Protecting Identity Using Biometrics Protection Systems

Fathimath Sabena sabenaadam@hotmail.com
University College of Technology and Innovation (UCTI)
Kuala Lumpor, 5700, Malaysia

Ali Dehghantanha ali_dehqan@ucti.edu.my
University College of Technology and Innovation (UCTI)
Kuala Lumpor, 5700, Malaysia

Andy Seddon andy@ucti.edu.my
University College of Technology and Innovation (UCTI)
Kuala Lumpor, 5700, Malaysia

Abstract

Biometrics Identity Management (BIdM) is a newly rising and developing discipline which could be expressed as the study of verification and validation methods for the next generation. The two key terms enclosed in the title of this paper are– "Biometrics Vulnerabilities" and "Identity Management". Every one of us has an identity. By utilizing this identity along with distinctive characteristics we distinguish ourselves from one another. By cross referencing the data from both sources, a guideline that would adapt the best practices to maintain the sequence of BIdM and identity theft integrity was designed. Based on the findings a guideline is proposed to the experts and end-users to use. A walk through with the BIdM consultant was done to identify areas of improvement to fine tune the artifact.

For proper identity management this guideline can be used as the processes in data collection and data maintenance procedures are included. The procedures include extracting the data from data collection for proofs, data matching and handling the data in an appropriate way. The guideline will have its proper BIdM techniques by having the best practices of tackling its vulnerabilities.

Databases having biometric data are themselves a threat to privacy. While distinguishing gaps in BIdM and discovering new approaches to tackle the vulnerabilities, issues and protect such databases and increasing the awareness programs, this research can be further extended.

Keywords: Biometrics, Identity Management, Biometric Systems, Biometric Technologies, Technical Vulnerabilities, Social Vulnerabilities, Privacy vulnerabilities, Identity Fraud, Review of Biometrics Vulnerabilities.

1. INTRODUCTION

Biometric technology can be described as the computerized detection of a person's behavioral and bodily attributes. Physically individuals to records of identity, creating a one-to-one communication among records and people, it can associate limiting individuals to single record or

single person to proceedings. While identity administration, although biometric technology is a usual tool, many believe that it intrudes privacy. According to the Computer Crime survey 2006, published by Computer Security Institute and the FBI, *"Unauthorized access continues to be the second greatest source of financial loss*" [1].

Biometric information is a sensitive form of data. It may have a much larger effect on the individual in certain ways if it gets infringed or stolen. The data is unique and of high quality. It concerns with the person's physical characteristics hence it should be treated with the utmost importance to make sure it is firmly saved, encrypted and only reachable to authorized individuals and when no more required destroyed under the intentions in which it was gathered.

For improving privacy and guaranteeing a one-to-one communication amid people and records, biometric technologies have been suggested as a natural tool in identity management procedures. But regarding their values some commentators raised questions, is biometrics an effective tool for regulating individuals?

Monitoring of an identification technique of biometric contribution, the user's biometric transparently may not be agreeable for the user, or gathering biometric templates in a crucial database since a biometric of user's could be utilized for offensive reasons if the biometric is acquired by an unofficial person. Users biometric can give information which a user willingly may not want to provide. For example, reasons for law enforcement, a fingerprint interpretation can be utilized while medical information could be obtained from an eye scan.

Upon which a biometric technique can be used, there are eight points, as pointed out by [2]. Although the greatest publicity was received for fake biometric attack, all further usage needed some kind of entrance to the biometric techniques and methods possibly signifying additional serious threat.

Cost is constantly a vital issue when implementing a new technology. Regarding the cost of a biometric system people frequently concentrate specially on the cost of hardware, sensor and linked software, although the definite cost of the fundamental elements usually goes much further while executing any biometric system. Furthermore, there will be extra operating expenses linked with administration, integration, user education, installation, and system maintenance and data collection.

This paper will explore identity management. It will specifically address biometrics vulnerabilities, why we should care about biometrics vulnerabilities with identity management, what are the best options which are available to solve the vulnerabilities, what are the solutions and why some are more effective than others.

2. REVIEWING of RELATED WORKS

BIdM system must abide with Protection of Data and by means of the Convention on Human Rights in Europe. Data is copied by cloning the Hard Disk Drive. The interviewee's pointed out that the vulnerabilities and issues controlled should be protected according to their respective countries data security laws. The Data Protection Act controls the means of organizations dealing with data that recognizes users. In BIdM technologies situations, transparency and proportionality are both standards overriding in each situation which will pertain. Transparency or clearness denotes putting it to understand how and why data is utilized and with no preceding agreement not moving ahead. Proportionality necessitates the use of individual's biometric data, or an individual's private life is not interfered, with the advantages of the system should be reasonable. It commonly denotes matching organization's privileges or public at large with the rights of the individual. In legal terms personal data is more important than any other data BIdM "private" information its dealing with.

By closing off, admission to the system is vital in preventing the suspect from sabotaging the system. When the data gathering is conducted, the intruder's log on to the system should be completely blocked. Through data gathering phase, the most skillfully required items are logs as they enclose information about the intruder's actions. Moreover, to make certain no data is written onto the intruder's computer the BIdM administrator's team requires to directly pulling off the computer plug from the wall socket. Additionally, this will preserve the files such as temporary files and swap files. The data has to be kept for further planning (how it was performed, should it

be reserved as a data security and handling exercise and the hard disk drive required to be cloned).
The data duplicated by the inspector is same as per the intruder's original hard disk drive is ensured by the imperative factor called Hashing. The precise copy of the hard disk should be done ensuring all the information duplicated is same as the original when duplicating the intruder's hard disk. To ensure that the data is not changed it should be done at the intruder's location. The images must not be general copies. It should be genuine bit by bit or close images of the originals.
Inspectors may at times accidentally delete the proof critical for the investigation whilst recuperating proof from the system. By applying the write blocker technique this can be prevented from the intruder's workstation writing or deleting proof. Extreme consideration should be given when extracting data from the intruder's workstation as it is a very important aspect during data gathering.
The items collected should be labeled and documented in order to keep those as sequence of custody. These will come to assistance during the management in internal, civil and criminal inspection. During the reporting stage where the inspector requires rebuilding the BIdM based on the proof in these documentations will be of benefit.
All magnetic data is collected in antistatic wrapping, for example, paper bags, no scratching or folding of computer media is allowed, etc. To prevent loss, demolition of data, modification and physical harm all proof is labeled. Therefore, the guideline distinguishes that computer equipment are "fragile" electronic devices that are receptive to physical shock, static electricity and magnetic sources, temperature, humidity in wrapping and while transportation of proof. Additionally, during transportation, all proof should be kept at a distance from magnetic sources.
In common the interviewees revealed the information maintenance methods for BIdM from different policies and standards. It should be stored in a safe and secured place where intruders cannot reach and only authorized persons can access the room to prevent the proof being tempered. The people who access the storeroom should be logged.
The use of BIdM software to analyze the data to prevent accidental tampering of the data is recommended by the interviewees. To analyze the information the interviewees agree that a secure place or a laboratory should be utilized. Utilizing bootable diskette Hard disk drive is investigated to avoid the operating system. The lab that is secured and regimented to perform the analysis work is suggested. From all the computer systems such as applications, network and log files more proof are searched for. Selection of the right tool to acquire the data will secure the proof.
The interviewees agreed that BIdM activities are recorded proof to the legal and domestic inquiry teams and reporting is vital. The reports should be free from technical jargons and should be in a straightforward way to understand in any language it may present to the authorized concerned people. Also the report will enable to tackle similar problems in the future.
Based on the survey questions the main areas using the BIdM technologies in the three countries are government, health, financial, travel, consumer market and private areas. Among these areas government area embodies the leading BIdM technologies for end users. BIdM technologies are used in government organizations, offices, departments, federal agencies and military areas.

3. PROPOSED MODEL

In this research much more will be discussed on how and what should be done when an intruder tries to attack the system, what are the vulnerabilities detected, classified, handled and the procedures used for handling such cases. As the topic is very wide, data protection aspects will be highlighted in this research.
Nevertheless, to sustain these principles in practice can be challenging. For instance, lack of reliability in BIdM systems is one of the vulnerabilities either from their vulnerability to interference or from error. It is not always "accurate", is the second vulnerability of BIdM, for instance, as additional data accrue in huge databases not only of comparative consistency, but also the fingerprint checks are credible to reduce over time. "Function creep" is a vulnerability to BIdM systems. At the time the data was gathered data is utilized in a way not permitted nor foreseen.

The BIdM guideline will form part of the incident response plan that deals with any types of BIdM related incidents as shown in Figure 1.

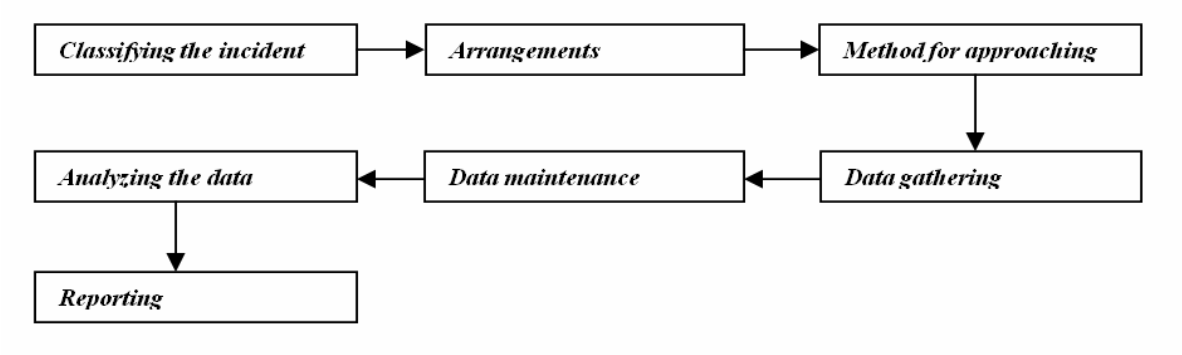

FIGURE 1: An Overview of the BIdM guideline

The three parties involved in this guideline abide by the computer law in their respective countries on computer crimes. These organizations have their own policies on BIdM and computer crime. BIdM will normally execute the monitoring, identification and preliminary evaluation of the vulnerabilities, issues and data maintenance as shown in Figure 2. When a concern is raised the issue will be taken to the top management and to perform the processes in the BIdM it will be treated by the help of the guideline.

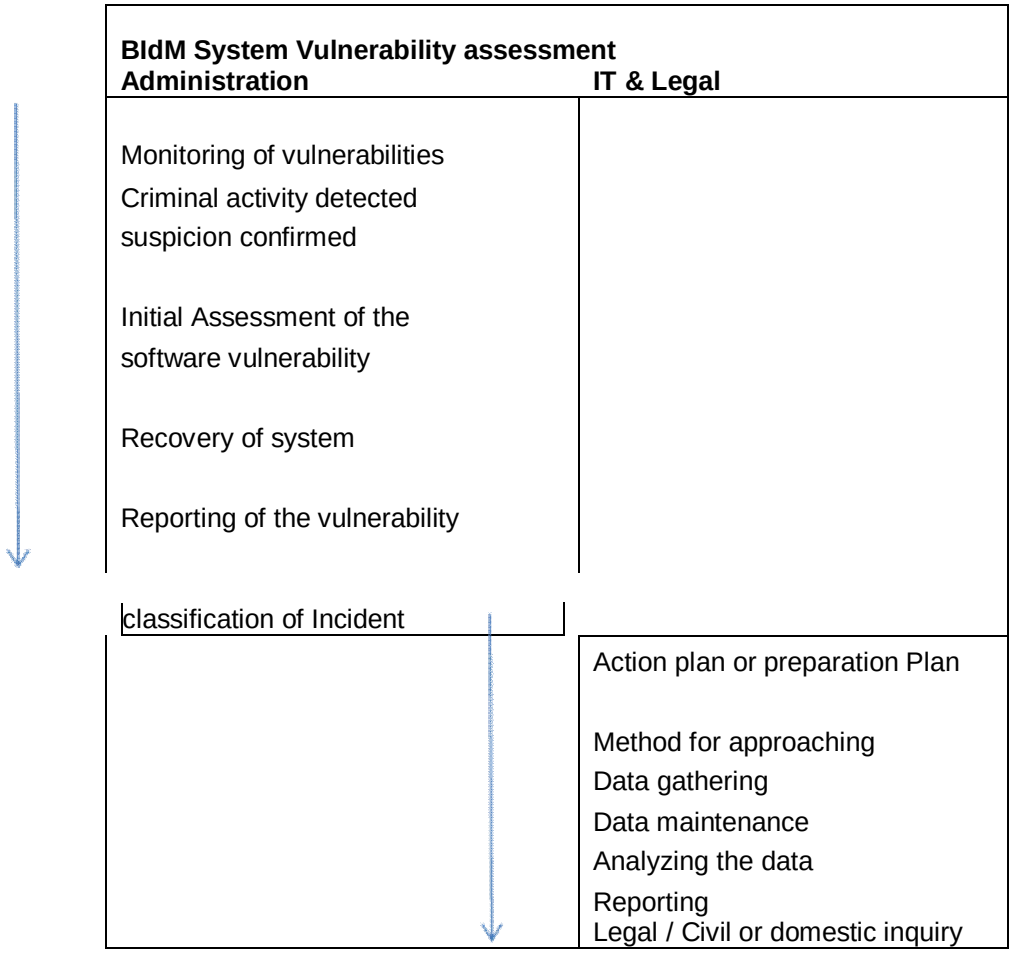

FIGURE 2: BIdM Process paths

The organization's structure will also be maintained by the BIdM team as that will provide an indication of the association of other personnel and sections that will be supporting through the BIdM vulnerabilities, issues controlling and administration with concerned computer crimes as shown in Figure 3.
The sections will be Information Technology (IT), Human Resource (HR) and Legal department. Linking with third party will be carried out by the legal department such as the regulator of legal matters or law enforcement agencies. It indicates that IT personnel can support gathering and investigating of data of proof as they possess expertise in the matters, supported on the chart for BIdM including experts in technical, security administration, matters with administration.

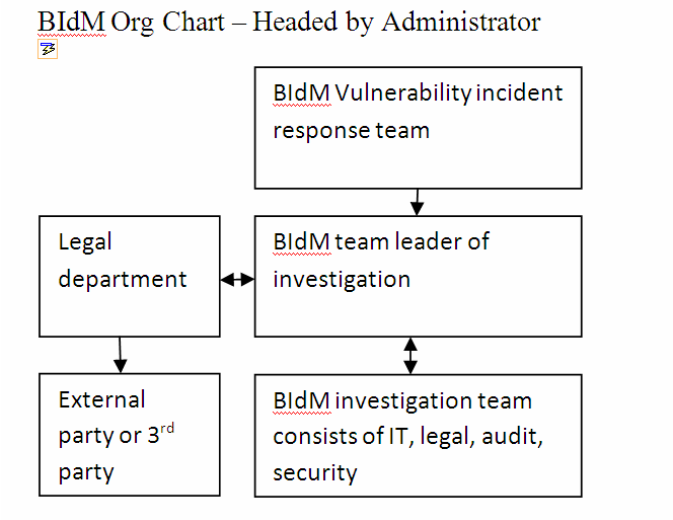

FIGURE 4: BIdM Org Chart

The above phases are considered from the interviews and from the literature review conducted. BIdM is a key global facilitator for managing digital identities while establishing trust and protecting personal information. BIdM is a hub of infrastructure protection capability and continuously evolving and growing cyber security. Operating networks comprises of controlling access to a network or service, complying with local legal and regulatory requirements, and performing online e-transactions.
There are many activities that relate to BIdM standardization as BIdM is becoming an important issue throughout the world as shown in Figure 5.

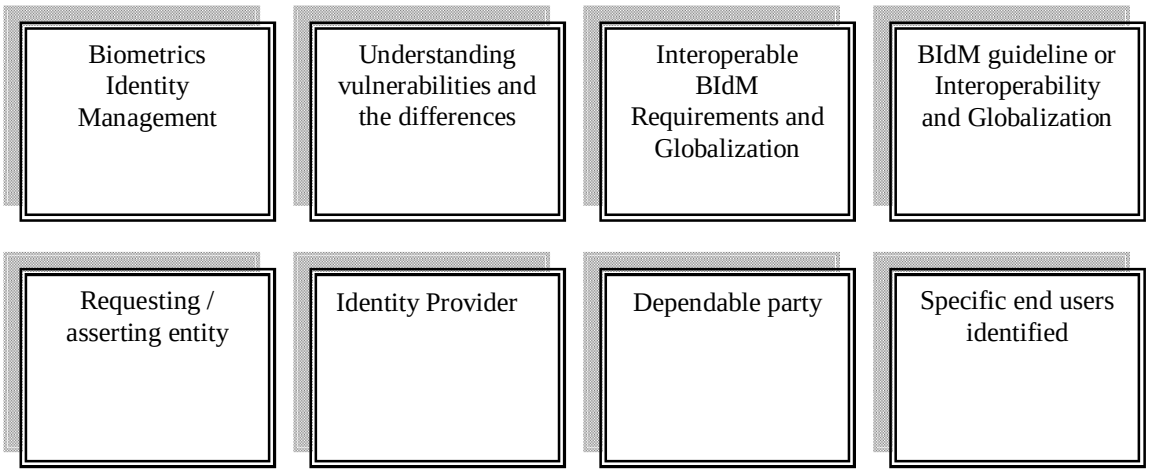

FIGURE 5: BIdM guideline for global interoperability

At present there are BIdM competence and resources across the globe often vague private and public sector limitations which employ and manifest enormous global arrangement of communications networks, Information and Communications Technology systems and services. Among various environments the demanding requirements have resulted in a rapid expansion of BIdM proprietary standardization work and solutions.
Nevertheless, if the discussions, standards, recommendations, guidance etc., are to be comprehensible, easily understood and unambiguous, it is imperative that the terms are described as accurately as possible and a mutual terminology is utilized.
At a higher level the vulnerabilities expressed in the BIdM cause and effect diagram, failure due to an intrinsic and adversary attack are the two methods of failure in a biometric technique.
In adversary attacks for personal benefits a capable intruder or perhaps a group arranged tries to get around BIdM technique. Adversary attacks can be further classified into three types established on factors such as system administration, biometric obviousness, vulnerable infrastructure that permit to negotiate security of the system with an adversary.
Intrinsic failures take place due to the limited discrimination of the specific biometric trait, corresponding technologies or trait extraction as well as intrinsic limitations in the sensing.
The analysis and recommendations are determined on the findings from the real life experiences, interviews, questionnaires and the survey conducted.
The administrator will commence working cautiously with the IT personnel to figure out the vulnerability when BIdM system vulnerability is brought up to him. Subsequently to perform the event classifying phase he will next inform the management and work with them. The administrator will discuss with human resource, legal department and internal audit accordingly when conducting a vulnerability evaluation involving a computer crime. The departments will provide extensive assistance to the system administrator when the vulnerability is classified major or minor. Urgent attention is required if it is a major vulnerability while a minor one needs to be concentrated on basis of time frame prearranged. The administrator can officially commence the mission of inspecting the vulnerability assessment phase called the “arrangements phase” once the event has been classified.
The administrator must make sure before the investigation commences that he has the appropriate tools and software that will be required for the following steps that the BIdM guideline indicates such as during the stages of data gathering and data analysis.
The administrator has to make certain that through the data gathering stage, the application of necessary medium to obtain the information is handy. For maintaining the sequence of legal measures, administrator also requires having notebooks, sequence of custody forms, tags, labels and logs.
As stated by the predefined policies all media utilized should be handled cautiously.
According to Privacy Impact Assessment for the DHS / UK visas Project, as the data is saved at U.S. Citizenship and Immigration Services (USCIS) for a brief period, the risks concerning privacy are less. Although the risks are less, USCIS assures the security control and access are ascertained to alleviate risks concerning privacy with authoritative and illegal users, explicitly abusive and improper distribution of information. Consecutively tracking and identifying illegal uses of system data audit trails will be kept. Additionally, the ASCs abide with security guidelines of the Department of Homeland Security (DHS), which give strengthened measures for securing computers, computer services, networks and against incidents and illegal information distribution [4].
The administrator requires developing a strategy when executing the data gathering phase to make sure the following are taken care of accordingly:

- To assist in the vulnerability evaluation the resources that will be required.
- In the intruder’s working area probable location of data source.
- With minimum interruption to the organizations’ systems particularly the critical servers and networks when the essential data is gathered.
- Measures to make certain the proof is not damaged or corrupted.
- Perception of technical information about the intruder’s linked and attached devices including network.

- To make sure proof gathering events are legally permissible and stick to respective country's law and organization policy.

1) Entire possible information sources must be contemplated by the administrator. From various data sources that may derive from various applications or devices the proceedings related to the vulnerability can be acquired.

- The logs may enclose precious information such as when the document was initially created and when it was last opened or changed, these logs are required to be given importance over non volatile data. Before they vanish the administrator must seize the logs.
- The intruder's system that was potentially utilized to execute the computer vulnerability for instance network details, the place of the computer system, information on operating systems and related application system.
- Volatile information could be possible sources of proof. Mostly, if a computer is shut down it passes the information to system time that is missing.

2) Distinguishing important steps to be taken to prevent maintaining information integrity and tampering for instance hashing techniques, image copy of hard disk and write blocker.

3) While handling the data gathering stage it is necessary to avoid bringing down crucial equipment such as the systems, servers and networks to minimize disruption to the organization.

4) The administrator has to make certain that the process he conducts does not interrupt the organization's IT and legal policies and for this purpose resource assignment is necessary for providing assistance and guidance on the inspection procedure. Consequently, it is vital to seek advice from HR personnel, legal department and internal audit. Additionally, support is required from the victim of the computer crime such as the IT department, management, line manager, system owner and application owner and business process owner.

5) In data gathering and analysis phase the personnel should be skilled on the significance of protecting the data against any unintentional tampering and conserving its integrity. It is also vital that all personnel at the site be sufficiently briefed on their functions and responsibilities.

6) The investigation should be conducted cautiously so that the intruder is uninformed that he is being scrutinized and the persons engaged in the inspection must know this. The intruder may try concealing his tracks and eradicate the proof if he is conscious about the inquiry.

7) Any advancement and revising of the vulnerability will be scrutinized by the administrator. Overall picture of the vulnerability crime case can be reviewed with a "vulnerability assessment board" that can provide details. To perform the event construction phase during the data analysis phase would be effortless for the administrator.

3. MODEL ANALYSIS

Laboratory is suitable for the analysis phase. While ensuring data integrity is conserved the data analysis can now be performed on the collected data.

a) Using the toolkit that endow with easy analysis of data at the lowest level the inspector analyses the data accumulated, searching for proof in the data that was gathered by investigating across a wide span of areas.

b) To make certain that the data investigated is not modified; write blockers can be utilized throughout the process to avoid writing to the said hard disk drive. Access to the image copy should be only as read-only. Solely on the replicated copy of the hard disk drive the analysis phase must be performed.

c) The intruder may have intentionally deleted or accidentally damaged some files. To reconstruct these lost files a toolkit can be utilized.

d) By comparing proof to activities and sources the inspector will then try to reconstruct the case. In reconstructing the case the case board will be helpful and if required, respect personal history or information of the intruder and other proofs (notes, photographs etc).

e) Only authorized people must be permitted into the laboratory. It should have an entrance control list having who had access to the collected data in the laboratory with dates and times.

Reporting is vital as it gives information of proceedings taken by the inspector to reconstruct the proof and inspecting. During the guideline process it should be emphasized that the sequence of protection and integrity of proof was sustained.

This research is utilized to explain to the people who use BIdM in any angle that the analysis was done in a fair and dependable manner and reporting is not utilized only for the internal, legal or criminal investigation. To demonstrate to the workers in the organization that the investigation was conducted in a reasonable and consistent manner according to the country's respective law, organization's policy and there should be transparency presented in the investigation.
The designed guideline was presented to the Assistant Controller on paper and on slides to enhance the things which were reviewed in the guideline. The Assistant Controller was selected as he is available all the time rather than the administrator and the consultant. The user was not opted as the Assistant Controller has vast experience in the field of BIdM systems management. The guideline has mentioned numerous vulnerabilities in the field of BIdM. However it concentrated more on one single area instead of all the areas as for this study it would be a vast topic if all the areas were covered. The vulnerabilities from user's side are one important fact that needs to be tackled. Business rules, standards, policies, frameworks and guidelines are very important for proper access control requirements.
For the guideline there are some areas that need to be improved.
It requires coordination among the concerned people such as the victim, IT department, the line manager, management, and any possessor of the system or the application that were involved by computer crime sequentially for the guideline to be effective.
Assistance will be provided to the inspector by these employees on an understanding of the effect of the computer crime to their application system. While preserving data integrity they can also provide information on ways to obtain critical proof from the applications.
During the progression the service of a case board will be beneficial as this can represent the entire sequence of events in a diagrammatical perspective:

- The place of the target system and intruder
- Organization chart / Network map
- How the computer crime was performed
- To identify the profile the intruder's history
- Evolution of the computer crime
- Congregated proof and additional proof that requires to be gathered or situated

To make certain that the authentic incident is captured before the computer investigation team does their work at the intruder's location during the data gathering phase. Hence prior to the proof collection or shifting from the intruder's place, the recording of incident such as obtaining photographs should be done.
Thorough method for approaching profiling of the intruder is vital, since it is important to know the individuality of the intruder particularly through data gathering and data analysis stage.
Personal history of the intruder is imperative for the inspector. The inspector could possibly build a profile of the intruder and his patterns in perpetrating the computer crime if he knows the intruder's criminal history. For instance, when dealing with a technically competent intruder the inspector has to be very cautious as he may have committed the computer crime utilizing convoluted technical skills.

- DNA Matching - Proof definite identification of an individual can be formed with this supreme biometric technology.
- Body Odor - For identification body odor can be digitally verified. Mastiff Electronic System Ltd is laboring on a similar system which is a British company.
- Vein pattern credentials - In that it utilizes infrared light creating the copy of pattern of vein in individual's wrist, hand, or face similar to retinal credentials.
- Keystroke Dynamics - Keystroke dynamics, is an innovative biometric technology and also referred to as typing rhythms.
- Ear shape credentials - The ear shape (geometry) is measured for this.
- Body salinity (salt) credentials - Progress in this part has been conducted by Massachusetts Institute of Technology (MIT) and IBM.

The inspector and the BIdM team at this point will be at the intruder's work area or in the physical site. The following must be conducted once the inspector reaches the site:

a) Avoid closing down any programs which are running while unplugging the power supply from the rear of the computer. To protect losing the basis of the proof a normal or graceful shut down should not be performed as temporary files, swap files or any malicious program will be erased.
b) Send unwanted people away from the computer by the security personnel and secure the place. This will prevent the proof from been damaged by anyone especially the intruder who would want to erase all proof.
c) The inspector should inspect to make certain that no self damaging program has been executed if the computer was running upon arrival. If such a program is operational the inspector should instantly remove the power cord from the wall socket.
d) To avoid other individuals who are accomplices from entering the intruder's computer via the network or internet to manipulate the data, the inspector should unplug the network cable / modem.
e) At the scene, to be documented the following should be accomplished:

- With accurate time and the proceedings carried at the site,
- Scene should be sketched by means of a network map,
- Place where the computer is situated, details of individuals nearby,
- Specifications of the computer such as the model number, serial number, operating system, IP address, system dates and other applications should be noted,
- Peripherals attached to the system, monitor details, etc.,
- If required, video tape or photographs should be taken.

f) To make certain it does not modify information on the primary medium where the backup or copy is, the inspector must utilize write-blocker specifically software support or hardware.
g) Preliminary interview should be performed by requesting constructive information relevant to the user identification, password information and about the computer system affected.
h) The items required to be printed out immediately are the things in volatile medium in the current memory such as logs, temporary files and printer buffer.
i) To ensure that the data is not tampered and permissible for legal explanation the inspector needs to authenticate the integrity of the data. Example of such techniques is hashing (This technique is used for authenticating biometric parameters via biometric hashing).
j) Make sure that completed exhibit labels are attached to the system, connection modes, peripherals and all objects have been signed.
k) The computer connectivity maybe restructured at a later date when the cables and the parts are tagged.
l) Prior to leaving the scenario let the intruder sign the proof, media and documentation gathered from the incident. The computed hashing of the hard disk drive must also be signed by the intruder.
The moving of detained media, computers and peripherals must be dealt with cautiously to prevent heat, damage or jostling for example, the place where the intruder maybe situated in a distinct physical location for instance in a branch office. Media devices must be kept in anti-static bags and be secluded from magnetic fields. To preserve the sequence of protection the carrying details should also be documented. Before moving the proof the inspector should note the names of title of all handlers of proof, the time of leaving from the computer crime scene, the advent time to the laboratory or store location.
Identity theft is one of the fastest growing crimes in the present day. Hence if industries require fighting this rising prevailing, data confidentiality and integrity is vital. This guideline will give ways on how to handle the crime scenes of identity theft, to gather information on such events, revealing trouble by existing verification systems, to provide robust verification, demonstrating how a resolution of biometric can be utilized, and considering additional advantages of utilizing multifactor authentication performances.

- Cloning Identity - To establish another life in this offense the imposter utilizes the victim's information. They live and work as a different person. For instance, criminals running away from warrants, unlawful aliens, turning into a "new life" to abandon a poor work and financial history or people disappearing from cruel situations.

- Criminal Identity theft - When blocked by law enforcement, the imposter in this crime gives the victim's information as an alternative to the imposter's own information. Ultimately it is in the identification of victim's when the warrant for arrest is released.
- Financial Identity theft – In this case normally the imposter focuses on the victim's identification and Social Security number (SSN). The imposter may request for credit cards, personal loan, buying merchandise, leasing cars or apartments and telephone service.
- Commercial or Business Identity theft - businesses are victims of identity theft as well. In the name of the business usually the imposter acquires checking accounts or credit cards. The business only finds out when the dejected suppliers send collection notification or when their business rating results are affected.
- Web spoofing - In this case the imposter monitor and change all web pages forwarded to the victim's machine and scrutinize all information the victim key in into the forms.

Instead of tokens or passwords, BIdM devices are able to offer improved security however they can give extra issues in engineering if proper standards, policies, frameworks and guidelines are not followed. Organizations planning to exploit BIdM strategies must seek recommendation from various aspects.

There are five major weaknesses the systems are prone to such as, user's workstation, communication paths facing interference, public network connections such as internet, dial-in-lines and interfaces with other systems in the network.

BIdM system's vulnerabilities can be reduced with well designed security architecture with principles of defense incorporated. Communication paths require encryption and other techniques, unattended workstations need physical security, conjunction with firewall intrusion detection system, connections should be permitted to public networks with approved firewalls, to any operating system accessing the network strong controls must be applied, firewall and standard circuits, local area networks (wireless), border controls and proper application of access control. The sensitive systems should be isolated while monitoring systems are accessed and used.

3. CONCLUSION & FUTURE WORK

Biometrics Identity Management (BIdM) is an intricate combination of the technological, cultural, legal and social aspects. Although standards, policies, frameworks, guidelines, methods and procedures for authenticating, securing and maintaining principle's confidential information is highly recommended. It is not simply about it all, even if this does have a vital component in its comprehension. Security with access control plays a major role. From unauthorized access, the repository which stores BIdM objects must be sheltered. To secure critical objects, cryptography and one-way hash functions may be vital. A prudent balance between Privacy and Security needs to be accomplished.

Due to revolutionary dynamics of organization, BIdM crime is on the rise, unsuccessful security system, upsurge in employee misconduct and lesser hacking expertise needed. BIdM worldwide is continually faced with threats and incidents of computer crime. BIdM standards, policies and guidelines are important processes that provide methods for organizations to take proper action against these employees, which will prevent future occurrences of computer crime. BIdM may offer organizations a stronger method of authentication as it is uniquely bound to individuals, with reliable user authentication and must ensure that an attacker cannot masquerade as a legitimate user. The BIdM was created based on literature review, primary and secondary research. Using appropriate technologies the planned BIdM contains seven phase tactic to extract proof centered on the intruder's workstation. The data gathering approach was very helpful as people from three different countries consisting of BIdM experts and the potential users of the computer BIdM participated.

In conclusion the BIdM which comprises of the stages and procedures were formed. A walk through with the BIdM manager who has vast knowledge and extensive experience in dealing with BIdM vulnerabilities especially in the area of network environments, revealed the areas for improvement. For instance, profiling the intruder the participation of the victim in the BIdM process and linking a case board. These were later incorporated into the guideline to make it more effective.

The data gathered must be secured and well protected ensuring that the contents cannot be overwritten in any way and it should be kept in a place where it would be free from any possible tampering, for instance, a protected location to keep the data.

Some organizations may not have standard procedures for assessment and backup for system and applications. Moreover there are also challenges in the proof gathered. Since it may not be permissible, organizations that possess these procedures may not be able to manipulate the data gathered as proof.

As stipulated by the regulator the usage of BIdM is more extensive where it is utilized for monitoring, evaluation of product, assessment of system, system auditing, data acquisition and data recovery.

IT Security must align with business needs and accept the importance of team work as engagement from other departments is crucial in order to make security work for the organization. Collaboration is best opted for any type of business.

In raising levels of quality most people are still usually unaware of the role played by the policies and standards, safety, efficiency, reliability and interchangeability as well as in providing such benefits at cost-effective manner. In general, these policies and standards can be made available from experts of a technical committee or working groups who meet to discuss and debate until they reach consensus on a draft agreement, or some new policies and standards or revision of existing policies and standards to bring to effect to follow up in the organization.

Based on the experts' views and present conditions, two critical areas of standardization with utilizing appropriate policies and the use of hybrid technologies are heavily dependent on the future of BIdM systems. Additional efforts and research on BIdM needs to be scrutinized and exploited in the manipulation of the user's private information such as what is exposed to whom and its influence guiding their awareness of BIdM in the world of e-commerce and the outline of the user's behaviors. The importance is being understood by users, designers and implementers of BIdM systems, managers, legislators, which will not be a minor task. It is also vital for national biometric associations, international biometric associations and regional biometric associations to collaborate and enhance their cooperation to establish international quality standards in biometric industry.

4. REFERENCES

1. Gordon, A., Loeb, M., Lucyshyn, W., Richardson, R., 2006, Computer Crime and Security Survey, [Online], Computer Security Institute & FBI, [Online] Available from: http://pdf.textfiles.com/security/fbi2006.pdf [Accessed on 19th July 2009]
2. Roberts, C., 2006, Biometric Technologies – Fingerprints, [Online] Available from: http://www.ccip.govt.nz/newsroom/information-notes/2006/biometrics-technologies-fingerprints.pdf [Accessed on 22nd July 2009]
3. Managing Australia's Borders, "The Department of Immigration and Citizenship (DIAC) [Online], Available from: http://www.immi.gov.au/managing-australias-borders/border-security/systems/identity.htm [Accessed on 12th September 2009]
4. Patentdocs, 2009, Systems and Methods for Accessing a Tamperproof Storage Device in a Wireless Communication Device Using Biometric Data [Online], Available from: http://www.faqs.org/patents/imgfull/20090193519_07 [Accessed on 10st October 2009]
5. Home Office – Identity and passport service, "Identity cards for airside workers", [Online], Available from: http://www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xsl/964.htm [Accessed on 30th September 2009]