1-1-2007

The benefits & concerns of public data availability in Australia: a survey of security experts

Roba Abbas
University of Wollongong, roba@uow.edu.au

The benefits & concerns of public data availability in Australia: a survey of security experts

Abstract

This paper gauges the attitudes of security experts in Australia with regards to public data availability on critical infrastructure protection (CIP). A qualitative survey was distributed to a individuals considered experts in CIP-related research in Australia, in order to address the censorship versus open access debate concerning public data. The intention of the study was to gain an insight into the perceived benefits and threats of public data availability by security experts, and to provide the basis for a security solution to be utilised by the Australian Government sector (at all levels). The findings however can also be applied to other data supplying agencies. This includes the identification and assessment of the technical and non-technical security mechanisms that can be enforced to protect sensitive public data elements that reveal information about Australia's critical infrastructure.

Keywords

benefits, concerns, public, data, availability, Australia, survey, security, experts

Disciplines

Physical Sciences and Mathematics

Publication Details

Abbas, R. (2007). The benefits & concerns of public data availability in Australia: a survey of security experts. In K. Michael & M. G. Michael (Eds.), The Second Workshop on the Social Implications of National Security (pp. 117-127). Wollongong: Univeristy of Wollongong.

10

The benefits and concerns of public data availability in Australia: a survey of security experts

Roba Abbas

Graduate, School of Information Systems & Technology, University of Wollongong

Abstract

This paper gauges the attitudes of security experts in Australia with regards to public data availability on critical infrastructure protection (CIP). A qualitative survey was distributed to a individuals considered experts in CIP-related research in Australia, in order to address the censorship versus open access debate concerning public data. The intention of the study was to gain an insight into the perceived benefits and threats of public data availability by security experts, and to provide the basis for a security solution to be utilised by the Australian Government sector (at all levels). The findings however can also be applied to other data supplying agencies. This includes the identification and assessment of the technical and non-technical security mechanisms that can be enforced to protect sensitive public data elements that reveal information about Australia's critical infrastructure.

Keywords: critical infrastructure, critical infrastructure protection (CIP), public data, security mechanisms, security

1 Introduction

Critical infrastructure protection (CIP) refers to safeguarding essential services from harm. CIP has gained recognition as a priority area on the national security agendas of many countries in recent years, most notably Australia, due to events that have compromised the critical infrastructure (CI) of other nations. The importance of the CIP process is evidenced extensively in the related literature, where the major phases of the process are discussed. Traditionally, the CIP focus is on the three major stages of vulnerability identification, risk assessment and risk management. A study conducted by Breeding (2003) introduced the risk of 'sensitive but unclassified' data to America's infrastructure, viewing the threat on CIP from an alternative viewpoint. 'Sensitive but unclassified' data refers to information that may not on its own appear harmful but when amalgamated with additional data elements can be truly revealing about CI, thus posing a threat to CIP.

The primary aim of this study was to raise awareness with respect to the censorship versus open information access debate, which is presently a prominent issue. Of great importance is to deliberate on whether certain CI-related information should be restricted from the public arena in the interest of national security, through a survey of security experts in Australia.

The primary objective of the survey is to gauge the attitudes of the experts with regards to the public data availability dilemma, a dilemma that is conflicted between whether public data should be restricted from public availability or be freely available. Public data related to critical infrastructure (CI) provide details about the characteristics of the CI, and in some instance can reveal sensitive information that can compromise the CIP process.

A qualitative survey was distributed to individuals considered experts in CIP-related research within Australia. Due to the vast and unstructured nature of public data availability, it is evident that many components and aspects of the protecting public data must be considered and a multi-faceted security solution must be devised, based on non-technical and technical mechanisms.

The solution provided throughout this paper is based on the outcomes of the survey, which highlights the need to evaluate alternative security mechanisms, and determine a possible restriction process through the use of a stakeholder matrix. The solution offered is focused on providing practical tools and recommendations that can be applied by government agencies and other data supplying bodies in Australia to assist in protecting CI from the negative implications associated with public data availability.

2 Background to the study

Critical infrastructure (CI) are the essential services that contribute to the stability and security of a country (Chakrabarty and Mendonca, 2004; Rinaldi et. al., 2001). A comprehensive listing of critical infrastructure includes energy, banking/

finance, water, transportation, agriculture, health and emergency, information and communications, storage and transportation, government, law and order, and cultural services (Breeding, 2003; Chakrabarty and Mendonca, 2004; Scholand et. al. 2005). A standard, global definition of critical infrastructure is not available; rather, each respective country determines their critical categories independently, based on the relative importance of each infrastructure item.

Critical infrastructure protection refers to safeguarding the identified services from potential harm, including physical and/or electronic attacks (ASIO, 2006). Although minor variations exist regarding the specific phases of the CIP process, it is widely agreed that the typical steps encompass vulnerability assessment/scanning, risk assessment, and risk management (Luiijf and Klaver, 2004; Jones et. al., 2003). The CIP process is a crucial consideration today, particularly due to the prevalence of national security issues as a result of global events, including 9/11 and the Bali bombings.

CIP has been a global concern since the Cold War. However, the issue has gained increased exposure in Australia since the incidents of Y2K, September 11, 2001 and Bali, 2002 (Luiijf and Klaver, 2004; Emergency Management Australia, 2003).

Additionally, the importance and increased use of the Internet and Information and Communication Technologies (such as biometrics, database processing, geospatial information exploitation, video processing and visualisations) have amplified the risks on critical infrastructure (Popp et. al., 2004). These technologies provide outlets for data/information exchange, and have simplified the ability to transmit data. Of particular importance to this research is the exchange of 'sensitive but unclassified' public data; data that on its own may be considered unclassified, but when combined may reveal previously unobvious or revealing patterns, which may prove harmful (Thuraisingham, n.d.). Access to such information does serve positive purposes, but can also expose the weaknesses of particular CI, thereby potentially compromising national security efforts if the data is applied maliciously.

An introductory study into the consequences of public data availability on critical infrastructure states that there is an increase in the education levels of the individuals/groups attempting to penetrate critical services (Breeding, 2003). In particular, their use of technologies, and the availability of certain tools, has become progressively sophisticated, allowing room for the collection, use and duplication of information. These concepts are supported by authors such as Weinmann (2006), who asserts that the Internet offers a vast repository of data that may potentially be exploited, and be used to compromise the CIP process, and consequently undermine national security.

The amalgamation of the abovementioned factors has resulted in, or prompted the need for national security to become a major global concern. While there are current government and research initiatives in place focussed on CIP and national security, inadequate attention is paid the notion public data availability in Australia

as a fundamental consideration in the CIP process. Furthermore, it is evident that the benefits of providing and accessing CI-related information online are generally promoted, whereas the negative implications are often ignored. The focus of CIP efforts, to date, have been on the establishment of risk assessment and management strategies, thus reinforcing the need for perceiving CIP from an alternative, but equally significant viewpoint.

This paper will attempt to address the public data availability issue through a survey of individuals considered experts in the CIP field. The study will focus on whether the experts are aware of the apparent threat, and will document the opinions of the individuals, in addition to possible solutions to the identified dilemma.

3 Critical infrastructure protection (CIP) survey

The *Critical Infrastructure Protection Survey* was distributed in hardcopy, at the National Security Technology Conference (21 September, 2006) and also subsequently online. The primary objective of this survey was to discuss issues relating to public data availability in Australia. Of great importance was to determine and gain an appreciation of the public data availability situation, as perceived by security experts. A key factor was to provide an outlet for security experts, researchers and interested parties who are knowledgeable about CIP to communicate their concerns and attitudes, and assist in providing suggestions to solve the public data availability dilemma. This dilemma is centred on the debate of whether public data concerning Australia's critical infrastructure should be restricted from the public domain to ensure that high levels of security are maintained, and that critical infrastructure are not compromised.

An additional objective of this research was to develop a solution using both technical and non-technical security measures. It is clear that the required solution must offer equal benefits to the four distinct community member groups or stakeholders within the Australian community, so as to ensure that a particular stakeholder is not disadvantaged in terms of public data access. The stakeholders include Australian Government agencies, operators of critical infrastructure, educational institutions and research networks, and the general public (citizens).

4 The profile of survey respondents

The qualitative survey yielded twenty-one security expert responses, almost half of which came from individuals employed by the government sector. With respect to the response rate, the survey was primarily focused on qualitative responses to public data availability concerns and the establishment of a practical solution. Therefore, it must be emphasised that the number of responses received was not a limiting factor to the study.

The collective profile of survey respondents reveals a heavy reliance on the use of free public data, or a combination of both free and purchased data. An interesting observation is that not one individual (organisation) depended solely on purchased

public data; a majority of the respondents found that free public data is beneficial for their purposes and in many instances is sufficient for their use.

In terms of day-to-day uses of critical infrastructure data, over half the respondents utilise public data to conduct risk assessment/risk management activities. Additional uses include government intelligence purposes, business intelligence purposes, service provisioning, Customer Relationship Management (CRM), navigation, construction, supporting response agencies with geospatial information, and research (tertiary education) purposes.

The overall profile of the respondents revealed that the group is knowledgeable concerning public data use, and that the data is beneficial for accomplishing daily tasks. Consequently, such information provided the foundations for determining the perceived benefits and concerns of public data availability in Australia, and working towards a solution to reach a balance between restricting data from the public domain and openly providing access.

5 The benefits and concerns of public data availability

Security experts reinforce the need for a balance between data accessibility and restricting access to data. The survey responses generally indicate that the difficulty in this situation stems from the fact that public data availability can present both positive and negative consequences, depending on how the data is applied.

The respondents felt that the benefits accruing from public data availability include promoting community trust, allowing immediate responses in time-critical situations, and assisting in the completion of daily tasks in specific occupations. The use of public data for such applications is crucial; therefore, the security experts generally maintained that it would be unwise to restrict access to the relevant datasets in such situations.

A number of security experts felt that community members have a basic right to access information concerning their surroundings and community. According to a respondent in the government sector, encouraging the concealment of basic community data and enacting harsh restrictions will inevitably result in Australia becoming a "secretive, scared society", which is a disagreeable effect. An additional point raised was that CI-related data should be publicly accessible "to ensure that governments and infrastructure providers are not relying on security through obscurity." Trust is an imperative factor in this situation, particularly in view of sustaining a positive relationship and level of transparency between the Australian Government and citizens.

Certain applications, such as emergency management, rely on the transfer and exchange of CI-related data in a timely fashion. A common notion expressed in the survey is that in such applications, direct data access is essential. Public data can therefore aid with activities including continuity planning, evacuation, infrastructure protection, and emergency management for incidents, such as earthquakes, cyclones, tsunamis, bushfires, infrastructure disruptions, and terrorist attacks.

Additionally, the survey revealed that the majority of respondents rely on public data in their respective industries to accomplish daily tasks. Public data access is beneficial in these situations, and increases safety in particular occupations. For instance, a security expert in the construction industry maintained, "as a structural engineer, information such as ground levels, location of buildings, location of electricity, water, gas, etc is critical to the safe design of buildings and infrastructure." Therefore, access to relevant CI-data, regardless of sensitivity, is required.

Despite these positive aspects, the situation is complicated due to the potentially devastating implications of public data availability, which encourages that the issue of data restriction be considered in order to minimise the existing threats. The concerns relating to public data availability include impacting on national security efforts (and therefore CIP), facilitating other forms of misuse, and affecting the privacy and confidentiality of individuals. These concerns are further explained.

The major concern identified regarding public data availability was the potentially damaging effects on national security and CIP programs, more specifically the use of public data for aiding in terrorist-related activities. As a survey respondent noted "access to data should be well-controlled to minimise the possibility of use by foreign and domestic adversaries". This thought is shared by other experts, one of which claims "if potential terrorists can access good quality data over the Internet, this can eliminate the need for on-site reconnaissance, which in turn eliminates the opportunity for the behaviour to be noticed, investigated, and attacks disrupted." Disregarding this concern can result in widespread and immeasurable physical and psychological consequences.

The concerns associated with public data availability are not limited to terrorist-related activities. Security experts expressed that CI-related public data can aid other forms of misuse and offences, with consequences such as increased crime, services disruption, vandalism, identity theft/fraud and obtrusive telemarketing.

Privacy and confidentiality are also key concerns in this discussion. While the data of interest to the research is CI-related, a number of respondents felt that personal privacy is an additional concern, which introduces the 'personal safety' dimension to the study. This is an important area for future research.

Therefore, public data availability presents positive and negative implications, although a government official responded that open access to data results in "CONCERNS ONLY". Similarly, a respondent in the education industry claimed that there were "no major benefits", as the positive aspects of public data availability are somewhat overshadowed by the potentially devastating damage. However, the majority of respondents feel that strict censorship and data restriction is not a viable option.

A common thread in the survey responses is that information should be available on a "need-to-know basis", to the appropriate personnel who require the data for carrying out tasks that are advantageous in some way. That is, "the TRADE-OFF between what one needs to have to do their work well, and what needs to be

kept sensitive because it may be used against a nation" must be managed. This is based on the concept that data should not be made available to individuals with no "legitimate" purpose to access it. Legitimate, in this instance, refers to whether an individual can justify that the data accessed will be used positively.

6 Achieving the balance: the public data availability solution

A notable outcome of the survey is that data should only be accessed for "legitimate" reasons. While in theory, this argument is seemingly valid and rational, in practice it is difficult to accomplish. For instance, a number of important questions emerge that require further thought:

1) What CI-related data elements will be available to certain individuals?
2) What conditions define a "legitimate" purpose?
3) How will the process as a whole be enforced?

The basis for a solution utilising non-technical and technical security mechanisms is put forward based on the survey results, providing practical answers to these questions.

An important outcome is the introduction of a stakeholder matrix, which is a non-technical method that can assist in establishing the sensitivity of CI-public data elements. The stakeholder matrix provides a sensitivity-based grading system that determines the relative sensitivity of CI data elements, and recommends who should be granted access to that particular element. The underlying concept behind the stakeholder matrix is to clearly outline the three grades that can be assigned to a data element. The first grade is 'unclassified/public' defining that a data element can be accessed by any individual; the second grade is 'restricted' meaning that only certain stakeholders are granted access and the final grade is 'classified/private' indicating that a data element cannot be publicly accessed under any circumstance.

The recommendation with respect to such a matrix is that it be used by data supplying agencies and bodies to decide which data elements may require censorship or restricted access. A sample matrix, based on the findings of the survey, is provided in Figure 1. The diagram depicts a possible classification system to be used as the foundation of the proposed public data availability solution. In its present form, the matrix can be used as a guideline; however, it is suggested that an expanded matrix be devised containing a comprehensive list of CI-related data elements and a similar analysis be performed by any agency that makes CI data available to the public.

The grade assigned to each specific data element in the matrix is based on whether security experts felt that the particular element should be available to the respective stakeholder. For example, if more than 66 percent of security experts felt a data element should be available, an 'unclassified' grade is assigned; if between 33 to 66 percent of security experts believe a data element should be available, a 'restricted' grade is assigned and if less than 33 percent of security experts believe it should be available, a 'classified/private' grade is assigned.

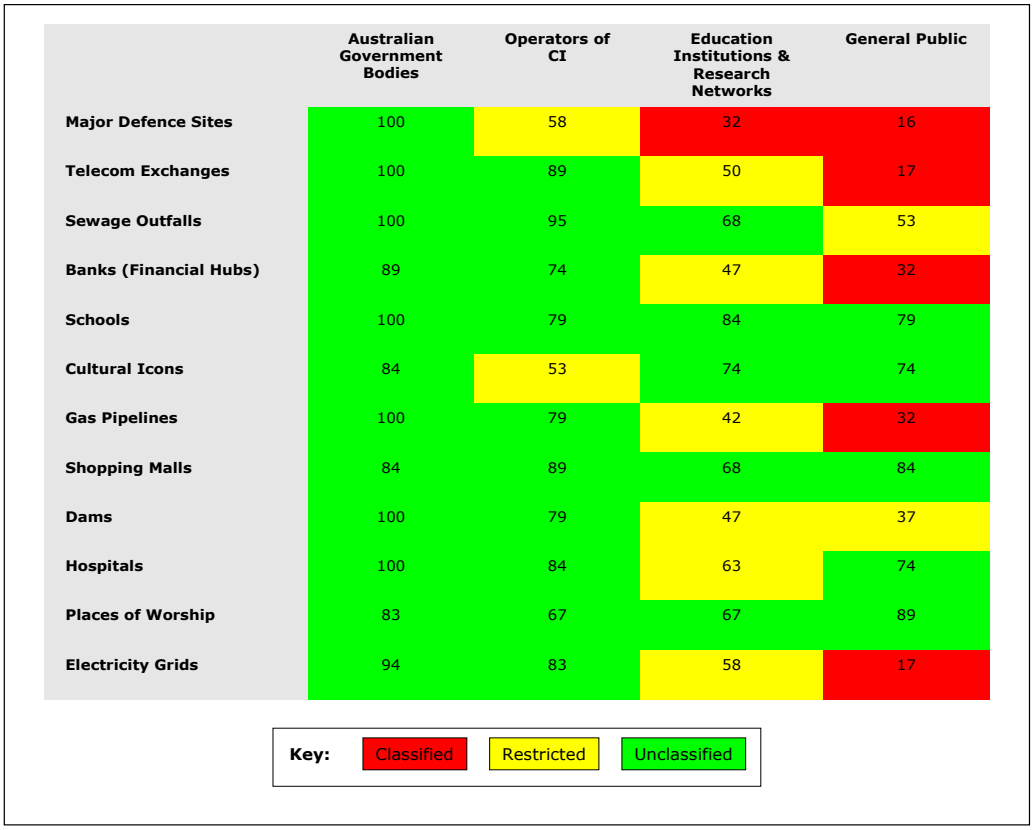

Figure 1. Data Sensitivity Stakeholder Matrix

The stakeholder matrix is a fundamental concept that will form the basis or foundation of any public data protection campaign, and is currently a missing element from the censorship versus open access debate. The survey reinforced the idea that this mechanism should be supported by additional security techniques, both non-technical and technical in nature.

Non-technical security mechanisms refer to public data protection tools that do not require the use of technology to be accomplished. Survey respondents feel that non-technical security techniques can be beneficial in public data protection initiatives, the most appropriate being:

- Legal and licence agreement containing conditions of use, defining the owner of the data elements and "WHO" will enforce the agreement
- Legislations, regulations and penalties, such as fines for breach of legislation or for inappropriate use
- Unambiguous policies and guidelines, accessible by the public
- Developing a register of approved users, and defining how they may use data. A suggestion was the use of "access control matrices", auditing and classification

- Communicating frequently with users about their rights and responsibilities with respect to data use. Educating users is particularly important; "Educate staff in government agencies about how data can be used, and what tabs governments are keeping. E.g. internal audit systems that run on intrusion detection systems might keep logs of all transactions to do with spatial and statistical data"
- Limiting sharing between departments and agencies, particularly within the Government sector, as it is not possible to distribute data and be sure that the data will be used appropriately
- Introducing physical security on assets to ensure correct storage, and prevent illegitimate physical access of data
- Encouraging a coordinated 'whole-of-Government' approach to data protection
- Prohibiting companies from selling data, which is an extreme option and is not realistic given the nature of the commercial data sector
- Using "common sense"

Information and Communication Technologies (ICTs) facilitate access to public data through the Internet, and consequently are at the centre of the public data availability dilemma. However, there is the potential to supplement the above-mentioned security techniques with technical measures in certain situations, and use ICT to assist in protecting and restricting access to sensitive datasets. According to the surveyed security experts, technical security mechanisms may include:

- Secure networks not displayed to the public on networks and the Internet, containing regular and real time encryption, logging, auditing, standard protection from damage (firewalls, intrusion detection systems) and appropriate filters
- Access control, and password protection, requiring identity checks to be performed for more sensitive data, such as defence information
- Security clearance for access to sensitive data, including providing proof of identity and justification in terms of data use
- "Deliberately non-integrated systems"
- "Central storage and distributed access"
- Review and update of technical security techniques, and measuring their effectiveness

7 Conclusion

A key outcome of this survey is that the public data availability situation may be interpreted in many ways, and one solution alone (for example, a technical solution) cannot be employed. Rather, there is the need for a responsive solution that targets

specific stakeholders, and is concerned with the sensitivity of public data in terms of compromising the CIP process, and protecting individual CI elements. However, it is important to note that the response suggested requires further work, and that the approach itself is not infallible.

An important point raised by a respondent is that perhaps the public data availability dilemma is being approached from an incorrect angle, that we should not address the issue only in terms of the mechanisms that can be implemented. Rather, it may be "about facing the root problems of terrorism, and addressing them." Extending this point beyond the terrorist threat, it may be valuable to address other adverse issues such as vandalism, fraud and competitive intelligence, and engage in why such activities take place and attempt to limit or address the causes. This requires further research, as it is beyond the scope of this paper.

When considering critical infrastructure protection, it is worth noting that CIP is one aspect of a broader solution. As stated by a security expert, "a government cannot hope to achieve a comprehensive approach to critical infrastructure protection if they are giving away data about their own infrastructure." Providing a wealth of CI-related data online can result in unscrupulous individuals conducting their own risk assessments, defining areas where the greatest losses will occur, and easily identifying the location of the CI elements. However, censorship is not the answer.

As demonstrated in this paper, a balance is crucial and many elements such as employing a structured approach using technical and non-technical mechanisms, in addition to determining the root cause of detrimental activities that can be carried out using public data, is essential.

References

Abbas, R. (2006). 'The Risk of Public Data Availability on Critical Infrastructure Protection', in K. Michael and M.G. Michael (eds), *The Social Implications of Information Security Measures on Citizens and Business*, University of Wollongong, NSW, Australia, pp. 201-212.

ASIO (2006). 'ASIO's Work: Critical Infrastructure Protection' [Online], Available: www.asio.gov.au/Work/Content/CIP.htm [Accessed January, 2006].

Breeding, A. J. (2003). Sensitive but Unclassified Information: A Threat to Physical Security, SANS Institute [Online], Available: http://www.sans.org/rr/whitepapers/country/ [Accessed December, 2005].

Chakrabarty, M. and Mendonca, D. (2004). 'Integrating Visual and Mathematical Models for the Management of Independent Critical Infrastructures', *IEEE International Conference on Systems, Man and Cybernetics*: 1179-1184.

Emergency Management Australia (2003). 'Mapping the Way Forward for Large-Scale Urban Disaster Management in Australia' [Online], Available: www.ema.gov.au [Accessed February, 2006].

Jones, E.V., Lyford, V. J., Qazi, M. K., Solan, N. J. and Haimes, Y.Y. (2003). Virginia's Critical Infrastructure Protection Study. *Systems and Information Engineering Design Symposium, IEEE*: 177-182.

Luiijf, E. A. M. and Klaver, M. H. A (2004). Protecting a Nation's Critical Infrastructure: The First Steps. *IEEE International Conference on Systems, Man and Cybernetics*: 1185-1190.

Popp, R., Armour, T., Senator, T. and Nymrych, K. (2004). 'Countering Terrorism Through Information Technology', *Communications of the ACM,* 47(3): 36-43.

Rinaldi, S. M., Peerenboom, J. P. and Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *Control Systems Magazine, IEEE* 21(6): 11-25.

Scholand, A. J., Linebarger, J. M. and Ehlen, M. A. (2005). Thoughts on Critical Infrastructure Collaboration. *Sandia National Laboratories, ACM* November 6-9: 344-345.

Thuraisingham, B. (n.d.). Data Mining, National Security, Privacy and Civil Liberties. *SIGKDD Explorations* 4(2): 1-5.