Chapter 20
Cyberspace Security Threats and Attacks on E-Records Management at Moi University, Eldoret, Kenya

Carolyne Nyaboke Musembe
University of KwaZulu-Natal, South Africa

Stephen Mutula
University of KwaZulu-Natal, South Africa

ABSTRACT

The digital revolution and internet connectivity are the power behind digital-based models in organizations. The broader reach and impact of cyberspace which is accelerating across Moi University seems to be generating complex challenge to address issues of e-records at Moi University. This chapter emanated from a thesis on e-records security management, and therefore investigates cyberspace security threats and attacks on e-records management at Moi University with a view to offering practical and policy interventions to address this challenge. Data was collected from Moi University staff using interviews and questionnaires and was analysed thematically and using Statistical Package for Social Sciences (SPSS) version 24. Findings revealed cyberspace as an e-records security challenge. Cybercriminals (hackers and crackers), when new technologies emerge, concurrently invent and discover new ways to tap in the new technologies with the intention to steal and corrupt e-records for their benefit, thus hurting the veracity of e-records and university's reputation. Cyber-attacks including an attempted attack on the network, viruses, and worms were widely mentioned in the findings as a threat to both the e-records, and the computer system that host them and storage devices. The chapter recommends that the university should set dynamic security strategy and vision, developing and implementing policies and adopting standards, threat analysis and assessment, integrated and intelligent cybersecurity management service, and investing in e-records security awareness campaigns and training for employees, among others.

DOI: 10.4018/978-1-7998-6618-3.ch020

1.0 INTRODUCTION AND BACKGROUND

Digital revolution has transformed and shaped the running of organizations worldwide. Digital-based models such as e-governance, e-education, e-commerce, e-agriculture, e-health, and e-environment are seen as development enablers. Consequently, high demand for internet and computer connectivity has led to the integration of computer technology in fundamentally all modern services. (International telecommunication union 2012).

The digital revolution and internet connectivity are the power behind digital based models in governments. This is referred to as Cyberspace. The term cyberspace was first coined and widely used by a science fiction author, Gibson (referred to us father of cyberspace) in his award-winning debut in 1984, Neuromancer. Gibson's networked artificial environment anticipated the globally internetworked technoculture (and its surveillance) in which we now find ourselves (Wired 2018). It is a term that is now widely used to mean the environment in which communication over computer networks occurs. Carnaghan (2019) defines cyberspace as a non-physical domain of information flow and communication between computer systems and networks. The author further indicates that any device connected to the internet has direct access to cyberspace which can be used for everyday tasks such as sending and receiving an email, making purchases online as well as managing personal bank accounts and paying bills among others.

Consequently, the digital environment made up of e-records that are used and shared, through networks including the physical systems, such as computers and databases that enable exchange of the e-records as well as the users who make use of the systems, is referred to as cyberspace (US national association of county and city health offices (NACCHO) 2015; Friedman and Singer 2014).

Therefore, the broader reach and impact of cyberspace which is accelerating across national and international boundaries is making it a complex challenge for any government to address issues of e-records security (Ministry of ICT, Kenya 2014; Omotosho and Emuoyibofarhe 2014). The cyberspace challenges are capable of shutting down critical infrastructure, computer systems linked together within the confines of cyberspace. The United States national counterintelligence and security centre (2010) concurs that cyberspace attacks disrupt, disable, destroys or maliciously controls computer environment/ infrastructure or/and destroy e-records.

For instance, in 2007, a series of cyberattacks that lasted for three weeks on Estonia government (which is referred to as 'web war 1' concerted denial of service attacks on websites of Estonia parliament, banks, ministries, newspapers and broadcasters. This prevailed through websites being flooded by tens of thousands of visits jamming and disabling them by overcrowding the bandwidths for the servers running the sites. This was the first known incidence of such an assault on a state (Traynor 2007).

Further, it has been reported that China's Huawei endures around a million cyberattacks per day on its computers and networks. The attacks are focused on stealing state-of-the-art 5G technology that the Chinese government has developed. The Huawei 5G technology is thought to permit the transmission of large amounts of e-records at tremendously high speeds, allowing telecommunication devices to connect to almost all products and services, including those related to military affairs, through the wireless network. The cyberattacks include but not are limited to IP-theft and theft of confidential e-records by sending a computer virus by email (Doffman 2019; Suffolk 2019).

Similarly, the African continent has not been spared. In 2013 a Symantec report noted that cyberattacks were increasing in Africa at a faster rate than any other region in the world. The increasing attacks in the continent can be attributed to vulnerable systems and lax cyber-security practices (Symantec