Journal of Music Science, Technology, and Industry
Volume 4, Number 2, 2021
e-ISSN. 2622-8211
https://jurnal.isi-dps.ac.id/index.php/jomsti/

Contingency Planning in IT Risk Audit on Music Digital Recording Company

Isra Ruddin[1], **Handri Santoso**[2], **Richardus Eko Indrajit**[3], **Erick Dazki**[4]
[1,2,3,4]Magister Technology Information, Universitas Pradita,
Scientia Business Park
[1]isra.ruddin@student.pradita.ac.id, [2]handri.santoso@pradita.ac.id
[3]eko.indrajit@pradita.ac.id, [4]erick.dazki@pradita.ac.id

Article Info

Article History:
Received:
August 2021
Accepted:
October 2021
Published:
October 2021

Keywords:
Contingency Plan, IT Risk Audit, Music Digital, Mobile Platform, Android

ABSTRACT

Tujuan: Aplikasi dan layanan musik harus menciptakan pengalaman privasi yang baik dan menghasilkan kepercayaan dan keyakinan. **Metode penelitian**: Kunci untuk mewujudkan tujuan ini adalah kerangka kerja yang kuat dan efektif untuk perlindungan keamanan, berdasarkan prinsip transparansi, pilihan, dan kontrol. **Hasil dan pembahasan**: Sistem Apex memperluas Android untuk memungkinkan pengguna secara selektif mengizinkan, menolak, atau membatasi akses dengan izin khusus yang diminta oleh aplikasi. Efek samping dari penolakan akses ke sumber daya adalah aplikasi dapat melempar pengecualian dan menghentikannya. **Implikasi**: Pengembangan ProtectMyPrivacy (PMP) diharapkan pengguna memiliki perlindungan yang lebih kuat terhadap serangan yang berfokus pada privasi, tetapi kehilangan perlindungan terhadap serangan runtime.

INTRODUCTION

Music is a powerful expression of human emotions and an art form that has existed for centuries and can be considered a creative social process. The evolution of musical instruments over time has created multiple interaction mechanisms for musicians to be creative and express themselves (Woldecke, Geiger, Reckter & Schulz, 2010). Making music on mobile devices is a popular and diverse way. A large number of mobile applications have been developed that turn mobile devices into music playing

devices, allowing individuals to create and perform music (Zhou, Percival, Wang, Wang & Zhao, 2010).

Today's digital development, music can be connected in a mobile application. The aim of this mobile application is to build an easy-to-use music player with a hosting server in the cloud that facilitates data authentication. Mobile application design and development must take into account the important limitations of mobile devices and design applications that meet the specific habits of users. Some of the limitations include CPU performance characteristics, memory and storage space, battery life, screen size, device mobility, etc. This project addresses each of the specific characteristics of mobile applications in the design, development and testing phases.

UI design is an important part because it is the link in interacting directly with the user of the application and provides music visualization of a clean and easy to use user interface, simple color scheme and various ways of navigation. Users can navigate from the home page to the song to be played, by album or artist. These different ways to find a song provide different navigation paths and can be much easier when there are a lot of audio files on the device. Another important feature is the music visualization. Three different visualizations available added in visualizer. Users can add any song they want during playback (Savage, Ali & Chavez, 2010).

The emergence of mobile platforms and open mobile convergence have created a vibrant and dynamic mobile ecosystem enabling individuals to form and present personal identities online, connect with communities of choice, and engage with, innovative applications and services. Many rely on real-time access and use of personal information that is often transferred globally between applications, devices and enterprises. While these capabilities serve as drivers of innovative business models and personalization of applications and services, they may also provide a tacit access link to users' personal information. Even apps that legitimately access and use personal information may fail to meet user privacy expectations and undermine user trust in the organization and the wider mobile ecosystem. Problems occur when users are not given clear and transparent notices about the app's access to their personal usage information, or when they are not given the opportunity to express meaningful choices and control over the use of their information for purposes secondary to and beyond those necessary for the operation of an app. or service.

1.2 Goal

Music apps and services must create a good privacy experience and generate trust and confidence. The key to realizing this goal is a strong and effective framework for security protection, based on the principles of transparency, choice and control. This guide adopts the Privacy by Design approach and is intended to help ensure that mobile applications are developed protecting the privacy of users and their personal information.

1.3 Benefits

As a guide applying privacy design principles to applications and their related services designed for mobile devices. They are intended to be applied to all parties in the application or service delivery chain that are responsible for collecting and processing users' personal information data - developers, device manufacturers, platform and OS companies, mobile operators, advertisers, and analytics companies.

1.4 Threats and Risks

According to NIST SP 800-30 (2012) a threat is any situation or event that has the potential to have an adverse impact on the operations of assets, individuals and other organizations through unauthorized access, destruction, disclosure or modification of information. Threat events caused by threat sources.

Risk is a combination of the probability of an event and the consequences of the event, with the possibility that there is more than one consequence for one event, and the consequences can be positive or negative. (Shortreed, et al. 2003). But risk is generally viewed as something negative, such as loss, danger, and other consequences. The loss is actually a form of uncertainty that should be understood and managed effectively by the organization as part of the strategy so that it can be added value and support the achievement of organizational goals.

According to Gondodiyoto (2006, p302), threats to security can be natural, human, negligent or intentional, including:

a) Threat of fire

Some security measures for fire threats:

a. Have automatic fire extinguishers and fire extinguishers.

b. Have an emergency door/ladder

c. Perform routine checks and tests on the fire protection system to ensure that everything is properly maintained.

b) The threat of flooding

Some of the implementation of security for the threat of flooding:

a. Use waterproof roofing, walls and floors

b. All material asset information is placed in a high place

c. Energy source voltage change

d. Implementation of safety to anticipate changes in energy source voltage, For example: using a stabilizer or power supply (UPS).

c) Structural Damage

Implementation of safeguards to anticipate structural damage, for example: choosing a company location where earthquakes, hurricanes, floods are rare.

d) Intruder

The implementation of security to anticipate intruders is the placement of guards and the use of alarms or surveillance cameras.

e) Virus

Implementation of security to anticipate the virus are:

a. Preventive, such as using anti-virus and updating regularly

b. Detectives, for example, scan files before use.

c. Corrective, for example ensuring virus-free data backup, use of anti-virus against infected files.

f) Hacking

Some security implementations to anticipate hacking:

The use of logical controls such as the use of passwords that are difficult to guess. Security officers regularly monitor the system in use.

g) Network failure, system and data failure several security measures to anticipate these risks:

a. Recovery Time Objectives (RTO) is the length of time required for system and data recovery. If there is a dependency between service components or service components, then the recovery time is calculated serially for interdependent components. If the service components are not interdependent, recovery time can be calculated in parallel between service components. Maximum RTO is 80% of the maximum tolerated service downtime or MTDL.

b. Recovery Point Objectives (RPO) are thresholds for how much data can be lost since the last backup was performed. If the backup is done once a day

at night, while system/storage failure can occur a few minutes before the backup process is run, then the RPO value is 24 hours. In other words, RPO is a statement of how long an information/data may be lost.

1.5 Business Impact Analysis (BIA)

Svata (2013), suggests that Business Impact Analysis (BIA) is the basis of risk management and continuity management which thoroughly analyzes and identifies critical resources and timeframes that must be returned when disruption occurs which allows for realistic strategic considerations of strategy. Business recovery, where the approach in conducting Business Impact Analysis (BIA) to be able to analyze which risks are accepted and which are not accepted using two parameters, namely:

a. Risk Appetite is the amount of overall risk to a company or other entity that is acceptable or acceptable in achieving company goals.

b. Risk Tolerance is an acceptable relative variation in achieving a goal which is measured in the same unit used to measure the related objective. The main output of Business Impact Analysis (BIA) is the recovery requirements for each critical function/process. Where the recovery requirements consist of related information:

a. Business needs for recovery of important functions.

b. Technical requirements for recovery of critical functions. Where the recovery requirements are expressed with the help of two values:

1. Recovery Point Objective (RPO) is an acceptable amount of time in recovering data.
2. Recovery Time Objective (RTO) is an acceptable amount of time in restoring functionality. (Solehudin, 2005), stated that Business Impact Analysis (BIA) is a process carried out before making a Disaster Recovery Plan where Business Impact Analysis (BIA) is used to help business units understand the impact of a disaster. Carrying out risk analysis and determining the impact on the company if the potential loss identified from the risk analysis actually occurs. Where is the main purpose of.

Business Impact Analysis (BIA) is to create a document that will be used to help understand the impact of a disaster on a company's business processes where the impact can be financial (quantitative) or operational (qualitative, such as the inability

to respond to customer complaints).). In addition, Business Impact Analysis (BIA) has 3 main objectives, including:

1. Critical priority

Where each critical business unit process must be identified, prioritized, and the impact of the disaster event must be evaluated. More specifically, time-bound business processes to be implemented have a lower priority level for recovery than time-bound business processes.

2. Estimated Downtime

Estimated Business Impact Analysis (BIA) is used to help estimate the Maximum Tolerable Downtime (MTD) or the maximum length of downtime that can be tolerated and practiced by the company.

3. Resource Needs

Resource requirements for vital processes can also be identified in the Business Impact Analysis (BIA), processes that are highly time dependent will be prioritized for resource allocation. (St-Germain, Aliu, Dewez, & Dewez, 2012), argues that Business Impact Analysis (BIA) is an activity that allows organizations to identify important processes that support their main products and services, where there are interdependencies between processes and resources involved. Provided necessary to operate the process at an acceptable minimum level.

In the Business Impact Analysis (BIA) (Solehudin, 2005), stated that the things that must be done in the Business Impact Analysis (BIA) include:

1. Collect the required assessment materials

The initial stage of the Business Impact Analysis (BIA) is to identify which business units are the most important (critical) to keep running at the permitted operating level. Questions that need to be asked in this BIA include:

a. Information resources that are important to the organization

b. Business processes that if not running will have a fatal negative impact on the company. Where each process needs to be considered its criticality, with indications including:

a. Processes related to one's life

b. A process that will lead to tremendous financial losses

c. Processes that must comply with applicable regulations, for example: the financial sector, or Air Traffic Control.

After the materials have been collected and the business operations functions identified, the Business Impact Analysis (BIA) process will examine the relationship between these business functions on several factors such as business success, priority scale between business units, and alternative process procedures that can be used.

2. Conduct risk analysis

Conduct risk analysis the function of this analysis is to analyze the impact of disasters where there will be 2 parts of the analysis, namely financial (quantitative) and operational.

Generic Model BCP

According to Ankur Kumar Shrivastava, et al, (2012:85) the emphasis is on the importance of:

1) Understand business contingency needs and the need to establish policies and objectives for business continuity.
2) Implementation and operation of controls to ensure an organization's global business continuity risks.
3) Monitoring and reviewing the performance of the business contingency plan.
4) Continuous improvement based on business contingency objectives, measurement.

METHOD

Stage 1: Conducting BIA

According to the Federal Financial Institutions Examination Council (FFIEC), a business impact analysis (BIA) is the first step in the BCP planning process which includes the following:

- Assessment and prioritization of all business processes and functions
- Identifying the potential impact of disruption to the business that can cause an uncontrollable event to occur in business functions and processes
- Identification of the regulations needed for business processes and functions
- Estimate the maximum tolerable downtime and the acceptable level of loss associated with business functions and processes
- Estimate recovery time objectives (RTO), recovery point objectives (RPO) and recovery critical path

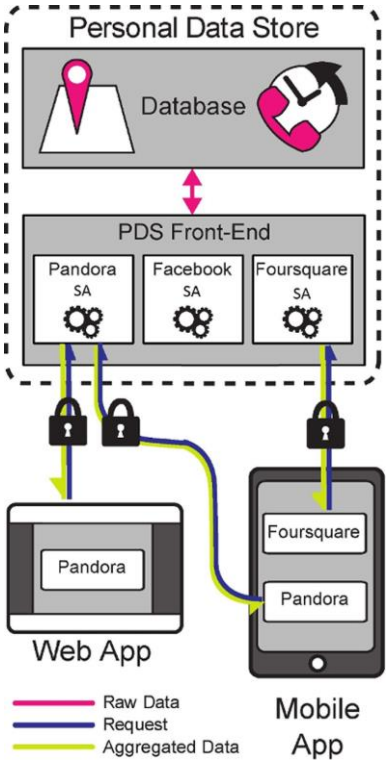


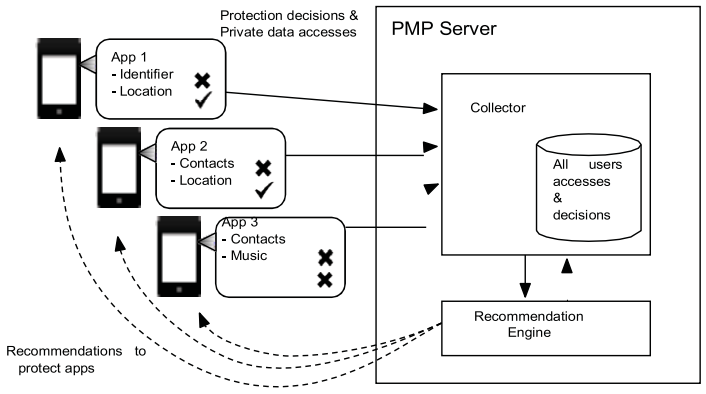
Figure 3.1 BIA (Source: NIST, 2010)

From the BIA example in Figure 3.1, it can be seen that BIA is an analysis and prioritization process to identify potential impacts that can occur on business processes and related system components in the event of a disruption. This BIA design is used for prevention with an accurate security system, in addition to providing a backup for the container for storing song material so that it is not stolen.

Stage 2: Creating IRP

IRP consists of a set of detailed processes and procedures that anticipate, detect, and mitigate the consequences of unwanted incidents that endanger information resources and organizational assets, when these incidents are detected to actually occur and affect or damage information assets. Incidents are threats that have occurred and attack information assets, and threaten the confidentiality, integrity or availability of information resources. Incident Response Planning includes incident detection, incident response, and incident recovery. The related work on smartphone privacy falls into four general categories namely data access control mechanisms, studies on privacy issues, mechanisms for mitigating privacy concerns, and finally user perceptions of app privacy. The first step to protecting user privacy is to detect apps that are accessing sensitive data.

In order to protect user privacy, it is important to understand when an application accesses personal user data for legitimate reasons such as to provide location-based services, and distinguish it from questionable reasons such as sending data to ad networks. The Apex system extends Android to allow users to selectively allow, deny or restrict access with specific permissions requested by apps. A side effect of denying access to a resource is that the application can throw an exception and terminate it. Mockdroid proposes to modify the Android OS replacing private data with mock data such as constant values or values when an application requests it. TISSA is developed for Android which provides various types of mock data in place of private data at runtime to untrusted applications based on user preferences. Here is a design drawing



Stage 3: Creating DRP

Disaster Recovery Plan (DRP) is a plan designed to restore or recover the operations of a system, application or computer facility in another alternative place after a disaster occurs. Making DRP first requires an analysis of the company's business processes and needs which will later aim to prevent the impact during an emergency.

Another definition of DRP was conveyed by the National Institute of Standards and Technology (NIST), that DRP is a plan that focuses on information systems that have been designed to restore replacement or alternative condition systems after a disturbance occurs. Disaster Recovery Plan (DRP) is a part of business continuity that focuses on how to deal with the impact of an event. DRP contains steps in the planning stage that can be implemented to stop the impact of a crisis that was never planned before.

Disaster Recovery Planning (DRP) and Business Continuity Planning (BCP) discuss planning for emergencies that threaten business continuity and continue the business even if a disaster occurs. The goals of BCP and DRP are to keep the business operating despite disruptions and to save information systems from further disaster impacts. Disaster Recovery Planning (DRP) is very important for companies so that company operations can continue even though a disaster occurs. If the company's operations are hampered, the company will experience losses. The following are the stages of Disaster Recovery Planning:

1. Risk Assessment

Risk Assessment is the process of identifying threats that may occur, both from within and from outside. The analyzed disasters include natural disasters, technical failure disasters, and human factor threats. Risk Assessment plays an important role for the sustainability of the overall development of the Disaster Recovery Planning because it can be considered as the initial basis that will influence the subsequent stages. Risk Assessment is usually followed by Impact Analysis, where the identified potential disasters are then analyzed for their impact.

2. Priority Assessment

When a disaster occurs and disrupts various business processes and operations, it is very important to have a clear order of process priorities. The processes that are considered the most vital for the sustainability of the system will later get the greatest

allocation of attention to be restored before other processes. Thus, the objective of the development of the Disaster Recovery Plan, which is to ensure the system can function as well as possible as soon as possible after the disruption of a disaster, can be accomplished. Priority assessment for the process is usually very relative to the time and place of the occurrence of a disaster. Prioritization at this stage is very crucial and is related to the execution of the Disaster Recovery Plan in the field later if a disaster occurs, this stage must be carried out carefully and through various kinds of careful considerations.

3. Recovery Strategy Selection

The choice of recovery strategy should be carefully considered. A good recovery strategy must meet several criteria, namely:

- The recovery strategy must meet the key requirements defined in the previous stage.
- The recovery strategy must be cost effective commensurate with the risks and priorities
- The recovery strategy should be applicable to current conditions and allow for improvement if the technology or related business develops in the future.

The recovery strategy that has been designed must then be poured into a well-documented Disaster Recovery Plan so that it can be easily implemented in the event of a disaster.

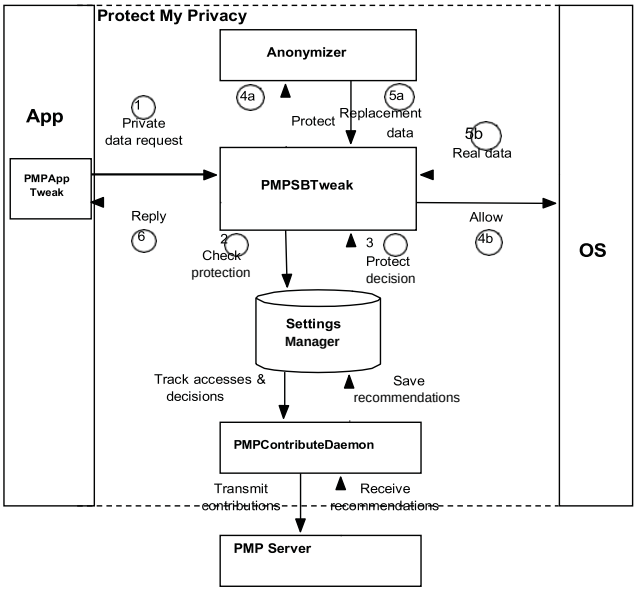
4. Plan Documenting

The results of the analysis and strategic design that have been produced from the previous stages must be well documented, so that when a disaster occurs again in the future, and human resources or employees who work for the organization can follow the previously documented DRP document. Therefore, the Disaster Recovery Plan must be documented in a structured manner so that it is easy to understand when needed. There are various standards for documenting a Disaster Recovery Plan. Toolkits and guidelines for preparing Disaster Recovery Plan documents are also widely available.

The disaster recovery plan used is ProtectMyPrivacy (PMP). First, the PMP must be designed in such a way that it can be evaluated by a large population of actual smartphone users, regardless of its technical complexity. Second, the PMP must be

able to detect runtime access to private information, and determine whether to allow or deny access (either by prompting the user or automatically). Third, the PMP must have an easily accessible user interface (UI) for configuring privacy settings across applications.

PMP must run transparently as a plug-in to any unmodified application run by the user, while communicating with its own database to store settings. The next type of personal data that PMP protects is the user's address book which is stored in a database on the device, containing contact information such as name, address, phone number, and email. The designed PMP should empower users to allow access to their address book, or protect it by diverting access to an alternate address book, which is populated with unauthorized entries (name, email and phone number) for each application. Sending unauthorized information not only protects users but also reduces the integrity of a rogue developer's remote database, making it difficult to distinguish between genuine and authorized data, reducing value and potentially preventing sales. An old issue is location privacy. If an application does not require location for an obvious or required feature, then the PMP must allow the user to protect its location. For the same reason, as with UDID, the PMP must provide a random location or allow the user to select a fake location to prevent profiling. The following is a Disaster Recovery Planning design to protect music data in the application.



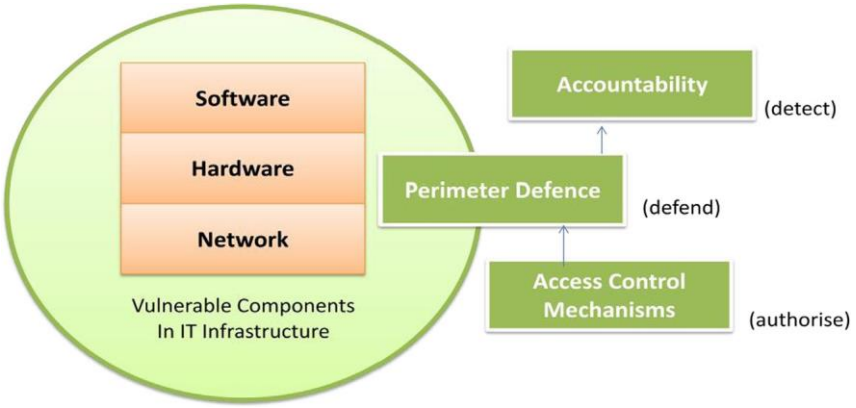
Stage 4: Creating BC

For this BC stage, it focuses on virus attacks that can make applications not function properly and are prone to data theft. Many cybersecurity experts believe that malware is the weapon of choice for malicious intent to breach cybersecurity efforts in cyberspace. Malware refers to a broad class of attacks that are loaded on a system, usually without the knowledge of the rightful owner, to harm the system for the benefit of the adversary. Some examples of malware classes include viruses, worms, trojan horses, spyware, and bot executables. Malware infects systems in various ways for example spreading from infected machines, tricking users into opening contaminated files, or luring users to visit websites that spread malware.

In a more concrete example of a malware infection, the malware could load itself onto a USB drive that was inserted into the infected device and then infect every other system where the device was then inserted. Malware can spread from devices and equipment that contain embedded systems and computing logic. In short, malware can be inserted at any point in the system's lifecycle. Victims of malware can range from end-user systems, servers, network devices (e.g., routers, switches, etc.) and process control systems such as Supervisory Control and Data Acquisition (SCADA). The proliferation and sophistication of malware, which is rapidly increasing in number, is a major concern on the Internet today.

Traditionally, malware attacks occur at a single surface point among hardware devices, software sections or at the network level exploiting design and implementation vulnerabilities that exist at each layer. Instead of protecting every asset, the perimeter defense strategy has been used primarily to put a wall on the outside of all internal resources to protect everything inside from unwanted intrusion from the outside. The majority of perimeter defense mechanisms use firewall and anti-virus software built into the intrusion prevention/detection system. Any traffic coming from outside is intercepted and checked to make sure no malware is getting into the resources. The general acceptance of this perimeter defense model has come because it is much easier and apparently cheaper to secure a single perimeter than to secure a large number of applications or a large number of internal networks. To provide more defined access to certain internal resources, access control mechanisms have been used in conjunction with perimeter defense mechanisms. However, the combined efforts of perimeter defense strategies have proven increasingly ineffective as malware advances and sophistication improves. The ever-evolving malware always

seems to find loopholes to bypass the perimeter defense altogether. We describe in detail the most common exploits in the three different layers of an information system present at the hardware, software, and network layers. Malware evolves over time by taking advantage of new approaches and exploiting vulnerabilities in emerging technologies to evade detection. The unique characteristics of each of these emerging technologies and how malware takes advantage of these unique characteristics to reproduce itself.



RESULT AND DISCUSSION

3.1 BIA

Overall the BIA process is carried out through nine stages as follows: (1) determining the objectives, scope and assumptions needed to create/process the BIA; (2) prepare a BIA questionnaire based on the agreed objectives, scope and assumptions; (3) prepare a BIA Scoring Tool to assess all BIA questionnaires from business functions; (4) conduct an internal pre-assessment to sharpen the BIA assessment of business functions in the “Very Critical”/Critical Business Function (CBF) and “Critical” categories; (5) conduct a BIA workshop, namely socializing the procedures for filling out the BIA questionnaire and distributing it to all business/support units; (6) collect BIA questionnaires from all business/support units, as well as assist business/support units that require assistance in filling out questionnaires; (7) review the BIA questionnaire to review the BIA questionnaire data that has been submitted by the relevant business/support unit (identification of business functions, financial and non-financial impacts, maximum tolerable downtime (MTD), minimum resources, internal

& external dependencies, vital record , recovery point objective (RPO), and readiness of business/support units in the face of disturbances/disasters); (8) identify critical functions of each business/support unit using the BIA scoring tool; (9) prepare BIA & approval reports, namely to make resumes of all business functions that have been identified based on their criticality level, followed by requesting consent and approval from related parties.

4.2 IRP

User PMP builds will have stronger protection against privacy-focused attacks, but lose protection against runtime attacks. Also, it's possible that the App Store app detects the jailbreak, downloads it, and then executes the unreviewed payload, potentially replacing the PMP method that was reverted back to its original form. To limit this risk, various integrity checks were added to PMP, and a recommendation for users to only install trusted apps from the App Store. a dedicated PMP server to collect user PMP activity, run various back end analysis, and finally provide recommendations.

No	Asset	Identification	Risk	Threat Scenarios	Problem Solving
1	Material soft copy master song	Catalog storage of song material for sale that amounts to hundreds or even thousands of songs	Prevention Currently there is no prevention from storage which when storage is only done on PC and Google drive	If there is no prevention, it is feared that the songs will leak before being released by the singer.	Immediately provide prevention with an accurate security system, besides providing a backup for the container for storing

					song material so that it is not stolen.
2	Applications Platform Digital Music Distribution	This platform is provided by an aggregator partner where every music distribution will be carried out around the world using only this 1 application	Currently there is no prevention but last week there was a scam from a Russian proxy who uploaded a music video to YouTube via our platform	If prevention is still not done, the impact of fraud or scamming will continue to occur, so that consumers will lose trust.	The solution is to improve the system to make it safer than before to avoid scamming.
3	Laptop dan Computer	Because almost all the work of almost all employees are related to the digital world, both music production to sales, all use computers and laptops, but currently the device has not been provided	Possibly in the near future an anti-virus tool will be provided to all devices	If the antivirus device is still not installed, it is feared that the user's laptop and computer will experience a decrease in RAM and hard disk,	Install a bona fide and compatible anti-virus device on each PC and don't forget to activate internet security.

		with a capable anti-virus.		besides that, the worst thing is that the user will lose personal data on the PC.	
4	Platform application client report	In connection with the need for reports related to revenue / royalties to several partners, this platform is very important, including companies that can see profit and loss, invoices in out	Currently there is no prevention from the application and it is possible to backup via the cloud or otherwise	A platform client report is needed to find out how effective or successful a platform is, if it is not provided, it is feared that the developer will not be able to improve or improve the platform so that consumers are reduced.	Create a client report platform as quickly as possible so that consumers can report everything and we can improve or improve it.

Security concerns with understanding the issues surrounding diverse attacks and designing defense strategies (i.e., countermeasures) that maintain the confidentiality, integrity and availability of any digital and information technology. Confidentiality is a term used to prevent disclosure of information to unauthorized individuals or systems. 1) Integrity is a term used to prevent modification/deletion in an unauthorized manner. 2) Availability is the term used to ensure that the systems responsible for conveying, storing and processing information are accessible when needed and by those who need it.

CONCLUSION

Deployment of PMP applications and their components does not impose a visible advantage in terms of performance by measuring the interactive and latency of different applications with and without PMP installed. Additional delays do occur when an application accesses a protected feature and the user is shown a pop-up to make a protection decision, but this is only to request user input on first access.

When using PMP, users will have stronger protection against privacy-focused attacks, but lose protection against runtime attacks. In addition, it's possible that the App Store app detects the jailbreak, downloads, and then executes the unreviewed payload, potentially replacing the PMP method that was reverted back to its original form. However, in that scenario, an attacker could circumvent PMP completely by reading files outside the sandbox that Apple's runtime review normally detects. To limit this risk, we added various integrity checks to PMP, and we recommend that our users only install trusted apps from the App Store.

Development of a common logging framework, called Leo, which uses Doctrine ORM, MySQL, PHP and Apache. Leo enables storage and retrieval of data in an extensible format using simple insert and query APIs, with optimized transmission to minimize mobile data usage and secured using SSL. Leo uses 'layers' for application data types, for example, protection decisions, access detection, and recommendations, each stored in a different layer.

REFERENCES

Savage, N.S., Ali, S.R. & Chavez, N.E. 2010. Mmmmm: A Multi-modal Mobile Music Mixer. Proceedings of the 2010 Conference on New Interfaces for Musical Expression (NIME).[Online] Available: http://www.nime.org/proceedings/2010/nime2010_395.pdf.

Woldecke, B., Geiger, C., Reckter, H. & Schulz, F. 2010. ANTracks 2.0 – Generative Music on Multiple Multitouch Devices. Proceedings of the 2010 Conference on New Interfaces for Musical Expression (NIME). [Online] Available: http://www.nime.org/proceedings/2010/nime2010_348.pdf.

Zhou, Y., Percival, G., Wang, X., Wang, Y. & Zhao, S. 2010. MOGCLASS: A Collaborative System of Mobile Devices for Classroom Music Education. MM. [Online] Available: http://www.comp.nus.edu.sg/~yzhou86/mmshc05843-zhou.pdf