Scientific and Practical Cyber Security Journal (SPCSJ) 8(2): 68 – 75 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

SYSTEM SURVIVABILITY THREATS AND FACTORS INFLUENCING ATTACKS IN HEALTH FACILITIES

Joseph SIMIYU[1] Dorothy RAMBIM[1], Jasper ONDULO [1]
[1]Masinde Muliro University of Science and Technology, 190, Kakamega, 50100, Kenya

ABSTRACT: The adoption of e-health offers affluence medical benefits, unfortunately source of effective data is poorly protected, it is also susceptible to dangerous threats and attacks. While the volume of medical data dictates the use of technology, a failure of e-health systems to include security survivability as apriority in making e-health systems compromise easier. With this numerous security issues, the system can suffer more and never recover to assure users on their mission mandate. Despite efforts to secure Kenya's cyber space by assuring Kenya electronic transactions and online services such as e Government and health, system survivability and security attacks continues to jeopardize e-health confidentiality, credibility, reliability and availability for both providers and users. Therefore, it is important to understand issues around system survivability after attack rather than just security. Overall, this paper will try to come up with a system survivability issues for fighting information systems crime in the health sector in Kenya. Specifically, this research study will seek to outline the major system survivability threats and vulnerabilities within health sector in Kenya.

KEYWORDS: *e-health, Survivability, System Vulnerabilities, Security Risks*

1. INTRODUCTION

Survivability is defined as the ability of a system to provide essential services in the presence of attacks and failures, and to recover full services in a timely Manner. According to M. Farrukh Khan, Raymond A. Paul, in Advances in Computers, 2012) [i]. Survivability has been considered as a key inherent property of a reliable system. A survivable system continues to function, despite the presence of malicious attacks or arbitrary faults. The fact that a system has well-defined functions and correct implementations does not guarantee that the system is survivable. Some damages, which are resulted from novel, well-orchestrated malicious attacks, are simply beyond the abilities of most system developers to predict. In those situations, even a strong system with well-established security could possibly be compromised.

Globally Information technology is a very important tool in any current organization. Today organizations are driven by emerging technologies of which when implemented improve the welfare of clients and changes how people interact and promote social participation. These new technologies improve the productivity and competitiveness of organizations while opening up new areas to be explored and creating business and job opportunities as hold forth by Shenoy, A., & Appel, J. M. (2017).[ii].

In Africa, many countries have reported the upsurge of digital threats and malicious activities. The threats has been as a results of sabotaged public infrastructure, losses from digital fraud and illicit financial flows, and national security breaches involving espionage and intelligence theft by militant groups. While the individual governments on the continent seem to be very slow to appreciate the importance of the concept of information systems safety, the regional political body, the African Union (AU) seems to be making some gains in raising awareness and advocating for better cyber safety, to the continent's ministers of Information and Communications Technology. The African Union Commission (AUC) put out a call for experts to join its African Union Cyber Security Expert Group (AUCSEG) based on a resolution by its executive council and also created Africa Cyber Security collaboration and coordination committee to advise the AUC and policy makers on Cyber strategies, with many other specific tasks. Call for experts, AU, (2018)[iii]

This study determines the nature and characteristics of threats, assess the emerging threats and vulnerabilities that influence the health sector in Kenya and more specifically Referral Hospital

hospitals. A qualitative review was undertaken by a literature search of the survivability and vulnerabilities to identify threats and the factors influencing system survivability attacks in healthcare. In this paper, we examine the major system survivability threats and factors influencing them in healthcare facilities. The rest of the paper is organized as follows, II. provides emerging survivability threats and vulnerabilities in the health facilities, Factors Influencing system survivability attacks in healthcare is provided in section III, section IV discussion and conclusion.

2. EMERGING SYSTEM SURVIVABILITY THREATS AND VULNERABILITIES IN THE HEALTH FACILITIES

There are several issues that make health care security more complicated and have increased vulnerability over time (Burns, 2016)[iv]. In addition to this proliferation in emerging technology, many healthcare companies tend to use obsolete systems in many fields, such as Window XP, which has not been supported since 2014. (Milliman, 2016)[v], enabling hackers and malware to easily avoid detection, for example, the recent WannaCry attack. The propriety nature of medical device software means that healthcare IT teams may not be able to access the internal software in medical devices, so they rely on manufacturers to build and maintain security in those devices which were lacking. There is also a problem with lack of funding for security and system survivability, while hospitals and other organizations spend funding to become more integrated; they do not spend enough time and money to keep software updated and systems safe (Kotz *et al*., 2016)[vi]. This is exacerbated by a lack of industry expertise on system survivability security resulting from a general lack of technology and the prohibitive expense of security personnel. In summary, a rapid shift to electronic health records and interconnected devices, along with historical and ongoing lack of investment in survivability of systems and a lack of understanding of health personnel ’s safety work behaviors have made the health sector vulnerable to attacks.

Although healthcare has vulnerabilities to exploit, attackers need to be motivated to commit attacks. Motivation includes the potential for financial and political benefit and possibly taking life in a cyberwarfare process. Economic benefit is the highest of those motivations. Data on health care is far more valuable than any other data. The value can exceed €888.05 for a complete set of medical credentials (Sulleyman, 2017). Stolen medical identification may be used by claiming somebody ’s identity or insurance records to access health care and prescription drugs. Uses extend to organized crime perpetrating sophisticated fraud. Fraudsters have earned billions in the last few years by filing fraudulent claims and dispensing drugs to sell on the dark web (McCarthy, 2016). Sometimes there is even sufficient information in medical records to open bank accounts, secure loans or obtain passports.

Effects of Cybercrime on Healthcare: The health sector has seen a drastic increase in the amount and scale of data breaches in the last few years. Breaches lead to financial loss, reputational loss and reduced patient safety. Report indicates the average cost of missing or stolen medical records containing confidential and sensitive information is massive (Seh AH, 2020)[vii], and continued advertisement associated with large breaches may jeopardize patient trust which may result in less willingness to share data (Whitler, 2017**)**[viii]. This is especially problematic for patients with conditions such as sexual or mental health conditions being stigmatized.

Despite warnings issued and the availability of security patches, the scale of the WannaCry attack was exceptional, with over 300,000 computers worldwide demanding that users pay ransoms on bitcoin (Scott & Wingfield, 2017)[ix]. A number of hospitals have experienced system wide lockouts, patient care delays, and loss of function in connected devices such as MRI scanners, and refrigerators for blood storage. This attack was not directed specifically at healthcare organizations, yet the damage was widespread. Other ransomware targeted specifically the healthcare sector.

Many malware attacks have led to major incidents, such as healthcare trust suffering an unspecified cyber-attack which results in the shutdown of IT systems and scheduled operations and outpatient appointments being cancelled for days (Evenstad, 2016)[x]. Medjack (Medical Device Hijack) is attack that was detected to inject malware into unprotected medical devices for lateral movement through the hospital network (Storm, 2015)[xi]. The infected medical devices creates poor ties in hospital safety

defenses, including diagnostic equipment (including MRI machines), therapeutic equipment (e.g., infusion pumps), and life-supply equipment (including ventilators).
Simulated attacks by 'White Hacker' have highlighted that there are other vulnerabilities which mean "Medical devices are the next security nightmare". There is potential for attacks similar to what used to be considered science fiction. For example, brain jacking where a suitable device could be inserted (Pycroft *et al*., 2016)[xii]. Simulated attacks on devices such as pacemakers and defibrillators, insulin pumps and pumps for drug infusion have been carried out. These attacks have remotely controlled machines to modify surgery or send lethal doses of drugs. Though currently only simulated such attacks may occur (Klonoff, 2015)[xiii]. Risks will continue to increase if cybersecurity has not been designed from the start of the product or project lifecycle.

Ransomware and other Malware: Malware is a serious problem across all industries, however, in healthcare, a malware infection can mean life or death. Healthcare operates an intricate series of interconnected reporting and services. The interlocking network that communicates information on our behalf to better our health is especially vulnerable to ransomware and other malware attacks. In the aforementioned NHS WannaCry attack, hospitals are forced to close their doors to new patients, and existing patients' treatment are interrupted because of an inability to access records. The HHS 'Wall of Shame', which lists healthcare data breaches data breaches affecting almost millions of individuals. Healthcare is among the leading cyber-criminal-targeted industries (Kruse et al., 2017)[xiv]. Breaches may be caused by hacking, malware and threats to insiders. While insider threats are issues created by employee errors or deliberate actions (e.g., responding to phishing emails, a social engineering attack to extract login credentials or launch a malware attack, erroneous security settings, password misuse, loss of laptops and sending unencrypted emails). This thus becomes a moderating factor together with DDOS and ransomware attacks.

Ransomware exploits vulnerabilities to hijack monetary benefit infrastructures for target information technology (IT). Because of the nature and value of information, access to medical information allows cyber criminals to commit identity theft, medical fraud, and extortion, and to illegally get controlled substances. Medical information's utility and versatility, extensive centralized storage of medical information, relatively weak IT security systems, and the expanding use of healthcare IT infrastructure all contribute to an increase in cyber-attacks on healthcare institutions. Research suggests that an individual's medical information is 20–50 times more valuable to cyber-criminals than personal financial information (Kruse *et al*., 2017). As such, cyber-attacks targeting medical information are increasing 22% per year (Kruse *et al*., 2017). Ransomware uses a hybrid encryption system that combines the two cryptographies to create an asymmetric cryptosystem in which data is encrypted using a randomly generated symmetric key, which is then encrypted using a public key where one party has the appropriate private key (Krisby, 2018)[xv]. The cyber-criminal uses the private key to decrypt the symmetric key to decrypt the data back "into "plaintext" and give the key back to the victim, who can then use it to access their device again (Krisby, 2018). When encrypted, the code is unavailable and indecipherable. The user receives a pop-up notification that requires a ransom payment (usually in untraceable digital currency such as bitcoin) in exchange for the decryption key (Pope, 2016)[xvi].
Often, Ransomware does not destroy data but will lock up data before a ransom is paid (Richardson & North, 2017)[xvii]. Even if the infection with ransomware is removed the data can remain encrypted. But it is necessary to remember that the mere infection of a ransomware computer does not suffice. To get an encryption key and report its results, the ransomware has to communicate with a server (Richardson & North, 2017). This includes a server hosted by a corporation that avoids criminal activity and ensures anonymity for the attackers (called Bulletproof Hosting). These businesses are often located in China or in Russia (Richardson & North, 2017).
During a ransomware attack, malware is injected into a network to infect and encrypt sensitive data until a ransom amount is paid.
Ransomware attacks are a growing threat amongst healthcare providers according to an analysis last year. More than 1 in 3 healthcare organizations globally fell victim to a ransomware attack in 2020.
The reason for its prevalence is that hackers understand how critical it is for the healthcare sector to minimize operation disturbances. During a ransomware attack, healthcare victims panic, fearing the

regulatory consequences that follow the theft of patient data. Data Breach Investigations Report (DBIR).

Phishing: Like all industries, healthcare is at risk from phishing. According to Data Breach Investigations report (Verizon, 2023)[xviii] around 66% of malware was initiated as an email attachment. Although the WannaCry ransomware was unlikely to have begun its life in an email, much malware continues to be executed via phishing. However, phishing emails and texts are also a threat to personal data, including login credentials.

The National Health Information Sharing and Analysis Center have recently reported that the healthcare industry is at the most risk of fraudulent emails. However, little is being done to combat this, with 98% of healthcare organizations not taking the first steps in helping to prevent phishing by setting in place Domain-based Message Authentication, Reporting & Conformance (DMARC).

Insider threats: Insider threats to hospital resources are a concern across the board and can be carried out by patients as well as staff and can be both malicious and accidental. The HIMSS Cybersecurity Survey (2017), found that Insider threats were deemed to be worrying enough to set up specific programs of protection by 75% of respondents.
Spoofing: Spoofing is when someone hides their identity to evade detection for their wrong acts and pretends to be someone else in an attempt to gain trust and get sensitive system information. The common spoofing done by changing the hardware or MAC address is called MAC cloning, changing the IP address or the unique identity on the network is called IP spoofing, and impersonating as someone else in their digital communication is called email spoofing.

Information-gathering attacks: Information gathering is the practice of attacker gaining priceless details about probable targets. This is not an attack but only a pre-phase of an attack and is totally passive as there is no explicit attack. Systems including computers, servers, and net-work infrastructure, including communication links and inter networking devices, are sniffed, scanned, and probed for information like whether the target system is up and running, what all ports are open, details regarding the operating system and its version, etc. Some of the information-gathering attacks are sniffing, mapping, vulnerability scanning, phishing, etc.

Password attacks: The simplest way to achieve control of a system, or any user account, is through a password attack. If the personal and behavioral details of the victim are known, the attacker starts with guessing password. Frequently, the attacker uses some form of social engineering to trace and find the password. Dictionary attack is the next step in password attacks and is automated.

Virus: Computer viruses are the most communal threat to the computer users. Computer viruses are malicious software designed to blow out from one computer to another through file transfer, piggybacks on genuine programs and OS, or e-mails. The email attachments or downloads from particular websites contaminate the computer and also other computers on its list of contacts by using the communication network. Viruses influence the system security by changing the settings, accessing confidential data, displaying unwanted advertisements, sending spam to contacts, and taking control of the web browser According to Thomas C. (2009), the viruses are identified as executable viruses, boot sector viruses, or e-mail viruses.

Worms: Computer worms are fragments of malicious software that reproduce swiftly and blow out from one computer to another through its contacts, again spreading to the contacts of these other computers and so on and reaching out to a large number of systems in no time. Captivatingly, worms are prepared for spreading by exploiting software vulnerabilities. Worms display unwanted advertisements. It uses up tremendous CPU time and network bandwidth in this process thereby denying access to the systems or network of the victim, creating chaos and trust issues on a communication network.

Trojans: Trojans are programs that appear as perfectly genuine but, in reality, have a malicious part embedded in it. Trojans are spread usually through email attachment from the trustworthy contacts and also on clicking on fake advertisements. The payload of Trojans is an executable file that will install a server program on the victim's system by opening a port and always listening to that port whereas the server is run on the attacker's system. Hence, whenever the attacker wants to login to the victim machine, they can do so by means of the backdoor entry making it hidden from the user.

Spyware and adware: Spyware and adware are software with a common property of collecting personal information of users without their knowledge. Adware is intended to track data of the user's surfing behaviors, and, based on that, pop-ups and advertisements are displayed. Spyware on the other hand gets installed on a computer and gathers information about the user's online activities without their knowledge. Spyware contains key loggers that record every-thing typed on the keyboard, making it unsafe due to the high threat of identity mugging.

Botnets: A collection of compromised systems or bots acts as a team of infected computers under the control of a bot master to remotely control and send synchronized attacks on a victim host. This army of bots, agents, and bot master constitute a botnet. Botnets are used for sending spams and also for distributed denial of service attacks.

Denial-of-service attacks: Denial-of-service (DoS) attacks as the name suggests denying users from accessing or using the service or system. This is mainly done by overwhelming the bandwidth, CPU, or memory wherein the access to the network of the victim machine or server offering the service gets

denied. DoS attacks thus interrupt the service of a computer or network systems, making it inaccessible or too inferior in performance.4.16 Distributed DoS In distributed DoS (DDoS) attacks, the victim is targeted from a large number of individual compromised systems simultaneously. The DDoS attacks are normally done with the help of botnets. The botmaster is the attacker who indirectly attacks the victim machine using the army of bots or zombies. DDoS attacks occur when a large number of compromised systems act synchronously and are being coordinated under the control of an attacker in order to totally exhaust its resources and force it to deny service to its genuine users. It is the upsurge in the traffic volume that loads the website or server causing it to appear sluggish (Thomas C. 2009)

3. FACTORS INFLUENCING SYSTEM SURVIVABILITY ATTACKS IN HEALTHCARE

Top Management should be responsible for informing their employees of the importance of systems survivability, make it efficient for people to participate, take ownership and manage their responsibilities (Abbas *et al*., 2015)[xix]. They also ought to invest in a solution that benefits everyone and finally monitor performance. Further, organizational resources come in whereby organizations lack industry expertise on survivability attacks resulting from a general lack of technology and the prohibitive expense of security personnel.

Game theory models the attacker and system administrator's fundamentally selfish and aggressive actions and analyzes the potential strategies bringing in the human aspect of cyber security (Shiva & Sankardas, 2010). Securitization theory suggests there is currently a general perception that there is a lack of awareness and information in Kenya on systems security matters, leading to IT literacy as an individual factor. For systems survivability, intersectionality can help us better understand how system attacks issues are not just technical but are both legal and governmental, and cultural and economic, and so on which leads to policy formulation of IT policies for cyber security.

Based on the above from the literature review, the researcher aimed at reviewing organizational and individual factors, coupled up with mediating factors to come up with a framework for system survivability. From this, the researcher aimed to develop and validate a framework that addresses the human factors, organizational culture, and IT policies side of system survivability in the health sector.

Increased use of Cloud computing and online security

Cloud computing is being taken up by healthcare as it offers benefits such as improved access to data and cost efficiency. The use of Cloud computing within healthcare is set to soar, however, cloud computing brings its own risks (I Kravchenko, 2021). Data within cloud repositories need to be correctly protected, according to Open Web Application Security Project (OWASP) guidelines. Protecting data at rest and during transit across web services requires not only robust encryption measures but also appropriate and effective authentication, such as second factor and risk based.

Internet-enabled healthcare attacks (Internet of Things - IoT devices)

Healthcare has embraced Internet-connected devices in a bid to use health data to improve patient outcomes. Apps like OpenAPS which are an optimized data-driven insulin delivery system and internet enabled activity trackers which help in cancer treatment are paving the way for the IoT to improve healthcare. However, the IoT has known security and privacy issues. Many healthcare based IoT devices aggregate personal data which is then stored in a cloud repository and used to analyze conditions, treatments, among others. Security issues such as DDoS attacks like the massive Mirai Bot (NJCCIC, 2016), which are based on IoT devices, are a potential threat that could disrupt treatment. The protection of personal data to prevent exposure is another. Redundancy issues are also another area of concern, as more hospitals become dependent on Internet-enablement of systems.

Lack of Data Encryption

Protecting sensitive business data in transit and at rest is a measure few industries have yet to embrace, despite its effectiveness. The health care industry handles extremely sensitive data and

understands the gravity of losing it which is why HIPAA compliance requires every computer to be encrypted (Thakur, K., Hayajneh, T., & Tseng, J. 2019)[xx]

4. CONCLUSION

Some of the survivability crimes and threats are wrongdoing that are executed utilizing PCs or are in any case identified with them. Access to boundless information over the world is great yet it accompanies its reasonable portion of issues. In this paper, we have explored the principal vulnerabilities and risks that target health systems survivability and proposed a comprehensive system survivability model to address these challenges. Through the analysis of a case study and a review of relevant literature, we have developed a model that can be adopted for use as a strategy to overcome. By adopting this model, organizations can enhance their ability to identify and mitigate vulnerabilities in their environment, thereby improving their overall security posture.

REFERENCES

1. [i]. Farrukh Khan, Raymond A. Paul, 2012. In Advances in Computers, M
2. [ii] Shenoy, A., & Appel, J. M. (2017). Safeguarding Confidentiality in Electronic Health Records. *Cambridge quarterly of healthcare ethics : CQ : the international journal of healthcare ethics committees*, *26*(2), 337–341. https://doi.org/10.1017/S0963180116000931
3. [iii] Experts, A. U. (2018). *Call for Experts.*
4. [iv] Burns, A. J., Johnson, M. E., & Honeyman, P. (2016). A brief chronology of medical device security. *Communications of the ACM*, *59*(10), 66–72.
5. [v] Index, M. M. (2016).
6. [vi] Kotz, D., Gunter, C. A., Kumar, S., & Weiner, J. P. (2016). Privacy and Security in Mobile Health: A Research Agenda. *Computer*, *49*(6), 22–30. https://doi.org/10.1109/MC.2016.185
7. [vii] Seh AH, Zarour M, Alenezi M, Sarkar AK, Agrawal A, Kumar R, Khan RA. Healthcare Data Breaches: Insights and Implications. Healthcare (Basel). 2020 May 13;8(2):133. doi: 10.3390/healthcare8020133. PMID: 32414183; PMCID: PMC7349636.
8. [viii] Whitler, Kimberly & Farris, Paul. (2017). The Impact of Cyber Attacks on Brand Image: Why Proactive Marketing Expertise Is Needed for Managing Data Breaches. Journal of Advertising Research. 57. 3-9. 10.2501/JAR-2017-005.
9. [ix] Scott, M., & Wingfield, N. (2017). *Hacking attack has security experts scrambling to contain fallout*. New York, USA: New York Times.
10. [x] Coventry, Lynne & Branley-Bell, Dawn. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas. 113. 10.1016/j.maturitas.2018.04.008.
11. [xi] Storm, D. (2015). *MEDJACK: Hackers hijacking medical devices to create backdoors in hospital networks*. London, UK: Computerworld.
12. [xii] Pycroft, L., Boccard, S. G., Owen, S. L. F., Stein, J. F., Fitzgerald, J. J., Green, A. L., & Aziz, T. Z. (2016). Brainjacking: implant security issues in invasive neuromodulation. *World Neurosurgery*, *92*(1), 454–462.
13. [xiii] Klonoff, D. C. (2015). Cybersecurity for connected diabetes devices. *Journal of Diabetes Science and Technology*, *9*(5), 1143–1147.
14. [xiv] Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1–10.
15. [xv] Krisby, R. M. (2018). Health care held ransom: modifications to data breach security & the future of health care privacy protection. *Health Matrix*, *28*(1), 365.
16. [xvi] Pope, J. (2016). Ransomware: minimizing the risks. *Innovations in Clinical Neuroscience*, *13*(11–12), 37-41.
17. [xvii] Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, *13*(1), 10-12.
18. [xviii] Data Breach Investigations report (Verizon, 2023

19. [xix] Abbas, A., Bilal, K., Zhang, L., & Khan, S. U. (2015). A cloud-based health insurance plan recommendation system: A user centered approach. *Future Generation Computer Systems*, *43*(1), 99–109.