# When Hackers Turn To Blackmail

## Introduction

In the field of computer technology, a hacker is someone who has the knowledge, ability and skills related to operation of computers and their working mechanisms. A hacker can breach all security measures put in place to protect programs, software’s or information stored in any computer system. The 21st century has seen widespread use of computer and electronic information management systems which have been proved to be efficient in offering of different services (Al-Ammal, 2014). However, people with the ability to infiltrate past security protocols to access classified information have risen in the recent past (Eisenmann, 2017). These hackers have different motivational factors when pursuing their mission. Some want to gain profit, obtain specific information, protesting, offering to challenge the strength of a given firewall, testing the effectiveness of given software or merely for recreation. However, most cases of computer hacking have been associated with terrorism, seeking ransom money or protests (Al-Ammal, 2014). In this case, hackers have accessed the computer information system for keeping and managing patient’s medical records for a small hospital and they are demanding a ransom of 100000 dollars to put the system back to normality (Eisenmann, 2017). This is an act of extortion by the hackers and paying the cash will only encourage their mission. In this case the hackers have no regard to moral code of offering patients with the best possible medical care. They are only after fulfilling their demands. For a period of three years the hospital’s IT department have never faced such a scenario and they were caught by surprise. The major issues portrayed in this case include the fact that most people using computerised systems fail to understand the extent of damage that can be caused by hackers (Eisenmann, 2017).

## Sunny Lake Hospital Hacking

Hackers have lost their moral grounds and perform acts that put human life at risk (Eisenmann, 2017). Submitting to the demands of hackers will be conforming to extortion which is prohibited by law. Moreover, this would be a win for hackers and would encourage them to develop decryption programs that would be used for extorting money from companies and even government organisations. The Sunnylake Hospital case sends a message to all organisations using computer systems in information management to be aware of the threats posed by hackers (Eisenmann, 2017). This is also a message to all institutions that any security system can be breached. Therefore, considering the amount of damage that could be caused by failure to protect computerised information from malicious software, there is a need for all institutions using computer technology in managing information to put into placed updated computer protection.

In solving the immediate situation, a malware check on all hospital workstations should be done to determine the source of attack. Layman should identify and engage a negotiator who would facilitate dialogue between the Hospital and hacker to find a common ground to solve the standoff (Fleck, Volkema, Pereira, Levy & Vaccari, 2014). During this time, experts in the IT department should direct all their resources in restoring normal operation of the computer information management system. By initiating dialogue, the hacker will lose focus on their system which will offer the IT department the chance to promptly decrypt the system before the demand of the hackers are met. From the dialogue, the motivation behind the malicious attack can be identified which will provide the hospital with options and measures that can be taken to curb future software attacks (Fleck, Volkema, Pereira, Levy & Vaccari, 2014).

The use Electronic Medical Records tremendously improved efficiency in the delivery of medical care to patients in the Sunnylake Hospital (Eisenmann, 2017). Despite previously having doubts on the efficiency of EMR, the system proved to be reliable and effective in handling patients medical history and retrieving crucial information regarding patient emergency situations. However, the EMRs are constantly faced with hacking threats which not properly monitored; it can lead to companies to pay huge losses and legal damages from failure to protect their systems (Gupta & Anand, 2017). While adopting electronic medical recording would be effective, paper recording for patient’s medical details should be retained as a manual backup in the event of loss of electronic data. The records department should have kept filed copies of patient’s medical history to avoid situations of loss of data (Sreedevi, 2015). Therefore, Layman should revamp the record department where they would liaise with the IT section to produce hard copy files of crucial patient information which would be of help during emergency situations.

Layman as the CEO of the Hospital should make an inquiry of the staffing needs of the IT department and employ competent people (expert) who will develop decryption and encryption programs that would ensure safety of all medical records. The IT staff will be specifically tasked with developing and maintain up to date software’s and programs that would instantly detect security breach and respond or offer protection before any damage could be done (Sreedevi, 2015). The IT department should also be tasked with identifying weaknesses in the encryption programs protecting patient information. This would include developing information access clearance levels that would only be accessible to specific staff such as doctor. This would prevent possible leakage of information and the EMR security details to the hackers by workers in the Hospital. The experts should in turn identify solutions to eliminating the weaknesses to ensure prompt availability of patient records at any instant. The staff should also design appropriate defences against possible hacking. This would include developing worst-case hacking scenarios and designing the fastest possible means of rectifying the problem (Gupta & Anand, 2017). Moreover, the Hospital should send and engage IT professionals to train its IT personnel on the latest encryption and decryption techniques including new technologies to protect information from outside hackers and other malicious organisations.

Given the sophisticated nature of the hacking organisations, the management of the Hospital should allocate more resources in developing robust infrastructure and equipment that would ensure real-time detection of any malicious activity in handling of information. The IT department should acquire the necessary facilities that would ensure up to date maintenance of the security software’s to ensure optimum and effective operation to prevent attack on information (Sreedevi, 2015). The department should also set up electronic file backup system that would ensure fast retrieval of patient information in case of emergency or invasion of cloud stored information.

Moreover, Paul Layman should inform relevant authorities such the crime detection department and the anti-terrorism units on the malicious activity going on which poses a substantial risk to the lives of patients. Layman, through the medical care organisations and associations should engage the government to increase resources in fighting cyber crime. By limiting cyber crime and enforcing strict laws on cyber attacks, the level of malicious hacking would reduce. This is one of the strategies that Layman would prove effective in the longer term. It would not only benefit his Hospital but all other organisations and institutions dependent on electronic recording. The mass media should also be used in sensitising the general population on the danger of providing detailed personal information to unknown sites in the internet. Such information is sometimes used by hackers to conduct security breaches on sensitive classified information of different organisations (Brown, 2014). The media can play an important role in exposing such hackers and limiting their criminal activity (Eisenmann, 2017).

## Conclusion

To obtain lasting solutions to the problem, all stakeholders involved in electronic data recording and storage should understand how much sophisticated the hacking organisations are and the amount of socio-economical losses they would cause on failure to prevent them. All organisations and institutions using computerised or electronic information systems need to be aware of the level of vulnerability and that no computer systems is 100 percent secure (Brown, 2014). It should also be understood that the failure of the IT department also reflects on the collective failure of the management (Brown, 2014). The top management should also be quick and effective in dealing with any information regarding computer security breaches. Such information should be shared promptly to all relevant departments to ascertain the level of risks posed and the amount of possible damage and legal consequences of not pursuing effective decisions. Therefore, Sunnylake should develop a practical and proven backup system to ensure normal hospital operations at all time. The doctors and the personnel handling the patients should be dynamic and be creative so as to come up with ideas of solving immediate problems without compromising the well-being of the patients (Brown, 2014). Therefore, the IT facilities should not be a substitute for treating patients.

## References

Al-Ammal, H. (2014). A hacking case study: Detection, communication, and code. *Journal of advances in computer networks*, *2*(1), 18-23.

Brown, J. (2014). Accuracy of transition of care records. *Air Medical Journal*, *33*(5), 206.

Eisenmann, C. (2017). *When Hackers Turn to Blackmail*. *Harvard Business Review*.

Fleck, D., Volkema, R., Pereira, S., Levy, B., & Vaccari, L. (2014). Neutralizing Unethical Negotiating Tactics: An Empirical Investigation of Approach Selection and Effectiveness. *Negotiation Journal*, *30*(1), 23-48.

Gupta, A., & Anand, A. (2017). Ethical Hacking and Hacking Attacks. *International Journal of Engineering and Computer Science*.

Sreedevi, B. (2015). Evaluation of Quality of Service Metrics for Hacking and Counter Hacking Mechanism in Institutional Networks. *Indian Journal of Science and Technology*, *8*(23).