Information Act [6] is also discussed. The following section will provide background information and highlight the existing need for such a system.

II. Information security standards and limitations when applied at a national level

Cyber security has been defined as “*a computer or network system’s resistance to becoming unavailable or unusable due to unauthorized uses; resistance to attacks that corrupt data stored on the system and cause information to leak out of the system; and a guarantee that data can be restored after an attack*” [7]. Assessing the information security posture of a single organization is already a complex task owing to different risk profiles and unique operational environments. Any number of the more prominent information security standards can be used such as ISO/IEC 27000 series [8], ITIL, COBIT, the King report [9] and PCI. All these standards are valuable in establishing and evaluating the maturity of an organization’s information security. While the relationship between the varying standards and frameworks are complex a graphical representation of the major framework and standard relationships is depicted in Figure 1 [10].

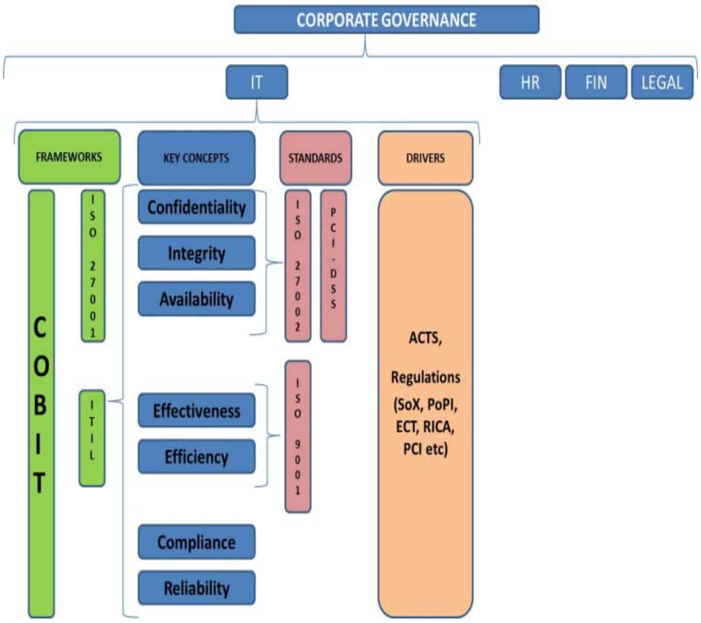


Figure 1: Relationship between standards, frameworks and their drivers [10]

The models and standards in Figure 1 have reached a relatively high level of maturity but several problems remain when attempting to apply them on a national level. By way of example ISO/IEC 27002 will be used to illustrate a point since it is presumed to be the most widely used standard [11]. Under ISO/IEC 27002 a section called asset management requires two main items [8]:

- All assets should be accounted for and an owner be identified.
- Information should be classified and handled according to its classification.

While achieving inventory compliance might be possible in an organization, it is nearly impossible to achieve on a national level if only for a lack of manpower, resources and access to information. The internet is not exclusively owned by government but by private individuals and organizations that also connect their infrastructure to the national network. Yet, government cannot simply step back and ignore the problem since it has a mandate to maintain national security [12]

While challenges exist it does not mean that it is not possible to achieve a national view of infrastructure connected to the South African internet infrastructure. Several technical solutions exist to obtain a view of a large number of Internet facing assets in a country as will be demonstrated in the following sections. Internet facing devices are of critical importance. In a typical network attack scenario, internet facing devices have the highest risk of being attacked. Thus, asset management by cataloging all internet facing devices in a country could satisfy part of the ISO/IEC 27002 requirement. Unfortunately since the entire standard cannot be realistically satisfied due to the abovementioned reasons, it becomes less suited to a national undertaking. Adhering to international standards is recommended where possible but preference should be given to practical security until suitable national security standards evolve. Bear in mind that standards enforcement does not always lead to a real rise in information security; often it simply degrades into a compliance exercise [13].

III. TRADITIONAL MEASUREMENT OF INFORMATION SECURITY IN ORGANIZATIONS

When measuring the information security of an organization, various methods have been attempted over the years with varying degrees of success. The latest traditional measurement technique to be critiqued is a component in a number of information security metrics. The number of vulnerabilities available on the network as measured by the Common Vulnerability and Exposure (CVE) metric [14] is but one such a measurement. A CVE entry is a description of a vulnerability, and can be used in metrics to aid in the:

- Measurement of the number of days that the system was exposed to the risk
- Severity of the vulnerabilities available on the network
- Identification of software packages affected by the vulnerability described in the CVE notification

A number of researchers since 2013 have shown why basing organizational security architecture and implementation on CVEs alone is not adequate. Various factors influence CVE notification accuracy and reliability, such as the following examples [15, 16]:

- CVEs are generated by unregulated third parties
- The severity score is guided by recommendations but is completely arbitrary and up to the individual reporting the CVE
- There is no single repository of CVEs; various entities perform an admirable task of collecting and collating individual CVE entries but duplication and unreliable data is unavoidable.

It should be noted that this does not detract from the importance of efforts such as CVE since it allows for information sharing. It simply means that CVEs alone are not nearly enough for an effective information security measurement implementation. The CVE effort however remains an important component of a larger view and is still one of the best de facto standards available for information sharing currently [16].

Various other metrics are available for organizational use such as the following [17]:

- Mean time to incident discovery
- Mean time to incident recovery
- Patch policy management and compliance
- Incident rate

It should be noted that the above metrics all provide individual pieces of data that should be collated into the whole organizational information security landscape. Individually the metrics tell but a small tale of the overall security posture of an organization.

The question remaining is that while the CVE metric is a flawed indicator of real security, can it still be used effectively as a measure of readiness indication? The answer is simply yes it can be used but it should not be used as the only measurement technique to assess the security posture of an environment [16].

IV. MEASUREMENT OF INFORMATION SECURITY ON A NATIONAL LEVEL

While there are several researchers active in the field of organizational security measurement [18], publicly available research on national security measurement has been sadly neglected. Work in this area that has been performed was found to primarily be in the areas of policy and strategy [12] and specific sectors of critical infrastructure such as power grids [19]. Very limited technical work has been described and the following reasons can be highlighted to underscore why this is the case:

- No clear responsibility
- Infrastructure and cost

Yet, if governments are serious about protecting their critical infrastructure the first step would be similar to a private organization wishing to protect its assets. The established international security standard ISO/IEC 27001 [8] prescribes a Plan, Do, Check, Act (PDCA) cyclical process model to achieve better security. The “Plan” phase requires that policy be implemented to improve security to a level the organization requires. The “Do” phase calls for implementation of policy, procedures and processes. In the “Check” phase, constant monitoring and comparison against the required result is required with changes to the environment as required. The final “Act” phase is to either alter the status quo or to allow the process to move on to the next critical item.

Moving deeper into specific controls such as those specified in ISO/IEC 27002, the recurring theme of asset inventory and classification is enforced. Inventory of hardware, software, people and processes are mandatory in several controls. This is done to determine the risk factor and also the attack surface available to an attacker to target. The available attack surface is one of the most prominent factors in determining the security and risk posture of an organization [20].

Our view is that the hardware and software components can be effectively measured as indicators with existing data sources, even on a national level. While it is logical that national infrastructure will present a significant attack surface, as with any other type of assessment, priorities can be assigned. With this type of system in place, researchers can move forward to device models to assess the cyber security readiness of nations. This will not only be based on the investment they have in policy and governance structures but similar to organizations include a bigger percentage of all the variables.

V. DATA SOURCES THAT CAN BE USED FOR INFORMATION SECURITY METRICS ON A NATIONAL LEVEL

Several commercial data sources exist that could shed light on the state of a nations information security. By applying standardized information security measurements to the available datasets, measurement on a national level can be achieved. Additional data sources are typically from either a company sharing data publicly or an individual sharing privately collected data. Regardless of the source, certain benefits exist in the utilization of these existing data sources instead of putting the infrastructure into place to collect and update the data continuously. Legal considerations are also a prime constraint for making use of third party data sources at present in South Africa. Case law has not proven if it is illegal to actively scan and probe networks in South Africa. Several sources provide indications that it might be legal [21, 22] but a variety of legislation needs to be considered. While it can be argued that the external parties had to scan and probe networks in order to obtain the very data used in the implementation, the act of scanning was not performed by local systems under South African law.

A serious drawback that is present when making use of external parties’ data sources is the lack of control over information obtained. Should the need arise to scan for a specific non-standard port, it is not simply a task of adjusting the scanning application. Another consideration is that there is a time delay between data availability and implementation. varying from data source to data source. This results in a system with a historic view rather than a real time view due to the delay in obtaining all the required pieces of information. This is a serious drawback but until South African case law sets clear guidelines regarding the legality of scanning, it might be the only option. Regardless of the limitations presented, the sheer volume of currently vulnerable systems is bountiful enough to warrant continued implementation with the current architecture. Increasing accuracy and detection rate should still be a priority but initial reporting and remediation of critical systems can be identified and prioritized concurrently.

The data sources used in the current experimental implementation are the following:

- ShodanHQ [1] data that contains a list of all detected devices in the South African IPv4 domain along with a list of all open ports and services detected. Nmap is one of the standard tools used in the ShodanHQ system making it a reliable, repeatable source of information.
- Maxmind [2] commercial geo location database is included in the processing phase to plot the location of the servers obtained from ShodanHQ on a map.

[1] http://www.shodanhq.net
[2] http://www.maxmind.com

- Google [3], Bing [4] and OpenStreetMap [5] API's implementations to visualize the geolocation data to the operator.
- NIST CVE [6] database that contains a comprehensive collection of vulnerabilities and exploits. This is mapped to the ShodanHQ data to classify each host in the collection as either Low, Medium or High risk.
- A custom dictionary generated by the research team containing common Leet Speak. This dictionary is then used to detect defacements and activity of unauthorized access.

While not specifically aimed at the South African landscape, each of the databases listed contain information regarding South African infrastructure as part of the data collection. Should the system prove successful, the possibility exists to expand the scope and allow for the evaluation of numerous countries in a similar fashion.

It should be noted that various other types of datasets are available such as the recently released Internet Census data. Data was obtained by logging into devices with default usernames and passwords and then commissioned to extend the scan for more vulnerable hosts. While these types of datasets provide a rich set of static snapshots to analyze, data on the Internet is very temporally bound. Factors such as DHCP, device replacement and infrastructure movement all require that the data source have the ability to be continually refreshed in a reasonable timeframe. Due to this temporal limitation, datasets such as the Internet Census is ill suited to the task. In addition, there are significant legal concerns with the manner the data was obtained. In South Africa gathering data such as those presented by the Internet Census would potentially breach the ECT Act in Section 86 (4) [23].

VI. EXPERIMENT IMPLEMENTATION AND VISUALIZATION OF THE CHOSEN DATASETS

Humans thrive on visual feedback due to the way in which we process information [24]. This makes effective visualization techniques an ideal tool to represent complex data. This visualization can only happen if data is available in a format that can be processed and quantified according to the abovementioned standards. However, one of the biggest problems according to current research is that the application of standards are not widely implemented, thus making measurement and visualization an unobtainable goal [25]. The current most prevalent reason that standards are not implemented is due to complexity, cost and lack of incentive [1].

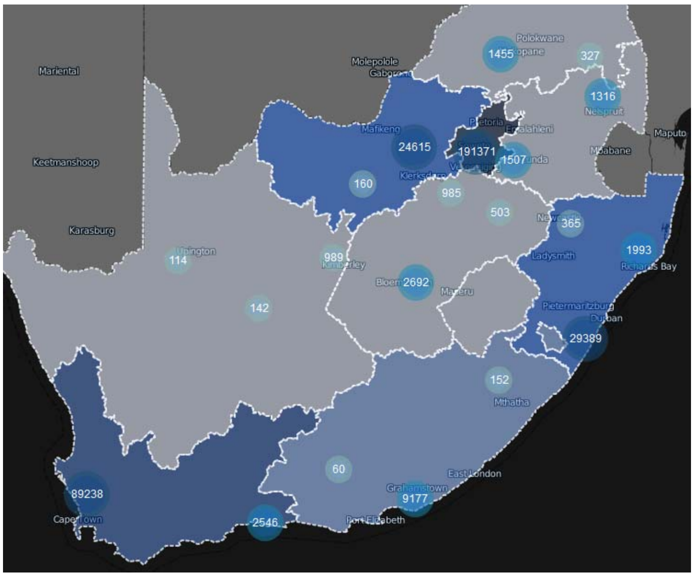


Figure 2: Initial view of RSA with devices grouped by geographic clusters

The prototype system initial view is presented in Figure 2 that depicts the ShodanHQ data merged with the Maxmind geo-location dataset and presented via the Google-map API. In order to allow the user the ability to obtain useful information several novel visualisation techniques had to be implemented. Zoom functionality was examined and used as a scale to determine the amount of clustering close by geo-located objects will require. The result of this type of operation is that the more the user zooms out, the more clustered the dataset becomes with specified thresholds between cluster groups.

Once the user makes use of the zoom function to move into a more detailed view of the map, the cluster groupings are regrouped into smaller clusters based on proximity to each other and zoom level. An example of this can be seen in Figure 3 that breaks the initial grouping of devices located across the province Gauteng into smaller clusters across city regions Johannesburg, Midrand and Pretoria. With a higher zoom level the devices will keep on breaking down into smaller clusters until street level view is reached.

[3] https://developers.google.com/maps
[4] http://www.microsoft.com/maps/choose-your-bing-maps-API.aspx
[5] http://api.openstreetmap.org
[6] http://nvd.nist.gov/

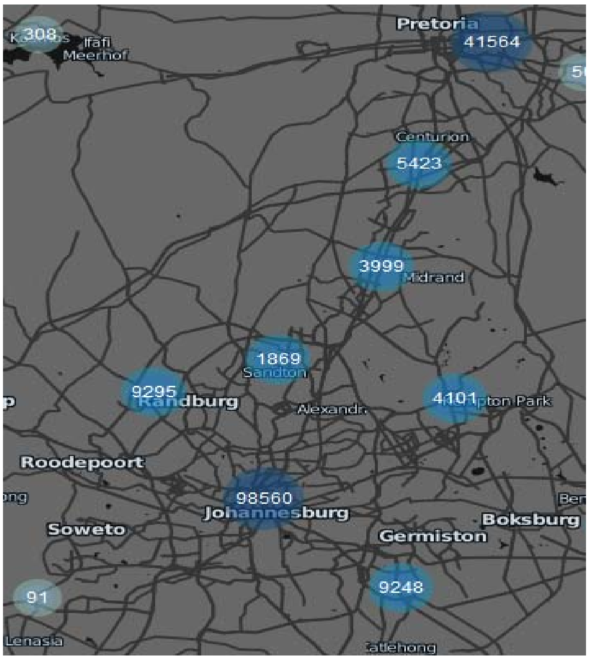


Figure 3: Zoom functionality creates smaller clusters in a deeper zoom value

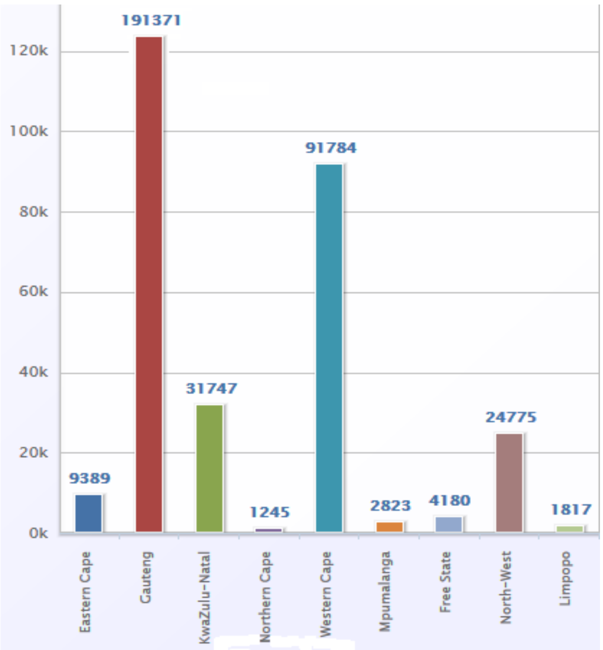


Figure 4: Device count visually represented and grouped by province

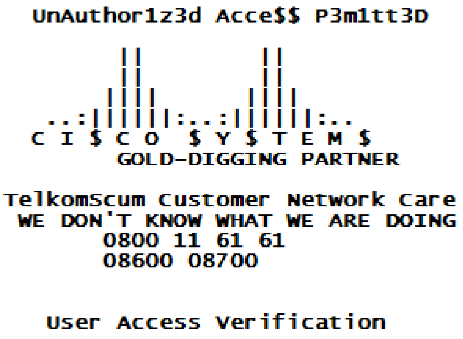
Various groups in business requires differentiated views and this remains true on a national level. Figure 4 is a graph view representing all internet facing devices grouped by their detected province. While not strictly related to security, such a view can be beneficial when determining risk distribution.

In the following section two case studies will be presented. These case studies will serve to display the potential a system implemented on a national level might have to increase the national readiness.

VII. CASE STUDIES

CASE STUDY A: LOCATING HACKER ACTIVITY

For an initial test the system was constructed and loaded with a current host dataset acquired from ShodanHQ, Maxmind and fused with the Bing map datasets. The host dataset was then parsed and processed with natural language filters to search for words similar to those contained in a generated leet speak dictionary. Several instances were found such as the banner in Figure 5, indicating that there might have been illegal access gained on the device. While leet speak is only an indicator, communication with the administrators confirmed that breaches did indeed occur. It was troublesome to determine the location of the device for the administrators and through the use of geo-location an approximate region to investigate was pinpointed.



```
   UnAuthor1z3d Acce$$ P3m1tt3D

            ||        ||
            ||        ||
           ||||      ||||
      ..:||||||:...:||||||:..
   C I $ C O  $ Y $ T E M $
          GOLD-DIGGING PARTNER

 TelkomScum Customer Network Care
  WE DON'T KNOW WHAT WE ARE DOING
         0800 11 61 61
         08600 08700


     User Access Verification
```

Figure 5: Example of leet speak detected in the South African dataset of Shodan

With the use of device banner information, hostname, who-is lookups and email communication, the administrators were notified. In some instances the administrators were part of vast organizations and could not immediately pinpoint the location of the devices in their network. The geo-location data were most helpful and allowed them to task the correct office to configure the devices. The devices were corrected and in the next iteration of data analysis, no instances previously reported were detected. Since the devices in question were Internet gateway devices for the most part, they were not always scrutinized by administrators and it is unsure how long ago the devices were potentially breached. It might therefore be beneficial to implement a monitoring system to regularly check local device configurations from the outside. This will allow Computer Emergency Response Teams to be alerted to sudden suspicious changes timeously.

CASE STUDY B: LOCATING A HOST WITH A CRITICAL VULNERABILITY

While implementing a system such as this has been proven to be technically feasible, success depends on more than just the detection of vulnerabilities. Relevant stakeholders will have to work together to ensure the successful reduction of vulnerabilities and to increase the national security posture. A full breakdown of role players is beyond the scope of this article but Internet Service Providers (ISPs) will be key in achieving information security readiness. This is due to the fact that machines located on the national Internet infrastructure make use of ISPs' infrastructure. When a query regarding the owner of the IP address is performed, it will resolve to the ISP and not to the owner. Only the ISPs will have information regarding the owner of the machine unless the machine in question provides a direct link to it's owner.

As an example a high level view of Gauteng is presented in Figure 6. A heatmap was generated based on the risk profile of the available hosts in the region. Matching is achieved by evaluating the host description against the various CVEs available. The heatmap color scheme can be implemented in various ways but in this experiment the common method of increasing color intensity to match severity is used. Hosts with a critical CVE will be assigned a red color while hosts with lower severity scores will be assigned less intense colors. In this instance yellow for intermediate scoring hosts and teal for low scoring hosts were used.

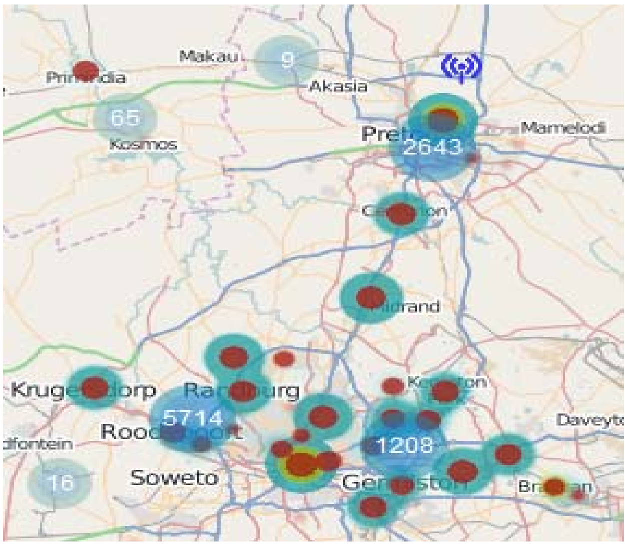
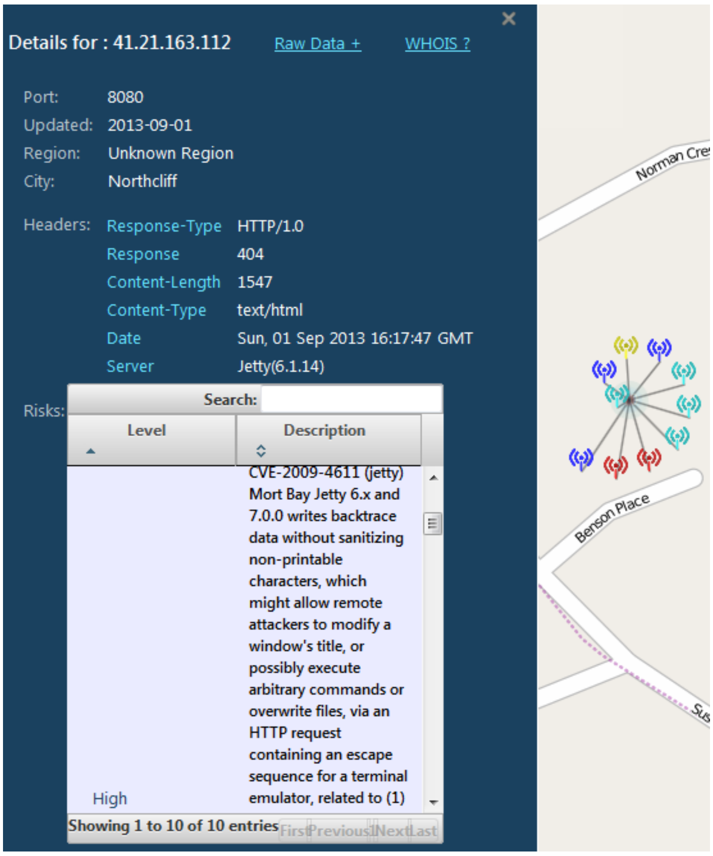


Figure 6: Heat map implementation of low medium and high CVEs affecting internet facing hosts

While heat maps work well when the zoom level is at a low enough level, as soon as specific details were required it became cumbersome. Instead the color scheme was retained but applied on individual hosts as soon as the level of zoom was sufficient to start identifying individual hosts.

In Figure 7 a host with a critical vulnerability was identified and the only manner to negate the vulnerability was to update the server software. As much information as possible was retrieved regarding the server, but no identifying information could be located relating to the owner of the server. Instead, the owner of the IP address used was contacted. Since this type of request is not normal for ISPs the turnaround time for the request was not immediate. However, after explanations and assurances, the service provider contacted the owner of the machine via e-mail and assurances were made that the machine would be updated.



Details for : 41.21.163.112 Raw Data + WHOIS ?

Port: 8080
Updated: 2013-09-01
Region: Unknown Region
City: Northcliff

Headers:		
	Response-Type	HTTP/1.0
	Response	404
	Content-Length	1547
	Content-Type	text/html
	Date	Sun, 01 Sep 2013 16:17:47 GMT
	Server	Jetty(6.1.14)

Risks:

Search:

Level	Description
High	CVE-2009-4611 (jetty) Mort Bay Jetty 6.x and 7.0.0 writes backtrace data without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator, related to (1)

Showing 1 to 10 of 10 entries

Figure 7: Individual selection of a host with associated detail panel

VIII. LIMITATIONS OF THE IMPLEMENTATION EXPERIMENT AND FUTURE CHALLENGES

While it might be possible to apply some of the available standards in such a way that it will allow for the measurement at a national level several factors limit the effectiveness of such an approach.

As it is, the current design will only provide a view on the devices directly connected to the Internet. This excludes any device behind a service such as a proxy server that obfuscates the individual device. Thus, it should be clear that the number of devices that have access to the Internet will be far greater than the number reported by the current datasets. This is due to the fact that only a single machine needs to be directly connected to the Internet for all internal machines to make use of it via services such as Network Address Translation (NAT).

With the implementation of IPV6 networks, the addressable space that had to be monitored effectively exploded. While it was possible with current hardware to effectively scan the whole IPV4 network address space in three months or less, this is not the case with IPV6. The much larger address space effectively increases the time to scan the whole range to near infinite with current hardware [26]. This is an advantage on one hand since it should reduce the effectiveness of worms and other malicious software that use automated means to scan the available networks. A disadvantage on the other since it becomes much harder to effectively detect devices in the IPV6 space.

Since the system makes use of commercial datasets, it is reliant on the external vendors for updates to the required infrastructure. Contacting persons responsible for the flawed detected hardware remains a manual task that is currently hard to automate. Typically the contact information for the person responsible for the flawed device/software on the Internet can be obtained to a limited degree via a WHOIS query. Unfortunately this is not always possible if the device that has a flaw is a router with a dynamic IP address. Should a system such as this be implemented, the co-operation of various ISPs would be required to effectively inform end-users. In addition to actually finding the flaw, some form of government agency, national department or appointed contractor would have to be available to assist the contacted personnel to correct the detected flaw should they not have the required skill themselves. This has been effectively implemented in the USA where the NSA will assist a company to secure their internal networks according to the national security specification.

IX. Metric implementation on a national level

In Section III examples of three calculations that will provide useful information security information were highlighted: The following section will apply the data found in the experiment to the highlighted examples for evaluation.

A. *Measurement of the number of days that the system were exposed to the risk*

Required components to calculate this metric are:
Disclosure date of the vulnerability (Available)
Time since the system was online with the vulnerability identified (Not available)

This metric is thus not viable to implement currently. Only after the experimental system has been up and running for a prolonged period of time will this metric become viable.

B. *Severity of the vulnerabilities available on the network*

Required components to calculate this metric are:

List of all discovered vulnerabilities available on the network (Available)

Severity of the discovered vulnerabilities (Available)

Since the current experiment is limited to host and software configurations this metric can be implemented.

The results obtained for the calculation in the example experiment returned a total of 8266 vulnerable hosts with a average CVE score of 5.24. A detailed breakdown is available in Table 1. The hosts and services were sourced from available Shodan data and merged with NIST vulnerability libraries.

CVE Severity	2	4	5	6	7	8	9	10
Number of Hosts affected	3047	1226	442	27	3046	25	101	352

Table 1: Breakdown of host with vulnerabilities by severity

It should be noted that other vulnerabilities such as physical security weaknesses is beyond the scope of this experiment and will thus not be reflected in the results of this metric. This reduces the accuracy of the current measurement but since a PDCA process is prescribed by ISO/IEC 27001, additional variables can be incorporated in future approaches.

C. *Identification of software packages affected by the vulnerability described in the CVE notification*

Required components to calculate this metric are:
Identified CVEs (Available)
Products related to CVEs (Available)

By performing a query on the experiment dataset for all software packages that contains vulnerabilities, a list of 699 different software packages were returned. While this list is too long to include, it is possible to group the software packages by vendor. The top ten products is listed in Table 2.

Vendor	**Number of products identified**
Cisco	114
Microsoft	69
IBM	20
Avaya	18
RedHat	18
VMWare	16
Nortel	14
Sun	13
Oracle	12
Suse	10

Table 2: Number of packages by vendor responsible for vulnerabilities

X. Conclusion and future work

While currently relying heavily on a variety of external data sources, the experimental system implemented has shown great potential to visualize information security data coherently. Visualisation techniques such as graphing, heat maps, clustering and layering were effectively used to present an easy to navigate system. Combined with an underlying data fusion engine, the potential to obtain information security metrics on a national level has been demonstrated. While true that not all metrics could be assessed, the system can continually be improved by following the PDCA process.

When looking towards the future, it is clear that additional research needs to be conducted to establish the percentage of error in results obtained. Investigating legal aspects to implement custom scanning infrastructure should also be considered to improve accuracy. While the system currently only focuses on Internet facing hardware devices, the scope for electronic legislation enforcement has great potential. With minimal alteration a similar system could prove useful in the regulation of recently passed legislation such as POPI. External data sources that already index Internet resources could be utilized to assess if any personal information is available. Once the information is obtained, the host IP could be correlated against geo-location databases in an attempt to locate the owner of the data.

By moving from a reactive to a pro-active enforcement model, there is a very real chance that it might lower losses suffered on a national level currently.

REFERENCES

[1] PwC UK, "UK cyber security standards," PwC UK, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/261681/bis-13-1294-uk-cyber-security-standards-research-report.pdf, Tech. Rep. 1, 2013.

[2] R. Böhme and F. C. Freiling. "On metrics and measurements," in *Dependability Metrics* (1st ed.), I. Eusgeld, F. Freiling C. and R. Reussner, Eds. 2008, .

[3] M. Hathaway. (2013/11/08). *Cyber Readiness Index 1.0* [Cyber Readiness Index 1.0]. Available: http://belfercenter.hks.harvard.edu/publication/23607/cyber_readiness_index_10.html.

[4] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. van Eeten, M. Levi, T. Moore and S. Savage. "Measuring the cost of cybercrime," in *The Economics of Information Security and Privacy* (1st ed.), R. Böhme, Ed. 2013, .

[5] South African Government Gazette, "South African National Cyber Security Policy," 2010.

[6] South African Government Gazette, "Protection of Personal Information Act," 2013.

[7] A. J. Burstein. Amending the ECPA to enable a culture of cybersecurity research. *Harvard Journal of Law and Technology 22(1),* pp. 168-222. 2008.

[8] International Organization for Standardization. (01/01/2013). *Information Security Management Standard 27001* [ISO 27001 standard]. Available: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.

[9] The Institute of Directors in Southern Africa. The king code on corporate governance for south africa. The Institute of Directors in Southern Africa. 2009.

[10] P. Jacobs, A. Arnab and B. Irwin, "Classification of security operation centers," in *Information Security for South Africa, 2013,* Johannesburg, South Africa, 2013, pp. 1-7.

[11] M. E. Whitman and H. J. Mattord. The enemy is still at the gates: Threats to information security revisited. Presented at 2010 Information Security Curriculum Development Conference. 2010, .

[12] M. Grobler, J. J. van Vuuren and L. Leenen. "Implementation of a cyber security policy in south africa: Reflection on progress and the way forward," in *ICT Critical Infrastructures and Society*Anonymous 2012, .

[13] J. Webb, S. Maynard, A. Ahmad and G. Shanks. Towards an intelligence-driven information security risk management process for organisations. Presented at 24th Australasian Conference on Information Systems Proceedings. 2013, .

[14] MITRE. (2014/03/17). *CVE - Common Vulnerabilities and Exposures* [CVE]. Available: http://cve.mitre.org/.

[15] S. Christey and B. Marion, "Buying into the bias: Why vulnerability statistics suck," BlackHat, Las Vegas, USA, Tech. Rep. 1, 2013.

[16] D. Geer and M. Roytman. Measuring vs. modeling. *;Login 38(6),* pp. 64. 2013.

[17] (2013/10/13). *CIS Consensus Information Security Metrics*. Available: http://benchmarks.cisecurity.org/downloads/metrics/.

[18] K. Brotby. *Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement* 2012.

[19] M. Hadley, L. Ning and A. Deborah. Smart-grid security issues. *IEEE Security and Privacy 8(1),* pp. 81-85. 2010.

[20] H. Vijayakumar, G. Jakka, S. Rueda, J. Schiffman and T. Jaeger. Integrity walls: Finding attack surfaces from mandatory access control policies. Presented at Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security. 2012, .

[21] S. M. Maat. Cyber crime: A comparative law analysis. 2009.

[22] G. Ebersöhn, "Internet law: Port scanning and ping flooding – a legal perspective," *THRHR no. 4 565,* vol. 565, pp. 66-70, 2003.

[23] South African Government Gazette, "Electronic Communications Security (Pty) Ltd Act," 2003.

[24] D. Grady. The vision thing: Mainly in the brain. *Discover 14(6),* pp. 56-66. 1993.

[25] R. Marty, *Applied Security Visualization.* Boston, USA: Addison-Wesley Professional, 2009.

[26] C. E. Caicedo, J. B. Joshi and S. R. Tuladhar. IPv6 security challenges. *IEEE Computer 42(2),* pp. 36-42. 2009.