International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

SECURITY CAPABILITY MATURITY MODEL FOR MOBILE APPLICATIONS

Srinadh Swamy Majeti[1], Barnabas Janet[2], Narendra P Dhavale[3]

[1]Research Scholar, NIT Trichy & IDRBT Hyderabad, India
[2]Assistant Professor, Department of Computer Applications, National Institute of Technology(NIT), Trichy, India
[3]Associate Professor, Centre for Mobile Banking, Institute for Development and Research in Banking Technology(IDRBT), Hyderabad, India
Email: [1]srinathswamy.majety@gmail.com, [2]janet@nitt.edu, [3]npdhavale@idrbt.ac.in

Abstract

Trend towards use of mobile applications (apps) is increasing resoundingly. Mobile app vendors extend their outreach taking the services to common man. As the technology is evolving at breakneck speed, the threat of unimaginable level of unauthorized activities done by hackers is also increasing. We don't know how secure the apps are? Thus, there is need for organizations to continuously measure their security control domains. In this context, security metrics and standards plays a vital and key role in security management systems. As of our present knowledge, there is no model yet, which can determine security score in particular for mobile apps. To improve the security performance, authors in this work suggested a framework named as Mobile App Security Capability Maturity Model (MASCMM). MASCMM is a 4-step GAME (Goals, Actions, Metrics, Evaluations) process. In the model, 321 Security metrics are defined based on GAP-GOES criteria covering 32 security control domains. By using our proposed framework, organizations can calculate security score and maturity level of each security activity, security control family and also of applications.

Key words: Mobile applications, Mobile app security, security score, CMM level, security metrics, MASCMM, security framework

Introduction

Due to its ongoing tremendous transformation of mobile technology and the remarkable communicative interface, smartphones have become important in our everyday life and activity is undeniably unending. Smartphones have become a colossal point of attention for all mobile users because of its incredible features and results in a whole new and innovative experience in mobile computing. Across the world, 3.5 billion people are using these smartphones [1]. This is made possible through the development of mobile applications (simply apps). Apps are programmed to fulfil our individual needs and requirements thus making life easier, comfortable, and more productive. At the same time, cyberattacks are escalating day-by-day. Hackers are deeply looking into loopholes of these mobile apps causing cyber intrusions and resulting our information to be lost and apps becoming insecure. There is a necessity to increase the measures taken by Application security management system to prevent these attacks. Here, readers must understand the relationship between cybersecurity and Application security. Cyber security is the superset of Application security. Cybersecurity is the process of protecting systems, networks, and programs from digital attacks [2]. In the other end, Application security encompasses measures taken to improve the security of an application often by finding, fixing and preventing security vulnerabilities. Organizations are not following standards, policies completely which degrade the performance of the security management system. These organizations are measuring the security controls sporadically. This became a golden opportunity for hackers. Hence, to gauge the performance of the security management system, security metrics and assessment of security controls act as an epicentre.

Metrics are the tools designed to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data [3]. The advantage of measuring and assessing the security control families will improve the performance of security management system. In this document, the authors will use two similar terms - Metrics and measurement mutually. Measurements are objective raw data and it can be generated by counting [4] .

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

Security metrics defines how many security objectives are satisfied by the organization. Security assessment must be done in perfect manner. According to [5], security assessment must define measurement, meta-metric in a standardized way. The main advantages of security assessment are:

1. Completely identify the security weaknesses of business processes and applications.
2. Able to check whether all the security controls and compliance are perfect.
3. Decide which security issues can be solved in high priority.
4. Are we (organization) achieving desired results?

As of our knowledge, security metric models, frameworks and standards are existing in cyber security area only which are theoretical, complex, hard to apply and context-specific. Mobile application security decision makers instinctively feeling bad and facing trouble to find the appropriate framework and assess the level of the security. The authors are not in intention to blame or criticize or efforts made by researchers are useless. This security research area is an immature field and researchers still actively doing research to make security management wing strong. In this work, the authors defined a security metric framework for mobile applications. The authors identified 32 security control families which mainly affect the performance of security management system and defined metrics. To assess the security, selection of efficient metrics is a difficult task. For this, we defined GAP-GOES meta-metric and based on this, we selected the security metrics. By using the proposed metric framework, organizations can measure assess the level of security. Finally, we validated our framework and compared our framework with existing models of cyber security. The authors will hope; this effort will give comfort to the decision makers for assessing the mobile applications.

Motivation

Mobile Apps are programmed to our individual needs and requirements thus making life more comfortable, easier and more productive. But, we cannot sure that we are using the secured mobile apps [6]. Many researchers did research on security issues of mobile apps. Krutz et. al. made research on mobile apps and tried to find out the relation between security and usability [7]. Akond Rahman et. al. predicted the security of an app by using static metrics [8]. Gemma et. al. [9] defined effort estimation metrics for mobile apps. These metrics will helpful in development phase of an app. Recently, Savola et. al. [10] defined risk driven security metrics for mobile apps. These risk driven metrics not covered all the security control families of an app. Hence, the authors are tried to figure out the metrics which defines the security score of mobile apps and proposed as Mobile App Security Capability Maturity Model (MASCMM). In 2013, W. Krag Brotby and Gray Hinson [5] defined 154 security metrics based on PRAGAMTIC meta-metric in 12 security control domains of cyber security. This really motivates the authors to develop the security metrics for defining mobile app security. The authors identified the security control domains with respect to mobile app security and defined 321 security metrics covering 32 security control families. By using this framework, organizations can calculate the security score of their app. For example, by using MASCMM, bank administration can easily calculate the security score of their banking apps.

The rest of the paper is organized as follows: Section 2 reviews perception about cybersecurity, models and standards, cybersecurity metrics. Section 3 presents proposed list of application security metrics. Section 4 presents mobile application security maturity model framework. Section 5 shows the results obtained by testing the apps with MASCMM framework.

Perception Of Cybersecurity:

2.1 Basic definition of Cybersecurity

The basic concept of security is defined as the quality or extent of being secure [11] .“The integrity of our personal privacy, to security of our critical infrastructure, to military threats and to the protection of intellectual property” is referred as Cybersecurity [12]. According to Gasser and Morrie [13], cybersecurity or IT security is “the protection of information systems from theft or damage to the hardware, the software, and to

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

the information on them, as well as from disruption or misdirection of the services they provide." ITU [14] defines Cyber security as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and users assets."

2.2 Cybersecurity Models and Standards:

Cyber security models and standards are useful to determine whether the organizations are implementing the procedures, standards in every security control domain or not. There are many cyber security models and standards exist based on the organization scenario. Issa Atoum et al. [15] classified cyber security models into 7 categories. They are standard models, decision support models, privacy models, infrastructure models, enterprise frameworks, generic frameworks and national frameworks.

2.3 2.3 Cyber Security Maturity Model (CSMM):

CSMM is a powerful tool to improve the organization's cyber security efforts. It provides a framework for measuring the maturity of a security program and guidance on how to reach the next level. Organizations must use CSMM and evaluate the security level of each entity because cyber space is now fully consisting of viruses, threats, vulnerabilities and many harmful things and we cannot say our organization is secure. CSMM will measure, assess and enhance our security programs. CSMM is derived from Capability Maturity Model (CMM) CMM is a level based framework. In 1989, Humphrey [16] proposed five level CMM numbered from level 1 to level 5, to assess the level of security program. According to Humphrey, Level 1 is "initial", means simple and less in security, level 2 is "Repeatable", level 3 is "Defined", level 4 is "Managed" and Level 5 is "complex" and more secure. To reach any maturity level, the security program must satisfy the defined standards. These maturity levels will provide where to enhance our security programs. For example, suppose, maturity level of one entity is 3, it means that entity satisfies the standards of level 1, 2 and 3. CMM identifies the gaps and gives suggestions/ enhancements to reach the next maturity level i.e. level 4. But, the main drawback of CMM is, it measured only by qualitative metrics.

2.4 Cyber Security Metrics

2.4.1 Metrics, measurement and its relation:

Metrics are the tools designed to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data [17]. If we use metrics in an efficient manner, then we can decide whether the organization is safe or not. It will define the exact state of the organization. Metric and measurement both are exchangeable. Basic definition of metrics is standard of measurement. Metrics are the tools designed to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. A deep analysis is required to generate the metrics.

In other hand, measurement defined in oxford online dictionary is the act or the process of finding the size, quantity or degree of something. Measurement is the assignment of a number to a characteristic of an object or event, which can be compared with other objects or events. Measurement can be obtained by performing counting.

2.4.2 Importance of Security Metrics:

Security metrics is the way of measuring the effectiveness of organization's security program. Security metrics are important to every organization because

1. Security metrics define the true/ exact state of cybersecurity posture
2. Completely identify the security weaknesses of business processes and applications.
3. Security metrics will evaluate organization's compliance with legislation and regulations

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

4. Able to check whether all the security controls and compliance are perfect.
5. Decide which security issues can be solved in high priority.
6. Are we (organizations) achieving desired results?
7. Security metrics will provide answers to high-level business questions regarding security, which facilitate strategic decision making by the organization's highest levels of management.

2.4.3 Categories of security metrics:

Security metrics are categorized based on different types of security assessments like process based assessment, functional based assessment, level based assessment and type based assessment [18] showed in figure 1.

1. In the organizations, some tasks may be service oriented, some are management related. we can call it as process. Metrics in service oriented, management related activities comes under process based assessment metrics. Process based assessment metrics included related to security governance, risk management, security directness, security policy, business continuity and compliance metrics etc.
2. In addition to this process based assessment, another category of metrics is functional. Independent elements in the process known as functions. Functional based assessment metrics related to HR security, IT security, access control, incident management metrics.
3. Other category of security assessment is based on the level. Level based assessment metrics covers strategic/operational metrics, input/output process metrics, maturity metrics and readiness metrics. Security assessments can be done by higher level persons in the organizations. These persons will take the decisions in a strategic manner. Evaluations happened at operational level. To achieve the results in lower level of organization, level of evaluation is based on the processing input/ output segments. Other level of evaluation is based on the security maturity of an organization. The last level of assessment is based on the readiness on the readiness of the organization.
4. While doing security assessment, type of data about security features may be quantities, some are descriptive and some are in both combinations. Hence, Type based assessment categories are qualitative, quantitative and semi-quantitative.
5. In addition to this, organizations like Centre for Internet Security (CIS) categorized the security metrics into three types namely management metrics, operational metrics and technical metrics.
6. Krag Brotby divided the security metrics into three categories namely strategic security metrics, security management metrics and operational security metrics.
7. Another classification is based on characteristics of metrics like metrics are measured directly or indirectly. Static metrics (without operating security activity) and dynamic metrics (by operating security activity) are other type of characteristics.

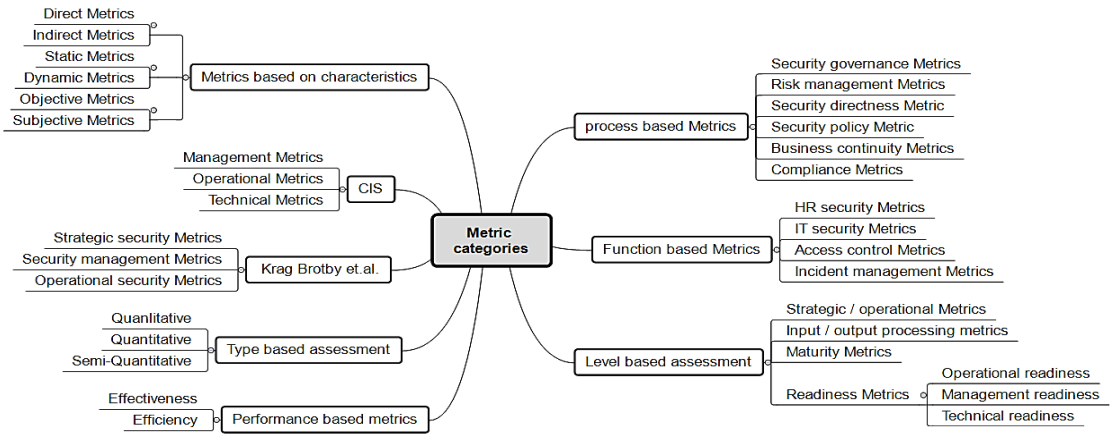

Figure 1: Metric categories

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

2.4.4 Criteria for making metric as Good:

To develop any model, framework or assessment, metrics plays a dominant role. Selection of metrics is not an easy task. In order to make the metrics Good, it must possess some characteristics (or meta-metrics). Many researchers suggested meta-metrics to make security metrics "Good". According to Jilin [19] , metrics should be "SMART" - Specific, Measurable, Attainable, Repeatable and Time-dependent. According to [20], security meta-metrics must have features of "CORES" - Clarity, Objectiveness, Repeatability, Easiness and Succinctness. Other characteristics of security metrics include accurate, precise, valid and correct, meaningful, reproducible, objective and able to measure towards a goal [21][22]. According to W. Krag Brotby and Gary Hinson [5], characteristics of security metrics must have the features of "PRAGMATIC" - Predictive, Relevant, Actionable, Genuine, Meaningful, Accurate, Timely, Independent and Cheap.

2.4.5 Need for Application security metrics:

3.5 billion humans are using smartphones. Means, around 44.98% of world population using smartphones. Mobile apps are one of the reason to became smartphones more popular. We can download apps from Playstore. Whenever we are downloading, we know only app rating given by Playstore based on the user ratings. This rating will be usability rating. But, **we don't know security score of the app. How much secure the apps are?** For example, if you are using any Ola app, we know only user rating 3.9 based on user ratings given by 14,15,921 users. But this is not security ranking or security score of Ola app. By using proposed security metrics, app vendors can calculate the security score.

Challenges with Mobile Application security measurement:

1. Application security is ever-evolving beast of new technology, emergent and irreducible. So, we cannot cover all vulnerabilities because new vulnerabilities will arise due to latest technology and old vulnerabilities attacking in newer ways.
2. Developing a security measurement plan and building up the team is bigger challenge.
3. Measure the goals considering organization's objectives.
4. Acquire the knowledge about security standards, vulnerabilities and measures.

2.4.6 Security metrics program

Security metrics program provides direction to manage, control and enhance the performance of security controls. Security metrics program will be set after selecting the security metrics by the organization. To implement the security metrics program, researchers suggested step by step process shown in figure 2. In 2006, Payne et.al. [23] suggested 7 step implementation process. In the same year, Campbell and blades et.al. [24] suggested 5 step implementation process. Kark and stamp et.al [25] suggested 7 step implementation process in 2007. In 2008, Whitman and Mattord et.al. [26] suggested 4 step implementation process. Chew et.al. [27] proposed 5 step implementation process. In 2011, Shon Harris proposed [28] 6 step implementation process. All the researchers proposed security metrics program implantation process based on their views and organization needs.

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

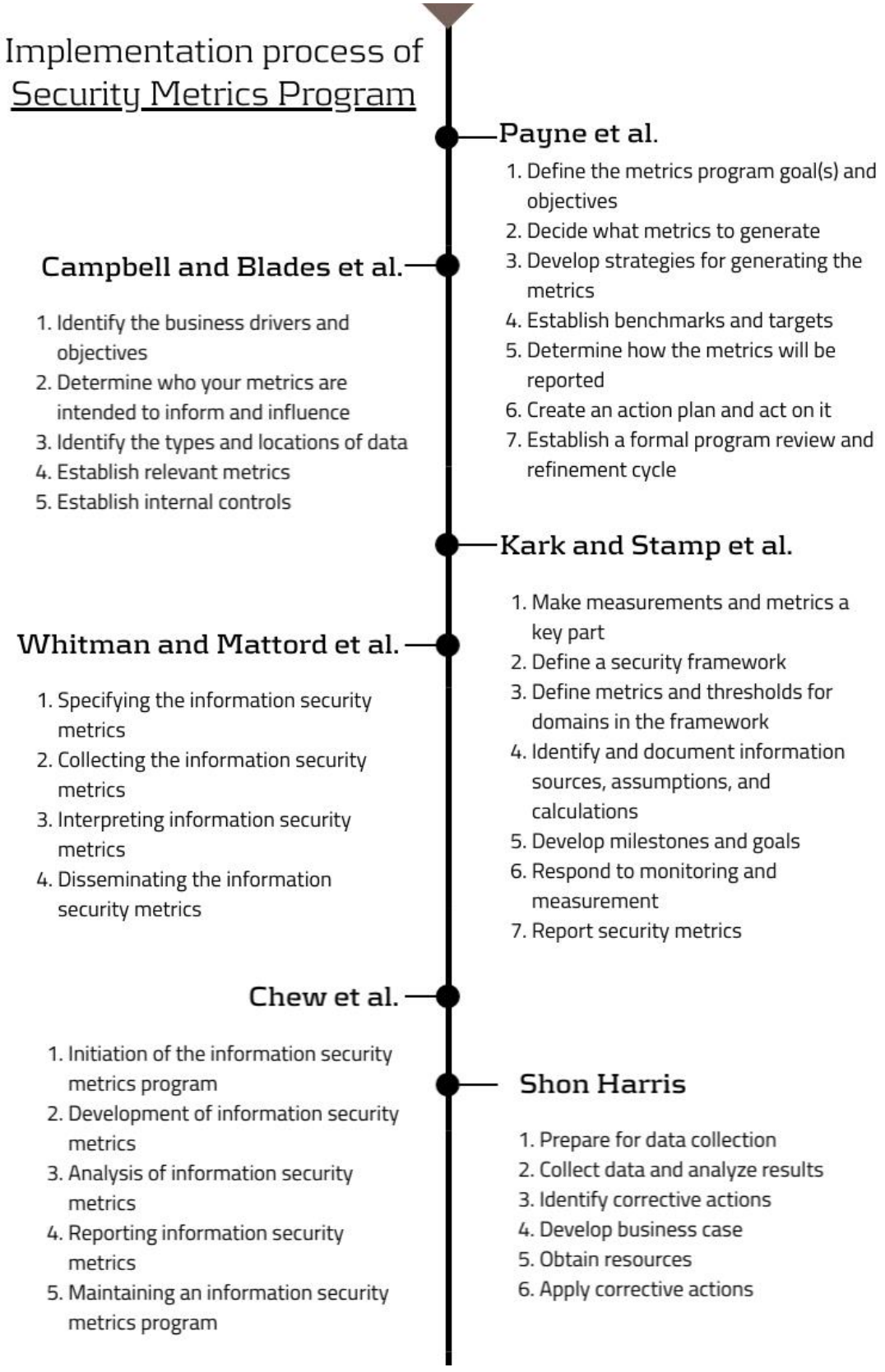

Figure 2: Implementation process of security metrics program by various researchers

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

2.4.7 Cyber security levels

Organizations are using cyber security models to calculate security maturity score to each business unit. The authors did literature on various cybersecurity models and maturity levels defined by organizations / researchers shown in figure 3.

In 2005, ISO defined Information Security Management System (ISMS) [29] defines the information security risk management through security standards. ISO defined the maturity levels as level 1: Performed; level 2: Managed; level 3: Established; level 4: Predictable; and level 5: Optimized. To prevent and mitigate incidents and to optimize the use of information, money, people, time and infrastructure, Information Security Management Maturity Model (ISM3) defined by ISM3 Consortium [30] in 2007. In the same year, NIST defined Information Security Maturity Model (ISM2) which provides a framework for review and measure the information security posture of an information security program. To provide security awareness and risk management in large international organizations, in 2009, Gartner defined Gartner's Information Security Awareness Maturity Model (GISMM) [31]. IBM defined an Information Security Framework (ISF) [32] in 2009 for analysing the security gap between business and technology. CERT defined a capability focused process model for managing operational resilience in 2010 and named it as Resilience Management Model (RMM) [33]. Gregory B. White defined Community Cyber Security Maturity Model which defines the community effort and communication capability in communities. In 2012, Department of Homeland Security (DHS) in US develops National Cyber Security Capability Maturity Model [34] provides a workforce planning for cyber security best practices. In 2014, again NIST provides Cyber Security Framework [35] which improves federal critical infrastructure through a set of activities designed to develop individual profiles for operators. In 2015, Pamela Curtis defined Cyber Security Capability Maturity Model (C2M2) [36] to assess the implementation and management in critical infrastructure.

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

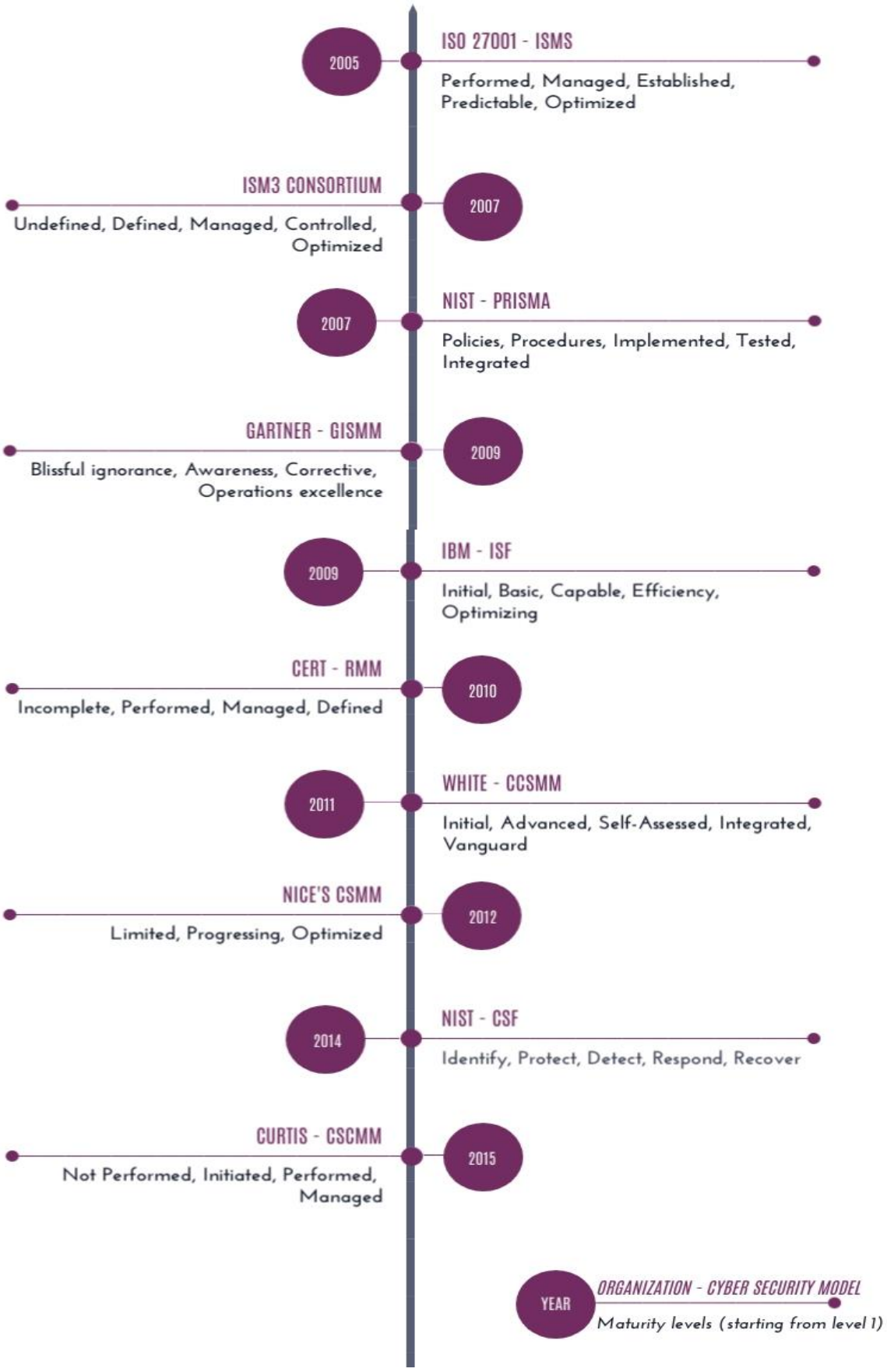

Figure 3: Cybersecurity models and its levels

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

Mobile App Security Capability Maturity Model (Mascmm)

3.1 Security domains

Each department in the security of organization can be defined as security domain or security control family. NIST defined 17 security domains that every organization must implement security strategies in their organization. Krag Brotby et. Al. [5] defined security metrics in 12 security domains. In addition to these, in our proposed model, the authors listed a total of 32 security domains which are important in application security field listed in table 1.

S. No	Name of security domain	NIST	Krag Brotby et.al. [5]	Proposed model
1	Access control	□	□	□
2	App security metric			□
3	Audit and Accountability	□		□
4	Awareness and training	□		□
5	Business continuity metric		□	□
6	Certification, Accreditation, and Security Assessments	□		□
7	Change management metric			□
8	Cloud security metrics			□
9	Compliance assurance metric		□	□
10	Configuration Management	□		□
11	Contingency Planning	□		□
12	HR security metric		□	□
13	Identification and Authentication	□		□
14	Incident Response	□	□	□
15	Information asset management metric		□	□
16	Information Security metric			□
17	IT security metric		□	□
18	Maintenance	□		□
19	Management/Governance metric		□	□
20	Media protection	□		□
21	patch management metric			□
22	Performance and effectiveness metric			□
23	Personnel security	□		□
24	Physical and Environmental Protection	□	□	□
25	Planning	□		□
26	Risk Assessment	□	□	□
27	Security policy metric		□	□
28	software security metric		□	□
29	System and Communications Protection	□		□
30	System and Information Integrity	□		□
31	System and services acquisition	□		□
32	Vulnerability management metric			□

Table 1: List of security domains

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

3.2 GAP-GOES criteria:

The basic idea of the GAP-GOES method briefly describe involves scoring application security metrics against seven carefully selected assessment criteria, simply, metametrics. Metametric means meta data, like information about metrics includes metrics about metrics. This GAP-GOES method for selecting application security metrics that are workable, useful and valuable. Core to the GAP-GOES method is a comprehensive set of seven metametrics or criteria for assessing and selecting metrics that together, construct the acronym GAP-GOES.

3.3 Security metric program

Security metric program for scoring application security metrics against GAP-GOES criteria contains 6 steps.

- Step 1: Determine the measurement objectives

The main objective of this step to measure the observation, knowledge of customers of the application security management wing with respect to efficiency and effectiveness so that the department manager can improve and manage the department more successful.

- Step 2: Specify the metrics

In this step, specified the metrics that what things to measure of application security department and who will receive metrics.

- Step 3: Design the metrics

To gather the information about customer perceptions, we conducted opinion survey and feedback forms. We used Likert scale to gain more meaningful granular information and developed the rating guide of GAP-GOES for security metric showed in table 2.

- Step 4: Score the metrics suing the GAP-GOES criteria
    - **Gullibility:** Gullibility security metrics provide unambiguity and not in complex while measuring the artifacts.
    - **Authentic:** Authentic metrics provide credible, straightforward as opposed to false measurement artifacts.
    - **Prompt:** Prompt metrics provide reasonable and accountable information for measuring artifacts.
    - **Guessing:** A good security metric is one that guessable security outcomes implying a strong correlation between metric and outcome
    - **Objectiveness:** Objectiveness security metrics provide metrics that are fairness and uninfluenceable in nature
    - **Eloquent:** A good security metric is one that is eloquent to the intended audience of the metrics. Metrics must be understood by the audience at any time.
    - **Serviceable:** Serviceable metrics gives the idea of a metric being immanently energizing and motivational.

Finally, we calculated GAP-GOES score for each metric. We calculated the average of seven meta metric ratings and rounded to nearest whole number.

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

- Step 5: Compare the GAP-GOES score against other metrics

In the above steps, it shows specification, development and scoring the metrics. We conducted additional surveying, conducted interviews and scored by assessors before directly interacting with customers. Because it could change our wording of the questions.

Criterion (GAP-GOES)	Rating Guide			
	0%	**33%**	**66%**	**100%**
Gullibility	Looks like complex and time complexity of this metric is high	This metric is unclear however it gives unclear signs while doing future works	This metric generally looks like simple and easy to measure	This metric is gullible in nature and no ambiguity while measuring
Authentic	Highly deceitful and phony. In some situations, it is not carrying relation with fact. It is unbelievable	has factors of the fact however there is a dependency on an absence of validity - means questionable on expectations	has feasible validity and backed by valid confirmation	based on valid facts and absolutely valid. No one will object it
Prompt	Arbitrary, any coincidence to the evidences are totally accidental	generally appears slow, it sets the capability while using	This metric generally prompts in perfect moment however it will be extra benefit if it appears speedily	This metric can be used instantly and maintaining data perfectly and available any time
Guessing	It is entirely classic and cannot guess the value	basically classic but provide an unclear sign of next works to be done like uncertain tendency	Obviously guessable but there is a mistrust	Extremely guessable, no ambiguity on works carried out in next days
Objectiveness	The metric can be easily influenced by the feelings of evaluator and unfairness in nature	generally it appears to be unfairness but while using it leads to unambiguous and uncertainty	The metric looks like fairness and carries objectivity	This metric was uninfluenceable and provide results based on observable experience
Eloquent	Unconditionally eloquent and causes distraction to all beneficiaries	it is a kind of unclear and unambiguous to all beneficiaries	Almost all the beneficiaries can derive simply what this metric measures	This metric is hugely eloquent and clearly understands by all beneficiaries
Serviceable	Beneficiaries don't know the opinion of this metric and nothing would do by beneficiaries	This metric will give clue, might give a small reply	This metric provides a favourable escort, would give an appropriate reply	This metric provides an acceptable and straight actionable and surely cause an perfect reply

Table 2: Rating guide for GAP-GOES criteria

3.4 List of security metrics

Based on the security metric program mentioned in 3.3, the authors listed 321 security metrics in 32 security domains. The table 3 showing various security metrics in security domains and average GAP-GOES score of security metric evaluated by using the above rating guide.

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

S.No	Name of security metric	G	A	P	G	O	E	S	Score (%)
Access control									
1	Rate of messages received at central access logging/alerting system	66	96	79	77	93	78	65	79
2	Information access control maturity	74	80	74	83	83	77	97	81
3	Days since logical access control matrices for application systems were last reviewed	67	74	63	81	67	80	76	73
4	Percentage of inactive user accounts that have been disabled in accordance with policy	68	76	66	93	90	67	85	78
5	Rate of detection of access anomalies	76	71	92	63	65	85	72	75
6	Logical access control matrices for applications: *coverage and detail*	81	63	65	90	94	80	65	77
7	Logical access control matrices for applications: *state of development*	84	82	92	86	93	92	82	87
8	Quality of identification and authentication controls	67	70	85	77	74	93	81	78
9	Percentage of business units that have proven their identification and authentication mechanisms	95	65	80	80	87	94	97	85
10	Number of times that assets were accessed without authentication or validation	89	69	93	66	91	74	75	80
11	Percentage of remote access points used to gain unauthorized access	84	69	64	76	96	85	82	79
App security metric									
12	Number of secured applications in the organization	75	96	70	77	94	65	72	78
13	Percent of Critical Applications	73	81	87	75	85	81	78	80
14	Risk Assessment Coverage	72	64	90	81	94	88	64	79
15	Security Testing Coverage	92	76	63	92	65	87	88	80
Audit and Accountability									
16	Average frequency of audit records review and analysis for inappropriate activity	69	79	91	69	85	71	75	77
17	Are there audit requirements?	80	65	89	74	71	67	80	75
18	How Satisfied Are the Internal Stakeholders?	67	79	92	83	93	83	79	82
19	What was the financial value of the internal audit?	78	73	65	75	83	82	96	79
20	How was the performance reported?	67	83	92	92	66	65	78	78
21	What was the audit plan coverage?	67	66	68	66	64	85	86	72
22	How rapidly were issues remediated?	85	86	94	89	74	83	90	86
23	Does the organization collect and review audit logs associated with all remote access points?	82	83	81	71	84	83	78	80
24	Does the organization have clearly defined criteria for what constitutes evidence of inappropriate activity within system audit logs?	88	90	83	95	97	63	64	83

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

25	For the reporting period, how many system audit logs have been reviewed within the following time frames for inappropriate activity?	85	81	92	80	72	90	81	83
26	Audit and Accountability Policy and Procedures	71	78	76	91	88	79	86	81
27	Response to Audit Processing Failures	90	70	80	66	75	80	69	76
28	Audit Record Retention	66	66	87	63	86	70	79	74
Awareness and training									
29	Number of Email Breaches Avoided or Detected	81	73	78	91	67	97	86	82
30	Clean Desk Index	65	68	82	71	80	75	70	73
31	Password Security	79	84	74	88	77	93	65	80
32	New Types of Attacks, Identified	72	69	67	66	88	86	78	75
33	Training attendance	91	67	86	67	96	90	89	84
34	NIST training security awareness checklist score	68	63	68	90	88	77	88	77
35	Percentage of information system security personnel that have received security training.	82	81	91	78	66	64	79	77
Business continuity metric									
36	Coverage of business impact analyses	95	68	70	63	93	77	66	76
37	Business continuity management maturity	94	93	97	76	67	88	76	84
38	Percentage of critical business processes having adequate business continuity arrangements	78	68	83	92	96	76	70	80
39	Percentage of business processes having defined RTOs and RPOs	64	84	81	69	79	80	75	76
40	Business continuity plan maintenance status	77	90	97	64	79	70	75	79
41	Disaster recovery test results	80	79	85	68	93	83	87	82
42	Uptime	64	64	93	74	67	74	78	73
43	IT capacity and performance	64	75	77	74	92	95	75	79
44	Mapping critical business processes to disaster recovery and business continuity plans	89	90	81	88	86	70	73	82
45	Business continuity expenditure	82	71	93	76	88	79	87	82
46	Percentage of critical systems reviewed for compliance with critical control requirements	78	82	82	93	77	80	97	84
Certification, Accreditation, and Security Assessments									
47	Ensure that the controls are effectively implemented through established verification techniques and procedures and give organization officials confidence that the appropriate safeguards and countermeasures are in place to protect the organization's information.	73	83	79	74	63	66	77	74
48	Has a security certification and accreditation of the system been completed?	88	67	75	83	80	68	76	77
49	Has the security certification and accreditation status been verified?	64	87	63	90	87	72	90	79

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

50	Are there security features in place to protect the confidentiality, integrity, and availability of the data and the systems being interconnected?	94	75	64	75	63	64	80	74
51	Are there titles of the formal security policy(ies) that govern each system?	63	80	69	92	74	86	79	78
52	percentage of systems accredited	87	91	87	73	93	84	95	87
53	Does management ensure that corrective information security actions are tracked using the Plan of Action & Milestones (POA&M) process?	67	76	63	65	73	67	76	70
Change management metric									
54	Mean-Time to Complete Changes	84	80	82	94	87	79	64	81
55	Percent of Changes with Security Reviews	77	77	87	76	76	67	94	79
56	Percent of Changes with Security Exceptions	74	63	77	86	95	89	79	80
57	Number of changes	78	86	69	88	84	85	64	79
Cloud security metrics									
58	Percentage of time in which data access is available to data owners	85	96	71	73	73	93	97	84
59	Percentage of time in which service access is available to users	66	79	78	90	95	75	88	82
60	Total expenses incurred due to compensatory damages	87	94	70	93	91	82	82	86
61	Average expenses due to compensatory damages	97	63	84	91	93	93	64	84
62	Cost of Incidents in cloud	71	66	67	94	68	73	70	73
63	Mean Cost of cloud Incidences	92	71	63	66	64	76	85	74
64	Mean Incident Recovery Cost	64	68	63	77	68	73	73	69
65	Mean Cost to Patch in cloud	88	94	88	86	78	67	88	84
66	Datacenter Location	69	88	87	64	69	91	80	78
67	Detection of Write-Serializability (WS) violation	96	74	73	89	83	88	85	84
68	Detection of Read-Freshness (RF) violation	70	71	82	75	70	76	81	75
69	Detection of Forward Secrecy (FS) violation	69	85	64	69	79	82	72	74
70	HTTP Strict Transport Security Activation	76	68	71	67	86	78	88	76
71	HTTP to HTTPS reedirect activation	84	64	95	93	70	80	72	80
72	Secure Cookies Enforcement	75	76	83	64	64	93	90	78
73	Certificate Pinning Activation	92	88	88	77	63	68	75	79
74	Vulnerability Scanning Frequency	85	95	70	74	71	97	80	82
75	Vulnerability-List Update Frequency	68	81	90	91	66	95	67	80
76	SW Update Check Frequency	81	88	95	97	74	91	93	88
77	Audit Record Generation Frequency	88	87	68	76	67	72	90	78
78	Level of confidentiality	76	71	82	86	83	75	95	81
79	Key Exposure Level	79	97	90	65	86	94	65	82
80	Account of Privacy and Security Training	94	88	85	69	70	89	73	81
81	Data Isolation Testing Level	96	84	69	75	77	79	93	82
82	Type of consent	65	69	72	89	80	83	92	79

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

83	Type of notice	97	92	67	67	74	83	92	82
84	Procedures for Data Subject Access Requests	97	76	88	96	97	72	63	84
85	Readability (Flesch Reading Ease Test)	83	80	85	70	65	70	91	78
86	Rank of Responsibility for Privacy	92	84	91	83	97	75	79	86
87	Log Unalterability	77	84	93	87	65	63	83	79
88	Identity Assurance	78	96	91	85	97	97	88	90
89	Type of incident notification	82	69	68	97	91	68	90	81
90	Cryptographic Strength	83	85	81	79	78	64	83	79
91	Level of Redundancy	88	91	80	77	86	83	89	85
92	Level of Diversity	75	71	82	85	85	74	95	81
Compliance assurance metric									
93	Information security compliance management maturity	75	95	63	69	95	77	92	81
94	Breakdown of exceptions and exemptions	92	69	82	82	75	79	74	79
95	Number and severity of findings in audit reports, reviews, assessments *etc*.	89	65	85	89	84	80	81	82
96	Status of compliance with externally-imposed information security obligations	75	75	85	80	86	76	66	78
97	Historic consequences of noncompliance	74	77	76	65	95	83	77	78
98	Number of systems whose security has been accredited	91	95	93	88	70	95	92	89
99	Status of compliance with internally-mandated (corporate) information security requirements	75	75	65	97	80	68	71	76
100	Number of unapproved/unlicensed software installations identified on corporate IT equipment	75	95	91	92	72	91	86	86
101	Percentage of security policies supported by adequate compliance activities	91	67	85	93	71	77	65	78
102	Compliance benchmark against peers	73	95	68	93	88	93	74	83
103	Number or rate of security policy noncompliance infractions detected	82	72	70	78	92	73	76	78
104	Embarrassment factor	83	73	94	81	82	88	80	83
105	Percentage of purchased software that is unauthorized	86	75	70	79	80	63	88	77
106	Proportionality of expenditure on assurance *versus* potential impact x likelihood	78	76	83	73	66	85	83	78
107	Percentage of software licenses purchased but not accounted for in repository	78	72	88	69	72	73	78	76
108	Percentage of critical information assets residing on fully compliant systems	73	89	79	84	91	64	88	81
Configuration Management									
109	Percentage of Configuration Compliance	83	76	85	84	77	89	84	83
110	Configuration Management Coverage	91	90	82	83	97	75	96	88
111	Current Anti-Malware Compliance	81	63	89	68	63	81	92	77
112	Percentage approved and implemented configuration changes identified in the latest automated configuration	74	94	66	68	63	85	81	76

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

113	Percentage of servers within a system with a standard configuration	97	79	77	78	89	97	81	85
Contingency Planning									
114	Maximum Tolerable Downtime (MTD)	73	75	87	83	78	83	68	78
115	Recovery Time Objective (RTO)	80	96	78	90	96	97	69	87
116	Recovery Point Objective (RPO)	66	86	73	65	85	79	71	75
117	Work Recovery Time (WRT)	75	97	79	83	94	71	87	84
118	Percentage (%) of information systems that have conducted annual contingency plan testing	88	86	76	78	66	63	92	78
HR security metric									
119	Human resources security maturity	74	97	79	78	92	74	81	82
120	Security awareness level	65	78	86	78	87	75	65	76
121	Rate of change in employee turnover and/or absenteeism	94	79	70	86	82	68	78	80
122	Staff morale & attitude	86	69	78	87	82	69	87	80
123	Tone at the top	73	82	93	81	75	84	70	80
124	Corporate security culture	96	78	72	85	71	86	86	82
125	System accounts-to-employees ratio	65	89	83	76	95	76	69	79
126	Opinion surveys and direct observations of the culture	90	73	63	78	71	81	80	77
127	Help desk security traffic volumes	74	96	72	75	71	66	76	76
128	Culture / world view	97	73	89	97	65	74	88	83
129	Employee turn *versus* account churn	91	88	63	63	87	66	75	76
130	Organizational dysfunction	71	86	78	78	69	95	65	77
131	Psychometrics	66	88	97	86	94	95	77	86
Identification and Authentication									
132	Time To Provision, Authorize, or deprovision	83	90	71	89	95	90	78	85
133	Number Of 'Ghost Accounts'	66	80	80	93	77	93	94	83
134	Password Hygiene Metrics	91	74	77	95	76	83	97	85
135	Percentage of users with access to share accounts	66	91	67	82	65	78	68	74
Incident Response									
136	Cost of Incidents	93	73	70	63	68	92	70	76
137	Mean Cost of Incidents	81	91	75	89	78	64	92	81
138	Mean Incident Recovery Cost	68	65	64	93	77	97	70	76
139	Mean-Time to Incident Discovery	70	90	74	77	71	70	68	74
140	Number of Incidents	77	79	88	66	89	67	71	77
141	Mean-Time Between Security Incidents	91	66	87	73	66	94	64	77
142	Mean-Time to Incident Recovery	95	95	78	95	84	69	79	85
143	Percentage of incidents reported within required time frame per applicable incident category	79	94	94	89	66	84	71	82
144	Information security incident management maturity	79	96	68	79	72	85	77	79
145	Time taken to remediate security incidents	77	67	69	69	71	73	97	75
146	Time lag between incident and detection	66	87	73	94	86	77	80	80

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

147	Percentage of incidents for which root causes have been diagnosed and addressed	85	65	80	84	64	84	89	79
148	Cumulative costs of information security incidents to date	69	81	74	83	74	75	73	76
149	Number of information security events and incidents, major and minor	71	71	70	85	85	88	84	79
150	Number of information security incidents that could have been prevented, mitigated or avoided	94	84	89	79	97	84	80	87
151	Non-financial impacts of incidents	79	89	91	75	64	67	82	78
Information asset management metric									
152	Number of orphaned information assets without an owner	96	69	74	63	64	65	65	71
153	Information asset management maturity	66	85	84	83	86	87	85	82
154	Percentage of information assets not [correctly] classified	79	87	65	72	81	79	63	75
155	Unowned information asset days	71	89	66	91	81	93	74	81
156	Integrity of the information asset inventory	80	79	83	66	74	92	87	80
157	Value of information assets owned by each Information Asset Owner	77	90	72	71	75	89	64	77
158	Percentage of information assets not marked with the [correct] classification	93	83	63	64	95	88	93	83
Information Security metric									
159	Level of preparedness	85	76	90	64	94	88	95	85
160	Unidentified devices on internal networks	95	96	88	68	74	73	74	81
161	Intrusion attempts	76	76	93	63	64	80	82	76
162	Security incidents	91	75	89	77	72	76	67	78
163	Mean Time to Detect (MTTD)	69	82	79	92	84	96	71	82
164	Mean Time to Resolve (MTTR)	91	86	92	82	76	66	85	83
165	Mean Time to Contain (MTTC)	63	69	64	82	80	82	97	77
166	First party security ratings	71	90	87	84	73	63	70	77
167	Average vendor security rating	90	97	67	86	74	66	74	79
168	Mean time for vendors to respond to security incidents	88	93	95	90	97	89	64	88
IT security metric									
169	IT security maturity	80	92	85	77	96	64	87	83
170	Percentage of systems checked and fully compliant to applicable (technical) security standards	73	87	75	83	68	64	64	73
171	Time from change approval to change	91	94	97	95	74	67	69	84
172	Correlation between system/configuration logs and authorized change requests	74	66	75	88	69	66	72	73
173	Percentage of IT devices not securely configured	71	96	68	82	67	91	70	78
174	Rate of change of emergency change requests	74	89	76	73	70	69	88	77
175	Percentage of highly privileged/trusted users or functions	79	70	70	88	73	87	89	79
176	Entropy of encrypted content	92	74	72	71	71	69	81	76
177	Percentage of IT/process changes abandoned, backed-out or failed for information security reasons	90	65	93	65	93	87	88	83

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

178	*Perceptions* of rate of change in IT	96	78	77	63	69	75	67	75
179	Number of viruses detected in user files	97	92	66	96	85	86	63	84
180	Number of firewall rules changed	81	96	74	93	93	86	81	86
181	Toxicity rate of customer data	68	64	90	83	73	97	64	77
Maintenance									
182	Planned maintenance percentage (PPC)	63	75	67	92	73	83	89	77
183	Overall Equipment Effectiveness (OEE)	87	91	70	63	74	82	66	76
184	Mean time to repair (MTTR)	82	68	70	90	65	63	93	76
185	Mean time between failure (MTBF)	73	86	90	96	76	75	74	81
186	Preventive maintenance compliance (PMC)	68	64	82	69	95	88	63	76
187	Maintenance Performance Measurement (MPM)	68	94	66	95	90	88	64	81
188	Unscheduled maintenance downtime	79	86	67	83	90	94	66	81
189	Percentage Available man hours used in proactive work	93	64	83	95	94	63	67	80
190	Number of work order requests	94	70	71	85	94	88	77	83
191	Percentage Scheduled man hours over total available man hours	94	96	66	73	73	76	89	81
192	Percentage Maintenance cost over replacement value	87	66	96	91	69	81	87	82
193	Percentage Maintenance cost over sales revenue	65	91	71	63	87	94	77	78
194	Maintenance cost per product unit	87	90	91	89	93	68	68	84
195	Number of safety, health and environment incidents	92	84	70	71	77	69	64	75
Management/Governance metric									
196	Quality of security metrics in use	90	89	92	93	95	67	85	87
197	Percentage of security controls that may fail silently	92	66	79	85	64	70	69	75
198	Security governance maturity	93	95	68	78	70	85	86	82
199	Information security ascendency	80	97	89	69	78	74	91	83
200	Percentage of controls unambiguously linked to control objectives	86	94	78	97	85	78	66	83
201	Number of controls meeting defined control criteria/objectives	73	72	77	68	74	85	85	76
202	Percentage of critical controls consistent with controls policy	72	76	82	91	90	74	76	80
203	Corporation's economic situation	82	76	66	67	68	94	80	76
204	Percentage of controls that are ossified or redundant	97	72	90	92	84	81	97	88
205	Control objectives tied to specific business objectives	97	79	93	72	72	74	95	83
206	Days since the last serious information security incident	90	94	83	91	69	94	93	88
207	Annual cost of information security controls	63	95	90	65	65	63	95	77
208	Number of different controls	93	83	83	70	94	70	85	83
209	Extent of accountability for information assets	89	64	92	89	73	93	76	82
210	Information security expenditure	64	80	80	95	89	91	77	82
211	Benford's law	78	63	82	66	97	81	65	76
212	NPV (Net Present Value)	79	65	87	75	91	74	69	77
213	ROI (Return On Investment)	80	74	75	69	92	88	73	79

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

214	IRR (Internal Rate of Return)	94	76	75	65	88	96	76	81
215	Payback period	90	85	63	71	65	67	77	74
216	Information Security Management customer satisfaction rating	77	76	89	89	85	89	87	85
217	Information security controls coverage	93	73	90	88	64	74	92	82
218	DEFCON level	75	73	95	75	85	87	85	82
219	Controls consistency	78	79	83	76	95	95	95	86
220	Scope of information security activities	96	89	83	90	76	91	93	88
221	VAR (Value At Risk)	65	89	87	83	93	78	96	84
222	ROSI (Return on Security Investment)	80	70	92	96	80	73	96	84
223	Security budget as % of IT budget or turnover	85	78	82	94	68	86	79	82
Media protection									
224	Determine sanitization level	80	71	96	67	71	90	64	77
225	media sanitization efforts	76	92	81	64	76	90	77	79
226	Heat-resistant and waterproof containers for backup media	72	82	96	72	90	89	65	81
227	System recovery on an alternate platform from backup media	63	86	80	83	78	79	67	77
Patch management metric									
228	Patch Policy Compliance	73	88	71	94	93	82	82	83
229	Patch Management Coverage	88	65	84	66	96	85	69	79
230	Mean-Time to Patch	91	84	77	97	75	80	96	86
231	Mean Cost to Patch	84	81	86	84	78	82	76	82
232	Delays and inconsistencies in patching	88	76	70	97	80	78	96	84
233	Patching cadence	74	65	87	85	97	90	92	84
234	Vendor patching cadence	91	72	94	93	77	66	68	80
Performance and effectiveness metric									
235	Metrics for measuring phishing susceptibility	92	76	63	89	82	80	69	79
236	Metrics for measuring malware susceptibility	90	80	88	79	94	78	91	86
237	Metrics for measuring password vulnerabilities	92	78	69	76	72	74	95	79
238	password meter metric	69	74	81	66	79	93	77	77
239	CWSS score	69	72	86	66	86	89	96	81
240	Encounter rate	66	70	81	66	84	94	74	76
241	Blocking rate	73	73	83	88	80	77	76	79
242	Breach frequency rate	64	77	68	73	66	84	70	72
243	time to first compromise metric	77	86	88	74	71	89	94	83
244	Penetration resistance metric	88	66	63	86	64	78	68	73
245	Network diversity	86	71	76	78	77	71	65	75
246	metrics for measuring zero day attacks	67	92	89	79	94	66	68	79
247	Metrics for measuring malware spreading	97	66	75	82	93	86	70	81
248	metrics for measuring obfuscation attacks	77	96	64	93	74	92	96	85
249	cybersecurity posture metric	91	65	65	73	87	64	83	75

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

Personnel security									
250	Ensuring that the agency has trained personnel to support compliance with information security policies, processes, standards, and guidelines	94	96	96	97	87	78	71	88
251	Personnel turnover	66	95	68	82	64	96	79	79
252	Ensure system users and support personnel receive the requisite security training	85	79	86	75	97	95	69	84
Physical and Environmental Protection									
253	Power consumed by the computer suite *versus* air conditioning capacity	83	91	97	77	67	92	80	84
254	Physical and environmental security maturity	68	90	73	90	88	87	81	82
255	Discrepancies between physical location and logical access location	90	87	64	68	67	79	69	75
256	Number of unsecured access points	97	87	91	76	76	93	84	86
257	Number of unacceptable physical risks on premises	80	72	67	86	68	97	64	76
258	Distance between employee and visitor parking	65	65	94	70	95	88	91	81
259	Percentage of facilities that have adequate external lighting	94	69	79	94	80	80	69	81
260	Percentage of physical security incidents allowing unauthorized entry into facilities containing information systems	95	79	90	92	82	76	76	84
Planning									
261	Cost Variance	97	80	73	66	71	91	66	78
262	Resource capacity utilization	79	95	68	74	90	70	94	81
263	Group and project portfolio utilization	64	66	81	88	93	89	91	82
264	Planned resources vs. resources in use	97	76	72	72	87	85	97	84
265	Planned time vs Used time	88	88	94	66	95	81	66	83
266	The Doomsday Metric	96	64	94	86	88	96	83	87
Risk Management									
267	Security risk management maturity	89	78	63	89	68	87	84	80
268	Number of high/medium/low risks currently untreated/unresolved	91	93	66	77	75	91	67	80
269	Information security budget variance	78	77	93	78	65	67	63	74
270	Process/system fragility or vulnerability	77	93	85	80	68	70	86	80
271	Number of unpatched technical vulnerabilities	81	90	93	92	72	96	95	88
272	Information security risk scores	96	71	76	94	88	74	81	83
273	Total liability value of untreated/residual risks	77	72	87	91	80	71	97	82
274	Coupling index	94	87	64	96	68	69	74	79
275	Changes in network probe levels	90	79	83	96	63	70	89	81
276	Organizational and technical homogeneity	73	88	65	90	92	92	87	84
277	Percentage of controls working as defined	84	90	88	93	93	74	88	87

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

278	Organization's insurance coverage *versus* annual premiums	95	69	70	89	79	81	66	78
279	Number of attacks	78	76	66	90	77	66	88	77
Security policy metric									
280	Number of security policies, standards, procedures and metrics with committed owners	69	64	69	77	86	88	88	77
281	Security policy management maturity	82	63	79	81	90	63	73	76
282	Traceability of policies, control objectives, standards & procedures	78	64	66	75	67	76	81	72
283	Number of important operations with documented & tested security procedures	85	85	70	80	76	90	89	82
284	Comprehensiveness of security policy coverage	64	69	83	94	66	71	80	75
285	Policy coverage of frameworks such as ISO/IEC 27002	63	94	65	94	71	68	63	74
286	Number or percentage of security policies addressing viable risks	78	87	81	93	69	90	87	84
287	Quality of security policies	75	96	74	88	93	81	89	85
288	Percentage of policy statements unambiguously linked to control objectives	81	69	67	95	97	70	92	82
289	Thud factor (policy verbosity/red tape index, waffle-o-meter)	63	67	74	75	91	97	63	76
290	Number of security policies whose review/reapproval is overdue	73	82	87	95	72	79	90	83
291	Flesch readability scores for policies, procedures, standards and guidelines	63	83	85	96	92	87	87	85
292	Number or percentage of security policies that are clear	87	93	69	65	78	96	85	82
293	Percentage of security policies that satisfy documentation standards	64	88	74	87	65	72	97	78
294	Number of security policies that are inconsistent with other policies or obligations	81	67	80	91	76	81	68	78
Situational awareness metric									
295	Are they preparing thoroughly to handle large-scale incidents or not	84	94	81	74	87	72	74	81
296	Establish and Maintain Accurate Notification Mechanisms	96	69	70	91	85	74	97	83
297	Develop Written Guidelines for Prioritizing Incidents	82	77	83	76	73	89	77	80
298	maximum response times incident response team	88	92	64	94	94	96	78	87
software security metric									
299	Software security maturity	87	69	67	89	64	71	90	77
300	Percentage of controls tested realistically	69	94	96	97	97	96	96	92
301	Software quality assurance	83	92	68	63	70	93	73	77
302	Quality of system security revealed by testing	82	76	88	77	96	93	92	86

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

303	Extent to which information security is incorporated in software QA	78	74	74	88	90	93	71	81
304	Extent to which QA is incorporated in information security processes	80	92	75	77	92	78	97	84
305	Percentage of configuration items in line with service levels for performance and security	66	90	70	63	80	65	96	76
306	Percentage of technical controls that fail-safe	84	80	89	86	87	70	68	81
307	Number of deviations identified between configuration repository and actual asset configurations	70	86	68	97	75	85	86	81
System and Communications Protection									
308	whether implementing system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance or not	97	79	84	64	71	87	69	79
System and services acquisition									
309	Determine how much of the product acquisition cost	79	69	89	65	86	88	84	80
System and information integrity									
310	whether implementing system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance or not	88	69	82	78	65	71	77	76
Vulnerability management metric									
311	Vulnerability Scanning Coverage	85	78	71	88	66	66	76	76
312	Percent of Systems with No Known Severe Vulnerabilities	91	72	90	72	93	66	86	81
313	Mean-Time to Mitigate Vulnerabilities	87	80	92	64	95	75	86	83
314	CVSS score	80	70	63	83	86	67	74	75
315	Number of Known Vulnerability Instances	92	90	92	84	86	94	64	86
316	Vulnerability index	95	83	69	87	85	81	88	84
317	Historical vulnerability metric	90	70	95	69	91	68	91	82
318	Historically exploited vulnerability metric	81	64	84	87	92	80	79	81
319	Future vulnerability metric	90	92	65	67	79	80	76	78
320	Future exploited vulnerability metric	92	77	87	83	82	77	83	83
321	Mean Cost to Mitigate Vulnerabilities	75	63	97	73	85	96	73	80

Table 3: List of security metrics in 32 security domains

Security Metrics Framework

Recently, Igor Khokhlov et. al. [37] proposed a framework to evaluate the data quality and security in mobile phones. But, this proposed framework not provided any security level/score of app. To determine security score of mobile application, the authors proposed Mobile App Security Capability Maturity Model (MASCMM). MASCMM framework is a 4-step GAME (Goals, Actions, Metrics, Evaluation) process.

Goals: The initial step in MASCMM framework is goals. In this step, proposed framework mainly focuses on identifying security requirements, business drivers, objectives and security requirements. This step

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

focus on what security activity/activities in security control domain have to measure and what are the security practices to be followed. High level management plays a key role while deciding these goals.

Actions: After selecting security activities for measuring, now it's time to develop the security assessment. Identify the list of security metrics for measuring the security activity. The authors proposed security metrics based on GAP-GOES criteria. Establish the benchmarks for each security activity based on the organization goals. Collect necessary data for measuring security activity. Measurement methods will differ to every metric category. So, identify the metric category and measurement method.

Metrics: In the metrics step, select the security metrics to be measured in the list of GAP-GOES based security metrics.

Evaluation: In the evaluation step, measure the security score for each security activity and calculate the security score for each security control domain and then calculate the security score for mobile application. Now, based on the security score attained, determine the maturity level for each security control domain.

Level 1: Performed informally

This security level of maturity is defined as unorganized and unstructured. Processes are not well documented and information security efforts are not repeatable.

Level 2: well defined

This security level of maturity is defined as well defined and information security efforts are repeatable. Processes are standardized and documented. Simply we can say "audit-ready".

Level 3: Quantitatively controlled

This security level of maturity can be defined as quantitatively controlled. In addition to level 2, this level satisfies the metric-driven process. In this level, performance measures can be analyzed, managed and quantitatively known.

Level 4: Continuously improving

This security level of maturity can be defined as world-class practices. In addition to level 3, this level acquires the feature of continuously improving the process

The authors used standard template[NIST] for documenting the process of metric development and evaluation process. By using this standard template, organizations will easily identify the analysis and reports easily and also used for future reference. Sample template shown in below table and flowchart of MASCMM is shown in figure 4. After calculating security score of each security domain, represent all of them in a spider chart shows the secured zone of the app. For instance, we selected 5 security domains and measured each security activity using above process and figure 5 shows maturity level of each security domain and security zone (showed as dotted lines) of the app.

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

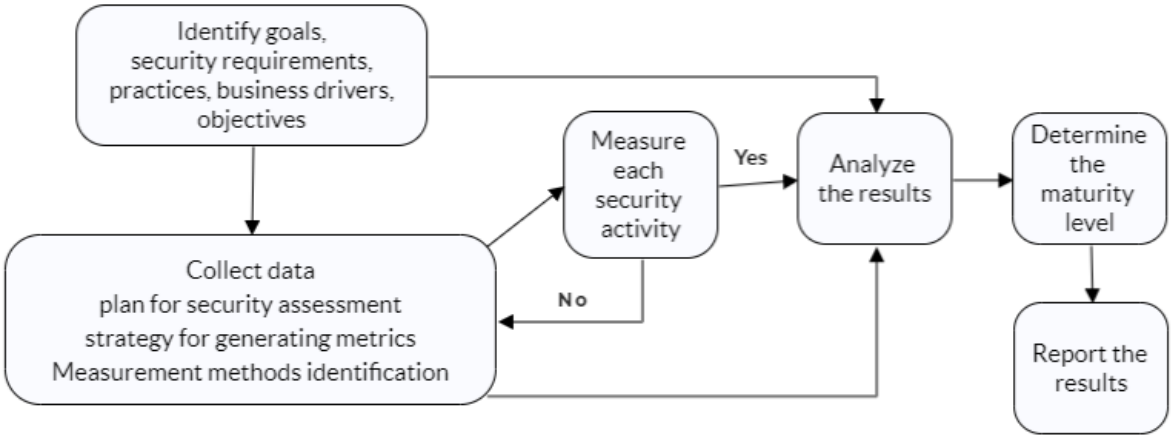

Figure 4: Flowchart of MASCMM

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

Name of control family	Vulnerability management
Name of Metric	Vulnerability scanning coverage
Version	1.0
Status	Final
Description	Vulnerability Scanning Coverage (VSC) measures the percentage of the organization's systems under management that were checked for vulnerabilities during vulnerability scanning and identification processes. This metric is used to indicate the scope of vulnerability identification efforts.
Type	Technical
Audience	Security Operations
Question	What percentage of the organization's total systems has been checked for known vulnerabilities?
Answer	Positive integer value that is greater than or equal to zero but less than or equal to 100%. A value of "100%" indicates that all systems are covered by the vulnerability scanning process.
Formula	Vulnerability Scanning Coverage is calculated by dividing the total number of systems scanned by the total number of systems within the metric scope such as the entire organization: $VSC = \frac{Count(Scanned\_Systems)}{Count(All\_Systems\_Within\_Organization)} * 100$
Units	Percentage of systems
Frequency	Weekly, Monthly, Quarterly, Annually
Targets	VSC values should trend higher over time. Higher values are obviously better as it means more systems have been checked for vulnerabilities. A value of 100% means that all the systems are checked invulnerability scans. For technical and operational reasons, this number will likely be below the theoretical maximum.
Sources	Vulnerability management and asset management systems will provide information on which systems are scanned for vulnerabilities.
Visualization	Bar Chart X-axis: Time (Week, Month, Quarter, Year) Y-axis: VSC (%)

Table 4: Template for specifying metric evaluation and its results

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

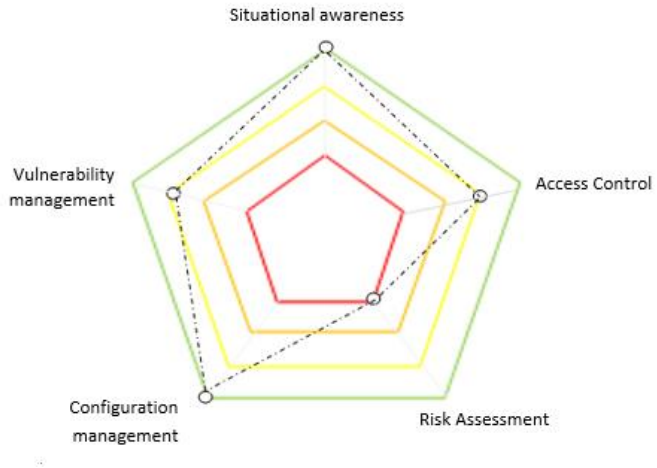

Figure 5: Security level of 5 security domains and security zone (showed in dotted lines) of the app

Results

Our R & D team (Centre for Mobile Banking, IDRBT, India) started security testing of mobile applications especially banking applications. This constituted static testing and dynamic testing with the help of automated tools and manual testing. For identifying security flaws in the mobile apps, starting point was, use of CVSS score and number of known vulnerability instances as metrics. But now, with the improved model, a list of 321 metrics is provided to the organizations (Bankers) which the organizations select based on organization's business requirements depending on practical considerations, such as availability of data, time to measure, etc. This facilitates calculation of the security score of their app, that is aligned with their business objectives. Recently, one bank (bank name cannot be revealed for confidentiality and security reasons) selected 26 metrics in 6 security domains for calculating security level of their mobile app. Our team calculated those 26 metrics and gave the security level of that mobile app. Some of the mobile apps we tested and their security levels (after masking organization and app name details) are shown in table 5 below.

S. No.	Name of mobile app (Name of the apps are renamed)	Total number of security domains selected	Total number of security metrics selected	Security level of mobile app
1	App1	1	1	2
2	App2	1	1	3
3	App3	1	1	3
4	App4	1	1	3
5	App5	1	1	2
6	App6	1	1	3
7	App7	1	1	4
8	App8	1	1	3
9	App9	1	1	3
10	App10	1	1	2
11	App11	3	6	4
12	App12	4	22	2
13	App13	3	14	2
14	App14	6	23	3
15	App15	5	20	3
16	App16	4	19	3
17	App17	4	21	3
18	App18	6	19	2
19	App19	4	17	3
20	App20	6	26	3

Table 5: Listing app wise security metrics calculated and its security levels

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

With this new model, we are creating awareness among, banks and other organizations, on these metrics and asking them to maintain necessary data for evaluating these metrics. This will facilitate improvement in their apps' security requirements (that are aligned with business requirements). We started testing with 1 metric and have now increased scope to testing with 26 metrics.

Conclusion

Usage of mobile apps is increasing. But, users don't know security score of the mobile app. In this work, authors proposed Mobile Application Security Maturity Model (MASCMM). By using MASCMM, app vendors/ organizations can calculate security score of the app. It is a 4-step GAME (Goals, Actions, Metrics and Evaluations) process. The authors identified 32 security domains and listed 321 security metrics in it. The authors defined GAP-GOES meta-metrics and based on this, derived security metrics. Based on the needs of an organization, users can select the security domains and security metrics; and evaluate the security score of security domain as well as an app and define the CMM level by using MASCMM. All the metric analysis, evaluations and results are documented in a standardized way.

Future Work

In this work, the authors proposed 321 non-functional security metrics. In future, these security metrics can be categorized based on type of mobile app. For example, if the mobile app intended for basic functionalities like Alarm, Notepad etc., we need not to check all 321 security metrics. So, in future, researchers can work on categorization of security metrics based on app functionality.

References

1. "How Many People Have Smartphones Worldwide (Dec 2020)." https://www.bankmycell.com/blog/how-many-phones-are-in-the-world (accessed Dec. 09, 2020).
2. "What Is Cybersecurity? - Cisco." https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html (accessed Dec. 09, 2020).
3. P. E. Black, K. Scarfone, and M. Souppaya, "CYBER SECURITY METRICS AND MEASURES," 2008. Accessed: Dec. 09, 2020. [Online]. Available: https://www.nist.gov/publications/cyber-security-metrics-and-measures.
4. Irc, "INFOSEC Research Council (IRC) Hard Problems List," *Distribution*, no. November, p. 57, 2005, [Online]. Available: http://www.cyber.st.dhs.gov/docs/IRC_Hard_Problem_List.pdf.
5. W. Brotby and G. Hinson, *Pragmatic security metrics: applying metametrics to information security*. 2013.
6. S. Chen *et al.*, "Are mobile banking apps secure? what can be improved?," *ESEC/FSE 2018 - Proc. 2018 26th ACM Jt. Meet. Eur. Softw. Eng. Conf. Symp. Found. Softw. Eng.*, vol. 2018, pp. 797–802, 2018, doi: 10.1145/3236024.3275523.
7. D. E. Krutz, N. Munaiah, A. Meneely, and S. A. Malachowsky, "Examining the relationship between security metrics and user ratings of mobile apps: A case study," *WAMA 2016 - Proc. Int. Work. App Mark. Anal. co-located with FSE 2016*, pp. 8–14, 2016, doi: 10.1145/2993259.2993260.
8. A. Rahman, P. Pradhan, A. Partho, and L. Williams, "Predicting Android Application Security and Privacy Risk with Static Code Metrics," *Proc. - 2017 IEEE/ACM 4th Int. Conf. Mob. Softw. Eng. Syst. MOBILESoft 2017*, pp. 149–153, 2017, doi: 10.1109/MOBILESoft.2017.14.
9. G. Catolino, P. Salza, C. Gravino, and F. Ferrucci, "A Set of Metrics for the Effort Estimation of Mobile Apps," *Proc. - 2017 IEEE/ACM 4th Int. Conf. Mob. Softw. Eng. Syst. MOBILESoft 2017*, pp. 194–198, 2017, doi: 10.1109/MOBILESoft.2017.31.
10. R. M. Savola, P. Savolainen, A. Evesti, H. Abie, and M. Sihvonen, "Risk-driven security metrics development for an e-health IoT application," *2015 Inf. Secur. South Africa - Proc. ISSA 2015 Conf.*, vol. 1, pp. 0–5, 2015, doi: 10.1109/ISSA.2015.7335061.
11. "M. Whitman and H. Mattord, Management of information... - Google Scholar." https://scholar.google.co.in/scholar?hl=en&as_sdt=0%2C5&q=M.+Whitman+and+H.+Mattord%2C+Management+of+information+security%2C+Cengage+Learning%2C+2013&btnG= (accessed Dec. 09, 2020).

12. M. Carr, "Public-private partnerships in national cyber-security strategies," 2016. doi: 10.1111/1468-2346.12504.
13. "M. Gasser, Building a secure computer system, Van... - Google Scholar." https://scholar.google.co.in/scholar?hl=en&as_sdt=0%2C5&q=M.+Gasser%2C+Building+a+secure+computer+system%2C+Van+Nostrand+Reinhold+Company+New+York%2C+NY%2C+1988.&btnG= (accessed Dec. 09, 2020).
14. D. Craigen, N. Diakun-Thibault, … R. P.-I. M., and undefined 2014, "Defining cybersecurity," *timreview.ca*, Accessed: Dec. 09, 2020. [Online]. Available: https://timreview.ca/article/835.
15. I. Atoum, A. A. Otoom, and A. Otoom, "A Classification Scheme for Cybersecurity Models A Computational Approach for Predicting Software Quality in Use From Software Reviews View project CMMI implementation View project A Classification Scheme for Cybersecurity Models A Classification Scheme for Cybersecurity Models," *Int. J. Secur. Its Appl.*, vol. 11, no. 1, pp. 109–120, 2017, doi: 10.14257/ijsia.2017.11.1.10.
16. W. Humphrey, "Managing the software process," 1989, Accessed: Dec. 09, 2020. [Online]. Available: https://dl.acm.org/citation.cfm?id=64795.
17. N. T. Le and D. B. Hoang, "CAPABILITY MATURITY MODEL AND METRICS FRAMEWORK FOR CYBER CLOUD SECURITY." Accessed: Dec. 09, 2020. [Online]. Available: https://opus.lib.uts.edu.au/handle/10453/121301.
18. A. Arabsorkhi, F. G.-2018 9th I. S. on, and undefined 2018, "Security Metrics: Principles and Security Assessment Methods," *ieeexplore.ieee.org*, Accessed: Dec. 09, 2020. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8661030/.
19. "Jilin, G.: SSE-CMM Security Metrics. NIST and CSSPAB... - Google Scholar." https://scholar.google.co.in/scholar?hl=en&as_sdt=0%2C5&q=Jilin%2C+G.%3A+SSE-CMM+Security+Metrics.+NIST+and+CSSPAB+Workshop%2C+Washington%2C+D.C.%2C+June+%282000%29&btnG= (accessed Dec. 09, 2020).
20. D. Gollmann, F. Massacci, and A. Yautsiukhin, *Quality of protection: Security measurements and metrics*. 2008.
21. R. Barabanov, S. Kowalski, and L. Yngström, "Information Security Metrics State of the Art," 2011. Accessed: Dec. 09, 2020. [Online]. Available: https://www.diva-portal.org/smash/record.jsf?pid=diva2:469570.
22. "Chapin, D. A. & Akridge, S.. How can security be... - Google Scholar." https://scholar.google.co.in/scholar?hl=en&as_sdt=0%2C5&q=Chapin%2C+D.+A.+%26+Akridge%2C+S..+How+can+security+be+measured%3F+Information+Systems+Control+Journal%2C+http%3A%2F%2Fwww.isaca.org%2FJournal%2FPast-Issues%2F2005%2FVolume-2%2FPage+s%2Fdefault.aspx+%282005%29.&btnG= (accessed Dec. 09, 2020).
23. "A guide to security metrics, SANS Security Essentials... - Google Scholar." https://scholar.google.co.in/scholar?hl=en&as_sdt=0%2C5&q=A+guide+to+security+metrics%2C+SANS+Security+Essentials+GSEC+Practical+Assignment+Version%2C+1+%282010%29.&btnG= (accessed Dec. 09, 2020).
24. G. Campbell, … M. B. of the I. A., and undefined 2014, "Building a metrics program that matters.," *europepmc.org*, Accessed: Dec. 09, 2020. [Online]. Available: https://europepmc.org/article/med/24707764.
25. "Kark, K., et al. "Defining an effective security... - Google Scholar." https://scholar.google.co.in/scholar?hl=en&as_sdt=0%2C5&q=Kark%2C+K.%2C+et+al.+%22Defining+an+effective+security+metrics+program.%22+Forrester+Research+%282007%29.&btnG= (accessed Dec. 09, 2020).
26. M. Whitman and H. Mattord, "Principles of Information Security Fourth Edition," 2011. Accessed: Dec. 09, 2020. [Online]. Available: https://books.google.co.in/books?hl=en&lr=&id=xboIAAAAQBAJ&oi=fnd&pg=PR9&dq=Whitman,+Michael+E.,+and+Herbert+J.+Mattord.+Principles+of+information+security.+Cengage+Learning,+2011.&ots=ov2-XYX9Um&sig=nax_kqvzFUiTJRbbnrAdZYSrcuw.

International Journal of Modern Agriculture, Volume 9, No.4, 2020
ISSN: 2305-7246

27. E. Chew *et al.*, "Performance M NIST Special Publication 800-55 Revision 1 easurement Guide for Information Security," 2008. doi: 10.5555/2206269.
28. "Security Metrics Development and Implementation Based on NIST Directives | Types | Pearson IT Certification." https://www.pearsonitcertification.com/articles/article.aspx?p=1675146 (accessed Dec. 09, 2020).
29. "ISO - ISO/IEC 27001 — Information security management." https://www.iso.org/isoiec-27001-information-security.html (accessed Dec. 09, 2020).
30. "About O-ISM3 | Information Security Management using O-ISM3." https://www.ism3.com/node/42 (accessed Dec. 09, 2020).
31. "ITScore for Information Security." https://www.gartner.com/en/documents/3231718/itscore-for-information-security (accessed Dec. 09, 2020).
32. "Security Framework and Risk Assessment Services | IBM." https://www.ibm.com/security/services/security-framework-and-risk-assessment (accessed Dec. 09, 2020).
33. R. Caralli, J. Allen, and D. White, *CERT Resilience Management Model-CERT-RMM: A Maturity Model for Managing Operational Resilience*. 2016.
34. "Department of Homeland Security Cybersecurity Capability Maturity Model White Paper," 2014.
35. "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," Gaithersburg, MD, Apr. 2018. doi: 10.6028/NIST.CSWP.04162018.
36. "Curtis, Pamela, Nader Mehravari, and James Stevens.... - Google Scholar." https://scholar.google.co.in/scholar?hl=en&as_sdt=0%2C5&q=Curtis%2C+Pamela%2C+Nader+Mehravari%2C+and+James+Stevens.+Cybersecurity+capability+maturity+model+for+information+technology+services+%28c2m2+for+it+services%29%2C+version+1.0.+No.+CMU%2FSEI-2015-TR-009.+CARNEGIE-MELLON+UNIV+PITTSBURGH+PA+PITTSBURGH+United+States%2C+2015.&btnG= (accessed Dec. 09, 2020).
37. I. Khokhlov, L. Reznik, and S. Chuprov, "Framework for Integral Data Quality and Security Evaluation in Smartphones," *IEEE Syst. J.*, pp. 1–8, 2020, doi: 10.1109/jsyst.2020.2985343.