Malware in Healthcare

Lorraine Osako

University of Hawaii, Maui College

May 2018

Problem Statement

A problem within small medical and dental practices is cybersecurity-oriented problems in the state of Hawaii. The research is wanting to uncover if these small practices are concerned with cybersecurity attacks and what needs to change for patient information hygiene.

Introduction:

Healthcare offices are a perfect target for ransomware cyberattacks because there is a growing demand for systems interactions, critical infrastructures and the use of cellular internet connections. Also, because small practices are low profile and are less likely to spend much time or practice on protection against attacks. This allows attackers to identify vulnerabilities and launch attacks (Abouzakhar, 2017). Attackers have been successful at attacking small practices because of low profile and low protection (healthit, 2010). Most offices are not aware they have been infected with ransomware until they see their computer screen demanding cyber currency. All information such as patients' records, financial information and anything else stored on the computer are held hostage unless the terms for release have been met. With simple steps, medical and dental offices can and should guard against these attacks.

Definitions:

Healthcare Malware is the cyberattack on medical and dental practices. This is a growing concern as hackers are able to take patient information hostage until a fee is paid. It also encompasses obtaining information for sale on the dark web. In the article, "Ransomware still evolving, but paying hackers is still the wrong idea", Davis reports that the attacks are becoming more sophisticated.

Bio Informatics is the science of collecting, analyzing and processing biological data for storage and retrieval. It is the science of information where methods and software are developed to understand and interpret biological data.

There needs to be precautions taken to protect healthcare professionals and their patients. As described in the article Wannacry Ransomware (Laskey, 2017), the attack was global and quickly infected over 200,000 systems in over 150 countries. The attack was not very sophisticated, but these attacks are gaining ground and becoming more dangerous. Because precautions need to be taken to protect the healthcare professionals and patients, this project is researched to provide simple steps that can be taken to secure objects, protocols and systems (Abouzakhar, 2017).

Precautions:

Use secured internet when transferring any office pertinent data, whether it be health information, banking information or sensitive staffing information.

Use strong passwords that change often. Unauthorized access can be blocked with changing strong passwords. Passwords should be used to login for any work to be performed. Passwords should be at least eight characters and not be found in the dictionary. Instead they could include

a combination of words mixed together, upper and lower-case letters, numbers and symbols to discourage unauthorized users to gain access. Passwords for different users can minimize the casual looker from guessing or misusing data.

Multi-Factor authentication would require adding additional information, like a fingerprint to access information. This added security feature will deter unauthorized users gaining access to information.

Maintain Anti-Virus Software. Small offices are vulnerable to viruses that users can accidently or unknowingly access through email, CDs, flash drives and/or downloads. By having up-to-date anti-virus protection, threats such as attackers taking control, are minimized.

Using an electronic health record system (EHR) and firewall will help safeguard a system. An EHR that is not connected to internet is safer from hacking due to its closed network system. However, having a firewall installed by a technician will enhance the safeguard from outside attacks.

Limiting access for each individual could minimize data breaches. Controlling personnel to having access to limited information, aggregated to different work processes will limit what information is at risk. Insurance billers should not have access to full health information. Patient health information should be accessed only by personnel who work with that information. Limiting which staff members has access to certain data is important, but more difficult in smaller practices with smaller staff.

Physical access of devices should be controlled. Hardware such as hard drives, hand held devices, flash drives and machines should be secured. The loss of these items could result in data access even if protected by strong passwords.

Conclusion:

Small healthcare practices are a target for attacks due to their limited security protocols and small office staff. Relying on human error, attackers can permeate a system before anyone detects the attack, resulting in exposure of data, data held for ransom and loss of data.

By taking steps to safeguard the practice, data and personnel, the healthcare professionals can minimize the attacks.

Resources

Abouzakhar, N. S., Jones, A., & Angelopoulou, O. (2017). Internet of Things Security: A Review of Risks and Threats to Healthcare Sector. In *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.62

Ayala, L. (2016). Detection of Cyber-Attacks. In *Cybersecurity for Hospitals and Healthcare Facilities: A Guide to Detection and Prevention*. https://doi.org/10.1007/978-1-4842-2155-6_6

Brykczynski, B., & Small, R. A. (2003). Reducing internet-based intrusions: Effective security patch management. *IEEE Software*. https://doi.org/10.1109/MS.2003.1159029

Colwell, J. (2015). Improve cyber security and protect practice finances: small practices often have the weakest security, experts say, leaving physician vulnerable to considerable threats. *Medical Economics VO - 92*.

Davis, J. February 1, 2018. Ransomware is still evolving, but paying hackers is still the wrong idea. Retrieved from: http://www.healthcareitnews.com/news/ransomware-still-evolving-paying-hackers-still-wrong-idea

Greenberg, A. May 15, 2017. Wannacry Ransomware. Retrieved from: https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes/

Healthit. (2010). https://www.healthit.gov/sites/default/files/basic-security-for-the-small-healthcare-practice-checklists.pdf

Keese, J., & Motzo, L. (2005). Pro-active approach to malware for healthcare information and imaging systems. *International Congress Series*, *1281*, 943–947. https://doi.org/10.1016/j.ics.2005.03.326

Keese, J., & Motzo, L. (2005). Pro-active approach to malware for healthcare information and imaging systems. *International Congress Series*. https://doi.org/10.1016/j.ics.2005.03.326

Lasky, S. (2017). WannaCry ransomware worm attacks the world. *SecurityInfoWatch.com; Fort Atkinson*.

Martin, N. L., & Imboden, T. R. (2014). Information security and insider threats in small medical practices. *Twentieth Americas Conference on Information Systems*.

Mashima, D., Srivastava, A., Giffin, J., & Ahamad, M. (2010). Protecting E-healthcare Client Devices against Malware and Physical Theft. In *1st USENIX Workshop on Health Security and Privacy*.

Nelson, E. C., Bise, B., Gagne, R., Ohler, J., Kirk, J., Sarro, J., & Scarinza, C. (1980). COMPUTERIZED MEDICAL INFORMATION NETWORK FOR SMALL PRACTICES. *Proceedings - Annual Symposium on Computer Applications in Medical Care*.

Newswire, P. R. (2015). Global Cyber Security Market Outlook (2014-2022). *NY-Reportlinker*.

Perakslis, E. D. (2014). Cybersecurity in Health Care. *The New England Journal of Medicine*. https://doi.org/10.1056/NEJMp1404358

Pope, J. 2016. Ransomware: Minimizing the Risks. Retrieved from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5300711/

Protection, S. E. (2010). Anti-malware software and medical devices. *Health Devices*.

Rudd, E. M., Rozsa, A., Günther, M., & Boult, T. E. (2017). A Survey of Stealth Malware Attacks, Mitigation Measures, and Steps Toward Autonomous Open World Solutions. *IEEE Communications Surveys and Tutorials*. https://doi.org/10.1109/COMST.2016.2636078

SecurityScorecard. (2016). 2016 Annual Healthcare Industry Cybersecurity Report. *Cdn2*.

Stolfo, S. J., Wang, K., & Li, W.-J. (2007). Towards stealthy malware detection. *Malware Detection*. https://doi.org/http://dx.doi.org/10.1007/978-0-387-44599-111

Tanenbaum, W. A. (2016). IT Systems Put Security into Health Care Cybersecurity. *Journal of Health Care Compliance*.

What you need to know about the massive hack that hit the British health-care system and elsewhere. Retrieved from: https://www.washingtonpost.com/news/worldviews/wp/2017/05/12/what-you-need-to-know-about-the-massive-hack-that-hit-britain-and-11-other-countries/?utm_term=.090a73628886