Association for Information Systems
AIS Electronic Library (AISeL)

SAIS 2016 Proceedings | Southern (SAIS)

2016

Criminal Court Redundancy Case Study: The Best Defensive is a Good Offense

Jennifer Breese
Middle Georgia State University, jennifer.breese@mga.edu

Johnathan Yerby
Johnathan Yerby, johnathan.yerby@mga.edu

Steven Tkach Jr.
27th Judicial Court of Pennsylvania, steven.tkach@washingtoncourts.us

CRIMINAL COURT REDUNDANCY CASE STUDY: THE BEST DEFENSIVE IS A GOOD OFFENSE

Jennifer Breese
Middle Georgia State University
Jennifer.breese@mga.edu

Johnathan Yerby
Middle Georgia State University
Johnathan.yerby@mga.edu

Steven Tkach. Jr.
27th Judicial Court of Pennsylvania
steven.tkach@washingtoncourts.us

ABSTRACT

This case study demonstrates the design suggested for modern court technology systems. The design and implementation of the new system prepares the court to serve the public and law enforcement needs continuity of essential court functions when the need arises. Lessons learned from natural disasters, cyber-attacks, and acts of terror have greatly influenced the resiliency and security of the new system. Consideration of multiple factors including: loss of power, domicile, security, and any potential disruption of service continuity will also be explored.

Keywords

Court information systems, forensic readiness, resilient systems

INTRODUCTION

Almost no one understands science and technology; this is a prescription for disaster. While we might get away with it for a short time, sooner or later this combustible mixture of ignorance and power is going to blow up in our faces (Sagan, 2011). Sagan's (2011) sentiment is indicative of the natural disasters which catapulted this issue into the national consciousness. Both the wrath inflicted by Hurricane Katrina on August 29th, 2005 and to a lesser extent Hurricane Rita thirteen days later caused court governing bodies to move to adopt additional preparedness measures. Swartz (2005) describes the damages caused by Hurricane Katrina as follows:

> By most accounts, Katrina left the Gulf Coast justice system in shambles. Mississippi and Louisiana court systems, like those of many other state governments, stored court files in the basements or lower levels of courthouses. As a result, both lost many records after Hurricane Katrina hit; records were washed away and, in most cases, there were no computer back-ups. The Louisiana State Supreme Court and Fifth Circuit Court of Appeals buildings were flooded, along with appellate files and evidence folders and boxes. The city and district courts in as many as eight parishes and three circuit courts were underwater, meaning the evidence and files stored there were ruined. According to Newsweek, there were 3,000 criminal cases in progress in New Orleans alone when Katrina struck, but now the district attorney might be forced to suspend many of those prosecutions because crucial evidence such as police reports, interview transcripts, fingerprints, and DNA samples were destroyed.

In the years since these storms and threats of pandemics, the Nation has had a chance to reflect upon the legal implications of both natural and manmade disasters (Wood, 2008). Post Katrina concepts that would otherwise be considered court security matters are either are presented alongside emergency management or with little distinction between the two. Further, many in the court community are unwilling or unable to present court security without including emergency management mentioning or they are intertwined (Cooper 2007; Raftery, 2007). Overlapping principles favor the presence of court related information technologists, the "C" levels, and the associated governing bodies. If the court system is unable to function as in the occurrence of Katrina little stands between citizens and the breakdown of law (Wood, 2008). Further, Greene (2009) discusses not only the need for continuity, but the legal aspect punishable by law if continuity is not accomplished by courts particularly if it is determined that continuity was accomplished for one societal group verses or over another.

The National Association of Court Management (NACM) and in turn state court governing bodies like the National Association of State Courts (NCSC) followed suit beginning the conversation for the obvious need for redundant systems located in separate geographies. A 2005 revision of the NACM *Court Security Guide* addresses potential impact of terrorism,

protection of users, and safeguarding resources and integrity of the court system (Cooper, 2007). The criminal court system was greatly impacted by the outages some examples include the loss of connectivity and access case management systems. In the aftermath of Hurricane Katrina, basic court functions were interrupted. Data centers (including some non-digitized records) were, in some locations, flooded and left inoperable because of an extended loss of electrical power. Telecommunication systems were also left inoperable because data communication circuits and even cellular telecommunication services inoperable or overwhelmed and thus jammed. Additional potential vulnerabilities are those most are well aware with regard to human factors: password strength, employee browsing, opening unsecured documents, using outside storage devices and the list could continue, but again the initial auspice for the project was Hurricane Katrina. Hacking in particular has great potential with regard to vulnerabilities; who would not want to ease their misdeeds or wreak havoc on the criminal justice system in these trying times? The moral of the story is that everyone is connected and everyone is vulnerable, but simple recognition of that fact is not enough. Looming systemic risks and vulnerabilities need careful planning and a continual protocol updates.

This case study focuses on the judiciary's response to and restoration of court services and is best explained by extensive preparation of Continuity of Operations Plans (COOP plans) developed for all federal courts throughout the country. COOP oversees the safety of employees and the public, ensures that essential functions and activities resume without interruption, and allow for resumption of normal services as quickly and as safely as possible (Huff, 2006). The installation and maintenance of a ready alternate site for technical services within each Judicial District materially expands the flexibility and viability of the established Continuity of Operations Plans (COOPs).

DESIGN PRINCIPLES

Recent research and critical incidents have brought a new attention to security, recovery, and readiness. Court directors must consider a range of complex issues such as physical security, employee safety, structure of data and communications, and their ability to perform in a disaster, policies to meet the needs of the public, and who is responsible (Birkland and Schneider, 2007). Outcomes from this system were to create a secure system, which was cost effective, simple to use, and the ability to search for media of many types and track changes made in the system. The rise of document management systems have become preeminent in meeting many of the challenges of providing access to court records from "birth to death" and allowing access to them from virtually any location with the requisite configuration(s). These systems also provide a comprehensive audit trail and tracking system(s) detailing even the most minute changes and/or access to court resources.

Security

As records and personal sensitive information moves from a box in the basement to a server connected to the world, security becomes increasingly complex and requires much more than a door lock and security guard. Securing business or home networks is fairly well understood by trained security professionals. Securing the unique resources of a court system requires a system and policies tailored to the type of assets it is protecting. Reviewed best practices can be found in the *Blueprint for the Security of Judicial Information (2013),* including Policy 3c: "Privacy Impact Assessments will be undertaken at the design stage of court information management systems that involve the potential collection, access, use, or dissemination of personal information." Another recommendation from the *Blueprint* document on implementation on section 110 as "If any system, compilation (database) or storage medium contains classified information, then the entire system, compilation (database) or medium must be so classified."(Blueprint, 2013). Recent research on the costs of an information assurance system and the resources it is protecting advocates for a tiered budgeting model. The optimal level of security investments should be determined by the change in the marginal productivity of the investment with respect to change in the vulnerability. Items with a higher level of importance received greater resources when designing the system (Gordon and Loeb, 2002). With that being said, Wood (2008) warns of over complicating the system.

Forensic Readiness

The concept of forensic readiness for a system means that there has been thought before an incident occurs to collect and log credible information that could be useful if an incident were to occur (Taylor, Endicott-Popovsky, Frinke, 2007). It is not feasible to build the most robust system ever thought of and have every single action logged because it would be costly and create more information than there would be a use. Tan (2001) described the two objectives of forensics readiness as: keeping costs for a potential incident at a minimum and the system should be able to collect a maximum of relevant digital evidence. Further, Tan (2001) demonstrated a scenario where a hacker spending 30 minutes on an attack would require an investigation time of at least 48 hours. The need for forensic readiness is two-fold when building a system that many will not only need to track what happens to the system, but also the extremely important information stored within the system. Evidence for old,

current, and future legal proceedings are being stored and accessed in this system. The system designed in this case needed to be robust enough to allow many users to search for, access, and log, but not modify, evidence they were authorized to access. The need for data integrity was and is paramount. Careful attention was given to the forensic readiness of the system designed collaboratively by the two court systems.

Additional benefits to the creation of a forensic ready system include; being a useful deterrent to insider attacks, ability to perform rapid investigations, systematic evidence storage saving time and money, demonstrates due diligence to stakeholders and compliance, and the ability to support sanctions for violations (Rowlingson, 2004).

Joint Venture

An agreement was established between the Court of Common Pleas of Allegheny County, Fifth Judicial District, and the Court of Common Pleas of Washington County, Twenty-Seventh Judicial District, to enhance the disaster recovery operations of both Judicial Districts by providing for redundancy capabilities for their respective information technology operations. The redundancy design could be classified as a sort of private cloud for each entity. There are well documented possible weaknesses with using a public cloud infrastructure such as the unknowing of who is handling your data, where your data is, what happens if your data is subpoenaed or ordered to be destroyed, is your data isolated, and what happens in an outage (Jansen & Grance, 2011). Utilizing a private cloud where managers from each site have the same type of business and understanding of the type of data, understood agreements in up-time, and securing the resources synergistic forces combine to create a tailored solution for the greatest benefit for each partner (Wood, Lagar-Cavilla, Ramakrishnan, Shenoy, & Van der Merwe, 2011). The sites are flexible on bandwidth as needed since the communication channels between the private clouds are private lines. With the private off-site disaster recovery partner nearby with private lines each court system could expect to see benefits in reduced time to restore files, if there are future partners with other off-site locations this would enhance the restore time, redundancy, and resiliency of the network (Chang, 2015).

Based both on the need and the previously established trust relationship, two Western Pennsylvania county court systems developed a protocol regarding levels of sustainably with certain systems as well as technology redundancies to ensure those most critical systems have maximum uptime. Systems that were not mission critical were given "acceptable" ratings for the ability to go without them for certain intervals for example: 48 hours, one week, two weeks and so on.

Resiliency

Each site has the necessary telecommunication circuits that allow for the connectivity to state and national database systems. With the replication of "critical" data at each of the court sites via the dedicated communication circuit, each site can provide connectivity to both each jurisdiction's "critical" data as well as to the necessary telecommunications circuits in the event that one of the data centers and/or court facilities became inoperable. The use of a "foreign" ISP service ensures that disruption in the local ISP service, such as in the floodplain prone downtown Pittsburgh location will allow the porting of Internet connectivity to the location where the "local" ISP service is unavailable due to either infrastructure of emergency/disaster issues. The replication technology uses a newer version of secure border gateway protocol to communicate between the two sites.

With the partnership between the two systems there were several benefits over outsourcing critical sensitive data of the legal system, such as; greater control and knowledge of where the information resides and lower TCO. The disadvantage of using this solution instead of outsourcing to a cloud provider is the potential for downtime in a massive outage or regional catastrophe.

SELECTED AGREEMENT PRINCIPLES

A. Each Judicial District will place information technology equipment under the physical control and authority of the other Judicial District. All equipment acquired pursuant to this MOU will be utilized for connectivity, backup and redundancy of information systems. The equipment will remain the property of the owning Judicial District, and liability for damage to said equipment will remain the responsibility of the owner Judicial District, absent damage caused by reckless or intentional misconduct of personnel of the housing Judicial District.

B. The Fifth Judicial District agrees to purchase all of the equipment and services necessary for this project. The Twenty-Seventh Judicial District will reimburse the Fifth Judicial District for the cost of any

equipment purchased for the primary use of the Twenty-Seventh Judicial District within thirty (30) days of receiving written notice of the cost and delivery of such equipment.

C. Initially, the Fifth Judicial District will enter into a contract for separate communication lines. The cost of this Internet connectivity line will be split proportionally between the Judicial Districts.

D. All purchases of equipment and services will be agreed to by both Judicial Districts and will be based upon sound, fiscally responsible information technology business practices that are compatible with each Judicial District's COOP.

E. The District Court Administrators of the Fifth Judicial District and Twenty Seventh Judicial District agree to provide exchange and maintain current names and detailed contact information of authorized representatives for each Judicial District designated to obtain and/or grant ready access to areas wherein the equipment covered by this agreement is located. Such access will be made available within one (I) hour of any request for access, on a twenty-four (24) hour, seven (7) day per week basis. All equipment covered by this agreement will be located in secure locations that are under the exclusive authority and control of the housing Judicial District.

F. The Fifth Judicial District and the Twenty-Seventh Judicial District agree. To review this MOU, minimally, on an annual basis, to ensure that the project has been implemented and is maintained in an efficient and effective manner that meets the respective needs of the parties.

G. The Fifth Judicial District and the Twenty-Seventh Judicial District agree that this MOU is effective upon execution by all parties and shall be fully incorporated into and made part of each Judicial District's COOP.

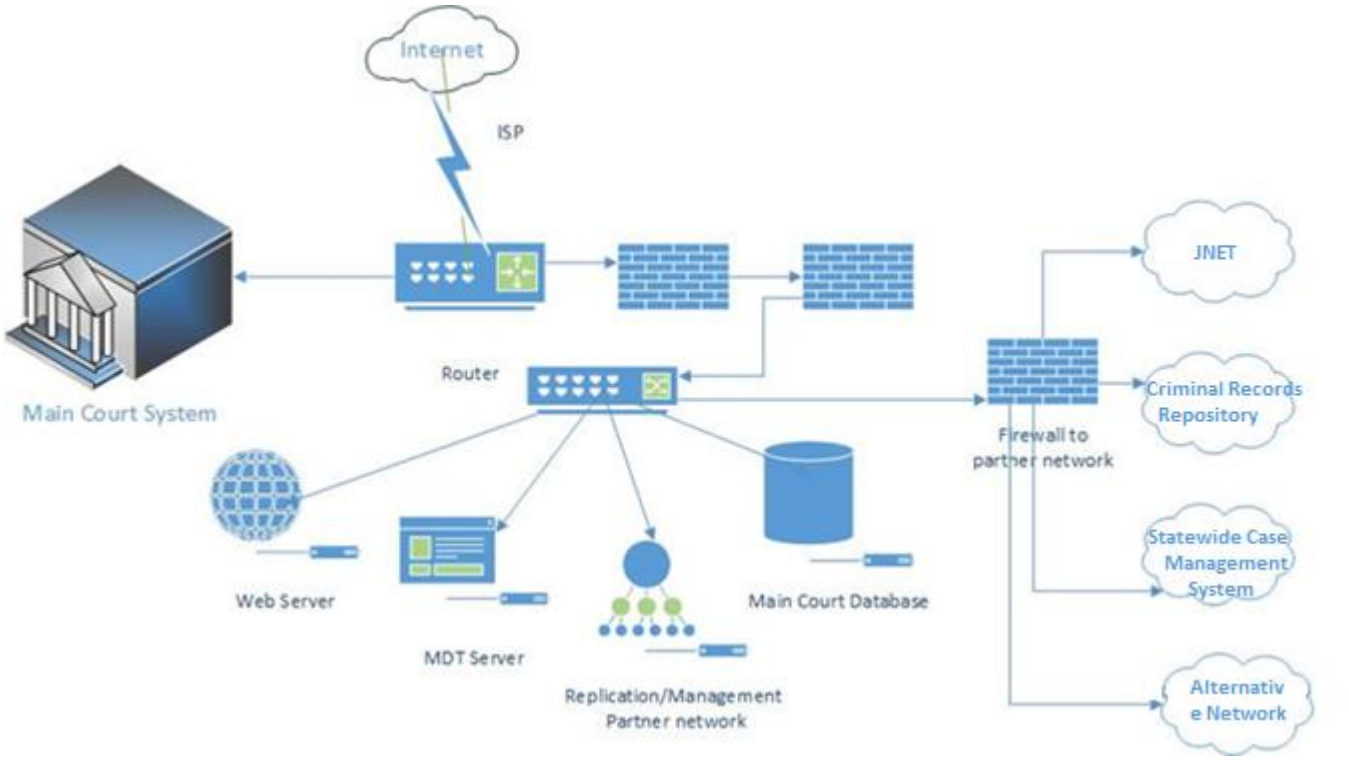

Figure 1. Diagram of court system

CONCLUSION

While our society tends to condemn courts that define the critical components post-crisis as a "blame game," or courts which have the situation defined for them in those terms will rightfully suffer from the associated condemnation (Raftery, 2007). Society focuses on vulnerabilities of credit card companies, banks, and health care with regard to safety, security, and function, but most importantly we need to refocus on systems like courts and criminal justice with even more vigilance. Additional future research should include what Bhasker (2006) termed a "Cyber Katrina" meaning an overall infrastructure failure among networks in the United States. Bhasker (2006) suggested a combination of processes based upon traditional investigative procedures supported by a computer security incident response team can utilize limited resources available and effectively protect citizens from a possible Cyber Katrina. A broader view of how Federal and State agencies plan to manage these potential cyber incidents would add a needed perspective to this case overall.

This case study adds clarity that court technology systems at local levels are both heeding directives and proactively designing for crisis scenarios based on historic events and those which we have yet to encounter. Digital records are the maxim by which many must follow, but when reviewing systems by which our liberty and the basis of law and order depend upon redundant systems that also need to follow suit. While civil courts are very important in democratic systems; moreover, the importance of the criminal courts ability to function in real time with little or no downtime is essential to ensure chaos does not ensue.

REFERENCES

1. Bhaskar, R. (2006). State and local law enforcement is not ready for a cyber Katrina. *Communications of the ACM*, *49*(2), 81-83.
2. Birkland, T. A., & Schneider, C. A. (2007). Emergency management in the courts: trends after September 11 and Hurricane Katrina. *Justice System Journal*, *28*(1), 20-35
3. Canadian Judicial Council, "Blueprint for the Security of Judicial Information", 4th ed (2013): Canadian Judicial Council.
4. Chang, V. (2015). Towards a Big Data system disaster recovery in a Private Cloud. *Ad Hoc Networks*, *35*, 65-82.
5. Cooper, C. S. (2007). The evolving concept of "court security". *Justice System Journal*, *28*(1), 40-45.
6. Greene, L. S. (2009). Government liability for the Katrina failure. *Hurricane Katrina: America's unnatural disaster*, 206-225.
7. Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, *5*(4), 438-457.
8. Huff Jr, G. B. (2006). Planning for Disasters: Emergency Preparedness, Continuity Planning, and the Federal Judiciary. *Judges J.*, *45*, 7.
9. Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing. *NIST special publication*, *800*, 144.
10. Raftery, W. E. (2007). Mini-Symposium ON Court Security. *Justice System Journal*, *28*(1).
11. Rowlingson, R. (2004). A ten step process for forensic readiness. *International Journal of Digital Evidence*, *2*(3), 1-28.
12. Sagan, C. (2011). *Demon-haunted world: science as a candle in the dark*. Ballantine Books.
13. Swartz, N. (2005). Katrina Devastates Gulf Records. *Information Management*, *39*(6), 24.
14. Tan, J. (2001). Forensic readiness. *Cambridge, MA:@ Stake*, 1-23.
15. Taylor, C., Endicott-Popovsky, B., & Frincke, D. A. (2007). Specifying digital forensics: A forensics policy approach. *Digital investigation*, *4*, 101-104.
16. Wood, D. P. (2008). Bedrock of Individual Rights in Times of Natural Disaster, The. *Howard LJ*, *51*, 747.
17. Wood, T., Lagar-Cavilla, H. A., Ramakrishnan, K. K., Shenoy, P., & Van der Merwe, J. (2011, October). PipeCloud: using causality to overcome speed-of-light delays in cloud-based disaster recovery. In *Proceedings of the 2nd ACM Symposium on Cloud Computing* (p. 17). ACM.