A New Approach to Risk Management in the Health-care Domain

E Smith[a] JHP Eloff[b]

[a]*University of South Africa, Department of Computer Science and Information Systems, PO Box 392, Pretoria, South Africa,* elme@pixie.co.za

[a]*Rand Afrikaans University, Department of Computer Science, PO Box 524, Auckland Park, Sout Africa,* eloff@rkw.rau.ac.za

Abstract

This paper is devoted to the presentation of a risk-management methodology (RiMaHCoF) that is specifically tailored for the health-care environment. The proposed methodology includes five successive stages in all, namely initiation, domain analysis, risk assessment, risk analysis and domain monitoring. This paper focuses on the risk analysis stage.

The RiMaHCoF ("Risk Management in Health Care - using Cognitive Fuzzy techniques") methodology enhances risk management in the specific domain of health care in the sense that it deems the patient's health-care information, processed and stored in a typical health-care institution, to be of utmost importance to such institution. The methodology further enhances risk management in this domain in that it incorporates cognitive fuzzy-logic techniques - as opposed to quantitative techniques such as annual loss exposure (ALE) calculation - to assess and analyse the information-technology risks. In this way, it is ensured that full cognisance is taken of the intuitive nature of human observation when assessing the possible IT risks to be incurred in a health-care institution. In addition, the methodology takes into account the vagueness of the decision making process with respect to securing patient information.

The cognitive fuzzy approach to the assessment and analysis of information technology risks in health care does not only identify the high-risk areas within a typical health-care institution, but also helps to manage risks by facilitating the decision-making process with respect to securing patient information.

Keywords: *fuzzy cognitive map, information technology risk value, risk analysis, risk assessment, risk-management methodology*

Computing Review Categories: *K.6.5*

1 Introduction

Information technology is currently being employed in health-care environments across the globe, resulting in significant improvements in the efficiency and quality of all services rendered in this realm [1-6]. The prospect of storing health-care information in electronic form does, however, raise concerns about the risks that could be incurred. The occurrence of a risk, such as the exposure of highly confidential and sensitive health-care information to outsiders, could compromise not only the patient's privacy, but also quite literally his/her wellbeing. It is, therefore, imperative to be able to identify possible risks in good time and to implement the necessary security controls in order to protect the patient in the health-care institution.

Broadly speaking, risk management can be defined as that process which can be used to identify and implement security controls that will, at best, prevent risks from occurring and, at worst, minimise their effect if they were to occur [7-9]. A number of powerful techniques (such as CRAMM) could be employed to facilitate the prevention and/or management of possible information-technology risks [10, 11]. In current risk-management techniques the emphasis has, however, mainly been placed on the input and manipulation of numbers. Human common sense and intuition, which form the basis of any risk-management exercise, are most of the time neglected.

Furthermore, health-care information systems are quite unique when compared to other information systems, with the result that they require a different approach to risk management [12]. One of the salient features of health-care institutions that sets them apart from ordinary institutions is the fact that they are principally aimed at *treating people*. The RiMaHCoF ("Risk Management in Health Care - using Cognitive Fuzzy techniques") methodology presented in this paper, therefore, is aimed at treating the *patient's health-care information* as being of utmost importance to a typical health-care institution.

Another salient feature of the health-care environment is the fact that it is often difficult, if not impossible, to isolate the assets of the health-care system from the traffic flow of patients, their visitors and doctors. The latter further increases the likelihood of sensitive patient information being exposed to unauthorised parties. It is, therefore, essential to protect the privacy of the patient and his/her health-care information.

Just as important as the need to protect the patient's privacy is the need to *share* accurate patient information in a timely fashion to ensure its availability to all authorised parties and in this way to ensure the proper treatment of

the patient. The dilemma of obtaining, using and sharing patient information to provide care whilst not breaching patient privacy is a serious concern.

Yet another salient feature of the health-care environment is the fact that most of the consequences of possible risks to be incurred are either very *difficult or impossible to quantify*, owing to their non-monetary nature. It is, for example, very difficult to determine the cost associated with the incorrect treatment of a patient owing to inaccurate patient information. Furthermore, some part of the patient information, such as the clinical information, could be considered confidential, whereas another part thereof, such as the geographical information, could well be considered unclassified. The latter, therefore, introduces a certain degree of *vagueness* regarding the decision-making process with respect to securing patient information.

In addition to vagueness, *intuition* also needs to be accommodated in the proposed methodology, as human observation, which is essentially intuitive, forms the basis of any risk-assessment exercise.

The principal aim of this paper is, therefore, not to discourage the use of powerful risk-management techniques (such as CRAMM), but rather to propose a new way of handling risk management in health care. The proposed risk-management methodology focuses specifically on information technology risks, in other words, on those risks that pose a threat due to the information technology used to store, process and disseminate patient information in a health-care institution.

Furthermore, the primary aim of any health-care institution is and should be to treat its patients. The proposed methodology is, therefore, specifically designed to protect the patients and their health-care information in order to ensure their proper treatment. The proposed risk-management model will, for this reason, address information security specifically by focusing on the *confidentiality* of patient information.

The methodology incorporates both the vague and intuitive aspects of the health-care environment by following a cognitive fuzzy-logic approach to the assessment and analysis of information-technology risks that might be incurred in this environment. The methodology is aimed at identifying the high-risk areas within a typical health-care institution. The methodology also helps to manage information technology risks by facilitating the decision-making process with respect to securing patient information.

The proposed methodology includes five successive stages in all, namely initiation, domain analysis, risk assessment, risk analysis and domain monitoring. The first section of the paper will be devoted to a high-level overview of the proposed methodology, followed by an in-depth discussion on the risk analysis stage.

2 A High-Level Overview of the Proposed Risk-Management Methodology (RiMaHCoF)

The proposed risk-management methodology, which has been specifically tailored for the health-care environment, enhances risk management in this domain by considering the patient's health-care information, processed and stored in a typical health-care institution, to be of utmost importance to such institution. The methodology further specifically focuses on the confidentiality of patient information. The other four information security services (identification & authentication, authorisation, integrity and non-repudiation) do not form part of the scope of the proposed model.

Risk management can be defined in terms of this methodology as starting with an initiation stage (see figure 1). The methodology further includes four successive iterative stages, namely domain analysis, risk assessment, risk analysis and domain monitoring.

2.1 Initiation

During the *first stage* (viz. initiation), an awareness of computer security needs to be established among all personnel members of the health-care institution. A special task-team needs to be appointed for this purpose. Another important function of the task-team is to determine the scope of the required risk-management project in order to propose a preliminary budget for the project. After having determined the scope of the risk-management project, a final proposal must be drawn up on its implementation and maintenance.

2.2 Domain analysis

The *second stage* (viz. domain analysis) must be devoted to an analysis of the hierarchy and organisational structure of the health-care institution in question. All the sections comprising the health-care institution must be identified. A typical hospital can, for example, include sections such as the intensive-care unit, the maternity section and the orthopaedic section. All patient information routes in the health-care institution must also be identified. A typical patient information route is, for instance, that route through which a patient's information travels when a typical patient is admitted to hospital to undergo an operation. A patient information route comprises a fixed number of phases. The term "phase" is used here to denote a specific section in a patient information route. For example, the registration section and the operating theatre are two phases within the patient information route when a typical patient is admitted to hospital for an operation.

Furthermore, the measure of information security currently provided by the existing security controls in each of the sections need also to be identified during this stage.

Finally, all components relevant to the health-care in-

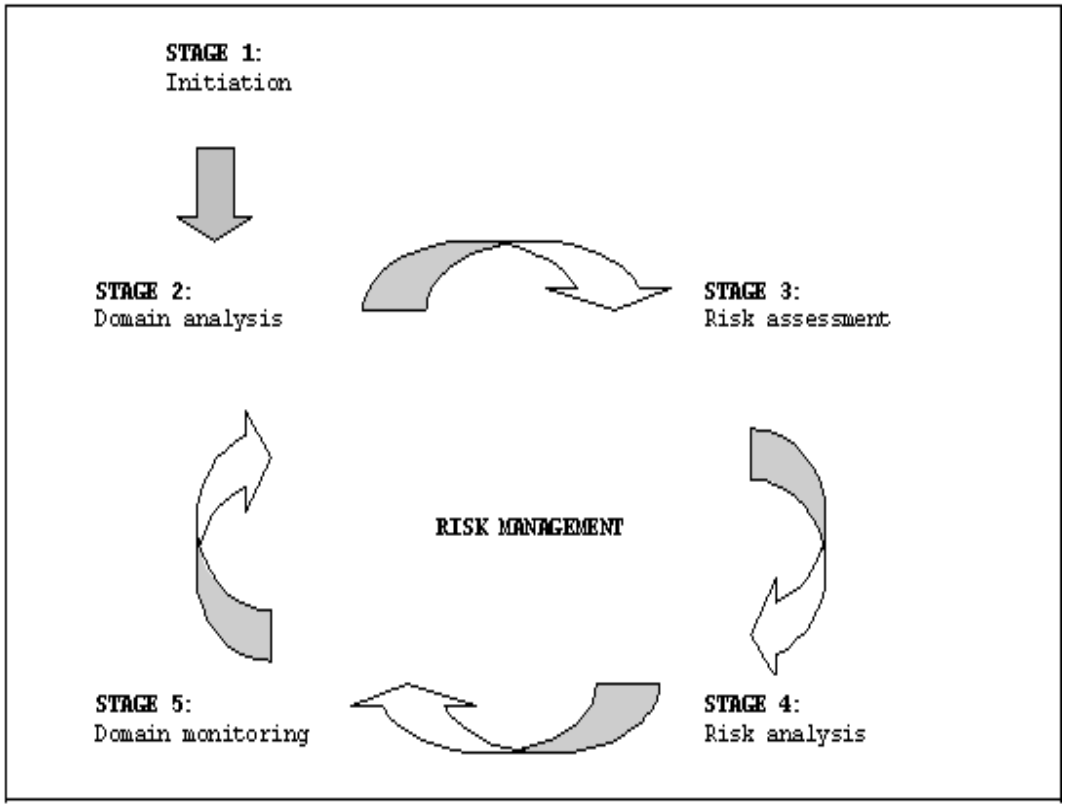


Figure 1: A graphic representation of the various stages in the proposed risk-management methodology for a typical health-care institution

stitution in question need to be identified. The technologies employed to store and process patient information (such as a database) and the security controls implemented are examples of *components*. These components do not, however, exist in isolation. They interact and, in this way, exert a distinct influence on the possibility of risks occurring in a typical health-care institution. When selecting an appropriate risk-management model not only the components that interact in a typical health-care institution should, therefore, be taken into account, but also their relationships with each other and their effect on the likelihood of IT risks being incurred.

2.3 Risk assessment

During the *third stage* (viz. risk assessment) the possible information-technology risks in this dynamic domain must be assessed. The principal aim of the risk-assessment stage is to determine an information-technology risk value for *each phase* in a patient information route. This risk value is based on the information-technology domain a typical patient's information will be exposed to in a specific phase of the patient information route involved.

The ultimate aim of calculating these IT risk values is to facilitate the process of determining which of the patient information routes in the health-care institution in question should be deemed critical with respect to information security. The critical routes should be investigated further in order to determine a way in which to decrease such risk value. On the other hand, low-risk patient information routes will imply that the security controls in place are sufficient.

A cognitive fuzzy-modelling approach is followed to calculate such IT risk values. This approach is, therefore, especially well suited to the health-care domain, where most of the consequences of IT risks being incurred are extremely difficult to quantify.

As a detailed explanation of the cognitive fuzzy-modelling approach falls outside the scope of this paper, the reader is referred to [13] for more information on this approach.

2.4 Risk analysis

During the *fourth stage* (viz. risk analysis) decisions are made regarding the IT risk values calculated in the previous stage (that is, the risk-assessment stage). The risk-analysis stage is aimed at identifying high-risk patient information routes (that is, *critical* patient information routes) in a typical health-care institution with a view to enhancing the information security of such institution.

This stage will be discussed in more detail in paragraph 3.

2.5 Domain monitoring

Finally, the health-care institution must be monitored during the *fifth stage* (viz. domain monitoring) in order to pinpoint any changes in its dynamic nature, including new risks that might occur. The latter stage, however, constitutes an ongoing process through which further or new risks could be identified that might even require a partial or complete iteration of the current risk-management methodology.

3 Stage 4: Risk Analysis

The activities to be performed during the risk-analysis stage are depicted in figure 2. The remainder of the paper is devoted to a discussion on the first three activities that form part of the risk-analysis stage.

3.1 Identify the *Critical Phases* along Each Patient Information Route by Inspecting the IT Risk Values of Each Phase (Stage 4 Task 1)

During the risk-analysis stage, decisions are made regarding the IT risk values calculated for each phase along a specific patient information route during the previous stage (that is, the risk-assessment stage). A phase could be classified as a "low-risk" phase if its IT risk value falls between 0 and 350, as a "medium-risk" phase if its IT risk value falls between 351 and 650 or as a "high-risk" phase, if its IT risk value falls between 651 and 1000. The latter classification is based on a numeric scale ranging from 0 to 1000, with 1000 representing the highest possible risk value. The phases classified as "high-risk" phases give cause for concern.

The risk-analysis stage is aimed at identifying high-risk patient information routes (that is, *critical* patient information routes) in a typical health-care institution with a view to enhancing the information security of such institution.

Consider, for example, table 1:

The phases "Registration," "Preparation ward" and "Recovery ward" are singled out as being *critical phases* in this example, because they are classified as high-risk phases according to their respective IT risk values.

Those phases along a patient information route associated with high IT risk values need to be identified as being the *critical phases* along that route.

3.2 Consolidate the IT Risk Values of the Phases along Each Patient Information Route and List the *Critical Patient Information Routes* Accordingly (Stage 4 Task 2)

The RiMaHCoF methodology proposes a set of heuristics for consolidating the IT risk values for all the phases along a specific patient information route. These heuristics are summarised in table 2.

In order to more clearly illustrate the consolidation of the IT risk values for the phases along a specific patient information route, consider the hypothetical scenario sketched in table 3.1. According to this scenario there are three critical phases along the patient information route, namely the "registration," "preparation ward" and "recovery ward" phases. In other words, exactly 50% of the phases along the specific patient information route (that is, 3 out of 6) are deemed critical. The IT risk value for the patient information route based on this scenario is, therefore, equal to the *sum* of the following: *the average of the IT risk values of all critical phases along this patient information route* (that is, 775) *multiplied by a weight factor of 0.6* (that is, 465) *and the average of the IT risk values of all non-critical phases along this patient information route* (that is, 230) *multiplied by a weight factor of 0.4* (that is, 92). This results in an IT risk value of 557 and the route being classified as a "medium-risk" patient information route.

The aim of consolidating the IT risk values of all the phases along a specific patient information route is to obtain an overall IT risk value for that patient information route. Such risk value could then form the basis for identifying *critical patient information routes* in the health-care institution. In this way, the high-risk areas in the health-care institution can be pinpointed. This will, in turn, present management with a clear picture of the specific patient information routes to be followed in the health-care institution that need to be investigated when deciding on the implementation of security controls with a view to enhancing the IS of the health-care institution in question.

3.3 Construct and Explore "What-If" Scenarios that could Possibly Help to Reduce the IT Risk Values of the Critical Phases (Stage 4 task 3)

The likelihood of database files containing patient information being exposed to unauthorised parties can, for example, be considered as an event. Implementing security controls (also an example of an event), such as access control, could decrease the likelihood that these database files would be exposed. The events that take place in a typical health-care institution are not, therefore, executed in isolation but interact with and influence each other.

As was mentioned before, most consequences of the events occurring in a typical health-care institution are not easily quantified. Ideally, therefore, one wants a representation mechanism that can be used in a cognitive and intuitive manner to represent the relationships between these events. A graph structure, called a "Fuzzy Cognitive Map" (an "FCM"), is one example of such mechanism [14 - 17]. FCMs are fuzzy-graph structures that provide an expressive and flexible method of capturing and representing complex relationships in an intuitive manner. In case of an intuitive activity such as IT risk management, the FCM naturally represents the "human" way of thinking.

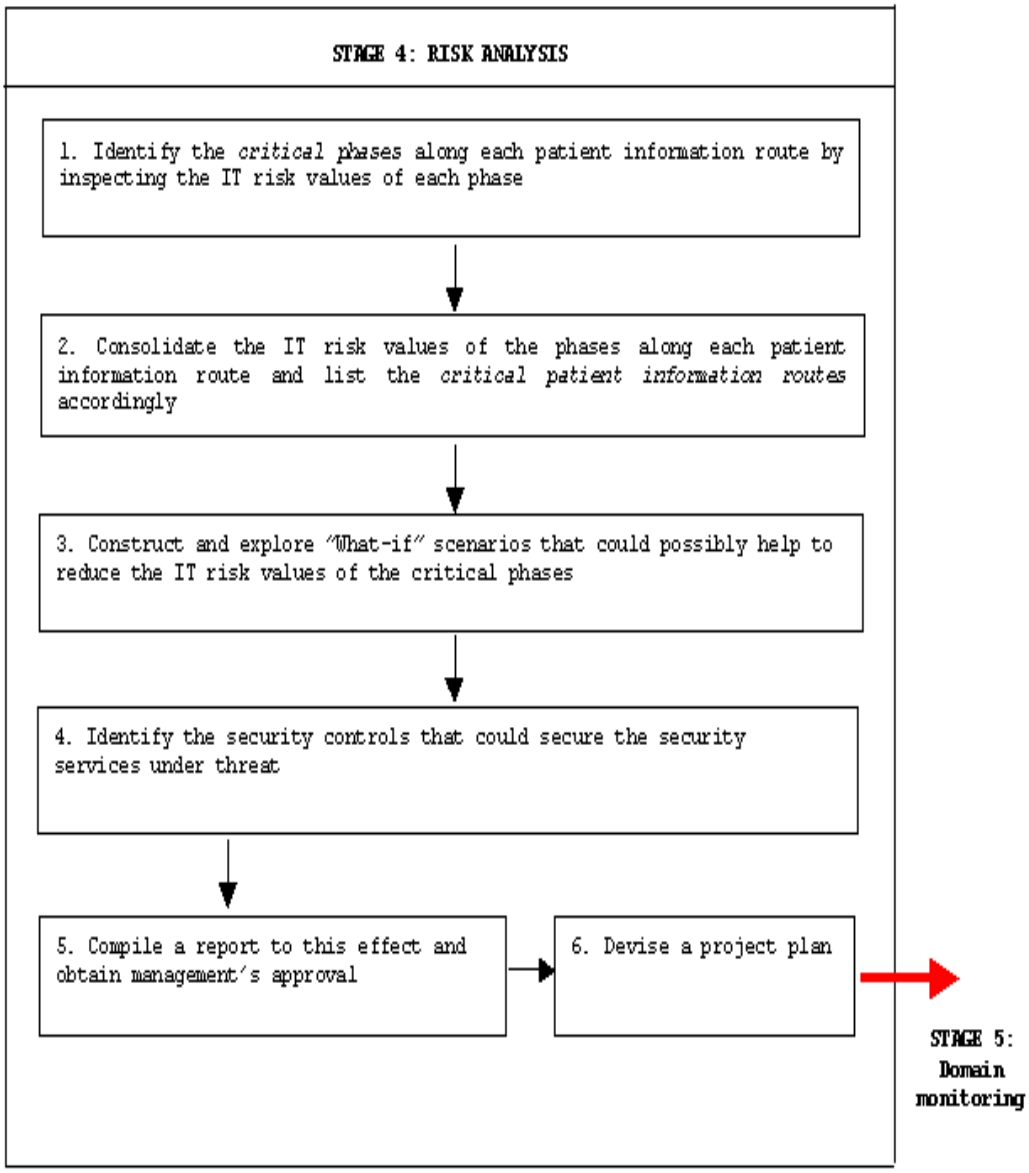


Figure 2: Stage 4: Risk analysis

Phase	IT risk value	IT risk category
Registration	710	HIGH
Preparation ward	850	HIGH
Operating theatre	220	LOW
Recovery ward	766	HIGH
Discharge	360	MEDIUM
Follow-up visits	111	LOW

Table 1: IT risk values for each phase effected along the route when a patient is admitted to hospital for an operation

Condition	IT risk value of patient route (R_{ROUTE})
Number of critical phases along patient information route $> 50\%$	$R_{ROUTE} = \sum_{i=1}^{m} R_i/m$, where m is the number of critical phases along the patient information route and R_i is the IT risk value of the i^{th} critical phase along the patient information route.
Number of critical phases along patient information route = 50%	$R_{ROUTE} = [(\sum_{i=1}^{m} R_i/m) * 0.6] + [(\sum_{j=1}^{n} R_j/n) * 0.4]$, where m is the number of **critical** phases along the patient information route n is the number of **non-critical phases** along the patient information route R_i is the IT risk value of the i^{th} **critical** phase along the patient information route R_j is the IT risk value of the j^{th} **non-critical** phase along the patient information route.
Number of critical phases along patient information route $< 50\%$ patient information route.	$R_{ROUTE} = [\sum_{i=1}^{m} R_i + \sum_{j=1}^{n} R_j]/p$,where p si the number of phases along the patient information route R_i is the IT risk value of the i^{th} **critical** phase along the patient information route R_j is the IT risk value of the j^{th} **non-critical** phase along the

Table 2: Heuristics as proposed by RiMaHCoF

3.3.1 Constructing Fuzzy Cognitive Maps (FCMs)

An FCM is used to represent the relationships between the events to be effected in a specific phase in a cognitive and intuitive way. An FCM consists of nodes which, in turn, represent the *events that may occur to some degree*, and edges that describe the *relationships* (causal flow) between these events. One of the functions that form part of the risk-analysis stage is determining the strengths of these relationships. The relationships have "fuzzy" strengths in the interval range [-1,1]. The strength of a relationship indicates the degree to which one event affects another. These strengths are determined intuitively.

Consider figure 3. Consider the relationship between the risk of patient information being exposed (C_6) and the number of communicating parties sharing that patient information (C_1). The *plus 0.8 relationship* between C_1 and C_6 implies, for instance, that if the number of communicating parties sharing patient information during the registration phase were to increase, then the risk of patient information being exposed during this phase would also increase by a degree of 0.8, that is, by 80%. If, by the same token, the number of communicating parties were to decrease, then the risk of patient information being exposed would also decrease to the tune of 80%. The strength of the relationship between the communicating parties sharing patient information and the risk of patient information being exposed is, therefore, 0.8. The other plus relationships work in the same way.

The minus relationships, on the other hand, indicate that the possibility of one event occurring increases while the possibility of another event occurring decreases, and vice versa. In this way, the minus 0.7 relationship between C_5 and C_3 implies that if the strength of security controls implemented for the registration phase were to increase, then the likelihood of database files containing patient information being exposed would decrease to the tune of 70%. The reverse is also true: if the strength of these security controls were to decrease, then the likelihood of database files containing patient information being exposed would increase by a degree of 70%. The strength of the relationship between the security controls and the exposure of database files containing patient information is, therefore, 0.7.

The final step in constructing the FCMs involves the specification of an activation threshold for each event. Such an activation threshold (indicated by the number in the concept node that represents the event) specifies the minimum strength to which the incoming relationship degrees must be aggregated in order to activate an event. In order for C_4, the exposure of paper files, to occur, the incoming relationships must be aggregated to a minimum of 0.8, that is, 80%. If, for example, the patient were to spend time during the registration phase (event C_2 occurs) and the doctors and nurses were to share the patient information (event C_1 occurs), then the incoming relationships (e_1, e_4) and (e_2, e_4) need to aggregate to at least 0.8 in order for the paper files to be exposed (C_4 occurs). The thresholds of the other events are determined in the same way. Like the strengths of the relationships between events, the activation thresholds are also determined in an intuitive manner.

3.3.2 Construct "What-If" Scenarios

A simple two-dimensional *edge matrix* can be used to explore various "What-if" scenarios in order to determine a

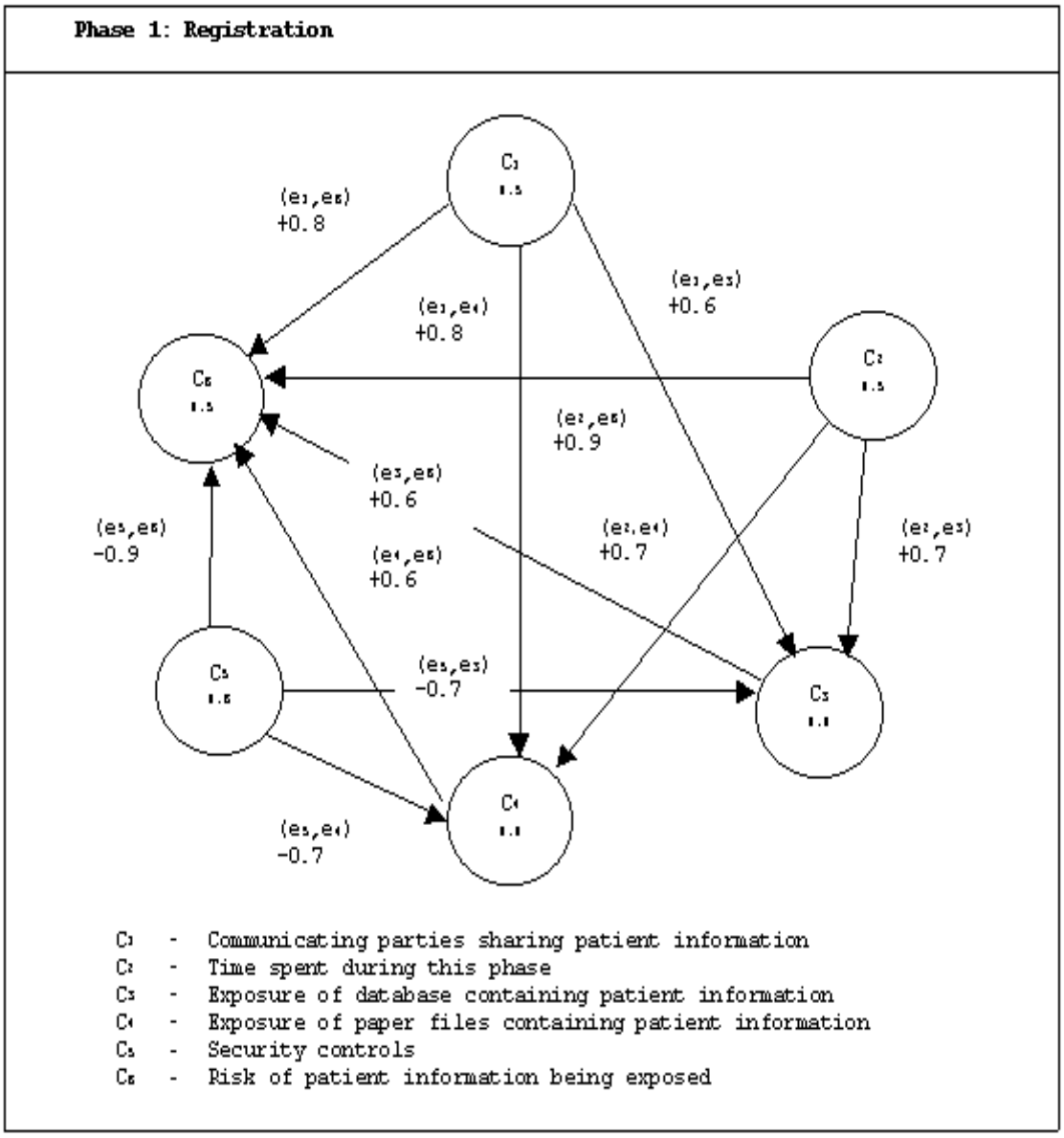


Figure 3: FCM representing the relationships between the events that take place during the registration phase of the patient information route to be followed when a patient is admitted to hospital

way in which either to decrease such risk value or to explore whether or not a certain scenario would increase the risk value. What would happen if, for instance, paper files containing patient information were to be exposed during a certain phase? "What-if" scenarios such as these need to be constructed for this purpose.

The edge matrix represents the strengths of the relationships between events. Following, an example of an edge matrix in figure 4.

The i^{th} row lists the connection strength of the edges (e_i, e_k) *directed out* from event C_i. The first row in the matrix indicates, for example, that the strength of the relationship (e_1, e_3) between C_1 ("number of communicating parties sharing patient information") and C_3 ("exposure of database files") is 0.6, that the strength of (e_1, e_4) between C_1 and C_4 ("exposure of paper files") is 0.8 and that the strength of (e_1, e_6) between C_1 and C_6 is 0.8.

Furthermore, C_i causally increases C_k if $(e_i, e_k) > 0$, decreases C_k if $(e_i, e_k) < 0$ and has no effect if $(e_i, e_k) = 0$. Event C_1 ("number of communicating parties sharing patient information"), for example, causally increases events C_3 ("exposure of database files"), C_4 ("exposure of paper files") and C_6 ("risk of patient information being exposed") to varying degrees, because $(e_1, e_3), (e_1, e_4)$ and (e_1, e_6) are all greater than 0.

Each event in an FCM turns one or more events on (1) or off (0). In order, for example, to model the "What-if" scenario, namely what would happen if, for instance, the paper files containing patient information were exposed to unauthorised parties during the phase under consideration, event C_4 ("exposure of paper files containing patient information") needs to be turned on, that is, to be set equal to 1. All other events remain at 0 (remain unchanged).

This input state can be represented by the state vector $[0\ 0\ 0\ 1\ 0\ 0]$, in other words, each event (node) in the FCM is represented by either a zero or a one in the state vector, depending on whether it be turned on or off. In our "What if" scenario, therefore, only the fourth element (representing C_4, that is, "exposure of paper files containing patient information") in the state vector has a value of 1. FCM input states such as these fire all the relationships in the FCM to some degree. This process will show how, in a fuzzy dynamic system, causal events affect each other to some degree as time goes by.

In order to model the effect of the input state $I_0 = [0\ 0\ 0\ 1\ 0\ 0]$ ("exposure of paper files containing patient information") on the FCM for the registration phase along the patient information route to be followed if a typical patient were to be admitted to hospital, the following technique is used to determine the new state (on or off) for each event C_i each time (t_{n+1}) an input state fires the FCM.

$$C_i(t_{n+1}) = S(\sum_{K=1}^{N} e_{ki}(t_n) C_k(t_n))$$

This technique involves a matrix vector multiplication to transform the weighted input to each event C_i. In the above equation, $S(x)$ is a bounded signal function, indicating whether C_i be turned off (0) or on (1). (A detailed explanation of this technique falls outside the scope of this article: consult Bart Kosko's book, *Fuzzy Engineering*, for more information [15]).

The above equation is applied to the FCM with initial input state $[0\ 0\ 0\ 1\ 0\ 0]$ (that is, C_4, "exposure of paper files containing patient information," is turned on) as follows: $I_0 = [0\ 0\ 0\ 1\ 0\ 0]$, then

$$\begin{aligned}
I_0E_c &= [\sum_{k=1}^{6} I_{0k}e_{k1}, \sum_{k=1}^{6} I_{ok}e_{k2}, \sum_{k=1}^{6} I_{0k}e_{k3}, \sum_{k=1}^{6} I_{ok}e_{k4}, \\
&\quad \sum_{k=1}^{6} I_{0k}e_{k5}, \sum_{k=1}^{6} I_{ok}e_{k6} \\
&= [0*0+0*0+0*0+1*0+0*0+0*0, \\
&\quad 0*0+0*0+0*0+1*0+0*0+0*0, \\
&\quad 0*0.6+0*0.7+0*0+1*0+0*-0.7+0*0 \\
&\quad 0*0.8+0*0.7+0*0+1*0+0*-0.7+0*0 \\
&\quad 0*0+0*0+0*0+1*0+0*0+0*0 \\
&\quad 0*0.8+0*0.9+0*0.6+1*0.6+0*-0.9+0*0] \\
&= [0\ 0\ 0\ 0\ 0\ 0.6] \\
&\xrightarrow{0.5} I_1 = [0\ 0\ 0\ 1\ 0\ 1]
\end{aligned}$$

where I_{0k} refers to the k^{th} element in the state vector $I_0 = [0\ 0\ 0\ 1\ 0\ 0]$; e_{k1} refers to the entry in the k^{th} row in the *first* column of the edge matrix E; e_{k2} refers to the entry in the k^{th} row in the *second* column of the edge matrix E, and so forth.

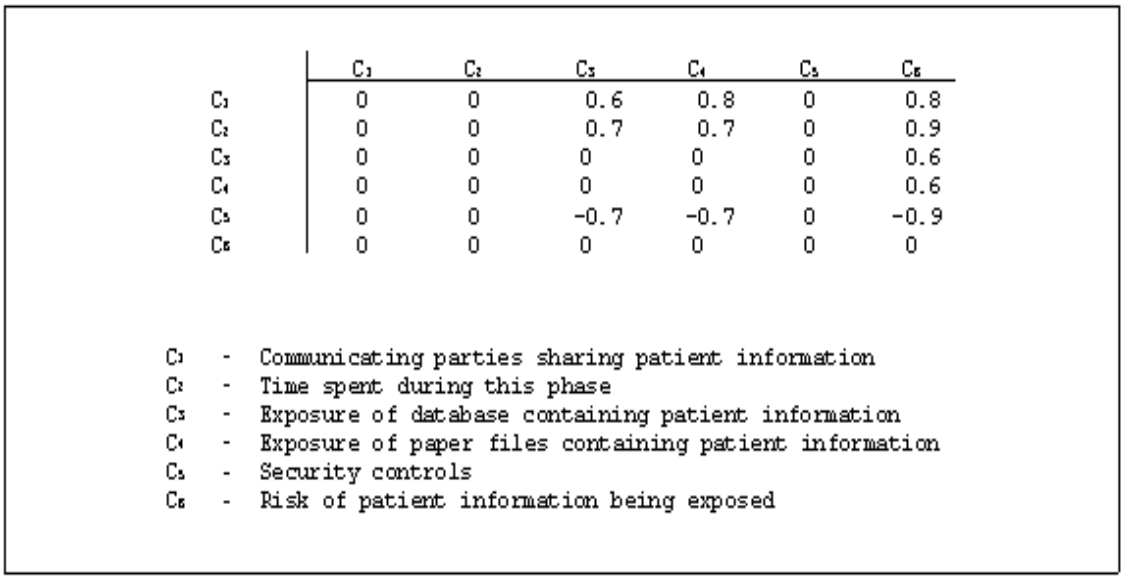
The arrow represents a threshold operation, with 0.5 the assumed threshold value. In other words, all entries in the state vector I_0E_c with values higher than or equal to 0.5 are turned on. In addition, C_4 is kept on, since we want to model the effect of a *sustained* threat of paper files containing patient information being exposed during the registration phase.

The following conclusion can, therefore, be made: when I_0 fires the FCM (that is, when I_0 occurs), then event C_6 ("the risk of patient information being exposed") is turned on. The next input state firing the FCM will, therefore, be $I_1 = [0\ 0\ 0\ 1\ 0\ 1]$.

The equation formulated earlier is applied to the FCM with input state I_1 in the same way:

$$\begin{aligned}
I_0E_c &= [\sum_{k=1}^{6} I_{0k}e_{k1}, \sum_{k=1}^{6} I_{ok}e_{k2}, \sum_{k=1}^{6} I_{0k}e_{k3}, \sum_{k=1}^{6} I_{ok}e_{k4}, \\
&\quad \sum_{k=1}^{6} I_{0k}e_{k5}, \sum_{k=1}^{6} I_{ok}e_{k6} \\
&= [0\ 0\ 0\ 0\ 0\ 0.6] \\
&\xrightarrow{0.5} I_2 = [0\ 0\ 0\ 1\ 0\ 1] = I_1
\end{aligned}$$

This results in C_6 remaining on. The next input state $I_2 = [0\ 0\ 0\ 1\ 0\ 1]$ is, therefore, equal to the previous input state I_1. For this reason, the FCM converges to a fixed point I_2 that turns on C_6 ("the risk of patient information being exposed"). This means that the exposure of paper files during the registration phase would increase the risk of patient information being exposed (C_6).



	C_1	C_2	C_3	C_4	C_5	C_6
C_1	0	0	0.6	0.8	0	0.8
C_2	0	0	0.7	0.7	0	0.9
C_3	0	0	0	0	0	0.6
C_4	0	0	0	0	0	0.6
C_5	0	0	-0.7	-0.7	0	-0.9
C_6	0	0	0	0	0	0

C_1 - Communicating parties sharing patient information
C_2 - Time spent during this phase
C_3 - Exposure of database containing patient information
C_4 - Exposure of paper files containing patient information
C_5 - Security controls
C_6 - Risk of patient information being exposed

Figure 4: An edge matrix representing the strengths of the relationships between the various events that take place during a critical phase

The foregoing example illustrates how an edge matrix constructed from an FCM can be used to explore "What-if" scenarios.

3.3.3 Identify the Security Services under Threat

The use of the foregoing modelling technique results in the *identification* of the security services (identification & authentication, confidentiality, authorisation, integrity and non-repudiation) under threat from a specific scenario, while *negating* the security services not exposed to risk. Modelling "What-if" scenarios by making use of FCMs can, naturally, greatly facilitate decisions on the implementation of security controls for a specific phase along a patient information route. If, for example, the confidentiality of patient information were under threat, security controls such as passwords, biometrics or encryption could be implemented in order to secure the information.

Consider the previous example (discussed under paragraph 3.3.2), which hinges upon the exploration of a "What-if" scenario. The outcome of the scenario was that the exposure of paper files would indeed increase the risk of patient information being exposed, the reason being that the exposure of paper files poses a threat to some of the critical security services rendered in the health-care institution in question. If the paper files were exposed to an unauthorised person, such person would compromise the patients' privacy by gaining unauthorised access to their sensitive patient information. The *confidentiality* of the patient information would, therefore, be under threat. Furthermore, an unauthorised person gaining access to patient information could also alter such information, thereby compromising its *integrity*. In the realm of a health-care institution, any such alteration could, naturally, have fatal consequences. If, for example, a patient were to be treated with medicine that he/she were allergic to as a result of inaccurate patient information, he/she could die.

In the foregoing example, confidentiality and integrity have been identified as the security services being under threat from the exposure of paper files. It is essential in this case, therefore, to implement security controls in order to protect the confidentiality and integrity of the patient information during the phase under consideration.

4 Conclusion

In this paper, a risk-management methodology specifically tailored for the health-care environment has been proposed. The aim of the methodology is to enhance risk management in the specific domain of health care by following a cognitive fuzzy approach to the assessment and analysis of IT risks. The advantage of using this approach is that the intuitive nature of human observation, which forms the basis of any risk assessment, and the vagueness regarding the decision-making process with respect to securing patient information, are both taken into account when assessing and analysing IT risks.

The risk-analysis (fourth) stage of the RiMaHCoF methodology has been discussed in detail in this paper. The principal aim of this stage was to help manage IT risks by facilitating the decision-making process. This was achieved by first identifying the **critical phases** (that is, the high-risk phases) along each patient information route by using the IT risk values calculated for each phase during the risk-assessment stage. Having identified these critical phases, **the critical patient information routes** (high-risk patient information routes) could be identified by consolidating the IT risk values of all phases comprising the specific patient information route. In this way, the **high-risk**

areas in a health-care institution can be pinpointed.

Furthermore, the cognitive fuzzy-modelling approach followed by the RiMaHCoF methodology also enables the investigation of these critical areas with a view to enhancing the information security of the health-care institution in question. This is achieved by making use of an FCM and by constructing various "What-if" scenarios to determine which of them might lead to the increase/decrease of IT risk incidence. In this way, the decision-making process with respect to enhancing the overall information security of a health-care institution is facilitated.

The proposed IT risk-management model could, however, be adapted to suite organisations in other business sectors and industries. The patient information route, which plays a pivotal role in the proposed model, might, for instance, be replaced by a transaction route in business enterprises. In this way, organisations in other sectors or industries may also benefit from the proposed model.

References

[1] W Raghupathi, W. 1997. Health Care Information Systems. Communications of the ACM, 40(8): 81-82, Aug.

[2] Anderson, J.G. 1997. Clearing the way for physicians' use of clinical information systems. Communications of the ACM, 40(8): 83-90, Aug.

[3] Luft, H.S. & Miller, R.H. 1996. FHF research studies results presented in Boston: The role of information in the changing models of managed care, October. (Federation of Health Funds Newsletter.)

[4] Barber, B, Treacher, A & Louwerse, K. 1996. Towards security and medical telematics. Amsterdam : IOS Press. 252 p. (Studies in Health Technology Informatics Vol. 27)

[5] Ginneken, A.M. Computer-based patient records. (In Van Bemmel, J.H. & McCray, A.T., eds. Yearbook '94 of Medical Informatics. Advanced communications in health care. Schattauer. p. 173-175).

[6] Kohn, P. 1995. Computer-based patient record systems: The future of health care is in digital technology. INFORM, 38-46, Nov/Dec

[7] Labuschagne, L. 1992. "Inligtingsekerheid, met spesifieke verwysing na risiko-ontleding." Rand Afrikaans University. Johannesburg, South Africa (dissertation (MCom) - RAU).

[8] Pfleeger, C.P. 1997. Security in computing. United States of America: Prentice-Hall International Inc. 574 p.

[9] Badenhorst, K.P & ELOFF, J.H.P. 1989. Framework of a methodology for the life cycle of computer security in an organisation. Computers & Security. 8: 433-442.

[10] Barber, B. & Davey, J. The use of the CCTA risk analysis and management methodology [CRAMM] in health information systems. (In Degoulet, P., Lun, K.C., Piemme, T.E. & Rienhoff, O., eds. MEDINFO '92. North-Holland: Elsevier Science Publishers BV. p. 1589-1593.)

[11] Warren, M.J., Furnell, S.M. & Sanders, P.W. 1997. ODESSA: A new approach to healthcare risk analysis. (In Proceedings of the IFIP TC11 thirteenth international conference on information security. Great Britain: Chapman & Hall. p. 391-401.)

[12] Eloff, J.H.P. & Smith E. 1998. Modelling risks in a health-care institution. (In Proceedings of the XV IFIP World Computer Congress. Vienna: Austrian Computer Society. P. 592-598.)

[13] Eloff, J.H.P. & Smith E. 2000. Cognitive fuzzy modeling for enhanced risk assessment in a health care institution. IEEE Intelligent systems & their applications. 15(2): 69-75.

[14] Cox, E.D. 1994. The fuzzy systems handbook: A practitioner's guide to building, using and maintaining fuzzy systems. Boston: Academic Press. p 515

[15] Kosko, B. 1997. Fuzzy engineering. New Jersey: Prentice-Hall. p 549.

[16] Kosko, B. 1986. Fuzzy cognitive maps. International Journal of Man-machine Studies. 24: 65-75.

[17] Cox, E.D. 1995. Fuzzy logic for business and industry. Massachusetts: Charles River Media Inc. p 601.