Boxes of Evidence  
U4O2 2011

This system uses new software installed within a networked system.

Red Rock Police HQ has a very large warehouse designed for the storage of materials associated with the criminal cases. Before this HQ was built, police officers stored materials gathered from crime scenes into boxes. The boxes were labeled and details were entered into a simple database.

|  |  |
| --- | --- |
|  | When an evidence box needed to be viewed, perhaps years later, the boxes were hard to find. New boxes would push the old ones into corners or they would be stacked up. The result was they would be placed way too far away to be found easily. It came to the point that when officers arrived, they planned to spend a full day just searching for a given box of evidence. |

Red Rock decided to implement a new software system which will be integrated into its current network. Red Rock has both Linux and Windows servers running a number of services such as the SQL server, Intranet, and mail server. It is a switched network with a Cisco router and firewall used with broadband ADSL2 connection to an upstream ISP. Gigabit Ethernet is delivered to the desktops using copper CAT6 cabling. Wireless access points allow wireless enabled laptops to be used within the HQ complex using 802.11n.

Here is how the new software system works.

On a box of evidence, an asset tag is attached and its code is matched with the case number and then stored in the database. This tag is a tiny transponder. It takes in a signal on one frequency and then transmits on another frequency. The tag remains in a sleep state until activated by a signal (someone wants to find the box).

When the tag receives a special signal, the tag wakes up. It sends a signal (on its other frequency) to a Receiver which does two things. This wake-up signal triggers the tag to emit a beeping sound from the local position and also a blinking light. The receiver decodes the signal from the tags and converts the data into records to the Wisetrack SQL Server files.

The files in the database now record the detective’s ID, the date stamp, the timestamp, and the box ID. When the box is returned this data is added to the record.

( for KK1, KK2) (www.wisetrack.com)

Using the new software, reports can be delivered – which include:

Date and time of a given evidence box being viewed and the case number and

IDs of the detectives who took the evidence box to view the contents.

How long the box was out of its storage spot.

*Scope* – The software is to be used with appropriate hardware (asset tags, asset transponders, Red Rock database server). There is yet no database of items which are stored within the boxes and therefore no search ability for contents.

There are 3 basic functions of this software:

It gives a visual and auditory signals to indicate the location of specific boxes.

It records how long the boxes were being viewed by detectives before being returned to their storage spot.

Question 1 *(8 marks)*

Propose 4 criteria for testing the security of the network. KS2

Include a testing technique for each criterion.

(6 marks)

|  |  |
| --- | --- |
| Criterion | Testing technique |
| *The network perimeter is secure from malware.*  *Viruses and other malware have been identified and trapped* | *Use SNORT or a penetration tester* |
| *All components such as routers have their default passwords changed (part of device hardening)* | *Check components for default passwords Hire White Hat hackers* |
| *Password ageing is enforced.* | *Users’ passwords are changed every 3 months*  *Log all access requests against authorized access attempts* |
| *Security patches have been installed(part of device hardening)* | *Obtain a list of all software patches and check the dates of installation* |
| *Firewalls prohibit the user of FTP* | *Use FTP to try to obtain webfoot access* |
| *The network perimeter has all unnecessary ports closed (part of device hardening)* | *Use SNORT* |
| *Encryption is employed on all wireless traffic* | *Use a packet sniffer such as Kismet to capture data sent by wireless* |
| *Encryption is strong* | *Use Cain and Abel to crack the encryption* |
| *All users are authenticated* | *Check policies for adding new users. Brute force cracking and dictionary attempts* |

Question 2 *(4 marks)*

Recommend two criteria and an associated technique for each to measure the ***effectiveness*** of the solution (KS3) (4 marks)

Criterion 1: *The date stamp and timestamps of requests to view an evidence box has been recorded accurately into the database*

Technique to measure: *Observe the detectives requesting a box of evidence. Check that the time observed is the date and time actually recorded.*

Criterion 2: *The auditory signal is loud enough to locate the box*.

Observation. *Place the box in an obscure, out of the way place. Activate the tag and walk through the warehouse to listen for the signal.*

Criterion 3: *The visual signal is reliable*.

Observation. *Activate the tag and look for the blinking light*.

Criterion 4. The system will remain reliable.

*Annually check that an evidence box, hidden in the back and under other boxes, can be found quickly.*

Question 3 *(4 marks)*

Recommend two criteria and techniques to measure the ***efficiency*** of the solution (KS3)

Criterion 1: *The time to locate the box is now 1 minute*

*Place boxes in hard to get to places and time how long it takes to find the box.*

*Time it.*

Criterion 2:

*The database controls are easily navigable and intuitive. (reduced effort)*

*Observation of officer using the database*

*Interview of officer using the database*

*Compile the number of complaints*

Criterion 3. *Blind spots for the wireless signals should be nonexistent.*

*Place a box of evidence in a hard to reach place. Activate the tag. The signals should be audible and visual immediately.*

Question 4 *(2 +2 marks)*

Justify the suitability of recommended strategies for evaluating the solution (KS4)

*Observers need training and practice but trained observers with much experience can provide adequate details.*

*Interviews take time and the interviewer must be able to tease out further information.*

*A way to list complaints must have been set up ahead of time to quantify this.*

*Someone hard of hearing should not perform the auditory signal test.*

Question 5 *(3 marks)*

All users (detectives, database managers and network managers) must undergo training.

Recommend training for the two groups of users (KK8 KK9)

|  |  |
| --- | --- |
| Group | Training |
| Authorised police staff. | *Entering queries into the Assets database.* |
| Database Manager. | *Creating reports of date and time stamps and length of time the box is out.* |
| Database Manager. | *Set up and maintain the database.* |
| Network managers | *Technical training on establishing, maintaining and troubleshooting the system.* |

Question 6

Propose strategies to evaluate the training and justify your choices for any 3 criteria.  
(KK8 KS5 KS6*) (4 + 4 marks)*

|  |  |  |
| --- | --- | --- |
| Criterion | Data collection method | Pros and cons of the strategy |
| Staff satisfaction. | *Survey or questionnaire. Complaints logs.* | *If staff don’t fill out the survey, no data is collected The survey must allow the staff to answer completely* |
| Accuracy of database reports. | *View reports from dummy tests done periodically.* | *Testing must be thorough or else it will be meaningless.* |
| Asset Tag equipment - robustness | *Breakdown logs.* | *Analysis of times and who used the equipment and maintenance logs is needed* |
| The training was adequate to perform the procedures and use the equipment | *Calls to help desk* | *Help desk logs must be monitored for the types of questions that are asked, and the length of time needed to fix the problem* |
| The time to locate a box of evidence is 1 minute – 5 minutes. | *Perform random searches and time how long they take.* | *This really needs accurate data from the time before the software was installed in order to perform a comparison. Apart from that, the tests need to be conducted on a regular basis.* |
| Technicians have been able to repair or help all users onsite. | *Logs of calls to Wisetrack or wireless providers* | *Accurate logs must be kept. Regular checks must be performed.* |

Question 7 *(4 marks)*

List types of system support documentation for each group listed below. (KK9)

|  |  |
| --- | --- |
| Group | *Documentation* |
| Authorised police staff. | *Procedures manual for the database to view results of search. Quick start guide for easy reference since the commands are new.* |
| Database Manager. | *Application manual for entering queries and producing and printing reports.* |
| Red Rock HQ IT technicians. | *Technical manuals on configuring the Asset Tag hardware and supporting database.* |
| Network Manager | *How to install the software and uninstall*  *Network diagrams backup plan for the database* |

Question 8 *(5 marks)*

Wisetrack has sold Red Rock the licence to use this system. The Network Manager has noted that remote logins from Wisetrack have occurred and the login activity resulted in someone viewing the reports in the database. Wisetrack maintains that they need to check on how well the system is working. (KS7)

Discuss this in terms of appropriate legislation. Comment on possible effects on stakeholders.

*The Privacy Act and Information Privacy Act require that all data collected must have its integrity preserved. Criminal cases involve information on many people and if left unsecured could cause damage to their reputation due to its sensitive nature.*

*With a set of ethical guidelines and a checklist of what needs to be protected and why, the person responsible for the purchase and installation of the software should have read the fine print. Someone unethical at Wisetrack could sell the data. It is the duty of the network manager to ensure all data is kept secure. This means no one can view the data or edit it without the usual level of access.*

Image source:

http://www.trade2europe.com/Trade2EuropeDailyFiles/WebPages/Fulfillment.asp