

Conduct Reactions to a Digital Assault in a Medical Clinic Climate

Samir Singh*

Department of Nursing, University of Delhi, Delhi, India

Description

Critical infrastructure (CI) institutions (for example, power grids, telecommunications networks, and healthcare facilities) ensure the availability of services and goods required by our society and economy. Cyberattacks on CI pose a serious risk because they jeopardise critical supply chains. Healthcare institutions, particularly hospitals, have a unique place among CI. They help to keep public services running and play an important role in saving people's lives. Furthermore, they generate, process, and store vast quantities of valuable medical data from thousands of patients. However, the combination of insufficient security for networked medical devices and surrounding systems, as well as a lack of physical entry barriers, makes these institutions easy targets for cybercriminals [1]. Due to these circumstances, we have already seen large-scale, non-targeted, and targeted attacks in the past. According to a 2017 study, 64 percent of all German hospitals have been victims of cybercrime. Hospitals are targeted by ransomware attackers in addition to non-targeted attacks. In September 2020, the German university medical centre of Duesseldorf was subjected to a large-scale ransomware attack. As a result, emergency care and major parts of the hospital infrastructure were disrupted [2].

Critical patient treatment areas such as operating rooms, emergency departments, intermediate care, and intensive care units are critical to the patient's well-being. Patients may suffer harm or die if a system is not available. Technical attack vectors exist in these systems due to the prevalence of networked medical devices. Patients rely on the medical equipment working properly and the medical staff using it correctly. In medical settings, crisis behaviours, in particular, play an important role [3]. Despite the fact that decisions are made by medical professionals, technically supported medical decision-making is critical in critical care areas. As a result, when dealing with cyberattacks, human behaviours must be considered.

In terms of cyber security, the human factor is either described as the "weakest link" or as one of the strongest defences. There are few published studies on IT-security incidents in a hospital setting. Different approaches have been used in behavioural research on victims of cyberattacks and the consequences of such attacks to investigate stress levels, socio-psychological impacts, and effects on team performance in general [4]. These works have

demonstrated a strong interaction between psychological and technical factors in a public-interest topic. Nurses' behaviour is critical in ensuring patient safety because they provide critical care in a high-demand, low-control, and high-risk environment. Because time is a critical factor in critical situations, their actions must be made quickly and under uncertain conditions.

The presented lab study provides insight into the nursing staff's behaviours during a simulated cyberattack on an Intermediate Care (IMC) ward's monitoring system. An IMC Ward typically includes advanced monitoring capabilities as well as the ability to use nearly all intensive care measurements. These facilities are intended for patients who require close monitoring but do not require the full spectrum of intensive care. We created a simulation of an attacker tampering with the values of vital monitors in order to make incorrect medical decisions [5]. Although this behaviour has not yet been observed in practise, it is technically possible as long as attackers have physical access to the device or access to the hospital network.

Conflict of Interest

None.

References

1. Martinsson, Andreas, Charlotte Andersson, Pontus Andell, and Sasha Koul, et al. "Anemia in the general population: prevalence, clinical correlates and prognostic impact." *Eur J Epidemiol* 29 (2014): 489–498.
2. Xu, Fengdan, Xiangyong Kong, Shunyan Duan, and Hongyan Lv, et al. "Care practices, morbidity and mortality of preterm neonates in China, 2013–2014: A retrospective study." *Sci Rep* 9 (2019): 18863.
3. Drennan, Vari M and Ross Fiona. "Global nurse shortages-the facts, the impact and action for change." *Br Med Bull* 130 (2019): 25–37.
4. Jackson, Debra, Caroline Bradbury-Jones, Diana Baptiste, and Leslie Gelling, et al. "Life in the pandemic: Some reflections on nursing in the context of COVID-19." *J Clin Nurs* 29 (2020): 2041–2043.
5. Paige, Sharon L, Sean Thomas, Cristi L Stoick-Cooper, and Hao Wang, et al. "A temporal chromatin signature in human embryonic stem cells identifies regulators of cardiac development." *Cell* 151 (2012): 221–232.

How to cite this article: Singh, Samir. "Conduct Reactions to a Digital Assault in a Medical Clinic Climate." *Adv Practice Nurs* 7 (2022): 243.

*Address for Correspondence: Samir Singh, Department of Nursing, University of Delhi, Delhi, India, Tel: +911127667647; E-mail: samir95@du.ac.in

Copyright: © 2022 Singh S. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Received 05 January, 2022, Manuscript No: apn-22-54603; **Editor assigned:** 07 January, 2022, PreQC No: P-54603; **Reviewed:** 10 January, 2022, QC No: Q-54603; **Revised:** 15 January, 2022, Manuscript No: R-54603; **Published:** 20 January, 2022, DOI: 10.4172/apn.2022.07.243