Digital Investigation 14 (2015) 46–52

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Identifying management factors for digital incident responses on Machine-to-Machine services

Sung Ryel Lim

Department of Communication Development Team, SK Holdings, Seongnam, South Korea

ARTICLE INFO

Article history:
Received 26 November 2014
Received in revised form 4 July 2015
Accepted 8 July 2015
Available online 21 July 2015

Keywords:
Digital incident response and management
Machine to Machine control
U-Healthcare
Mission critical system
Defendable software
Information assurance
Forensic readiness

ABSTRACT

This paper presents a recent case study about how South Korea has modified the way it addresses digital incidents. To determine the best approach to mission-critical instances, the Multilateral Joint Analysis (MJA) model was used as an enhanced two stage process. The Delphi method and Structural Equation Model (SEM) were employed to determine the final model. This process established a governance mechanism that uses measurable control variables and is presently in use in mission critical services to protect against digital incidents.

Introduction

In 2009, when North Korea faced heavy floods, it discharged the water of the Hwang Nam Dam into the upper Imjin river. Unfortunately, a group of South Koreans on the lower Imjin river were not evacuated in time because the Machine-to-Machine (M2M) sensors of the South Korean Early Warning System did not work. In this case, a South Korean judge found that the sensor control mechanism of the Emergency Warning System was at fault (Choi, 2009; Lim et al., 2012).

This paper presents a case study of how South Korea addressed the issues raised by this digital incident and became a leader in world e-government, achieving progress in and provision of cross-sector mobile applications for citizens (UN Dept. of Economic and Social Affairs, 2012). Ubiquitous computing, already a reality for some businesses, is making mobile management and compliance mechanisms an important topic for e-governance systems. In South Korea, the aim of e-government is to secure accountability and assure the integrity of mobile products at all stages, from requirements, through implementation, and, finally, into stable and responsive operational systems (Lim et al., 2012).

This study evaluates the new model against faults identified in the “Hwang Nam Dam” incident specifically. Using this model, robustness against digital disasters can be increased by determining the control mechanism of malfunctions in product deployments. For instance, this approach can more effectively coordinate the connection of mobilewarning sensors on the lower river as in the Imjin River case (Choi, 2009; Lim et al., 2012). This approach could help secure human life against the hidden defects that arise during the development of digital environments.

This paper is split into four major sections. Section Introduction discusses the need for this model. Section Realted work presents recent studies in this area. Section Multilateral Joint Analysis (MJA) on M2M services defines the key factors as components of a new theoretical model and then evaluates them. Section Conclusions concludes this paper.

E-mail address: audit@korea.ac.kr.

http://dx.doi.org/10.1016/j.diin.2015.07.003
1742-2876/

Related work

Recent work that relates to this subject falls in two categories. The first focuses on information assurance. Yashira et al. (2000) suggested a high assurance on-board computer system to enhance fault-tolerant technology. Nguyen and Ellis (2011) proposed experiences with assurance cases for spacecraft safety. In addition, Newman and Wander (2002) implemented a NASA mission success management framework that uses web-ready video interviews for evaluation. However, these studies are not based on real practices, instead they used model assumptions and then proved them by simulation data. But this proposed approach extends prior works by giving an enhanced two stage model and its components based on an actual domain dataset of major digital incident case and problem.

The second category concerns forensic readiness for defendable software deployments. Robert Rowlingson (2004) opened a business insight for forensic readiness. He proposed a ten step process in implementing a forensic readiness programme. Solms et al. (2006) set control objectives for a digital forensic control framework, and Mouton and Venter (2011) implemented a prototype for wireless sensor networks to achieve digital forensic readiness. In addition, Reddy and Venter (2013) proposed an architecture for a digital forensic readiness management system. These studies give useful guide and framework for forensic readiness. However none of these studies provided a model based on business practices that could be used to identify and evaluate model components using measurable control variables. This proposed approach extends prior works by giving implementation model.

Multilateral Joint Analysis (MJA) on M2M services

In the context of the Hwang Nam Dam disaster, this study initially proposed a set of control variables for defendable software deployment: “Accuracy,” “Admissibility,” and “Speed.” “Accuracy” refers to business integrity across ad hoc appliances, especially when allocating accountability across various real-time appliances. “Admissibility” is a measure of how strongly the chain of custody protects against vulnerabilities, thus securing admissibility of evidence in priority order. The final variable, “Speed,” is included as a tool to visualize the movement of management decisions across forensic readiness appliances during the mobile product development life cycle.

Furthermore, these variables were mapped to the carriers, “Policy” (South Korean Ministry of Administration and Security, 2011–2013; Cichonski et al., 2012), “Standard” (Hochstein et al., 2005), and “Architecture” (Tint et al., 2010; Wang, 2008). This mapping to carriers is to help user's understanding. For the example, the proposed variables are not clear for implementation in their current properties. Because all proposed variables are non-functional requirements. But the carriers give functional requirements for real practices. Thus these carriers provide objectivity and help to visualize management decision flow in the mobile application and its dashboard implementation. The carriers are taken from Cichonski et al. (2012) Computer Security Incident Handling Guide, NIST (National Institute of Standard & Technology). “Policy” is adopted as is, and the “Standard and Architecture” are an adaption of the original “Plan and Procedure” to strengthen product accountability to improve incident response in mission critical service case studies. The carriers in this study help relate business integrity and ad hoc product appliances, especially when allocating accountability across real-time incident responses.

In the final design, in the context of medical care, this study determined a new model for M2M convergent medical services and product cases with forensic readiness. As a result of the suggested control variables of the first and second steps, the “Accuracy” component remains in the model. And from the result of the Delphi method using medical experts, the “Reliability” and “Safety” components were selected for the for the final MJA model, which also considers u-Healthcare, a South Korean service for convergent medical services.

Thus, the final model elements are “Accuracy,” “Safety,” and “Reliability.” A professional dataset was created from the recent practices for mission critical services used by the Seoul National University Hospital (Lim and Lee, 2013). Finally, the Structural Equation Model (SEM) was drawn based on these real practices.

It is well known that design defects are considered to be the root causes of system vulnerability, as in the Imjin River Case. Digital incidents can always be blamed on natural occurrences or human error in the absence of suitable controls (Choi, 2009; Lim et al., 2012). However, it is impractical to expect this kind of expertise in every field, because digital forensics, which generally operate under a police organizational structure, tend to take a stand-alone approach. Thus, it depends mainly on individual experience and knowledge. This means that the maintenance of accountability and admissibility of evidence to court in the face of M2M convergent product vulnerability would have a major impact if such a system could be developed.

Hence, this paper developed the MJA model and applied it to the digital investigation of mission critical services. For instance, in the Imjin River case, were some safety logs that could not be used in court because they might have been tampered without this system. Another example might be a rural police department (Provincial police agency) that may now use medical records in its cases because it adopted this system.

Recently, Samsung group company of South Korea practiced this model in the strategic information workshop in June 2015, when they were given on-the-job training for ITIL (IT Infrastructure Library) and U-Healthcare systems. Especially the practice of this model is effective for building an e-Hospital. It can benefit from this model if the doctor's prescription is based on the M2M service. But if safety fails, none of citizens will use this service regardless of emergency for handling the blood pressure or infectious disease, etc. Futhermore, all the doctors would avoid this service because they are accountable for this failure in the law.

First round of model components

The experimental structure established for questionnaire design is shown in Table 1. The participant groups