Research and Application of Contingency Plan Based on Hospital Network and Information System Security

Xiaoyan Ma
College of information engineering, Taishan Medical University, Tai'an 271016, China

Hao Zou
Tai'an Power Supply Company, Tai'an 271000, China

Yujuan Li
College of information engineering, Taishan Medical University, Tai'an 271016, China

Received: August 24, 2011 Accepted: September 15, 2011 Published: November 1, 2011
doi:10.5539/cis.v4n6p105 URL: http://dx.doi.org/10.5539/cis.v4n6p105

Abstract

Network and information system play irreplaceable roles in hospital daily administration. The system is so huge that any fault during its operation will cause serious consequences to hospital administration and bring immeasurable loss to the hospital; therefore, to set up corresponding contingency plans becomes increasingly important. From the perspective of management, the article puts forward contingency plans in terms of following three aspects: hospital network system, office automation and hospital information system.

Keywords: Contingency, Hospital information system security, Network

Hospital network and information system is an application information system which makes use of computer and its network communication equipment and technology to automatically collect, process, store, transmit and use related information inside and outside hospital to serve clinical, teaching, scientific research and administration. With gradual development of the application of hospital network and information system in breadth and depth, the information process of hospital business is increasingly relying on the normal operation of hospital information system, which proposes higher request for the stability and security of the operation of hospital network and information system. To identify the risk links and factors in hospital information system security from omni-directions and multi-angles and set up strict contingency plans strategy may improve the contingency ability to deal with emergencies in hospital network and information system, effectively prevent and cope with network and information security emergencies correctly and rapidly, reduce influence and losses to the maximum so as to guaranteeing the safe and stable operation of network system.

1. The problems of hospital network and information system security

The contents of security include physical security and logic security. Physical security means that system devices and related facilities receive physical protection, avoiding system destruction, and data and information loss. Logic security is the integrity, privacy and usability of data and information. Integrity means that information cannot be revised illegally and the data is consistent; Privacy means that higher-level information may be delivered to lower-level objects and subjects only in the situation of authorization; Usability means that the normal requests of legal users can obtain response services timely, correctly and securely; therefore, the failure can be subdivided into following aspects:

1.1 Network breakdown

Network access has large arbitrariness, hospital network can visit each other freely, and information exchange and sharing are unobstructed. Entire network resource can be visited arbitrarily in any work site, so data can be stolen illegally easily.

1.2 The security of hardware and software system

The maintenance of the privacy, authenticity and integrity of information; the bugs of network and software or maintenance not in time will cause threats to data security; main device, operation system, middleware and

database software faults; the failure such that application program stops service; the data in application system loses.

1.3 Hostile attack

Large area of viruses breaks out; worms, Trojan horse programs, harmful code et.al; illegal invasion or organizational attacks; information distribution and service websites are subjected to attack and destroyed.

The problems of security also include environmental failure such as power supply of equipment room and air conditioner et.al, and other reasons such as natural disasters or man-made destruction et.al.

2. Basic principles of contingency plan

2.1 Prevention first and expectation ahead

Adhere to the guideline "safety first, prevention foremost". Make good plan, contingency resources preparation and guarantee measures preparations as well as put information system contingency incidents expectation ahead to cope with various information and network security sudden incidents. Make full use of current resource, formulate scientific contingency plan, timely organize and carry out contingency training and drilling, improve the ability to response and deal with various information and network security sudden incidents.

2.2 United command and manage at different levels

Through setting up contingency leader group and work group at different levels, establish systematic contingency organizations at different levels. Organize and carry out various contingency work including incidents prevention, contingency disposal, recover to operate and incidents publication. The formulation, revision of contingency plan and contingency disposal should definite the departments or units that take a lead and their duties and responsibilities related to the departments and units. In the process of contingency disposal, the departments and units that take a lead should initiatively coordinate various related aspects and participate in the unit to listen to the leader as well as keep in step with them.

2.3 Effectively organize and confirm the emphasis

Increase monitoring and contingency work in important system; effectively organize and bring the role of various contingency staff and resources into play, ensuring information is delivered in time and accurately and effectively control loss; to confirm emphasis, combine prevention with disposal and response promptly.

2.4 Technological support and sound mechanism

Based on making full use of current information resource, system and equipment, adopt advanced and suitable prediction, prevention, early warning and contingency disposal technology to improve and perfect contingency disposal equipment, facilities and methods, improve technological support abilities to cope with information and network security emergencies, really improve contingency disposal staff's quality, security protection awareness and scientific command ability and set up sound and effective mechanism to cope with information and network security emergencies.

3. Contingency disposal solution to network and information system

The contingency disposal of hospital network and information system include: information room, network, server, important business information system and general business information system. Important business information system includes hospital information system (HIS), office automation, and general business information system is the other business information system. Here the authors give corresponding contingency strategy about network, HIS and office automation.

3.1 The contingency plan of network system failure

Set up contingency group and immediately report information system contingency leader group; at the same time, prepare necessary drawing materials, backup medium and spare parts(room for spare parts, whether spares meet the need). Check the situations including appearance, power source and light indicator of core switch. For example, if it belongs to the fault of device power source, it should start room environment contingency plan. Otherwise confirm the scope of network and specific faults characteristics influenced and decide faults classification and points: whether it is the fault of firewall; if it is and cannot be repaired, central exchange will be connected to ATM directly, avoiding firewall contingency plan. Meanwhile, revise the configuration of central exchange and connect the switchboard of aggregation layer to central exchange; at the same time, revise the configuration of the switchboard of aggregation layer, ensuring that important users may have access to the website. Log on core switch, check the situations of the configuration and operation of switches and deal with them respectively. If unable to log on, you should review the logs through port logging.

1) If core switch is normal, check network channel or fiber optic jumper

2) If configuration files make mistakes, re-configure or re-load backup configuration

3) The faults of switchboard hardware: if there are spare parts, please change it; otherwise contact the manufacturer for technical support.

3.2 The contingency plan of office automation system server failure

Set up contingency group and immediately report information system contingency leader group; at the same time, prepare drawing materials, backup medium and spare parts. The relative responsible officer in the work group should immediately find out the reasons and classify them according to the phenomenon of the failure. If it belongs to office automation software failure, check tooltips in office automation service process and solve it; otherwise restart the computer and reload office automation system ; judge the reason for failure according to error message and remove it; if not, backup the latest data and then reinstall office automation software system. If it is server operating system failure, carry out corresponding operation according to the phenomenon of the failure; if not, on the basis of data backup, reinstall operating system and related software, reinstall office automation system, restore the latest data backup and system operation. If it belongs to server hardware failure, immediately change the damaged part with spare part if it is able to recover automatically. If not, please contact with the supplier immediately and ask them to send maintainer to repair it. If it is caused by network failure, please start network contingency plan. If the device cannot recover within four hours, report contingency leader group and notify each subordinate units of postponing to upload reported dat.

3.3 The contingency plan of information system security

The responsible officer in contingency work group should find out the reason for the security events and classify them according to the phenomenon of the failure. If it is the reason of virus infection, immediately isolate the infected host, backup host data, search and kill the virus and strengthen monitoring network host. For hacker attack, if it is within the intranet, immediately isolate the attacked server and protect the site; at the same time, search the source of attack and directive recover and rebuild the damaged system. If it is from outside network, firstly suspend the connection with the outside; meanwhile search the source and check where the bugs are in the security strategy that firewall prevent attacks.

4. Conclusions

Hospital contingency plan not only explores from secure, high-efficiency and accessible network environment in the system, but also continuously perfects network security measures and reduces the occurrence of data loss caused by various failures as possible as it can, in order to ensure that hospital information system operates in secure state. With practical contingency plan, if its role is brought into play really when information security events happen, emergency drilling work must be attached more importance. Emergency drilling is an important link in perfecting contingency plan and bringing its role into play. The next step should make plans for emergency drilling scientifically and organize emergency drilling regularly.

References

Chu, Yingguo, et al. (2009). Research and Practice on Network and Information Security Contingency Plan. *Computer Era*, 12(1), 18.

Liu, Qing. (2008). Hospital information system security maintenance and administration. *Medicine information*, 10(21), 10.

Wang, Jingming. (2004). Make use of digital method to improve the level of hospital administration. *HOSPITAL ADMINISTRATION JOURNAL OF CHINESE PEOPLE'S LIBERATION ARMY*, 11(4), 332.

Zhang, Dianyong, et al. (2005). Design and application of contingency plans based on hospital information network failure. *HOSPITAL ADMINISTRATION JOURNAL OF CHINESE PEOPLE'S LIBERATION ARMY*, 12(1), 90.

Zhao, Chunxiao. (2007). Discussion on the management of hospital information system. *Guide of China Medicine*, 7(10), 551.

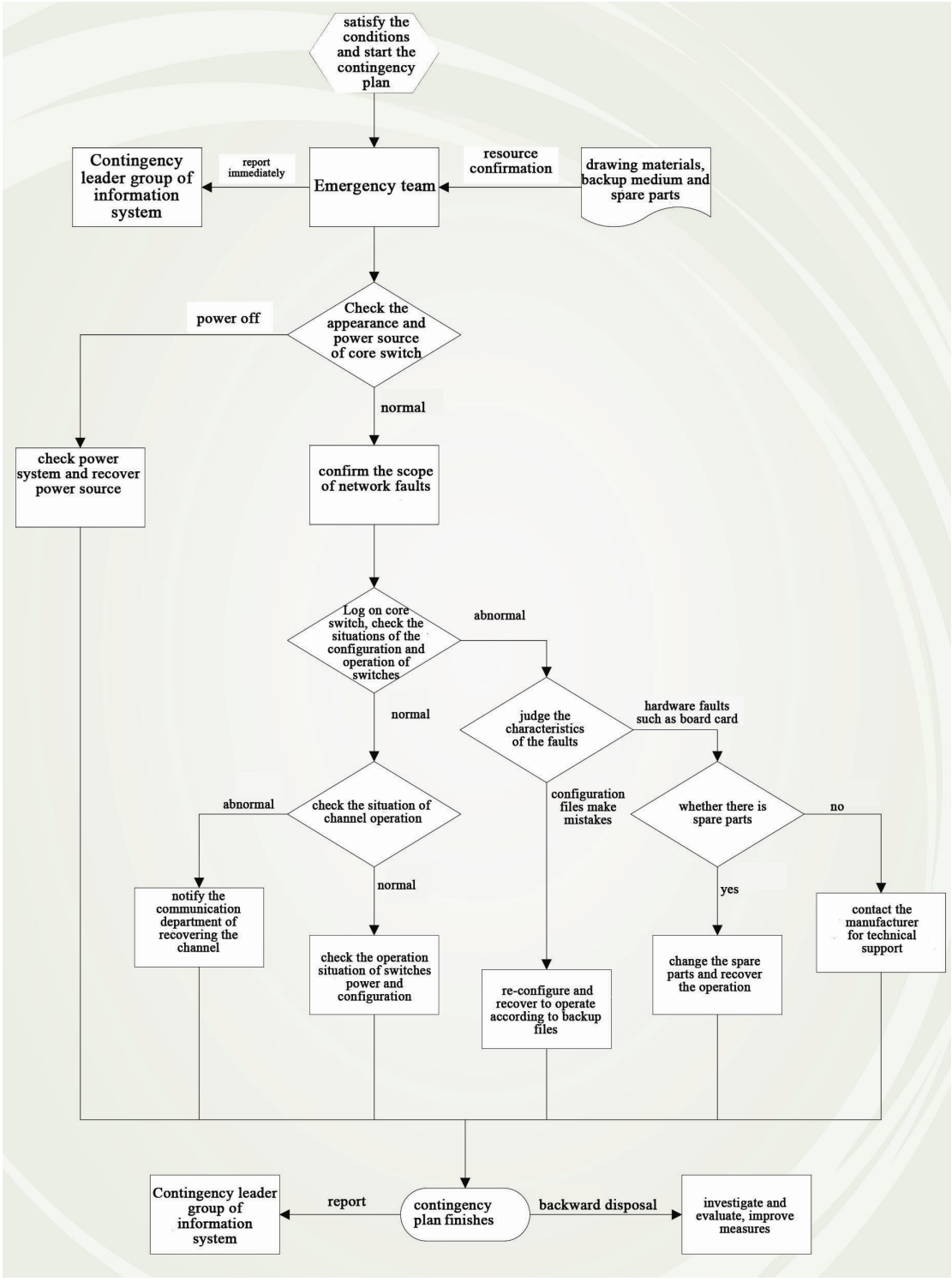

Figure 1. The flow chart of contingency plan based on network system fault

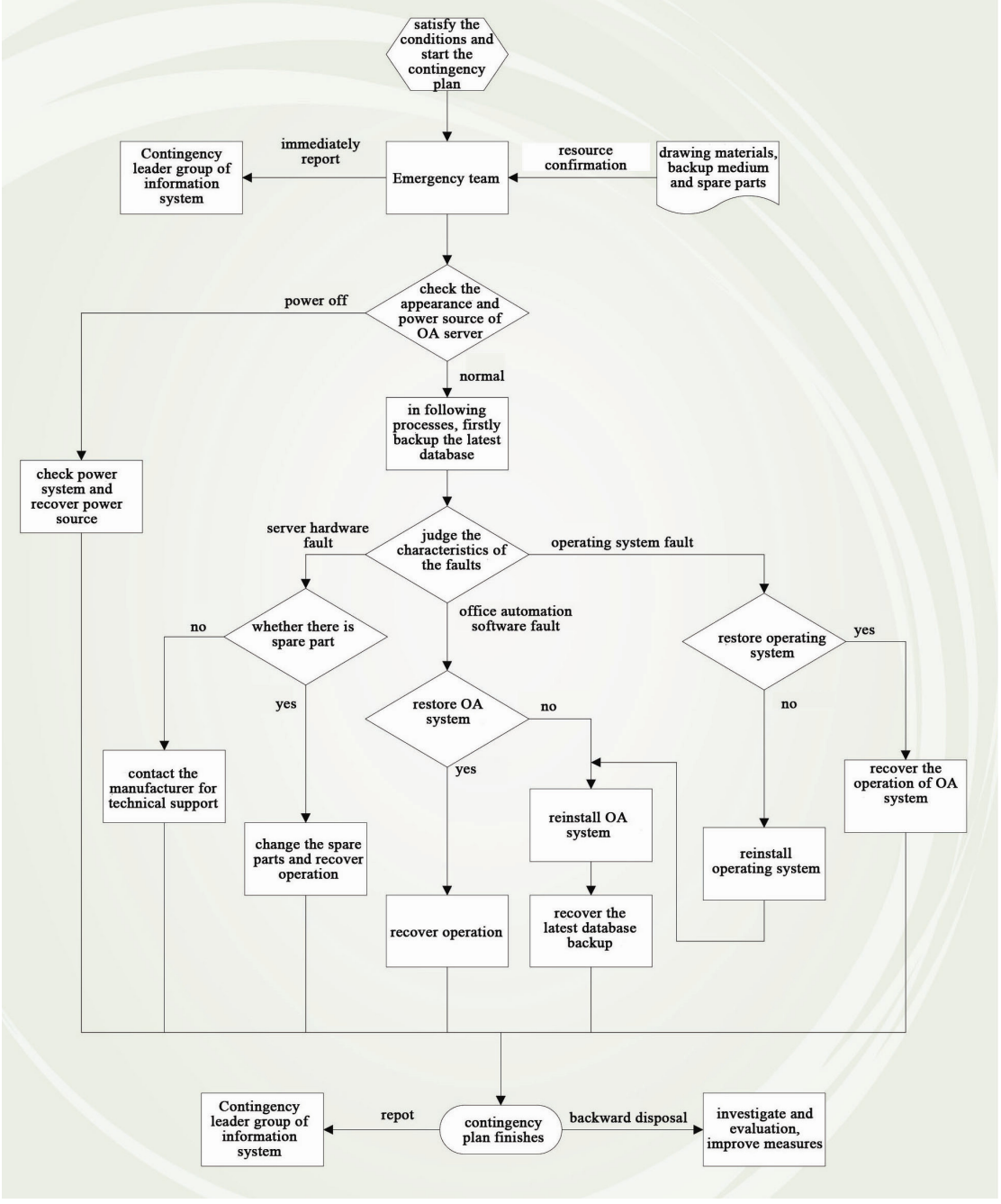

Figure 2. The flow chart of contingency plan based on office automation server fault

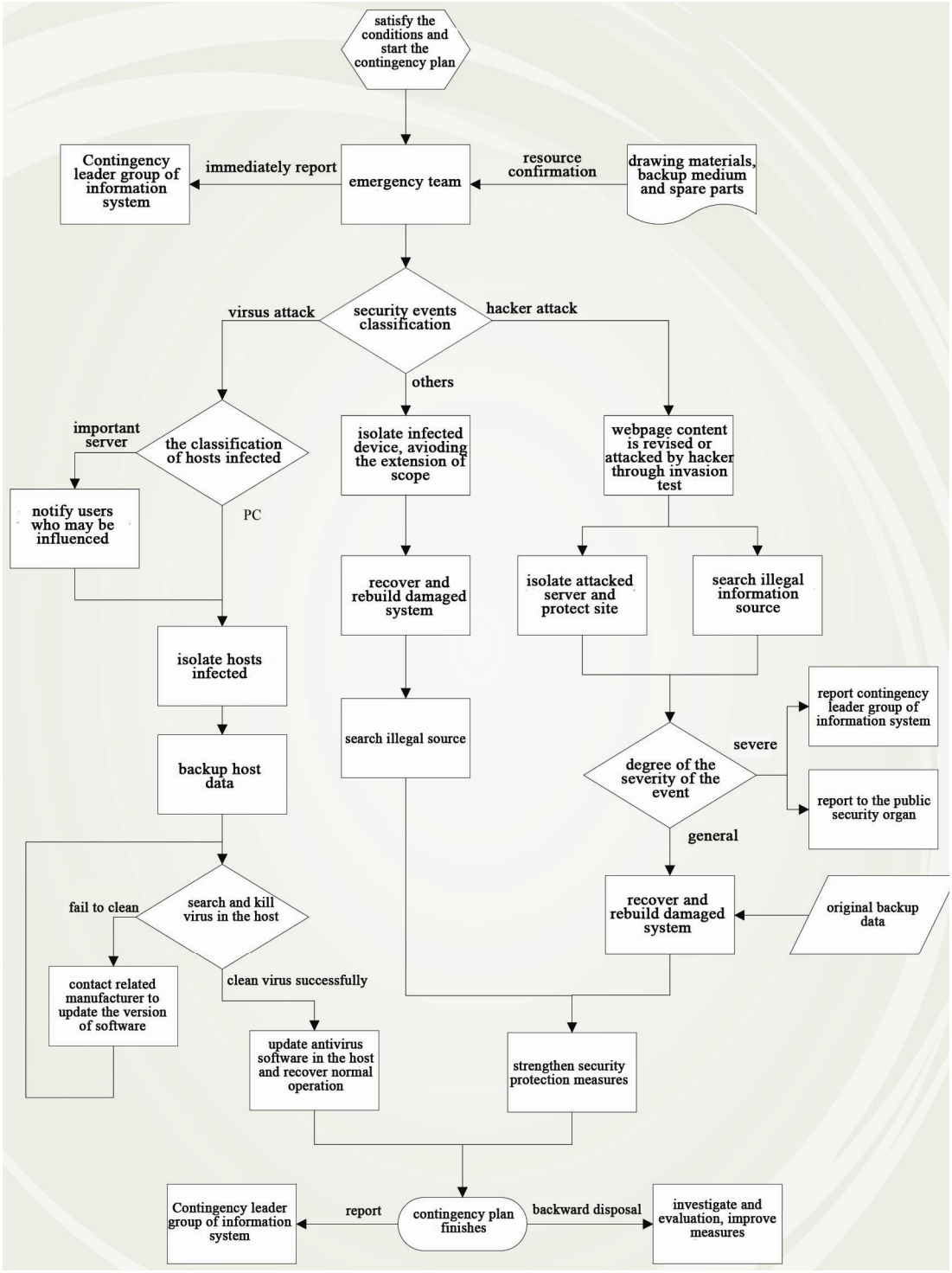

Figure 3. The flow chart of contingency plan of information system security