ISSN No:-2456-2165

Mobile Security Metrics

Drd. Ioan Adascalitei
Economics Informatics
Academy of Economic Studies
Bucharest

Abstract:- Measuring security is a complex task and requires a great amount of knowledge. Cyber security has always been a matter of concern since the advent of computers and the Internet but became more critical and necessary these days. With lots of threats concerning data security playing all over the digital and business landscape, but not restricted to that, it's only imperative for all the actors to have right cyber security metrics in place to help them evaluate if their efforts are effective or not. Security metrics helps in indicating the needs to focus on problematic areas and identifying trends that show changes in this area.

Keywords:- *Mobile; Metrics; Security.*

I. INTRODUCTION

Mobile devices became, in the last years, a very important and significant part of every person day by day life because the offer access to a lot of services, like mobile payments, food delivery and many more, services which are meant to simplify human life. All these diversion of services was possible due to the multiple forms of connectivity provided by and through mobile devices. Between these forms of connectivity are Bluetooth, 4G/5G, NFC, WiFi and others. All these multiple services came with a cost, in the same time with their increase the number of vulnerabilities increased as well. Therefore, smartphones represent now an ideal target for malware. Cyber security has always been a matter of concern since the advent of computers and the Internet but has become more critical and necessary these days. With lots of threats concerning data security, and more, it's only imperative to have the right metrics in place so we can determine if the efforts done in cyber security direction are effective or not.

What is a metric? - A concise dictionary definition of metric is a „standard of measurement".

Why do we use metrics? –When we measure something using consistent metrics we improve the ability to understand it, to control it, and in the case of a threat to better defend against it. According to the performance engineer H. James Harrington „Measurement is the first step that leads to control and eventually improvement. If you can't measure something, you can't understand it; if you can't understand something, you can't control it; if you can't control something, you can't improve it."

What makes a good metric? - Security professional Andrew Jaquith states that: „

- ➢ Good metrics should express results using numbers rather than high-low-medium ratings, grades, traffic lights or other nonnumeric methods.
- ➢ Good metrics must be clear and unambiguous
- ➢ Good metrics facilitates inexpensive collection (the cost of collecting data doesn't need to exceed the value of data)
- ➢ Good metrics supports decision making"

II. CONCEPT OF INFORMATION SECURITY METRICS

Understanding the various measurements accessible for data security begins with a review of what a measurement is. The Oxford online word reference characterizes metric as a framework or standard of estimation, also it characterizes estimation as the activity of implying something, the activity of finding out the size, sum, or level of (something) by utilizing an instrument or gadget set apart in standard units [1]. Metrics and measurements are personally connected. Despite the actual fact that they're frequently utilized one rather than the opposite, they're extraordinary. Within the remainder of this paper, the choice has been made to utilize them reciprocally, in reception of a stance just like the one in all Applied Computer Security Associates (ACSA) [1] [2]. Once we discuss metrics we confer with it as a conceptual and subjective attribute [1] [3], while when it's about measure we confer with it as a solid, target trait. Measurement results from an observation, utilizing some proper strategy to collect information and metric speaks to the watched information in kind of scale [1] [4]. In the wake of mentioning objective facts to acknowledge estimations, investigation is performed to produce measurements [5].

There does anyway appear to be a typical understanding that measurements is tied in with mentioning objective facts and that these are at a solitary point in time [6] [7]. Metrics then again are about investigation and examination [2] [8]. They should give you data about IT Security [6] [9]. Andrew Jaquith defines metric just like a standard of estimation [6] [10]. The standard ISO/IEC 27004 characterizes estimation because the way toward acquiring data about the adequacy of knowledge Security Management System (ISMS) controls [6] [11]. an identical standard characterizes measure rather like a variable to which the aftereffect of estimation is distributed. The term marker is additionally something that surfaces within the writing appreciate measurements [6].

Various publications regarding the matter, including benchmarks, systems, and different books and articles by autonomous specialists suggest that, so as to appropriately fill their expected need, data security measurements ought to have certain "perfect" attributes. One of such arrangements of perfect attributes initially instituted by John Wesner and here and there referred to by different sources, prompts that measurements ought to be "SMART", that is, specific, measurable, attainable, repeatable, and time-dependent. Some different instances of proposed meanings of perfect security metric attributes incorporate accurate, precise, legitimate, right, important, reproducible, objective and unprejudiced, and ready to quantify movement towards an objective [11] [12], reliably estimated, modest to assemble, communicated as a cardinal number or rate and utilizing in any event one unit of measure, and relevantly explicit [11] [13].

Despite the fact that the particular phrasing among the different sources varies, it very well may be said that "acceptable" measurements are, in general, expected to have the accompanying characteristics [11]:

- Measurements should measure and impart things that are important within the particular setting that they're planned, and be significant (in both the substance and also the introduction) to the conventional objective crowd

- The estimation of measurements should clearly not surpass their expense. Measures should be cheap/easy to amass with the goal that potential wasteful aspects of knowledge assortment don't pull the assets required for consequent phases of estimation or in numerous parts and elements of the association.

- The practicality and recurrence of estimation must be suitable for the pace of progress of the objectives of estimation with the goal that the inertness of measurements doesn't crush their motivation. It should likewise be conceivable to follow changes after a while.

- Great measurements should well be objective and quantifiable. this means they need to be gotten from exact and solid numeric qualities (and not subjective evaluations, which have potential for predisposition), and in like manner be communicated by utilizing promptly comprehended and unambiguous units of measure

The technological explosion these days forces associations to change their working and structures. Innovation turns into the primary factor for profitability development and associations' seriousness and permits successful cost decreases. The utilization of advancements, their job and significance are daily expanding. The current powerful globalization and de-localization phenomena ought not to be disregarded any more. Associations externalize their creation exercises following an alleged "organization without production line" model. In this way, an associations' correspondence community turns out to be progressively significant as they are relying more upon their data framework then they did before. A brokenness of such focus can paralyze the entire framework and could have grievous ramifications for the organization at numerous levels (money related, notoriety and so on.) [14]. The danger of loss of motion could be considerably increasingly basic for organizations whose foremost resource and included worth is data. A normal exceptionally helpless division for such dangers is for instance the administration area. Security issues inside an association should subsequently be treated as a need at top administrative level [14].

Thinking about whether security is quantifiable is a certified inquiry. Like traits, for example, magnificence, fragrance, or flavor, or factors, for example, inspiration and expectation, security is immaterial. Security offers then not many intend to work any immediate estimation. Security is a deliberation, an idea, a thought, instead of a reality or a material thought. Up until now, estimating impalpable happens all the time. Educators are estimating their understudy information when they grade them; supervisors are estimating their staff exhibitions when they grade them, IT expert's measure "vital arrangement", "consumer loyalty", "representative strengthening" or "improved execution" as advantages of IT anticipates while introducing them for choice of top administration. Douglas Hubbard [1] [15] is in any event, expressing that "everything is measurable ". At the point when he says that he hasn't found a genuine “immeasurable” yet, he has created, among many, measures of the risks of cyber-attacks [1].

The business rationale related with a measurement follows a straightforward handling design [8]:

- Create: Obtain essential info information from at least one legitimate supplier, including business items or homegrown client applications.

- Calculate: Apply a progression of systematic activities (called activities) on the essential information to determine an outcome and store the outcome in the measurement results database as at least one line in a table.

- Communicate: Communicate the measurement brings about any of the accompanying arrangements: default representation, email notice, email alert dependent on location of some approach infringement.

Experiences into some basic parts of security estimation are examined underneath. The design isn't to give a rundown of normal entanglements rather the goal is to feature those variables that are accepted to be appropriate to an examination exertion in security measurements [8]:

A. *Correctness and Effectiveness*: Correctness indicates confirmation that the security-upholding instruments are properly actualized (i.e., they are doing precisely what they're expected to try to, as an example, playing out some count). Adequacy means confirmation that the security-implementing instruments of the framework meet the expressed security targets (i.e., they do not do something besides what's planned for them to try to, while fulfilling desires for flexibility).

B. *Leading versus Lagging Indicators:* Leading and slacking markers reflect security conditions that exist separately previously or after a move in security. A slacking security metric with a brief dormancy period or slack time is favored over one with an extended idleness period. Numerous security measurements will be seen as slacking pointers

C. *Organizational Security Objectives Organizations* exist for different purposes, hold various resources, have diverse presentations to the final population, face various dangers, and have various resilience to alter. Thanks to these and different contrasts, their security destinations can change essentially. Security measurements are commonly wont to decide how well an association is meeting its security targets.

D. *Qualitative and Quantitative Properties:* Qualitative assignments will be utilized to talk to quantitative proportions of security properties (e.g., low methods no vulnerabilities discovered; medium, somewhere within the range of one and five found; and high, in more than five found). Quantitative valuations of some security properties may likewise be weighted and joined to infer a composite worth.

E. *Measurements of the Large Versus the Small*: Security estimations have demonstrated to be substantially more practical when the target of appraisal is no and simple as critical huge and sophisticated. Because the quantity of parts in an exceedingly framework expands the number of potential connections increments with the square of the number of segments. More noteworthy multifaceted nature and usefulness normally relate conversely to security and need more examination to assess.

Measurements can be a powerful instrument for security administrators to perceive the adequacy of different parts of their security programs, the security of a particular framework, item or process, and the capacity of staff or divisions inside an association to address security issues for which they are capable. Measurements can likewise help distinguish the degree of hazard in not making a given move, and therein way give direction in organizing remedial activities. Also, they could be utilized to boost the degree of security mindfulness inside the association. At last, with information increased through measurements, security chiefs can all the more likely answer hard inquiries from their administrators and others, as an example, [8]:

- Are we more secure today than we were previously?
- How we are compared to others in this regard?
- Are we secured enough?

Measurements may be a viable device for security directors to watch the adequacy of various segments of their security programs, the safety of a specific framework, item or process, and also the capacity of staff or offices inside an association to deal with security issues that they're mindful. Measurements can likewise help distinguish the degree of hazard in not making a given move, and in this way give direction in organizing restorative activities. Moreover, they may be utilized to boost the degree of security mindfulness inside the association [8].

III. SECURITY METRICS CLASSIFICATION

A. *Classification by performance*

The security measurements estimating the exhibition can be characterized in two groups [14]:

- Security measurements identified with the viability: To assess to what degree the destinations are being met;
- Security measurements identified with the effectiveness: This shows the proportionality between the targets being reached and therefore the outcomes being gotten. the employment of security measurements affirms that the association applies a proactive safeguard demeanor. These security measurements illuminate on the viability of the procedures, methodology and controls executed into the association.

B. *Metrics defined by CIS*

The CIS, Center for Internet Security [1] [16], has characterized lots of security measurements which will be gathered within the executives measurements, operational measurements or specialized measurements hooked in to their motivation and crowd, as appeared in table (1) [1].

Category	Scope
Management metrics	Give data on the exhibition of business capacities, and also the effect on the association
Operational metrics	Used to comprehend and enhance the exercises of business capacities
Technical metrics	Give technical details as well as a foundation for other metrics

Table 1:- The CIS Security Metrics [1]

C. *Metrics Imperatives for Information Security*

In the wake of investigating the determinants of the business goals for data security, Gary Hinson and Krag Brotby [1] [17] have made a kind of update to the rundown within the past passage. The determinants are the association's motivation, targets, business systems, dangers and openings and what the association must accomplish through data security. this can prompt the meaning of the safety metric that are required. For that determination, measurements are assembled in three classifications, as appeared in table (2) [1]:

Name	Description
Strategic security metrics	Measures concerning the info security components of great level business objectives, destinations and techniques.
Security management metrics	Measurements that legitimately identify with accomplishing explicit business goals for data security
Operational security metrics	Measurements of direct worry to individuals overseeing and performing security exercises: specialized and nontechnical security measurements refreshed on a week by week, every day or hourly premise.

TABLE 2:- TYPES OF SECURITY METRICS [1]

D. Metrics Supporting Control Objectives

The data security business has structured numerous security systems that are globally utilized. Among the foremost well-known are the Control Objectives for Information Technology (COBIT), the ISO 27000 arrangement of benchmarks, explicitly intended for data security matters and also the Information Technology Infrastructure Library (ITIL). Experts additionally frequently allude to the arrangement of reports about data security that the u. s. National Institute of Standards and Technology (US NIST) distributes under the Special Publication 800 Series. Those systems specify some measurements that are firmly related to the control destinations of the structures. The control destinations secured [1] [18] are:

- information security policy document
- review of the information security policy
- inventory of assets
- ownership of assets
- acceptable use of assets

With those different security measurements obtainable, IT experts can rely on a scorecard to help with utilizing the measurements outside the IT room. A scorecard is also a factual record used to quantify accomplishment or progress toward a specific objective. Such tools are entirely important while adjusting some capacity to the business, similar to the instance of information security. A security scorecard interfaces the association's methodologies and methods in data security to their capability to spice up the center business [1]. The protection scorecard is also a successful inward specialized instrument for associations. Various advantages are appended to a security scorecard. Fixing security programs for business improves usage of that program as there is not any more conversation about what are the qualities it adds to the business. The procedure of solicitation for assets is mellowed and believability of the solicitation while the one amongst the program is expanded. This goes with increment in responsibility: those designating assets know precisely what they're assigning them for and people answerable for usage [16] of the program have away from what results they are responsible for [1]. Foundation of a security measurements program or structure of a security scorecard involves an appropriate blend of some fixings that are normal, when combined, to deliver the one in all a sort item which will serve the association. Most creators, [1] [19], [1] [20] and [1] [17] as an example, demand the start stage being the association's motivation. The association's goals show why data security may be pertinent to the business officials. What's more, the response to it question is selecting which measurements must be available within the security scorecard [1].

IV. APPLICATIONS OF METRICS

When appropriately planned and executed, measurements can be utilized to distinguish and screen, assess and analyze, and impart and report an assortment of security related issues; encouraging dynamic with a level of objectivity, consistency, and effectiveness that would not in any case be practical. A portion of the significant employments of data security measurements from the hierarchical point of view incorporate [11]:

- Showing consistency or confirming the degree to which security prerequisites have been fulfilled, with respect to both outside specialists (for example laws, guidelines, measures, legally binding commitments) and inside ones (for example hierarchical arrangements and systems).

- Expanding straightforwardness and improving responsibility by encouraging location of explicit security controls that are not appropriately actualized (or not in the slightest degree) or are in any case incapable, and the partners in control

- Improving viability and productivity of security the board by giving the way to screen and measure the security pose considering various occasions and exercises, associate execution of specific security procedures with changes in act, show slants, and evaluate progress towards targets.

- Supporting asset allocation related choices by giving quantitative intentions to either legitimize and think about the earlier/current data security spending or design and organize future ventures.

- Empowering quality affirmation and evaluation of reasonableness when getting security items or administrations from outsiders and giving intends to think about various items and administrations.

Security measurements share an eminent relationship with chance administration. It tends to be said that huge numbers of the choices that the security measurements support are generally chance administration choices, since a definitive reason for all security exercises is the executives of security dangers. Along these lines, measurements can enhance explicit hazard the executives exercises by straightforwardly contributing for examination just as an association's general capacity to manage the dangers it faces by encouraging ceaseless upgrades to security. On the other hand, so as to appropriately immediate and organize the data security estimation endeavors taking into account the association's real business dangers, yield from the hazard appraisal exercises must be utilized [11]. This relationship is, for instance, featured within the ISO/IEC 27004 standard, where it's both expressly expressed that an association is required to own a sound comprehension of the protection dangers it faces preceding creating measurements and performing estimation, which the yield of estimation can validate chance administration forms [11] [20]. Hence, the connection between safety efforts and hazard the board is both reliant and commonly gainful [11].

V. CONCLUSIONS

Security measurements can be considered as a standard (or framework) utilized for quantitatively estimating an association's security pose. Security measurements are basic to extensive system security and CSA the board. Without great measurements, experts can't respond to numerous security related inquiries. Estimating data security is troublesome. Powerful estimation and revealing are required so as to show consistency, improve adequacy and proficiency of controls, and guarantee vital arrangement in a goal, solid, and productive way.

We would in this way suggest measurements must be planned utilizing a participatory structure process including the influenced security experts of the association. Also, utilizing a technique where the accessibility of information is organized higher than the culmination of the measurements is prescribed so as to test and improve the development of the data security program.

REFERENCES

[1]. Joël Hounsou Perpétus Houngbo, "Measuring Information Security: Understanding And Selecting Appropriate Metrics," International Journal of Computer Science and Security (IJCSS), vol. 9, no. 2, 2015.
[2]. A. C. S. Associates, Information System Security Attribute Quantification or Ordering (Commonly but improperly known as "Security Metrics"), 2001.
[3]. K. Scarfone, M. Souppaya P. E. Black, Cyber security metrics and measures, 2008.
[4]. S. C. Payne, "A guide to security metrics," Inst. Inf. Secur. Read. Room, 2006.
[5]. V. Verendel, "Quantified security is a weak hypothesis: a critical survey of results and assumptions," in Proceedings of the 2009 workshop on New security paradigms workshop, 2009, pp. 37-50.
[6]. Marte Tarnes, Information Security Metrics: An Empirical Study of Current Practice, 2012.
[7]. Lance Hayden, IT Security Metrics: A Practical Framework For Measuring Security & Protecting Data, 2010.
[8]. Kavita Arora, Sonia Duggal Deepti Juneja, "Developing Security Metrics For Information Security Measurement System," International Journal of Enterprise Computing and Business Systems, vol. 1, no. 2, July 2011.
[9]. Andrew Jaquith, Security Metrics: Replacing Fear, Uncertainty, and Doubt, 2007, Addison-Wesley Professional.
[10]. ISO/IEC 27004: 2009(E)., Information technology - Security techniques - Information security management - Measurement, 2009.
[11]. Rostyslav Barabanov, "Information Security Metrics: State of the Art," DSV Report series No 11-007 2011.
[12]. D. A., Akridge, S Chapin, "How can security be measured?," Information Systems Control Journal, vol. 2, 2005.
[13]. A Jaquith, Security metrics: Replacing fear, uncertainty, and doubt. Upper Saddle River, 2007.
[14]. Solange GHERNAOUTI-HÉLIE Igli TASHI, "Security metrics to improve information security management"," in In Proceedings of the 6th Annual Security Conference, New York, 2011.
[15]. D. Hubbard, Measure for measure: The Actuary, 2014.
[16]. T. C. for I. Security, The CIS Security Metrics, 2010.
[17]. M. Hoehl, "Creating a monthly Information Security Scorecard for CIO and CFO," SANS Institute, 2010.
[18]. L. Hudec J. Breier, "Risk analysis supported by information security metrics," in Proceedings of the 12th International Conference on Computer Systems and Technologies, 2011, pp. 393-398.
[19]. S. C. Payne, A guide to security metrics, 2006.
[20]. ISO, Information technology -- Security techniques -- Information security management -- Measurement., 2009.