USE OF INFORMATION AND COMMUNICATION TECHNOLOGY FOR DATA EXCHANGE AND CYBER SECURITY IN THE JUDICIARY

Muhammad Jiya

Assistant Director/Head of Department,
Information and Communication Technology
Department, Nigerian Financial Intelligence Unit
(NFIU), No. 12, Ibrahim Taiwo Street, Aso Rock Villa,
Abuja, FCT.

SEPTEMBER 2020

DELIVERED DURING NATIONAL WORKSHOP FOR INFORMATION AND COMMUNICATION TECHNOLOGY STAFF ORGANIZED BY NATIONAL JUDICIAL INSTITUTE AT MUHAMMAD BELLO CENTRE, AIRPORT ROAD, ABUJA, FCT.

Table of Contents

1.0 Introduction

Information and Communication Technology (ICT) is a general term used to describe all the technologies and services involved in computing, data management, telecommunications provision, and the internet. ICT permeates all aspects of life, providing newer, better, and quicker ways for people to interact, network, seek help, gain access to information, and learn. The rapid development of ICT opens up new opportunities to significantly improve the administration of justice. The Judiciary; as the arm of government that is constitutionally vested with the power to interpret and apply the law, settle disputes and punish law-breakers (Duru, 2012; The Australian Parliament, 2015) is not unaffected by the impact of advancements in ICT. According to Doma (2016) as the judiciary depends on a network of information, its form must constantly change to conform to the communicative devices present at any given time. Doma's assertion has been evident in the way technological advancements over the years have had consequential impacts on legal systems around the world. Examples of such changes include the automated case registers which replaced the traditional court docket books in Singapore (Sze, 2004); the use of optical character recognition (OCR) technology in Italy to digitize hardcopy documents thereby speeding up data-entry (Velicogna, 2007); the use of Case Management Systems (CMS) to automate court processes and monitor case activities in England and Wales (McMillan, 1995); the use of the email technology and forums for communication and collaboration in France (Velicogna, 2007); amongst others.

This article would discuss the use of ICT tools in the judiciary specifically for data exchange. It shall also discuss ways to secure these tools against cyber threats and to ensure that the data collected, processed, stored and disseminated are not stolen or compromised. This article is based on research and practitioner-reports in the field of e-judiciary/electronic judiciary.

2.0 Data Exchange in the Judiciary

The Legal and judicial process requires various levels of information gathering and communication between stakeholders; involves filing and serving of processes; the exchange of documents; etc. (Adamu, 2019). Traditionally, this process is paper-based and entails the creation, transfer and storage of hardcopy legal documents and paper-works which are in silos and confined within the four-walls of the custodian courts. There are two key approaches to automating the Judicial process:

1. **The Integrated approach**: This refers to a national one-size-fits-all approach to the digitalization of the judiciary such that every court uses the same system and database. Inherent in this approach is the use of universal database schemas which engenders ease of collaboration and data sharing within and between courts.
2. **The Siloed approach**: With this approach, each court or jurisdiction develops and maintains its own systems and databases at the state or federal level. Consequently, there will be multiple systems tailored to the needs of each court and developed according to the capacity and design preferences of the vendors or developers. Unless there is a nationally agreed and endorsed design-template covering design specifications, requirements and database schemas, this approach will result to and retain the silos and balkanization of data and information that characterized the traditional paper-based system. The ultimate consequence of this will be the challenge of integrating these siloed systems, and extracting and sharing meaningful information between them, i.e. the challenge of data exchange.

According to Fagin (2005), data exchange is the process of taking data structured under a source schema and creating an instance of a target schema that reflects the source data as accurately as possible. Simply put, it allows different computer programs to share data and would only be useful where the judicial process is automated using the siloed approach or where a national e-judiciary system needs to be integrated with the entire criminal justice chain, i.e. connecting to the systems used by the Police and the Prison/Correctional Services (Langbroek & Tjaden, 2009).

2.1 Current Automation of the Nigerian Judiciary: Data Exchange or Information Sharing?

Most countries are adopting the integrated approach to automating the judicial process, for example the United Kingdom (Ministry of Justice, 2016); the United States (United States Courts, 2013), and some European countries including Italy, Netherlands, France, Greece, Belgium, etc. (Langbroek & Tjaden, 2009; Velicogna, 2007). Fortunately, Nigeria is not left out of this trend and runs an integrated system called the Nigerian Case Management System (NCMS) which was developed by the National Centre for State Courts, USA and donated to Nigeria. The NCMS automates the case-flow management including case filing, case assignment, delivery of judgements and generation of statistics and reports (Adamu, 2017). The NCMS is also expected automate and ensure secure exchange of documents between different court levels enhance secure exchange of electronic. With such a system, focus should be more on the more practical aspect of information sharing than on data exchange until when the system needs to be integrated with other systems external to the judiciary but part of the criminal justice chain.

To further foster information sharing and communication within the Nigerian judiciary, the National Judicial Council deployed the Legal Mail System (Adamu, 2017) is based on the Microsoft Office 365 service (Adamu, 2019). According to the Nigerian Bar Association (N.D) Legal Mail System is for every Lawyer verified by the Nigerian Bar Association and would facilitate two-way lawyer-to-lawyer and court-to-lawyer communication.

2.2 Future Automation of the Nigerian Judiciary: From Information sharing to data exchange

Both the NCMS and Legal Mail System are integrated, insulated and exclusively used by the Nigerian Judiciary as in many other countries; therefore, there is currently no need to interact with external systems and consequently no need for data exchange. However, in the near future, there may be the intent to integrate the NCMS with the entire criminal justice chain, i.e. connecting it to the systems used by the Police and

the Prison/Correctional Services as has been attempted in the Netherlands (Langbroek & Tjaden, 2009). There may also be need to connect to other systems and databases outside the criminal justice chain therefore making data exchange a requirement.

A prospective automated criminal justice chain would most likely consist of multiple systems which were individually developed to be insulated and exclusive to the body that owns it. As such, theoretically, these individual systems may contain data in incompatible formats and it would be challenging to exchange data between them. To overcome this challenge, Application programming interfaces (APIs) are developed and used to enable communication between various systems. It provides a unified way to opening up information assets and sharing them easily thus facilitating data exchange. APIs can perform data exchange using one or a combination of data exchange languages like Atom, JSON, REBOL, YAML, XML, etc. However, XML (Extensible Markup Language) is most widely accepted, is an open standard and most systems come bundled with it. It is a generic data storage format that makes it easier to exchange data between incompatible systems and is being extensively used by the NFIU to integrate, share with and retrieve data from various stakeholders in the Anti-money laundering and counter financing of terrorism (AML/CFT) regime. XML would undoubtably be key when the Nigerian Judiciary makes the move from information sharing to data exchange.

3.0 Automation: The attendant Risks

The automation of work and communication flows simplifies work processes; enhances productivity and collaboration; and ushers in more efficient and innovative approaches to the collection, use and management of corporate data. However, with these benefits come new risks to the security of the automated systems and the privacy of the data they hold. According to Varonis, Data breaches exposed 4.1 billion records in the first half of 2019. A study by Sophos discovered that 7 in 10 companies have been hit by a cyberattack; and these attacks are frequent – According to a study by Ramsbrock, Berthier & Cukier (2007) are happening all the time to computers with Internet connections at the rate of 39 seconds on the average.

It is evident, therefore, that these threats are real and should be a challenge to the judiciary as much as they are to other sectors and businesses. There are, indeed, numerous examples of cyber attacks targeting the confidentiality, integrity and availability of judicial data, information and ICT infrastructure. For example, in 2014 and according to Bloomberg Law (2018), a group named the European Cyber Army successfully attacked government platforms around the world and this affected the US Public Access to Court Electronic Records (PACER) system as well as the official website of the US Federal court (www.uscourts.gov). In a separate incident, the Atlanta Municipal Court was hit with a ransomware attack which prevented it form accessing its electronically stored scheduling information and from validating outstanding warrants (Dixon, 2019).

4.0 Likely Attacks and Mitigation Techniques

4.1 Phishing attacks

Phishing attacks are the most common cyber threats and about 76% of businesses reported being victims (InfoSec, 2019). Through such attacks, corporate and sensitive data may be divulged; attackers may gain access to and can introduce malware to the corporate network. The Nigerian Legal Mail System would be certainly a target for phishers. To mitigate phishing threats, SPAM filters should be used to detect and block potentially harmful email messages; all systems must be kept with the latest security patches and updates; information security policies covering password expiration and complexity should be developed and implemented; and, most importantly, users of the email system must be trained to detect and react to possible phishing emails and put through mock phishing sessions.

4.2 Ransomware Attacks

Courts are now seen as a potentially lucrative source of sensitive data for hackers (Starks, 2020) and this has resulted in an increase in ransomware attacks against the judiciary. Ransomware is a form of malware that encrypts victims' files with the hacker demanding ransom, usually in bitcoin, before access can be restored. The

NCMS has been designed to receive and store enormous data that hackers may find attractive and is, therefore, susceptible to ransomware attacks. To prevent this, operating systems must be patched and up-to-date; system administrators and users must also be wary of software applications that demands for administrative privileges during installation.

4.3 Denial-of-Service (DoS) Attacks

There is also the denial-of-service (DoS) attack and its variants which aim to overwhelm corporate systems, servers or networks with traffic thereby exhausting resources and bandwidth and preventing the systems from functioning properly. The NCMS can be a target of such an attack although the severity may be insignificant because the system is currently not widely used and has not been adopted as the only means of carrying out day-to-day business activities in Nigerian courts; however, this may change in the near future. To prevent and mitigate this threat, early threat detection systems should be deployed; the network should be secured with a combination of firewalls, VPN, anti-spam, content filtering, load balancing, and other layers of DoS defense techniques; and there should be a response and recovery plan for when an attack was not prevented.

4.4 Man-in-the-middle (MitM) Attacks

Another likely attack is the Man-in-the-middle (MitM) attack which is also known as eavesdropping attack. This happens when an attacker inserts himself between the communications of a client and a server to filter and steal data. MitM attacks can be initiated over unsecure public Wi-Fi as the attacker can insert himself between a visitor's device and the network. It can also be initiated through the installation of malware or through social engineering techniques. It is obvious then that the NCMS and Legal Email System can be targeted by MitM attacks. To prevent this attack, there should be strong encryption mechanisms and router log in credentials on wireless access points to prevent unauthorized access to networks. Furthermore, websites should use and be accessed from browsers that enforce the Hypertext Transfer Protocol

Secure (HTTPS); this is so because in HTTPS, Transport Layer Security (TLS) is used to encrypt the communication protocol thereby preventing interference from attackers.

The last but definitely not the least likely threat is the insider threat which, ironically, is said to be the one of the most underestimated areas in cybersecurity even though it makes up about 60% of cyber-attacks in today's world and about 60% of organizations experience more than 30 insider attacks yearly (Deyan, 2020). Whilst some of these attacks may be malicious, majority of them are unintentional and due to negligence but with far reaching consequences. Both the NCMS and Legal Mail system can be affected by insider threats as data can easily be exfiltrated. To counter these threats, data use policies and controls should be created and enforced; employees should have training on insider threats amongst others; the principle of least privilege (POLP) should be adopted and user privileges must be reviewed periodically; physical and logical security must be established; and remote access from all endpoints must be monitored and controlled.

5.0 Conclusions and Recommendations

The Nigerian Judiciary has gradually started its journey towards automation with the Nigerian Case Management System (NCMS) and the Legal Mail System which would digitize the legal and judicial process and facilitate information/document sharing between courts and lawyers. Mirroring the approach to the automation of the judicial system on many countries, the NCMS and Legal Mail systems are insulated and exclusive for the Nigerian judiciary and currently does not allow data exchange.

However, in the near future, we are hopeful that the NCMS will be integrated to other systems and databases to facilitate data exchange between the Nigerian Judiciary, law enforcement agencies, anti-corruption agencies and intelligence agencies, etc. Such a system will assist the stakeholders in performing their duties to our country, Nigeria. The NFIU in particular will be open to working with the Nigerian Judiciary to engender a secure integration of our systems, collaboration and data exchange.

References

[1.]Adamu, M. (2017) *Nigerian Case Management System.* Available at: https://nji.gov.ng/images/Workshop_Papers/2017/IT_Workshop/s4.pdf

[2.]Adamu, M. (2019) *An overview of the Nigeria legal email system*. Available at: https://nji.gov.ng/wp-content/uploads/2020/03/An-Overview-of-the-Nigeria-Legal-Email-System.pdf prepared for national workshop for information and communication technology staff

[3.]Bloomberg Law (2018) *Confidentiality, Integrity, or Availability: The Cyber Threats to Our Judicial System.* Available at: https://news.bloomberglaw.com/business-and-practice/confidentiality-integrity-or-availability-the-cyber-threats-to-our-judicial-system

[4.]Deyan, G. (2020) *20 insider threat statistics to look out for in 2020*. Available at: https://techjury.net/blog/insider-threat-statistics/#gref

[5.]Dixon, H.B. Jr. (2019) *Cyberattacks on Courts and Other Government Institutions.* Available at: https://www.americanbar.org/groups/judicial/publications/judges_journal/2018/summer/cyberattacks-courts-and-other-government-institutions/

[6.]Doma, H. (2016) *Enhancing Justice Administration in Nigeria through Information and Communications Technology*, 32 J. Marshall J. Info. Tech. & Privacy L. 89. Available at: https://repository.jmls.edu/cgi/viewcontent.cgi?article=1786&context=jitpl

[7.]Duru, O. (2012) *The Role and Historical Development of the Judiciary in Nigeria*. Available at SSRN: https://ssrn.com/abstract=2142928 or http://dx.doi.org/10.2139/ssrn.2142928

[8.]InfoSec (2019) *Cyber security Statistics for 2019*. Available at: https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/

[9.]Langbroek, P., & Tjaden, M. (2009). *Organising data exchange in the Dutch criminal justice chain*. Transylvanian Review of Administrative Sciences, 5(28), 8-26.

[10.] McMillan, J.E. (1995) *Case Management Systems: The Four Bubbles.* Available at: http://www.ncsconline.org/WC/Publications/KIS_CasSysCTB1995McMillanPub.pdf

[11.] Ministry of Justice (2016) *Transforming our Justice System*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/553261/joint-vision-statement.pdf

[12.] Nigerian Bar Association (No Date) *Legal Mail*. Available at: https://nigerianbar.org.ng/legal-mail#:~:text=The%20Nigerian%20judiciary%20has%20taken,between%20lawy

ers%20and%20the%20courts.&text=Lawyers%20are%20required%20to%20obtain,%2C%202018%2C%20it%20became%20mandatory

[13.] Ramsbrock, D., Berthier, R., & Cukier, M. (2007*). Profiling attacker behavior following SSH compromises*. In 37th Annual IEEE/IFIP international conference on dependable systems and networks (DSN'07) (pp. 119-124). IEEE

[14.] Starks, T. (2020) *The Cyberthreat to U.S. Courts*. Available at: https://www.politico.com/newsletters/weekly-cybersecurity/2020/07/13/the-cyberthreat-to-us-courts-789121

[15.] Sze, T.Y. (2004), 'Singapore', in A. Oskamp et al. (eds.), IT Support of the Judiciary, p.48.

[18.] The Australian Parliament (2015) *The Role of the Judiciary*. Available at https://www.parliament.qld.gov.au/documents/explore/education/factsheets/Factsheet_5.1_RoleOfTheJudiciary.pdf

[19.] United States Courts (2013*) Improving court case management, financial systems and statistical reporting.* Available at: https://www.uscourts.gov/statistics-reports/improving-court-case-management-financial-systems-and-statistical-reporting

[20.] Velicogna, M. (2007*) Justice Systems and ICT: What can be learned from Europe?*, UTRETCHT L. REV. 3, 129. Available at: https://www.researchgate.net/publication/26463184_Justice_systems_and_ICT_-_What_can_be_learned_from_Europe