MOBILE HEALTH CARE SYSTEM E-LEARNING SECURITY SYSTEM DESIGN

Alex STEFAN

Bloomfield College, Bloomfield, New Jersey, USA

***Abstract**: The Mobile Health Care (MCHC) System has an e-learning component, to train IT managers in understanding the IT security policies and strategies, applied on real organizations, like for-profit provider of primary, acute and emergency care to a rural population in a 50 mile radius. The MCHC e-learning system can be also assumed as a remote control system, used for testing security algorithms in the designing system process.*

***Keywords**: e-learning, security systems, security algorithms.*

1. INTRODUCTION

Our task is to move our patient care system into the 21st century so that we continue to provide outstanding care, while maximizing revenue, to the following customers:

- Clinic, acute and emergency patients at our central location
- Satellite clinics in the surrounding community
- Outpatients and chronic care patients being treated at home
- Emergency patients in transit by ambulance

This requires secure information transfer between multiple user groups, accessing multiple applications via both wired and mobile devices, connected within the MCHC complex and remotely over the Internet.

The Mobile Health Care was design fist like an e-learning system to provide a better idea for the next step, implementation with the cooperation of the IT and security managers.

Concept of Operation

The patient data systems consist of the following:

- Patient identification
- MCHC Patient Healthcare departmental data will be assumed also as RCHC data (remote control health care)
  - Treatment history
  - Scheduling
  - Procedures, tests and results
  - Test and implant device communications
- Health Care Provider treatment plans and payment for treatments.
- Insurance providers
  - Payment authorization (billing is not directly handled by this system)
  - Treatment plan and outcome database.

Users will access the system through the following methods:

- Patients
  - Remote locations
    - Personal computers
    - Future generation m smart phones, capable of operating via wifi and VOIP.
  - Within the MCHC complex
    - Terminals in patient rooms connected client-server over the LAN.
- CHC personnel
  - Client-server over the LAN
  - Client-server over the Internet for outsourced billing coding.
- Satellite Healthcare providers
  - Within the MCHC complex
    - workstations in the treatment and testing areas
    - Future generation smart phones, capable of operating over WIFI and VOIP
  - Remotely

- Personal computers
- Smart phones

- Insurance providers
  - Remotely over the Internet

- Surgically implanted appliances and portable medical test devices
  - Remotely over the Internet
  - Client-server over the LAN within MCHC complex.

2. e-LEARNING SYSTEM SECURITY & SENSITIVITY RISK PROPOSAL

The e-Learning Security & Sensitivity Policy is intended to help MCHC employees to determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of MCHC without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction.

It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect MCHC Confidential information.

All MCHC information is categorized into two main classifications:

- MCHC Public
- MCHC Confidential

Table 1 MCHC Descriptive Security Policies Design for e-Learning System (extract)

Threat agents	IT ASSET AT RISK	Security Requirements	SECURITY POLICY
MCHC Employee	Patients Info	SR1: protect patients database from being seen by outsiders/unauthorized insiders SR2: protect the encrypted backup database from being seen by outsiders/ unauthorized insiders	- Information Sensitivity Policy - Employee Internet Use Monitoring and Filtering Policy - Network Support Policy - Remote Access Policy - Acceptable Use Policy - Password Policy - Acceptable Encryptions / Mobile Device Encryptions Policy - Email Use (retention, forwarded, instant messenger) Policy - Database Password Policy
WIRELESS Employee	Wireless Internal Access	SR1: protect patients database from being seen by outsiders/unauthorized insiders /wireless WPA/no broadcast SR2: protect the encrypted backup database from being seen by outsiders/ unauthorized insiders	• Information Sensitivity Policy • Wireless Device Policy • Employee Internet Use Monitoring and Filtering Policy • Network Support Policy • Remote Access Policy • Acceptable Use Policy • Password Policy • Acceptable Encryptions / Mobile Device Encryptions Policy • Email Use (retention, forwarded, instant messenger) Policy • Database Password Policy

HACKER	Wireless Sensitive Data	SR1: protect patients database from being seen by outsiders/unauthorized insiders /wireless WPA/no broadcast SR2: protect the encrypted backup database from being seen by outsiders/ unauthorized insiders SR2d: wireless monitoring	Information Sensitivity Policy Wireless Device Policy Employee Internet Use Monitoring and Filtering Policy Network Support Policy Remote Access Policy Acceptable Use Policy Password Policy Acceptable Encryptions / Mobile Device Encryptions Policy
MCHC MEDICAL ERRORS	MCHC Medical Practice	(covered SR15, SR16) (covered by SR19, SR17)	Personal Communication Devices and Voicemail Policy Acceptable Use Policy
System Admin	Power Server Loss	(covered SR15, SR16) (covered by SR19, SR17)	Acceptable Use Policy

Table 2 MCHC – e-Learning System Risk Management & Security Policies (extract)

Threat agents	IT ASSET AT RISK	RISK MANAGEMENT	SECURITY POLICY
MCHC EMPLOYEE	Patients Info	- Encryption stored MCHC P, HCPT - Daily backup MCHC P, HCPT, PTS, HCPT - OS patch - Firewall installed and maintain - Antispyware installed and maintain	Information Sensitivity Policy Employee Internet Use Monitoring and Filtering Policy Network Support Policy Remote Access Policy Acceptable Use Policy Password Policy Acceptable Encryptions / Mobile Device Encryptions Policy Email Use (retention, forwarded, instant messenger) Policy Database Password Policy
HACKER	Health care provider info	Antispyware update Employee contract of confidentiality Background check for System Administrator	Virtual Private Network Policy Ethics Policy Personal Communication Devices and Voicemail Policy Acceptable Use Policy
MCHC MEDICAL ERRORS	MCHC Medical Practice	Employee contract of confidentiality Logging updates and monitoring Logging layers with monitoring access Backup and encrypt sensitive data	Personal Communication Devices and Voicemail Policy Acceptable Use Policy
System Admin	Power Server Loss	Antispyware update Employee contract of confidentiality Background check for System Administrator Logging update and monitoring access	Acceptable Use Policy

3. e-LEARNING SYSTEM SECURITY RISK PROPOSAL ALGORITHM (EXTRACT)

The risk analyses was made by using a risk score calculation (proposal algorithm) over the MCHC Security Policy, an audit algorithm after the Security Policies were implemented.

The following steps have to be followed for risk score calculations:

- Decide the risk level of each item. The risk level of the item indicates its relative importance.
- Numerical value assign for the risk level:
  - Very High: 4;
  - High: 3;
  - Medium: 2;
  - Low: 1.
- If the response to the item is "Yes", give the "Yes Details. This could take up any of the given three values: "Planned/Just started", "partially completed" and "Fully implemented".
- The final risk score for an item is calculated as follows:
  - If the response is "NO" then the risk score is determined by the Risk level as follows:
    - If risk is "Very High" than the score is 4;
    - If risk is "High" then the score is 3;
    - If the risk is "Medium" then the score is 2;
    - If the risk is "Low" then the risk is 1.
  - If the response is "Yes" then the risk score is determined by both the risk level and the "Yes Details" as follows:
    - If risk is "Very High" than the score is 4* ("Yes Details" weight);
    - If risk is "High" then the score is 3* ("Yes Details" weight);
    - If the risk is "Medium" then the score is 2 * ("Yes Details" weight);
    - If the risk is "Low" then the risk is 1* ("Yes Details" weight);

Where "Yes Details" weights are the followings:

"Planned/Just started": weight 0.5

"Partially completed": weight 0.25

"Fully implemented": weight 0.

"Risk Upper Limit" is the maximum risk posed by an item, is used to calculate the "Percentage Risk Abated (%RA)".

ORGANIZATION: MCHC	RESPONSE	"YES" DETAILS	RISK	RISK SCORE	
SECURITY POLICY	YES NO N/A	- Planned/Just started - Partially completed - Fully implemented	VERY HIGH HIGH MEDIUM LOW	Results	RISK UPPER LIMIT
Have the Information Security Policies been issued to all employees, including third party personnel and contractors?	Yes	Planned/Just started	VERY HIGH	2	4
Have all employees formally acknowledge adherence to the Information Security policies?	Yes	Partially completed	VERY HIGH	1	4
Are all users required to sign an Internet usage and responsibility agreement that acknowledge compliance with Internet policy	NO		VERY HIGH	4	4
TOTAL				**19**	**77**

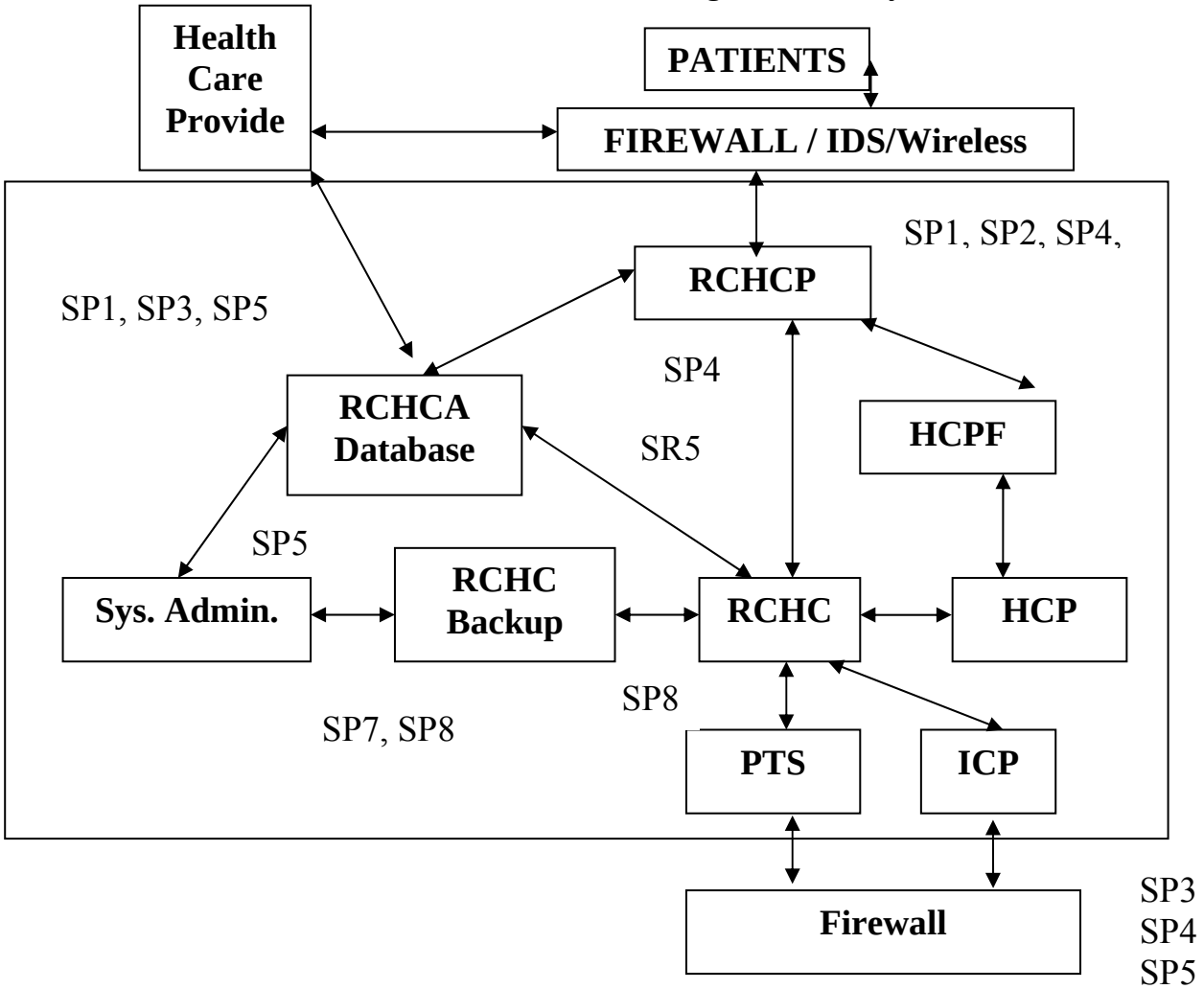
%RA= 1 - ∑ (Risk Score) / ∑ (Risk Upper Limit) = 0.23

4. CONCLUSIONS

After MCHC/RCHC Security analyses were low risk, the security architecture was ready for implementation.

The e-Learning system will implement the low risk architecture in order to train mobile system employee. The security analysis generates the password policies (SP5) and audit vulnerability scan Policy (SP8), also.

MCHC ARCHITECTURE: E-Learning with Security Policies



REFERENCES

1. *Implementing Network Security Systems*- Lab Source Files, Cisco Press, 2009;
2. Jeong, P., Stefan, A., *Implementing Network Security Systems*, Packet Tracer Manual, BC 2008, 2009;
3. *BankInfoSecurity*, 14 September 2005, Reports Shows Internal IT Attacks Rising. Retrieved on February 17, 2009;
4. Behar, R., *World Bank under siege in 'Unprecedented Crisis'*, FoxNews.com, International News, 10 October 2008, Retrieved on 22 February, 2009, <http://www.foxnews.com/story/0,2933,435681,00.html>;
5. Boatright, J.R., *Ethics and the Conduct of Business, Fifth Edition*, Pearson Prentice Hall, 2007;
6. Bush, V., Venable, B., Bush, A., *Ethics and Marketing on the Internet: Practitioners' perceptions of societal, industry and company concerns*, Journal of Business Ethics 23(3), pp. 237-248, 2000;
7. Castells, M., *Information Technology and Global Capitalism*, in Giddens, A. and Hutton, W. (eds) On the Edge;
8. *Living with Global Capitalism*, Vintage, London, pp. 52-74, 2000.