International Journal of Computing and Business Research
ISSN (Online) : 2229-6166
Volume 2 Issue 2 May 2011

SECURITY METRICS AND INFORMATION SYSTEMS IN E-GOVERNANCE

Subhash Chander
Assistant Professor
Govt. College, Sec-14,
Karnal (Haryana)

Ashwani Kush
Associate Professor
University College,
K.U.Kurukshetra (Haryana)

ABSTRACT

As much as the expansion of use of Information Technology (IT) in various processes in increasing the question of security is striking the mind time and again. Today we see various new applications of ICT are appearing day by day. Also the cases of security breaching are also on rise. We see in the daily newspapers about the terms like hacking/security breaching very common words. The concept of Computer Security is being heavily researched and this perfectly makes sense in a world where e-commerce and e-governance are becoming the norms of the day. Along with their potential for making life easier and smarter for people, these systems also carry with them the danger of insecurity. But security till date is taken as a qualitative measure. We can understand a subject complete and thoroughly through measurement. For measuring security we need certain metrics to say whether a particular system is secure or not. An effort has been made here to utilise certain available security metrics in the implementation of E-Governance services in India. In this paper a survey of various security metrics proposed in literature for information security and systems has been presented. Although the number of metrics are many but a few of these concentrating on security systems have been taken into account.

Keyword: RAV, ROI, ARO, ALE, SLOC, E-Governance

1.0 Introduction:

Information can not remains in the four walls of any organisation whether Government or private due to outsourcing. Any leakage of information can cause you to lose not only

money but also credibility, hence keeping our data, information and knowledge is becoming a big concern not only for private organisations but also for government enterprises. Even if you block the ports, scan all emails or work offline it can not guarantee data security [13].It is a widely accepted management principle that an activity cannot be managed well if it cannot be measured. Carefully designed security metrics can be used to offer evidence of the security behavior of the system under development or operation [4].Software analysis generally extracts arbitrary properties of software source code. Software metrics are a special kind of analysis focused on the structure of the source code. Classic software metrics range in variety from the very simple Source Lines of Code (SLOC) to more complex measures such as Cyclomatic Complexity measurements. Typical metrics report provides details on individual modules and summaries for subsystems. Such metrics are widely used to judge the quality of source code, enabling a software organization to more effectively focus its attention on the lower-quality portions of their portfolio [2]. The advantages of classical Metrics tools include wide acceptance of basic value of metrics, unbiased assessment of source code quality, repeatability of measurements, ease of measurement, and ability to judge progress in enhancing quality by comparing before and after assessments. In the Private sector, The companies' security advisors or security managers have to prove that their security programs are smart enough to keep the data safe and that the programs are offering satisfactory returns in lieu of the investment. This is achieved by measuring the security offered by a program or product at frequent intervals. These measurements are discrete data that show the effectiveness of the security program [3]. These information security measurements are then compared by testing the security systems at random intervals. The companies compare the effectiveness of a security program or software on several factors, including the number of risk factors that it is able to tackle. There are three critical components needed to ensure online security[6] namely website Certificates (Verisign) that prove that the website is owned by the company using the domain name, Encryption (SSL) which ensures that all customer data transmitted will reach the server without being "sniffed" or stolen in transit and website Security (Security Metrics) because Hackers are searching for websites with security holes. They

compromise those servers and download customer credit card data. Merchants are negligent if they do not test their server security how much loss they will have incur/face. IT is the tangible means by which information is manipulated and carried to its ultimate users. An information system is a collection of information and IT –including hardware, software, people, data, procedures- designed to deliver services intended to improve a social system [8].

2.0 Information Security:

The security thefts, threats and attacks are major problems for computer and Internet based businesses. Many managers and users of this area find it difficult to keep their information and IT assets safe and secure [11].According to Wikipedia Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Whereas Business directory defines Information Security as Safe-guarding an organization's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity. There are plenty of definitions for Internet Security on the Internet and libraries worldwide. However, the essence of all the definitions is the same. It is the combination of the above two definitions: 1) protection from unauthorized access and 2) maintaining the integrity of data. Plenty of methods are available and are under development so that your data stays safe in secure hands. The TLS (Transport Layer Security) and SSL (Secure Socket Layer) are some examples of such methods. SSL is generally used to make secure transactions over the Internet. You must have noticed the lock symbol while making a payment or when you access your bank online[3].If we use use a secure software having less vulnerabilities then we can motivate the people for using that software.Three pillars of software security are applied risk management, software security touch points and knowledge[9]. In computer software field rate of vulnerability is increasing as compred to last years . Various existing security models, security methods and security metrics are unable to provide security.To ensure that your data stays protected, scholars in the field use information security metrics to create, implement, and improve security systems that keep your data safe not only when it is stored on a

storage device, but also when it is being transmitted or received over a network or the Internet.Information security metrics help in creation and constant improvement of security systems so that you can use the Internet without any worries. Security metrics analysis means identifying tools and techniques that you can use to create actionable intelligence and organizational learning [7]. Information security is a complex area which makes it difficult but not impossible to identify useful metrics.

3.0 Security Metrics:

For businesses, developing the right set of metrics is a key part of maintaining security throughout the enterprise. Metrics provide organizations a measuring stick to use to effectively judge risk [10].Security metrics are the cornerstone of change control and information security in any information system.IT Security Metrics provides a comprehensive approach to measuring risks, threats, operational activities, and the effectiveness of data protection in your organization. Because any software system is an outcome of some software engineering process it makes sense to incorporate security considerations during the software engineering processes [1]. This is easier said than done because traditional software engineering approaches are requirements driven and pay less attention to security. Traditional software metrics do not address the issue of security well and now with security becoming an imperative necessity of most software systems, these metrics have to be adapted to take into account the security aspect [1]. Security Metrics are designed to be equally accurate whether calculating the security and loss controls measures for a military base, an office building, a bridge, a computer network, or a single, interactive application on a computer. Security metrics may also be termed as risk assessment Values (RAVs). The best use of RAVs is for measuring security in a consistent and repeatable manner. RAVs also allow for a percentage which is comparable through industry, organization size, region, policy, and financials. RAVs provide a benchmark that allows for third parties such as insurance companies, government auditors, industry regulators, and military personnel to correctly classify an organizational group from a single unit up to a national defense with one standard measurement [5]. The true benefits of metrics come when the data that they represent is

the end result of meaningful activities, actions that we take to accomplish a goal or a task[7]. Metrics bring not just information about IT security, but also costs and risks. Security metrics are a journey and not a destination. Metrics are conceptual data repositories—they define and standardize information. Metrics do not organize that information into knowledge, any more than well-defined word entries will transform a dictionary into literature. That job of transformation is done by people themselves.

4.0 Metrics today:

Security Industry is already having many security metrics and some of them are basis to improve security and reduce risk. But many of these metrics have limitation that makes them misleading indicators of security effectiveness. Some common metrics may be Risk, Annualized Loss Expectancy(ALE), Rerurn on Investment (ROI),Total cost of ownership (TCO) etc. we concentrate on these one by one as follows.

(a)Risk : Risk is a basis concept in IT security. When we start any work or business there is always risk factor in our mind. In IT security, risk is typically associated with some harm or loss to systems or data. But this definition is general and not accepted universally. Risk is also combined with other issues like threats, vulnerabilities, and parameters that are often imprecise which makes it difficult to measure. Risk means different for different people of various organizations. Risk can be estimated with the negative security event. As example if there is particular website and think of loss we will have to face if it is hacked. In case of E-Governance websites, the sites or systems related with land records, or financial transactions are more risky as compared to normal website providing general information about a system. The more the risk higher the security we need for that system.

(b)ALE : If vulnerability-related statistics is the measurement data in security, then Annualized Loss Expectancy (ALE) is the most commonly used conceptual metric. ALE refers to how much you think you will lose as a result of security incidents. ALE is pitched as a complete quantitative metric, with formulas and other statistical

goodness.The formula is expressed as ALE = ARO × SLE, where ARO is the annualized rate of Occurrence (how often you expect to experience the loss in a given year) and SLE is single loss expectancy (how much you expect one incident of the loss to cost you) [7]. This metric is hardly used and changed since its emergence in 1970 as part of Federal Information Processing Standards Publications (FIPS PUBS) published by the National Institute of Standards and Technology (NIST). This metric has developed into perhaps the most common single measurement in IT security. But unfortunately for security managers, ALE is a poor metric because of its expectancy factor. It deals in opinions and expectations primarily because IT security does not have the data necessary to define actual probabilities. Opinions we take through various surveys/questionnaires etc. Many private and government organizations do not have systematic programs for collecting and analyzing historical data even for vulnerability and incident data, that has caused a lot of losses due to security breaches. Many of the times these organizations are not even able to detect or track events that have led to this loss of data in real time. Industries like insurance function because they have made a science of collecting and sharing data regarding the risks that the industry faces as a whole. But IT security sector has not matured to a level at which we are able to do this and that is why we feel there is a need of verifiable security metrics. ALE can function only by assigning dollar costs to events (measuring tangible loss) whereas in IT sector intangible entities (like reputation, brand)are too much . ALE tends to focus specifically on technology systems, because they are the easiest to model. Lack of awareness is also one of the hurdles for our security environments.

© Return on Investment (ROI):

Return on investment (ROI) is a security metric that is used to calculate benefits (in Financial terms) from an investment being made. From the security point of view ROI is used in many ways. ROI is also related to ALE, which defines the expected security losses incurred in the absence of any preventative action. If preventative measure is costlier than the total benefit that is called negative ROI otherwise positive ROI is taken into account. Secondly ROI is used by security vendors as a means of marketing their products. Vendors may illustrate by building models how a particular organization would

get more ROI after buying their product. Vendors may also decide the prices of their on the basis of that ROI they are providing to its customers. Security activities are not performed for profit purposes as in case of business. Rather IT security has to do with loss reduction & prevention, much like physical security mechanisms such as locks, fences, and guards. But the reason behind use of this term in IT security is clear for motivating the people for the security of their information & systems. Until and unless we are not aware of the benefits we are not ready to invest a single penny.

(d) Total cost of Ownership (TCO):

ALE attempts to measure losses associated with IT systems and ROI attempts to measure the profit derived from them, TCO tells us about the quantity of the money that must be spent on the system throughout the entire ownership lifecycle, from initial purchase to final disposal. Purchase may include hardware, software, License fees, Infrastructure, Installation and maintenance, training, security and other hidden costs. As Example when we buy a new bike then we have to keep in mind long-term costs associated with it like insurance, maintenance, and fuel. Similarly In IT Security TCO attempts to think of costs associated with data protection systems more visible, so that a picture of the actual costs of a System is revealed. Negative point of TCO is that it can help you to understand how much a security product will cost over its lifetime, but that doesn't tell you whether or not it will meet your security needs. Security TCO also has certain data uncertainties like other common metrics. Because the security world can't agree on how to track or measure the impact of security incidents, and many costs remain hidden and are not available for analysis. TCO can be a useful comparative metric but it does not measure security operations. It is very much used in Industry sector. Every industry has to face with risk, uncertainty and complexity. The same is the situation with IT security. Here we are to secure our data and there are various sectors doing the same job like insurance. To compete in insurance sector security of data is must we can learn something from such booming sectors and follow some of the security metrics followed by these industries.

5.0 E-Governance:

E-governance is application of IT to the processes of Government functioning to bring out responsible, responsive, efficient and transparent governance. E-Governance refers to the use of information of Communication Technologies (ICTs) to improve the efficiency, effectiveness, transparency and accountability to government [15]. Traditionally we have to visit an office for any govt. or business service. But now with the emergence of ICT [16] it is possible to locate service centers closer to the citizens. E-Governance is composed of IT, people and governments. It is an application of electronic means to improve interaction between Government and citizens; and to increase the administrative effectiveness and efficiency in the internal Government operations [17]. It is application of IT to the Government processes to bring Simple, Moral, Accountable, Responsive and Transparent (SMART) Governance [17]. It is not only just computerization of services but also reinventing the new ways of governance. Advent of Internet Technology has changed the traditional Government to E-Government. Such a Government would bring transparency; check on corruption if it is implemented successfully. E-Government is a technology led administration where citizen can avail government services like getting a copy of land records, tax return filing, various types of certificates whereas E-Governance involves formulation of laws and regulations such as domain name to govern cyber space [14].E-Governance resources can be utilized by common people for their day to day basic problems. As after the birth of a child in family now it is compulsory to have birth certificate to admit him/her in school. To get that certificate is not easy job for a common man. He has to go in various offices situated at various places many kilometers away from each other. He will have to waste his precious time and money. To get that certificate in a fixed time may force a common man for bribing also. In away in such a society a poorer is becoming poorer. But now a person may get such type of certificates sitting at native village through CSC to be started in Haryana very soon. This CSC would be common and convenient place for (maximum 6 villages) and all basic certificates like birth, death, caste certificates, domicile certificates, land record certificates etc. would be available at these centers at a very affordable rates. These facilities may be increased at village level and daily crop

rates at seasonal level. Other services may also be provided like fill up forms online for proper counseling through online off campus .but major threat to such systems is security.

6.0 Security Metrics its use:

There are several uses of information security metrics. These metrics are helpful in determining the strength and weakness of any information security system at any given point of time. While one can assess the effectiveness of a security system using the information security metrics, they also find the metrics useful in improving the information security systems. Most of the security attributes such as confidentiality and integrity are terms of qualities [12]. But difficulties in measuring such qualities are different interpretations of what they really mean.The information security metrics obtained from different sources can also be used to create an efficient information security system from scratch. While creating an information security from scratch, the data is collected from different existing information security systems. The data should be enough to help create information security metrics. This also means that the information systems analyst must collect data more than once from each security system before creating the information security metrics. The difference in time offers more brevity to the metrics so that the analysts may study them and design the model of good and effective information security systems. information security metrics help in creation and constant improvement of security systems so that you can use the Internet without any worries.The information security metrics help in identifying the vulnerabilities and leaks in the security program being used by a company. They can inform the security engineers about the possible problems that can occur if a process is not implemented properly [3].

7.0 Present status of E-Governance in Haryana:

The Government of Haryana has given a special emphasis on implementing Mission Mode E-Governance Projects, identified under the National e-Governance Plan (NeGP). Haryana has its IT vision and a dream. A vision in which all citizens can access Govt.

and private sector services from their own villages and towns. The state's e-Governance Vision statement is "To achieve Efficiency, Transparency and Accountability in governance by providing ICT enabled access and opportunities for all, anywhere, anytime". Haryana Government has taken proactive initiatives to reduce the digital divide in the society for which the State Govt. has taken up many Mission Mode Projects under National E- Governance Plan of Government of India. A well-defined, transparent & efficient system for the systematic approval of the Departmental IT action plans has been put-up in place through various High Power committees which include State Level IT Steering Committee (ITPRISM), State Technical Committee, society for IT initiative fund for e-Governance initiatives at State level, District IT Society in each district [18]. Haryana has been treated as leader in e-Governance readiness index 2006 of the country. The state has been Winner of "Best e-Governed State Government" TELECOMM India Excellence Award 2007. Till date, state has received 18 prestigious national e-Governance Awards. Haryana has been ranked number 4th in the Dataquest-IDC e-Governance Survey 2008. The state has progressed from 18th position in 2007-08 to 4th position in 2008-09, ahead of Andhra Pradesh, Karnatka, Goa, Gujarat, Maharastra etc. The state has successfully organized 11th National e-Governance Conference during Feb. 2008. Haryana is first state to introduce on-line off-campus Counseling system and on-line Entrance examination system for admission to technical / professional courses. This project has received Gold Icon Award at 11th National e-Gov Conference at Panchkula organsed by Haryana in February 2008. The project has also received "Best e-Governed Project – Excellent Project" Award of CSI-Nihilent Excellence awards –2008. The Mustered Procurement Management System implemented in Rohtak District has received Silver Icon Award at 11th National e-Gov Conference. Administrative Reforms and publishing of all Results, admit cards, provisional certificates on web, received Skoch Challenge Award in March 2008. GOI has selected Haryana for implementation of Smart Card based PDS and Ration Card System on pilot basis. The Govt. of India has also sanctioned a pilot project IntraGov Haryana Portal with integration G2G & G2E applications under e-Office suite. The Export of Software, IT/ITES/BPO from Haryana has reached to Rs. 17,500/-Crores approximately in 2007-08

from Rs. 14,700/- Crore in 2006-07[19]. In principle, more than 71 IT/Cyber Parks /cities have been approved by State Govt. The establishment of these IT Parks will generate around 2.50 lakh employment opportunities in the State. A Technology Park has been set-up in Panchkula and a Nano city is planned to be set-up in Panchkula to create an environment and eco system, which would create a large number of jobs and bring economy prosperity in the region. The web portal of Haryana[18] has been redesigned to give a new look & feel and enhanced with G2G, G2C, G2B, G2E services. Haryana specific inputs (G2C services & information, schemes, forms, procedures etc.) are uploaded on India portal [20]. In Haryana the e-Governance efforts are supported by central agencies (namely State IT Department, NIC-Haryana State Centre, and HARTRON), which are providing the necessary Guidance in the use of correct methodology. The State IT department is facilitating the departments and NIC-HRSC & HARTRON are assisting on technical aspects. The DEIT, NIC Haryana and HARTRON has been working very closely under a common structure Secretariat for Information Technology Haryana, which has helped the state to achieve these land marks in e-Governance.

8.0 Conclusion:

The importance of quality data, the focus on security as a business process, and a greater respect for the role of people and social interactions in the security process are all important elements of a successful security metrics program. Whether a metric is good or bad, quantitative or qualitative, security professionals should be more concerned with whether their metrics meet are well understood, used and provide value and insight. By having a look at the current scenario of E-Governance we may utilize security metrics for measuring security of various E-Governance applications. But here our aim is not to earn profit but to provide reasonable security to the websites and information systems so that people may avail all facilities freely without any hesitation. People would utilize those services only if they are convinced about the security of the systems they are using.

REFERENCES

[1] Sree Ram Kumar T, Sumithra A and Alagarsamy K."The Applicability of Existing Metrics for Software Security" International *Journal of Computer Applications*, Volume 8 ,Number 2, Pp 29–33, October 2010.

[2] Available at semdesigns.com

[3] Available at www.brighthub.com

[4] Reijo M. Savola ," A security Metrics development method for software intensive systems" Advances in Information security and its application,Communications in Computer and Information Science, 2009, Volume 36, Part 1, 11-16, DOI: 10

[5] Available at www.isecom.org

[6] Available at www.securitymetrics .com

[7] Lance Hayden **,"**IT Security Metrics, A Practical Framework for Measuring Security & Protecting Data " What is a security Metric, Ch. 1 ,page 6, Mc. Graw Hill Publication, 2010

[8] Sanjay Kumar Jha," Information technology with management and Responsibility", International Journal of Information Technology and Knowlwdge Management,Volume 2,Pp. 79-82, January-June 2009.

[9] Deepshikha Jamwal, Simmi Dutta," Security issues of Software Development", International Journal of Information Sciences and Application, Pp 233-237, Volume2,Number 2 (2010).

[10] Available at www.eweek.com

[11]Binod Kumar,Kanak Saxena," Computer Security: selecting an effective business security model" International Journal of Information Technology and Knowledge Management, Pp. 425-427, Volume 3,No. 2 July-December 2010.

[12]Mukta Narang, Monica Mehrotra," Security issue : A Metrics Perspective ",International Journal of Information Technology and Knowledge Management, Pp. 567-571, Volume 3,No. 2 July-December 2010.

[13] Gagandeep Singh Sodhi,Manpreet Kaur ," Various risks, threats and standards of information security in Indian Economy",International Journal of Information sciences and Application, Pp 259-263, Volume2,Number 2 (2010).

[14] Gupta M.P., Kumar Prabhat, Bhattachrya Jaljit : “Government Online opportunities and Challenges”,Ch-1,2004,TMH Publication.

[15] D.N. Gupta,” E-Governance, A comprehensive framework” century Publications,2008

[16] Tutorial paper ,” what is ICT “ Makerere university,university library ,ICT awareness camp 6-7 July 2001,Uganda.

[17] B.Ramadoss , Ram Palanisamy Issues and Challenges in electronic Governance Planning

[18] Available at WWW.haryana.gov.in

[19] Available at WWW.india.gov.in