International Journal of Security and Its Applications
Vol.8, No.5 (2014), pp.403-420
http://dx.doi.org/10.14257/ijsia.2014.8.5.35

Developing Forensic Readiness Secure Network Architecture for Wireless Body Area Network (WBAN)

Abdul Fuad Abdul Rahman[1], Rabiah Ahmad[2] and Madihah Zulfa Mohamad[3]

*[1]National Vulnerability Assessment Center (MyVAC),
Security Assurance Department, Cybersecurity Malaysia, Malaysia
[2]Center of Research Innovation Management (CRIM),
Universiti Teknikal Malaysia Melaka (UTeM), Malaysia
[3]MyCyberSecurity Clinic, Department of Industry and Business Development,
Cybersecurity Malaysia, Malaysia
abdfuad@cybersecurity.my, rabiah@utem.edu.my, madihah@cybersecurity.my*

Abstract

Wireless Body Area Network (WBAN) is a wireless network that can be attached or implanted into the human body. This allows medical devices that are used for monitoring any bodily function to be equipped with a wireless network system. This system is vulnerable, similar to any other currently available wireless systems e.g. Wireless Local Area Network (WLAN) and Bluetooth. However, currently there were not many discussions on the WBAN security impact and security threats and if there is any, the issues were discussed through theoretical and simulation data. In this paper, a practical approach to assessing WBAN security impact is designed in order to identify, evaluate, and develop a Secure Network Architecture complete with the Forensic Readiness capability to secure WBAN implementation.

Keywords: *Secure Network Architecture, Forensic Readiness, Security Impact, Security Threats, Wireless Body Area Network (WBAN)*

1. Introduction

The development of Wireless Body Area Network (WBAN) technology started around 1995 based on the idea of Wireless Personal Area Network (WPAN) technology to implement communications onto a human body [1]. WBAN is a wireless network that can be attached or implanted to the human body [2]. They are developed based on Bodynet which enables sensors that is used to monitor any bodily function and body motion through wireless network system [3]. The main goal for WBAN is to replace wires and cables connects to body sensors [3]. The idea is to increase patient's comfort and provide the ability for healthcare professionals to monitor patients remotely. Henceforth reducing logistic constraint [3].

The development of WBAN must comply with the healthcare standards and requirements. One of the requirements is to be accessible at any time and can function continuously [4]. WBAN is targeted to be used in medical devices. Therefore, it is important for the system to produce accurate and reliable data [5]. The WBAN must be a low operating power, minimal weight, and miniature form-factor [6]. To date, since healthcare environment requires it to be a low powered sensor node, it will be extremely difficult to implement any advanced security mechanism due to the limitation of power consumption [5]. Henceforth, increase the WBAN security and privacy concerns [5].

ISSN: 1738-9976 IJSIA

The objective of this research is to combat the criminal risk and security threats to the WBAN system. Thus increase security and privacy to the WBAN system. In an attempt to increase the WBAN security and privacy, this research will develop a secure network architecture for WBAN. The secure network architecture will be equipped with Forensic Readiness capability, Preventive Mechanism and Detective Mechanism. The Forensic Readiness capability, Preventive and Detective Mechanism will be developed based on the data and variables obtained from a practical testing.

In this research, the Practical Impact Assessment (PIA) is a practical testing to assess the impact of WBAN security. The PIA is developed based on the requirements of the Convention on Cybercrime from the Council of Europe [7]. Each testing will be conducted practically by imposing other wireless security threats to WBAN system [8].

This paper will be divided into four phases as shown in Figure 1. In the first phase, the Practical Impact Assessment (PIA) will be discussed in details. During the PIA process, a couple of variables will be measured in order to assist the development of Preventive and Detective Mechanism for Forensic Readiness Secure Network Architecture. In the second phase, the theory of Additive Value Function (AVF) will be discussed in details. The AVF will convert all qualitative data obtained from the PIA, into quantitative data. In the third phase, the quantitative data will be used to quantify the Security Impact Level (SIL). The SIL will be used to assist the development of Impact Level for the Forensic Readiness Secure Network Architecture. In the final phase all the inputs gathered will be used to design the Forensic Readiness Secure Network Architecture.

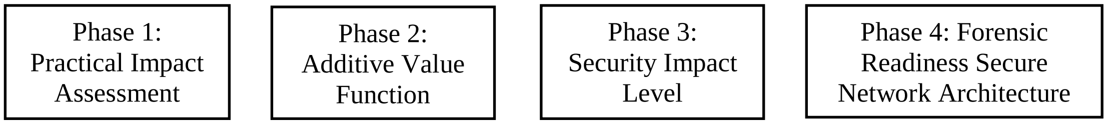
Phase 1: Practical Impact Assessment
Phase 2: Additive Value Function
Phase 3: Security Impact Level
Phase 4: Forensic Readiness Secure Network Architecture

Figure 1. Four Phases

2. First phase: Practical Impact Assessment (PIA)

The Practical Impact Assessment (PIA) is a practical testing to assess the impact of WBAN security threats. Each testing will be conducted practically by imposing other wireless technology security threats to WBAN system. A set of wireless security threats was selected based on Explanatory Report of Convention on Cybercrime. These four wireless security threats, PIA (x_m) as shown in Table 1 [7]. In this research, the selected PIA (x_m) is a simulation of an act of causing security breach and is considered as cybercrime based on the Convention on Cybercrime [7]. To date, the Convention on Cybercrime were acceded by 55 countries, including South Korea, Japan and United State of America [7]. Therefore, this research will refer to the Convention on Cybercrime in order to produce a reliable result and will be discussed later in the next section.

Table 1. Set of Four PIA (xm)

m	PIA (x_m)	Attack
1	PIA (x_1)	Eavesdropping
2	PIA (x_2)	Denial of Service (DoS)
3	PIA (x_3)	Authentication Bypass
4	PIA (x_4)	Role Bypass

2.1 Changeable Variable

Based on the Convention on Cybercrime, traffic data are referred as any data relating to a communication by a computer system that formed a part in the chain of communication, indicating the origin of the data, the destination of the data, the data route, the time stamp, the size of the data and packet of data, type of the data or service, and duration taken for the communication to be successful [7]. In any cybercrime cases, it is crucial for the digital forensic team to analyse and determine the location of the crime scene, crime scene perimeter and also the time of the crime committed [9]. Therefore, in order to fulfil Forensic readiness requirements, two variables will be measured during the PIA (x_m). The first variable to be measured is the time taken to execute a successful PIA (x_m), and the second variable to be measured is the distance between the attacker and WBAN system as shown in Table 2.

Table 2. Changeable Variable

No	Changeable Variable	Description
1	Distance	The distance between the attacker and WBAN target system as shown in Figure 2.
2	Time to Execute	The time taken to execute a successful PIA (x_m)

The time measured will provide inputs to estimate the amount of time taken for each PIA (x_m) conducted. The PIA (x_m) conducted from various distances to identify and investigate the minimum and maximum distance required, to execute a successful PIA (x_m) [9]. These two variables will be used as the main inputs to develop the Preventive and Detective Mechanism for the Forensic Readiness Secure Network Architecture and will be discussed further in the next section.

2.2 Impact Variable

The Convention on Cybercrime aimed at deterring action against the Confidentiality, Integrity and Availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data [7]. It is widely known that Confidentiality, Integrity, and Availability of a system are also referred as the Three Main Security Pillars (C.I.A) [8].

Table 3. Impact Variable

Impact Variable	Security Three Pillars	Description
C	Confidentiality	Protect the information to be disclosed only to authorized persons or organization
I	Integrity	Protect the information accuracy, authenticity, reliability, and completeness
A	Availability	Protect the information to be accessible to authorized users when required.

Furthermore, according to the Convention on Cybercrime, any impairment to the confidentiality, the integrity and the availability of a system are considered as security breached [7]. Therefore, the Confidentiality, the Integrity, and the Availability will be selected as variables to be measured. The Impact Variable as shown in Table 3.

For this research, the Confidentiality Impact captures the impact of confidentiality issues. If the WBAN system had been compromised on the communication confidentiality aspect. The Integrity Impact, captures the impact of integrity issues if WBAN system had been compromised on the information integrity aspect. Integrity in WBAN system should be protected in the highest effort because WBAN system intended to be largely used in healthcare and medical devices requires a high integrity assurance [3]. The Availability Impact, captures the impact on availability issues if WBAN system had been compromised on the information and the system availability aspect. It is very important for medical devices to be readily accessible at any time and can function continuously [3]. Therefore, it is important to ensure that the Availability for WBAN on medical devices shall not be compromised [3].

2.3 Basic Architecture Setup

All four wireless security attacks, PIA (x_m) will be setup based on the basic architecture setup as shown in Figure 2 [10]. The Basic Architecture will be arranged in a manner of clear line of sight between the WBAN System Target and an attacker [10]. The Basic architecture is defined as no other security mechanism such as Firewall, Intrusion Detection System, and Intrusion Prevention System deployed between Attacker and WBAN System Target [10].

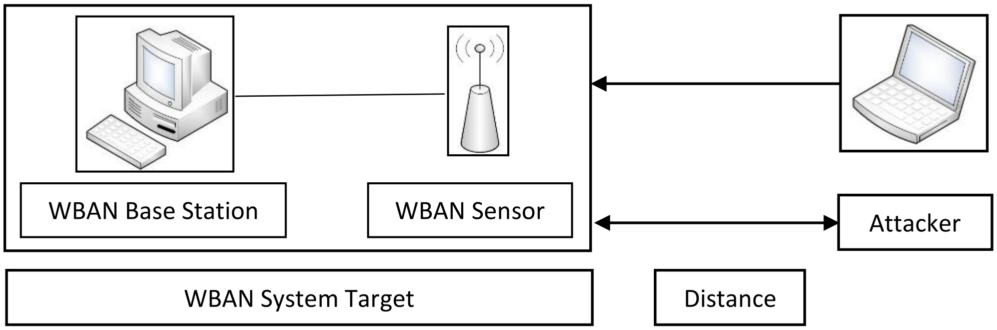

Figure 2. Basic Architecture Setup

2.4 Eavesdropping PIA (x_1)

Eavesdropping is an attempt of secretly listening to the other computer communication and in this research, the communication between WBAN Sensor and WBAN Base Station [11]. The Eavesdropping in this research is similar to the other network tapping process done in Wireless Local Area Network (WLAN) and Local Area Network (LAN) as shown in Figure 3.

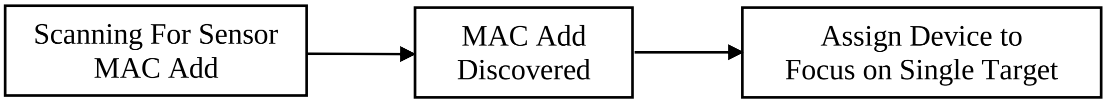
Scanning For Sensor MAC Add
MAC Add Discovered
Assign Device to Focus on Single Target

Figure 3. Eavesdropping Process

2.5 Denial of Service (DoS) PIA (x_2)

Denial of Service (DoS) is an attempt to make assets of the WBAN unavailable to its intended user [12]. In this research, DoS is an activity to make the WBAN sensors unavailable and unable to transmit its WBAN signal towards the WBAN Base Station. A sensor can be DoS using the Hello World packets as Deauthentication packets in an attempts to flood the network as shown in Figure 4 [13].

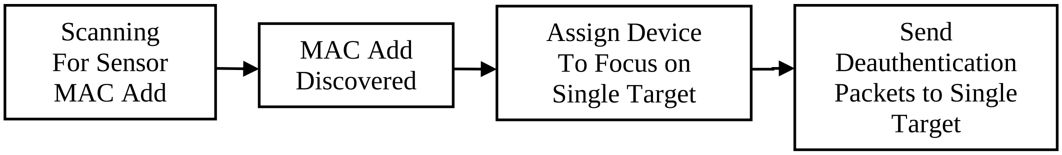
Scanning For Sensor MAC Add
MAC Add Discovered
Assign Device To Focus on Single Target
Send Deauthentication Packets to Single Target

Figure 4. Denial of Service Process

2.6 Authentication Bypass PIA (x_3)

Authentication Bypass is an attempt of exploiting the authentication system vulnerability in order to skip the authentication challenge process [14]. Based on the research conducted in 2010, a Stolen Verifier attack against a system will exposed authorized user credentials as shown in Figure 5 [15].

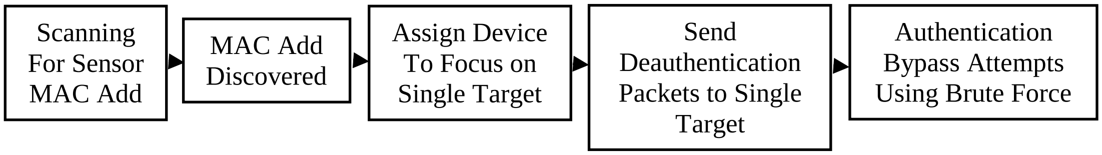
Scanning For Sensor MAC Add
MAC Add Discovered
Assign Device To Focus on Single Target
Send Deauthentication Packets to Single Target
Authentication Bypass Attempts Using Brute Force

Figure 5. Authentication Bypass Process

2.7 Role Bypass PIA (x_4)

In this research a Role is similar to an Access Control system providing access restriction. This Role can be exploited, in order to bypass the access restriction [16]. In this research, the Role Bypass is executed by using the Spoofing Credentials Attack [17]. An authorized user credential was obtained using the DoS attack and Eavesdropping attack [17]. The unauthorized user will then use the obtained authorized credentials to access the WBAN sensor as an authorized user as shown in Figure 6.

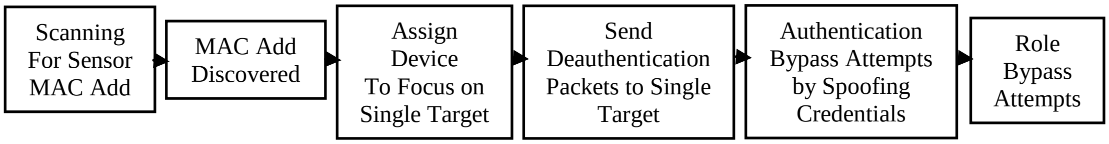
Scanning For Sensor MAC Add
MAC Add Discovered
Assign Device To Focus on Single Target
Send Deauthentication Packets to Single Target
Authentication Bypass Attempts by Spoofing Credentials
Role Bypass Attempts

Figure 6. Role Bypass Process

The PIA process simplified in flow chart as shown in Figure 7. The only set of variables from a successful PIA will be recorded. If the PIA conducted was not successful, the whole process will be repeated [8]. The success of the PIA was determined by the impact of the affected WBAN system, and the impact was verified using logs recorded by the WBAN system during the execution period of PIA [8]. The logs generated by the WBAN system will be used to verify which impact was affected [8]. At this stage, the inputs recorded is the Changeable Variables as shown in Table 2 and the Impact Variables as shown in Table 3.

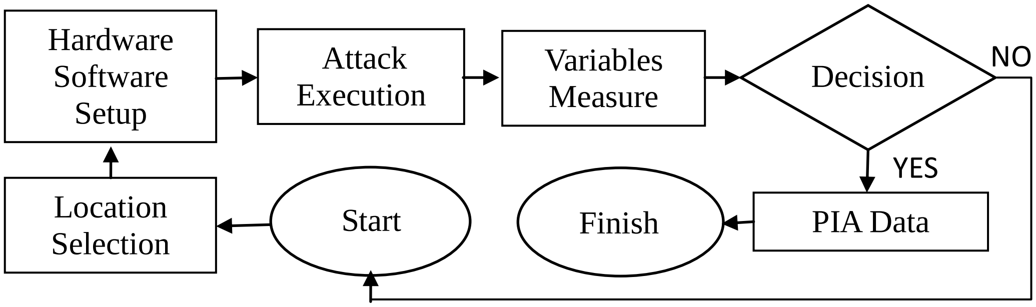

Figure 7. Practical Impact Assessment (PIA) Flow Chart

Table 4. Flow Chart description

Process	Description
Location Selection	During this process, the location of the WBAN Target System will be fixed and the location of the Attacker will be varied. The distance between the Attacker and the WBAN Target System will be measured and recorded as shown in Figure 2.
Hardware and software setup	During this process, all the hardware and software used in the PIA will be organized accordingly and switch on.
Attack Execution	The process of PIA(x_1), PIA(x_2), PIA(x_3) and PIA(x_4) as shown in Figure 3 to Figure 6 will be executed and during this whole process, the variable for Time will be recorded.
Variables measure	During this process, the Time Variable will be measured simultaneously with the PIA. All variables measured will only be recorded if the attack was successfully executed. If the PIA conducted was not successful, the whole process will be repeated.
PIA data	PIA data will be recorded from a successful PIA only.

3. Second phase: Additive Value Function (AVF)

After obtaining the qualitative data from the PIA, a suitable value model that able to convert all the experiments qualitative data into quantitative data is needed. There are two types of value models, Value functions and Utility functions [18]. The theoretical of Value functions were found in a study conducted by Krantz (1971) and Dyer and Sarin (1979) [18]. Although the original work for this type of model was presented in Luce and Tukey (1964) and Krantz (1964), which in the studies they considered only ordinal objectives when constructing this value functions based on strength of preference objectives prior developing this value model [18].

In 2009, a Value-Based Software Testing Process developed as a grading model to determine software testing priority ranking [19]. In this study, the Value Functions has been developed to include multi-objective and defined as the Additive Value Function (AVF). The AVF was used to determine which software testing process is deemed as the most effective based on quality risk, testing costs and business importance set as variables [19]. In this research, the Additive Value Function (AVF) equation will be used to quantify the security impact level on WBAN, quantitatively as shown in Equation 1:

$$V(X) = w_m \times v_m(x_m)$$

Where the $v_m(x_m)$ is the total score of PIA (x_m). Where w_m, are a set of non-negative weighting factor (constants). Since AVF verification consisted of the logic and mathematic checks, at every level within the model, the sum of weighting factor must always equal to one [20] as shown in Equation 2:

$$w_1 + w_2 + w_3 + w_4 = 1$$

According to Qi Li, for simplicity the weighting factor w_m can be assumed as same for all variables [19]. However, according to Ezell, the value for weighting factor w_m can be derived from research data and results [20]. In this research, the weighting factor w_m will be derived from the Changeable Variables and will be discuss in the next section. The AVF was chosen because of it has the ability to expand it to include not just one input but also multiple inputs [19]. From the previous section we know that the PIA have generated multiple inputs. Therefore the Additive Value Function will be modified into additive multi-objective value function to include multiple variables, therefore:

$$V(X) = [w_1 \times v_1(x_1)] + [w_2 \times v_2\ (x_2)] + [w_3 \times v_3\ (x_3)] + [w_4 \times v_4\ (x_4)]$$

Therefore, we get Equation 3:

$$V(X) = \sum w_m \times v_m\ (x_m)$$

Therefore the Additive Value Function (AVF) will be used to convert all the qualitative data to quantitative in order to calculate the Security Impact Level of each Practical Impact Assessment, PIA (x_m).

4. Third phase: Security Impact Level (SIL)

In the third phase, we present the results of all the PIA conducted previously. The data obtained from PIA will be merged with the AVF and the results was presented in Table 5.

Table 5. PIA Result

m	PIA (x_m)	Changeable Variable		Impact Variable			Value of PIA (x_m) $v_m(x_m)$
		Maximum Recorded Distance (m)	Time to Execute (s)	C	I	A	
1	PIA (x_1)	5.0	85.50	1	0	0	1
2	PIA (x_2)	5.0	123.23	0	0	1	1
3	PIA (x_3)	5.0	366.35	1	1	1	3
4	PIA (x_4)	5.0	529.66	1	1	1	3

4.1. Result and discussion

Table 5 shows that the time taken to execute a successful PIA(x_1), PIA(x_2), PIA(x_3) and PIA(x_4) was 85.5 seconds, 123.23 seconds, 366.35 seconds and 529.66 seconds respectively. The time differences were influenced by various factors, but the main factor is the complexity of different security threats, PIA (x_m) [21].

The Time Variable also depends highly on human skills [22]. It is known that without proper human motor skill practiced, it is well known that initial level of skilled performance will drop considerably [22]. Although the PIA was conducted multiples time in order to provide an accurate and reliable data, the PIA still much depends on the human skills who perform [22].

The maximum distance between the attacker and the WBAN target system recorded for all successful PIA (x_m) conducted was five (5) meters. This research was conducted in the actual environment, the distance recorded was in the manner of Clear Line of Sight, which means there was neither objects, nor walls in between the WBAN target system and PIA (x_m) setup. Although conducted on Clear Line of Sight, the Distance Variable is very much affected by the interference of other signals or frequencies operated on the same spectrum, as WBAN exists in the air. According to Mansouri et al. 2010, a study conducted in 2010 discovered that for the transmitting power on the distance estimation between a target and a low transmission power sensor node, the distance estimation error (RMSE) is at its highest value at six (6) meters [23]. The study was conducted on a tracking application using the Variational Filtering (VF) based on quantized proximity sensors [23]. Therefore, the theory of RMSE discovered by Mansouri et al (2010) can be used to explain why an attacker is required to be in a position less than 5 meters from the WBAN target system in order to execute a successful PIA [21].

Table 5 shows that the Impact Variable for Confidentiality of WBAN target system was compromised in PIA (x_1). The Impact Variable for Availability of WBAN target system was compromised by PIA (x_2). Both PIA (x_3) and PIA (x_4) was affecting more than one impact, when the Impact Variable for Confidentiality, Integrity and Availability of the WBAN target system were compromised. The PIA (x_3) and PIA (x_4) scored highest value among other PIA (x_m). Thus highlight the highest Impact of threats that WBAN developers should counter in the future [21].

4.2. Weighting Factor

According to the previous section, Qi Li and Ezell have a different approach of deciding the value for the weighting factor w_m [8]. However, in this research, the weighting factor w_m will be derived from the Changeable Variable measured during the PIA process. As shown in Table 4, the maximum recorded distance is 5 meters for all the PIA conducted. According to the theory of fraction, the numerator represents a number of equal parts, and the denominator, which cannot be zero, indicates how many of those parts make up a unit or a whole [8]. Since, the Distance Variable was unchanged, we set the Distance Variable as numerator and the Time Variable as the denominator [8]. From the previous section, Equation 2 shows that the sum of weighting factor w_m must equal to one. Therefore, the w_m for the PIA(x_1), PIA(x_2), PIA(x_3) and PIA(x_4) are 0.4791, 0.3325, 0.114 and 0.0770 respectively as shown in Table 6.

Table 6. Weighting Factor Derived From Changeable Variable

m	PIA (x_m)	Changeable Variable		Maximum Recorded Distance ÷ Time to Execute (ms-^{1})	Weighting Factor (w_m)
		Distance (m)	Time to Execute (s)		
1	PIA (x_1)	5.0	85.50	0.0585	0.4791
2	PIA (x_2)	5.0	123.23	0.0406	0.3325
3	PIA (x_3)	5.0	366.35	0.0136	0.1114
4	PIA (x_4)	5.0	529.66	0.0094	0.0770

4.3. SIL Quantifying Process

At this stage, all the information that the AVF needed to quantify the Security Impact Level on WBAN was successfully collected. All the result and information for Changeable

Variable, Impact Variable, and the weighting factor w_m collected is presented in Table 6. The calculation of Security Impact Level using Equation 3 for each PIA (x_m) presented in Table 7.

Table 7. Full Result Chart

m	PIA (x_m)	Changeable Variable		Value	Weighting	Impact Level of PIA (x_m)
		Distance (m)	Time to Execute (s)	$v_m(x_m)$	Factor (w_m)	$V(x_m)$
1	PIA (x_1)	5.0	85.50	1	0.4791	$V(X_1) = [w_1 \times v_1(x_1)]$ $= 0.4791 \times 1$ $= 0.4791$
2	PIA (x_2)	5.0	123.23	1	0.3325	$V(X_2) = [w_2 \times v_2(x_2)]$ $= 0.3325 \times 1$ $= 0.3325$
3	PIA (x_3)	5.0	366.35	3	0.1114	$V(X_3) = [w_3 \times v_3(x_3)]$ $= 0.1114 \times 3$ $= 0.3342$
4	PIA (x_4)	5.0	529.66	3	0.0770	$V(X_4) = [w_4 \times v_4(x_4)]$ $= 0.0770 \times 3$ $= 0.2310$

Since the PIA Impact Variable was based on three security pillar (C.I.A), the highest value of score v_m (x_m) will be three points [8]. Therefore the Security Impact Level should be set at three different levels [8]. High Impact Level represents the most vulnerable level, which carry three points. In other words, High Impact Level is when all three C.I.A, Confidentiality, Integrity and Availability of the WBAN system was compromised. Moderate Impact Level represents medium impact level, which carry two points. Finally Low Impact Level represents lowest vulnerable level, which carry one point.

Table 8. WBAN Impact Level

Score	Colour	Level
1	Yellow	Low Impact Level
2	Orange	Moderate Impact Level
3	Red	High Impact Level

To this point, as shown in Table 7, each of the four PIA have already measured and were given a value. To measure the Security Impact Level on WBAN system, based on four different PIA, we use the Additive Multi-Objective Value Function from Equation 3, and therefore:

$$\begin{aligned} V(X) &= [w_1 \times v_1(x_1)] + [w_2 \times v_2(x_2)] + [w_3 \times v_3(x_3)] + [w_4 \times v_4(x_4)] \\ &= 0.4791 + 0.3325 + 0.3342 + 0.2310 \\ &= 1.3768 \end{aligned}$$

The final result shows that based on four different PIA testing, the security impact level for WBAN is 1.3768 and categorized under Moderate Impact Level. From the result, it is proven that using the combination of theoretical and practical, to quantify WBAN security impact is achievable and successful. Further analysis in Table 7 will be discussed in the final phase. The Changeable Variables and the WBAN Security Impact Level will be used to develop a Secure Network Architecture for WBAN.

5. Forth phase: Forensic Readiness Secure Network Architecture

In the final phase, the Forensic Readiness Secure Network Architecture designed specifically for WBAN will be discussed. The forensic readiness and secure network architecture requirements will be discussed before merging it with the results obtained in the PIA process. All the information then convert into developing a secure network architecture, complete with Forensic Readiness capabilities, Preventive Mechanism and Detective Mechanism.

5.1. Forensic Readiness

Forensic Readiness means a forensically ready system that has the ability to investigate post incident event. One of the challenges in investigating cybercrime is obtaining all necessary evidence related to the crime [24]. The concept of forensic readiness is to improve the efficiency of a digital Forensic investigation [24]. The benefit of forensic readiness is not limited to improve efficiency of digital forensic investigation process, but to reduce the amount of man powers, investigation hours, and to provide a cost effective secure architecture [24]. Therefore increase the efficiency in response to any incident [24]. The proposed Forensic Readiness Network Architecture must consist of all the processes and components required as listed in Table 9 [24].

Table 9. Forensic Readiness Requirements

No	Process	Component	Description
1	Traffic Monitoring	WBAN Base Station	WBAN Base Station monitors all WBAN traffic. The WBAN traffic filtered by Firewall for both inbound and outbound WBAN traffic.
2	Logging	Capture Unit	All the monitored traffic were logs to a component called Capture Unit. The log file divided into separate storage areas with each storage area consists of 1 MB data. The Capture Unit then created a block of data per several MBs before Hashing it using SHA-3 to maintain integrity. The Hashing process is to produce strong evidence that the data has not been modified. Then sending it in a form of an accumulated block of data to Evidence Storage.
3	Preservation of Logs	Evidence Storage	The Evidence Storage is the central storage of all the hashed block of WBAN data monitored. The Evidence Storage must ensure no changes to the logs since the data collected.
4	Analysis of Logs	Evidence Storage	The analysis of hashed blocks of WBAN data will only take place if an incident occurs. The analysis is the process of creating an image of the Evidence Storage. The image of the Evidence Storage should be compatible with the commercial analysis, digital Forensic tools such as EnCase and FTK.
5	Produce Report	Report	The preparation of report process will have to obey the requirement in order to be accepted by the court of law.

At this stage, all the requirements of a Forensic Readiness have been captured. The requirements listed will be translated into a secure network architecture that have the enhanced ability to be investigate post incident, event in order to increase the efficiency of digital forensic investigation [21].

5.2. WBAN Secure Architecture

A study was conducted in 2012 and proposed a Forensic readiness network architecture for medical devices [25]. In the study, a common Hospital Internal Network is enhanced by adding a forensic server and drone within the wireless network to add a forensic readiness capability [25]. According to Cusack and Kyaw, the drone applied within wireless network is hidden from other wireless clients, but has the ability to record communication within their network and forward it to the forensic server [25]. In order to implement WBAN system to the Hospital Internal Network securely, this research proposed a Forensic Readiness Secure Network Architecture for WBAN that equipped with forensic readiness capability, and the ability to withstand internal and external attacks [21]. In order to withstand internal and external attacks, the PIA results will be used to develop the Preventive and Detective Mechanism [21].

5.3. Secure Space and Preventive Mechanism

From the PIA results, in order to execute a successful PIA, an attacker is required to be in a position less than five meters from the WBAN target system. This significant discovery allows us to estimate the distance between WBAN sensor and other unauthorized wireless devices [21]. Thus providing a Preventive Mechanism, that may apply to the proposed secure network architecture [21]. In this 5 meters distance, the communication of the standard WBAN sensor node was tested using PIA and the result was negative and providing no data or readings [21]. It can be concluded that no PIA testing that can be conducted beyond this 5 meters barrier [21]. This barrier justified if the discovery of Mansouri et al (2010) regarding the RMSE theory on low power sensor node applied [23]. However the explanations of the slight difference between those two distances can be researched further in the future.

Therefore, to this date, based on the results of this research, it saves to recommend that a WBAN system installation to have a minimum distance of 6 meters radius from other wireless system and devices [21]. A minimum radius distance of 6 meters will create a 113.14286m^2 Secure Space as shown in Figure 8 [21].

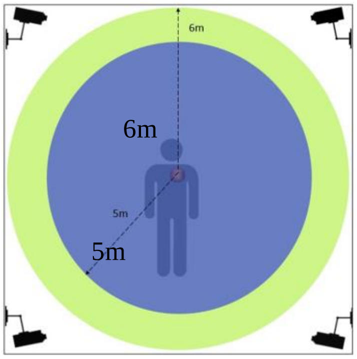

Figure 8. Secure Space

No other device with the wireless technology capability authorized inside this 113.14286m^2 space except for the Authorized Medical Officer's device [21]. It is proposed that this minimum 113.14286m^2 space created also equipped with Surveillance Cameras or Closed Circuit Television (CCTV) for monitoring purposes [21]. If an incident such as PIA(x_1), PIA(x_2), PIA(x_3) and PIA(x_4) occurs, from the PIA results we can estimate that the incident was executed within the 6 meters radius [21]. With the support of CCTV recording, the location where the attack was executed can be estimated. We can estimate the attacker location, and detect which attack was executed by using the information in Table 7 [21].

For example, a scenario of a DoS attack detected. Based on the CCTV recording, there were five people using wireless devices at the crime scene. Four of the suspects was within the radius of four meters from the WBAN target system. Three of the suspects spend less than 10 seconds in the crime scene, and the others spend more than 150 seconds. This allows us to narrow down our investigation to targeted person only.

Table 10. Investigation Checklist

Suspect	Wireless Device	Inside Secure Space	Outside Secure Space	More than 150 seconds	Less than 150 seconds
Suspect 1	✓		✓		✓
Suspect 2	✓	✓		✓	
Suspect 3	✓	✓		✓	
Suspect 4	✓	✓			✓
Suspect 5	✓	✓			✓

As shown in Table 10, this method has managed to narrow down from the five suspects into two suspects only. In order to validate our findings, the logs recorded in Evidence Storage installed within the secure network architecture can be used to provide further information such as Time Stamp and MAC address for investigation purposes based on the Explanatory Report by Council of Europe [26].

Therefore the findings in Figure 8 prove that the data obtained from the PIA can be used to develop the Preventive Mechanism for Forensic Readiness Secure Network Architecture for WBAN system implementation. This Preventive Mechanism provides the ability to reduce the security risk and therefore prevent an incident to happen [21].

5.4. Data Preservation and Detective Mechanism

The Convention on Cybercrime states that any service provider shall take all necessary steps to preserve records and other evidence in its possession upon request of a government entity for any lawful excuses [7]. However, data preservation has now turned into one of the risk management mechanism [27]. The idea of preserving data is to have detailed information if any incident occurs [27]. The data preserved will be analysed and produced as reliable evidence in order to be accepted in the court of law [26]. Therefore, it is important for this research to identify and analyse the data preservation requirements for the designed secure network architecture.

It is known that WBAN cannot handle a large volume of data due to the low link bandwidth [21]. For example, video streaming [21]. WBAN operates under low data rate of 250 kbps up to 500 kbps [21]. Therefore, theoretically WBAN must be able to generate data rate from 250 kb to 500 kb of data per one second of time. From the PIA it was discovered that the amount of time needed to execute an attack is 85.5 seconds to 529.66 seconds. Therefore the minimum and maximum volume of data for PIA, can be estimated and calculated and the results as shown in Table 11.

Table 11. Minimum and Maximum Data Storage

m	PIA (x_m)	Time to Execute (s)	Minimum		Maximum	
			Time (s) × 250 (kbps)	MB	Time (s) × 500 (kbps)	MB
1	PIA (x_1)	85.50	21375	2.6092529	42750	5.2185059
2	PIA (x_2)	123.23	30807.5	3.7606812	61615	7.5213623
3	PIA (x_3)	366.35	91587.5	11.1801148	183175	22.360230
4	PIA (x_4)	529.66	132415	16.163940	264830	32.327881

In this research, Data Preservation process will follow the Forensic readiness requirement. The forensic readiness requires the Capture Unit to create a block of data per several MBs, before hashing it using Secure Hashing Algorithm SHA-3 to maintain integrity, before sending it in a form of an accumulated block of data to the Evidence Storage [26]. From Table 11 the calculated minimum volume of data is 2.61 MB and the calculated maximum volume of data is 32.33 MB. Therefore, to this date, based on the results of this research, it saves to recommend that the Data Preservation process conducted by the Capture Unit to create a block of data per 3 MB before hashing it using SHA-3.

This estimation of calculating minimum and maximum volume of data has provided us the information regarding the amount of data generated for each PIA. This information will be used to develop the Detective Mechanism for secure network architecture. Based on Table 11, each PIA will generate data ranging from 3MB to 33MB. It is proposed that the generate data ranging from 3MB to 33MB will be set as signatures to identify an attack. The WBAN Base Station will be using this attack signatures to detect an attack against a WBAN system. If an attack occurs, WBAN Base Station may able to identify the attack using the Detective Mechanism, by looking at the amount of data transmitted by the unauthorized device.

Table 12. Investigation Checklist

Suspect	Wireless Device	Inside Secure Space	Outside Secure Space	More than 150 seconds	Less than 150 seconds	More than 1.5MB	Less than 1.5MB
Suspect 1	✓		✓		✓		✓
Suspect 2	✓	✓		✓			✓
Suspect 3	✓	✓		✓		✓	
Suspect 4	✓	✓			✓		✓
Suspect 5	✓	✓			✓		✓

Based on the previous example, the investigation has managed to narrow down from five to only two suspects. Both suspects identified spend more than 150 seconds within the Secure Space. One of the suspects was detected transmitted 7MB of data to the WBAN system, and the other one has only transmitted 1.5MB of data. From the information based on Table 11, any suspect who transmitted data ranging from 3.7 MB to 7.5MB within the secure 113.14286m^2 space, will be identified as the suspect with the highest probability of conducting DoS attack to the WBAN system. This allows us to narrow down our investigation to only one suspect. As shown in Table 12 the suspects are now reduced to only one person (Suspect 3). Although other evidences would be required to support the investigation, this method may reduce the dependence on MAC address and Time Stamp as the only source of digital evidence. Therefore the findings in Table 12 prove that the data obtained from the PIA can be translated into actionable information to develop the Forensic Readiness Secure Network Architecture for WBAN system implementation.

5.5. Impact Alert

In the previous section, the severity of an attack of the WBAN system can be calculated using the Secure Impact Level. The score for the Secure Impact Level for each PIA (x_m) was successfully calculated. Both PIA (x_1) and PIA (x_2) will be in the Low Impact and referred as Yellow Level and both PIA (x_3) and PIA (x_4) will be in the High Impact and referred as Red Level. Any attack or anomaly attempt of WBAN system detected by the within the Secure Space by the WBAN Base Station will trigger an Impact Alert [21]. For example, if the WBAN Base Station detected an unauthorized device transmitting more than 30MB of data, based on the previous set of signatures, the WBAN Base Station will trigger a High Impact Level Alert to the system administrator indicating that there is a High Impact Level attack executed against the WBAN system.

The Secure Impact Level is not limited to producing Impact Alert. The Secure Impact Level will provide the severity of each attack against a WBAN system accurately [8]. In the Convention on Cybercrime, the court did not have an accurate information on sentencing commensurate with the impact of the cybercrime committed. Therefore, for this research, the impact level can be used to gauge the severity of an attack against a WBAN system. Therefore provide an accurate information for the Prosecution in the court of Law.

5.6. Forensic Readiness Secure Network Architecture

In this section, all the discoveries in the previous sections will be translated into a secure network architecture that have the ability to withstand internal and external attacks. From the previous section, the PIA results have successfully produced, the Impact Alert and the Preventive and Detective Mechanism for the secure network architecture. The requirements for Secure Network Architecture and Forensic Readiness will be merged with the Detective and Preventive Mechanism, thus produce the Forensic Readiness Secure Network Architecture for Wireless Body Area Network (WBAN) as shown in Figure 9.

Table 13. Components and devices

No	Components	Description
1	WBAN Sensor Node	The sensors capable of sampling, processing, and communicating multiple data sent its data to the Coordinator.
2	Coordinator	The Coordinator received a WBAN signal transmitted by the wireless sensor node, process it, and convert it into a readable data before forwards it to the WBAN Base Station.

3	WBAN Base Station	The WBAN Base Station via a coordinator sets up and controls the WBAN sensor nodes, and forward all the data received to the Capture Unit. The WBAN Base Station will be used to detect any anomaly activities towards the WBAN system.
4	Capture Unit	The Capture Unit performs hashing algorithm SHA-3 before forwarded it to the Evidence Storage.
5	Evidence storage	Evidence Storage stores all WBAN communication in hashed block of data for enhanced integrity of data.
6	Database	The database will keep all data and the retention period of time is based on the Convention on Cybercrime data retention period.
7	Domain Controller	Domain Controller is a Server that capable of responding security authentication request
8	Switch	A networking device that links all network segments and devices
9	Internal Firewall	The Internal Firewall will control all incoming and outgoing communication traffic allowed by DMZ to the internal network. Recommended to use different brand from External Firewall.
10	DMZ	Demilitarized Zone is configured using two firewalls
11	External Firewall	Control incoming and outgoing communication traffic destined to DMZ only.
12	Router	Device that forwards data packets between networks
13	Wireless AP	Wireless Access Point will be configured as wireless drones

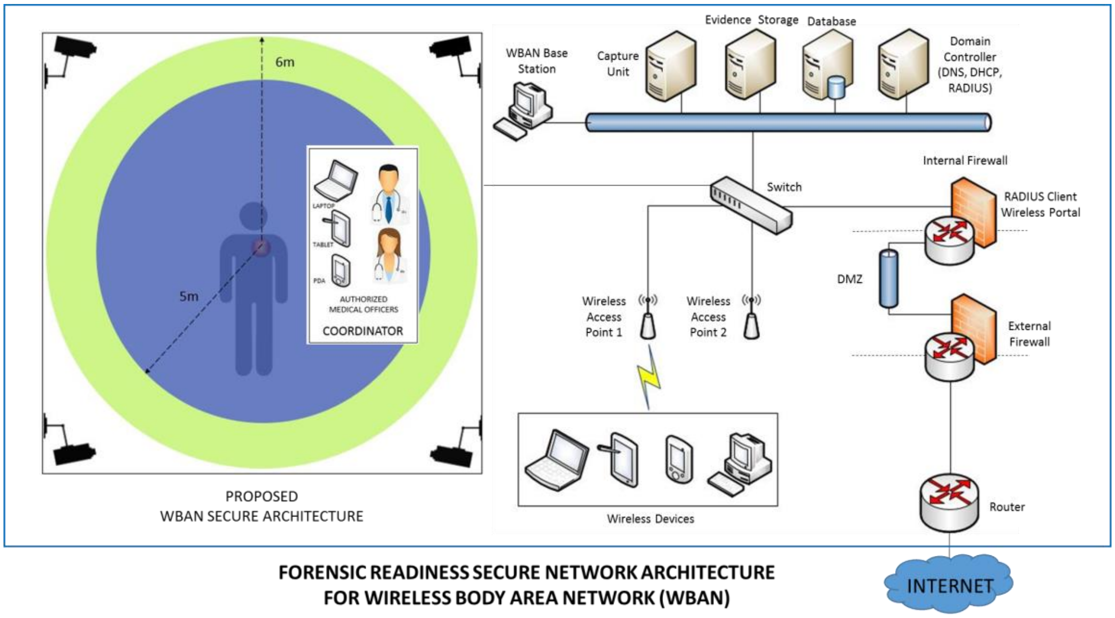

Figure 9. Forensic Readiness Secure Network Architecture

6. Conclusion

The forensic readiness requirements, Preventive Mechanism and Detective Mechanism was successfully included in the Forensic Readiness Secure Network Architecture for Wireless Body Area Network (WBAN). Therefore, the research objective of developing

Forensic Readiness Secure Network Architecture for WBAN in line with the Convention on Cybercrime using a practical testing approach is achieved. Thus setting a better foundation for securing WBAN researches in the future.

Acknowledgements

The authors would like to thank all the reviewers for their helpful comments. We also would like to thank the Universiti Teknikal Malaysia Melaka (UTeM) that provides the research grant for this project. This research is currently supported by the ERGS/2011/FTMK/PK02/1 under the Exploratory Research Grant Scheme (ERGS) funding by the Ministry of Higher Education Malaysia (MOHE) and National Vulnerability Assessment Centre (MyVAC) of Cybersecurity Malaysia, an Agency under the Ministry of Science Technology and Innovation Malaysia (MOSTI) for their contribution.

References

[1] S. Rashwand, “Efficient Wireless Communication in Healthcare System; Design and Performance Evaluation”, Department of Computer Science, University of Manitoba, **(2010),** URL: http://www.cs.umanitoba.ca/rashwand/SaeedRashwand-CandidacyPaper-FirstChapter.pdf.

[2] F. Tufail and H. Islam, “Wearable Wireless Body Area Networks. Proceedings of the Information Management and Engineering”, (ICIME ’09), **(2009)** April 3-5, Kuala Lumpur, Malaysia.

[3] B. Dolan, C. Psychol and Barrister, “Medical Records: Disclosing Confidential Clinical Information”, The Psychiatrist, vol. 28, **(2004).**

[4] H. C. Keong and M. R. Yuce, “Analysis of a multi-access scheme and asynchronous transmit-only UWB for wireless body area networks”, Proceedings of the 31st International Conference of the IEEE Engineering in Medicine and Biology Society, **(2009)** September 3-6, Minnesota, USA.

[5] S. Saleem, S. Ullah and H. S. Yoo, “On the Security Issues in Wireless Body Area Networks”, International Journal of Digital Content Technology and its Application, vol. 3, no. 3, **(2009).**

[6] S. N. Ramli and R. Ahmad, “Surveying the Wireless Body Area Network in the Realm of Wireless Communication”, Proceedings of the 7th International Conference on Information Assurance and Security, **(2011)** December 5-8, Malacca, Malaysia.

[7] “Council of Europe”, Explanatory Report of Convention on Cybercrime, URL: http://conventions.coe.int/Treaty/en/Reports/.

[8] A. F. A. Rahman and R. Ahmad, “Hybrid Method to Measure Vulnerability in Wireless Body Area Network”, Proceedings of the 6th International Conference on Sensor Asiasense, **(2013)** August 23-25, Malacca, Malaysia.

[9] E. Casey, “Handbook of Computer Crime Investigation, Forensic Tools and Technology”, Elsevier Academic Press, San Diego, USA, **(2007).**

[10] R. C. Deason, “Wireless Local Area Network Architecture for Naval Medical Treatment Facilities”, Naval Postgraduate School, California, USA, **(2004).**

[11] J. Deng, R. Han and S Mishra, “A performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Network”, Information Processing in Sensor Networks Lecture Notes. Computer Science, vol. 2634, **(2003).**

[12] A. Wood and J. Stankovic, “Denial of Service in Sensor Network”, Computer, vol. 35, **(2002).**

[13] D. R. Raymond and S. F. Midkiff, “Denial of Service in Wireless Sensor Networks: Attacks and Defenses”, Pervasive Computing, vol. 7. Issue 1, **(2008)**.

[14] S. Zhu, S. Setia, S. Jajodia and P. Ning, “An Interleaved Hop-By-Hop Authentication Scheme for Filtering Of Injected False Data in Sensor Network”, Proceedings of the IEEE Symposium on Security and Privacy, **(2004)** May 9-12, Oakland, USA.

[15] M. K. Khan and K. Alghathbar, “Security Analysis of Two Factor User Authentication in Wireless Sensor Networks”, Advances in Computer Science and Information Technology Lecture Notes in Computer Science, vol. 6059, **(2010).**

[16] C. Cornelius and D. Kotz, “On Usable Authentication for Wireless Body Area Networks”, Proceedings of the 1st USENIX Workshop on Health Security and Privacy, **(2010)** August 10, Washington DC, USA.

[17] T. Lee, C. Qiao, M. Demirbas and J. Xu, “ABC: A Simple Geographic Forwarding Scheme Capable of Bypassing Routing Holes in Sensor Networks”, Proceedings of the 17th International Conference on Computer Communications and Networks, **(2008)** August 3-7, Virgin Island, USA.

[18] R. L. Keeney and D. V. Winterfeldt, “Advances in Decision Analysis: From Foundations to Application”, **(2007)**.

[19] Q. Li, “Using Additive Multiple Objective Value Functions for Value Based Software Testing Prioritization”, University of Southern California Computer Science Department, **(2009),** URL: http://csse.usc.edu/csse/ TECHRPTS/2009/ usc.../usc-csse-2009-516.pdf.

[20] B. C. Ezell, “Infrastructure Vulnerability Assessment Model (I-VAM), **(2007),** URL: http://create.usc.edu/assets/ pdf/51834.pdf.

[21] A. F. A. Rahman, R. Ahmad and S. N. Ramli, “Forensic Readiness for Wireless Body Area Network System”, Proceedings of the 16th International Conference of Advanced Communication Technology (ICACT 2014), **(2014)** February 16-19, Pyeongchang, South Korea.

[22] R Ajemian, A. D. Ausillio, H. Moorman and E. Bizzi, “Why Professional Athlete Need A Prolonged Period Of Warm-Up And Other Peculiarities Of Human Motor Learning”, Journal of Motor Behaviour, vol. 42, no. 6, **(2006)**.

[23] M. Mansouri, A. Sardouk, L. M. Boulahia, D. Gaiti, H. Snoussi, R. R. Amoud and C. Richard, “Factors That May Influence the Performance of Wireless Sensor Networks”, Smart Wireless Sensor Networks, **(2010).**

[24] S. Ngobeni, H. Venter and I. Burke, “Forensic Readiness for Wireless Networks”, IFIP Advances in Information and Communication Technology. vol. 337, **(2010).**

[25] B. Cusack and A. K. Kyaw, “Forensic Readiness for Wireless Medical Devices”, Proceedings of the 10th Australian Digital Forensic Conference, **(2012)** December 3-5, Perth, Australia.

[26] A. Agarwal, M. Gupta, S. Gupta and S. C. Gupta, “Systematic Digital Forensic Investigation Model”, International Journal of Computer Science and Security, vol. 5, **(2011)**.

[27] C. Coutinho, “Data preservation of Business Assets as a Risk Management Strategy”, Proceedings of the Workshop on Open Source & Design of Communication, **(2013)** July 11, Lisboa, Portugal.

Authors

Abdul Fuad Abdul Rahman, a Senior Analyst with the National Vulnerability Assessment Centre (MyVAC) of CyberSecurity Malaysia. Prior to that, he has a System Security Certified Practitioner (SSCP) from The International Information Systems Security Certification Consortium (ISC)^2, GIAC Assessing Wireless Network (GAWN) from SANS Institute of America and Certified Network Engineer IPv6 (CNE6). He is currently appointed as the Technical Advisor to the Cybercrime Legislation Committee chaired by the Attorney General’s Chambers of Malaysia.

Rabiah Ahmad, she received her Ph.D in Health Informatics at University of Sheffield (UK) and Master of Science in Information Security from Royal Holloway University of London (UK). She is currently as senior lecturer (Associate Professor) with Universiti Teknikal Malaysia Melaka (UTeM). In the same time she is representing Malaysia for member of World Standard in Information Security Technique Working Group (Identity Management). She also certified as members of MyCC Scheme Certification Committee organized by Cybersecurity Malaysia. In addition, she is appointed as high committee members of Malaysia Society of Cryptology Research.

Madihah Zulfa Mohamad, a Senior Executive with the MyCyberSecurity Clinic of CyberSecurity Malaysia. Prior to that, she has a Certified Ethical Hacker (CEH) from EC-Council and Microsoft Certified System Engineer (MCSE) from Microsoft. She is currently focus in the field of Digital Forensic, especially in Data Recovery.