DATA DEFENDERS
Defenders of the Information World™

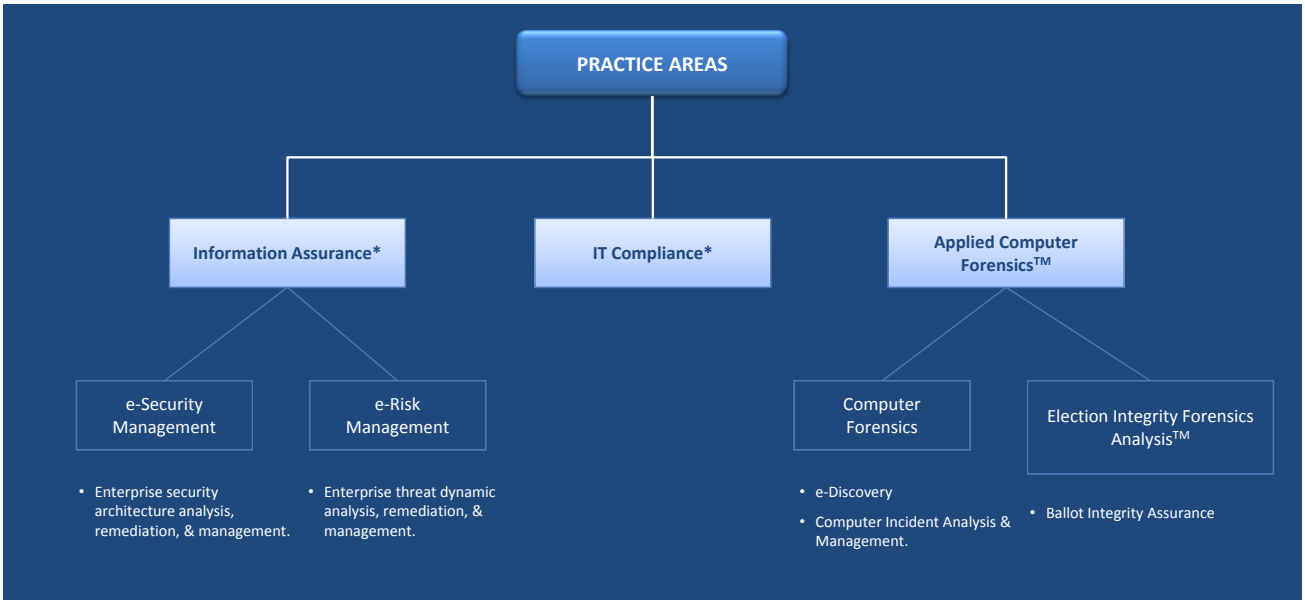
Forensics: The Vital Link In Election Integrity

A Case Study on Cook County, IL

About Data Defenders, LLC

Data Defenders was founded in February 2005. Data Defenders is focused on helping election jurisdictions maintain the public's trust and confidence in the voting process by delivering information assurance and applied computer forensics processes that assure ballot integrity.

Data Defenders developed a unique information assurance paradigm that merges the information security and computer forensics fields to create unique processes that are designed to enable the election jurisdiction to attain and maintain the highest level of operational integrity in their electronic voting and other enterprise information systems. Our information assurance services are divided into three practice areas: Information Assurance, IT Compliance and Applied Computer Forensics.



"Data Defenders – a positive, cooperative partner from the start – provides comprehensive auditing of our complex computer systems. Their work adds a valuable extra level of security to our election process. When I talk about forensic analysis with the public, they are pleased to see the analysis has demonstrated the safety and security of our system."

—David Orr, County Clerk
Cook County, Illinois

Applying Forensic Analysis Techniques in a Voting System Environment:

The 2006 General Election in Suburban Chicago

The 2006 election cycle in Cook County, IL was the first in which the county's new electronic voting system was implemented. The normal challenges associated with any new technology platform in an election environment were demonstrated. Despite new approaches in training and preparation for the fall general election, technical challenges resulted in the delay of some election night returns. Under the leadership of David Orr, Cook County Clerk, problems related to the transmission of results were not going to stand unaddressed for very long.

In the weeks after the Election, Mr. Orr appointed a technical review panel, headed by former United States Court of Appeals Judge Abner Mikva. It consisted of specialized experts in the computer sciences and among them was Cyrus Walker, CEO of Data Defenders. During its investigation of Cook County's voting system, the technical review panel was able to analyze and document the system's activities and review the actual sequence of events. The investigation found that the primary cause of the delays was the vendor's faulty communications link between the software and the modem inside the transmission devices.

As part of the panel's work, a forensic analysis of the county's voting system was conducted to prove its operational integrity. It was a "Eureka" moment for the County Clerk's office. The value of a forensic analysis approach in the conduct of future elections in Cook County was quickly recognized not only in a post-election audit process, but from an overall information technology risk-mitigation strategy. While computer forensic principles were applied in the post-election investigation, the most effective approach for computer forensics was recognized in its ability to monitor the voting system throughout the election management process.

Cook County quickly recognized that as the voting system moves from one stage of readiness to the next, valuable data could be analyzed for troubleshooting, the detection of security threats and the application of a robust auditing solution should future problems arise.

Computer Forensics: What Is It?

Computer Forensics refers to the practice of obtaining information in computers and digital storage media as evidence in a legal proceeding. All computers contain digital artifacts that are recoverable after a specific event, very much like physical crime scenes and the evidentiary proceedings popularized in television and movies. These digital artifacts include CD-ROMs, e-mail messages, hard drives and software (Schweitzer 2003). Any type of electronic device lends itself to a forensic analysis, or audit, for the purpose of identifying the sequence of events leading up to a system failure. When applied, computer forensics has the ability to recover data, detect system intrusions, preserve evidence and analyze a system's performance (Schweitzer, 2003).

The application of computer forensics is a growing field of study as our communities become more and more dependent on information technology. However, the application of computer forensics in the world of election administration has been extremely limited. In the past few years, well-publicized security reviews have been undertaken on voting systems providing an overall risk assessment, but these reviews both in the states of California and Ohio resulted more in an assessment of the quality of voting systems currently being manufactured and overall system vulnerabilities rather than an a comprehensive approach towards risk mitigation and system monitoring. Cook County conducted its own analysis and independent review of these studies and concluded that the system vulnerabilities indicated in each of these studies could be mitigated through the use of a computer forensics solution.

Applying Computer Forensics in the Election Environment

Since the 2000 election and the enactment of the Help America Vote Act of 2002, the United States undertook a tremendous leap forward in the use of electronic voting systems. Due to the vocal and well-publicized efforts of advocacy groups, the technology of Direct Recording Electronic (DRE) voting systems has now ebbed. The peak of electronic voting terminals in the United States occurred during the 2004 election (Election Data Services, 2008). Since that time, there has been a marked shift back to paper based balloting; however, DRE voting units remain in our nation's polling places for purposes of providing access for voters with disabilities. Taking the place of DRE voting units, as the primary voting technology, has been precinct-based optical scan devices which still rely on a combination of hardware and software for vote tabulation. During this tumultuous period of debate, our nation's election officials have responded by moving back and forth between technologies based on the shifting demand of their constituents; however, the development of assurance tools for verifying the integrity and stability of the technical processes in an election office have been lacking while reliance on new technologies and software in our nation's election infrastructure has remained intact.

The United States Election Assistance Commission (EAC) has attempted to address the concept of auditing and voting system security through its Quick Management Guidelines outlining the following best practices for local election officials including:

- Hash Code Testing—Comparing a file signature from the certified software to the software as it is installed in the local jurisdiction
- Acceptance Testing—Verification that the software and hardware present on a system are the versions certified for use and each unit is in working order
- Logic and Accuracy testing (pre- and post election)—Testing of the voting system's logic and tabulation functions to verify system accuracy based on a predetermined test election
- Parallel testing—Random sampling of voting units deployed in real-time election conditions to verify the ongoing correct logic and tabulation settings (EAC, 2010)

Unfortunately, all of these approaches are static analysis tools and do not capture the nuances associated with the software and hardware as it moves through an election event. Effectively, each of these reflects a minimum approach for capturing a "moment in time" and do not reflect the true behavior of voting technologies as they are deployed.

In today's election offices around the country, technology is increasing its role and dominance. The continued use of DRE voting systems, the use of computer software driving both the ballot formulation and ballot tabulation stage of the process and the application of electronic pollbooks are becoming more and more prevalent. In addition, innovative election processes such as early voting and instant runoff voting all lend themselves to the need for embracing more technology, not less. Regardless of the technology employed, all critical infrastructure components involved in an election can benefit from a forensic approach. Rather than focusing strictly on the end product of an election, forensics can enable a jurisdiction to anticipate problems as their technologies interact. The questions that election officials must ask themselves are:

> "Is my office able to produce verifiable evidence to support the validity of our election results?"
>
> "Am I doing enough to monitor my overall system performance to mitigate and detect potential threats?"
>
> "What is my plan of action if something goes wrong?"

The application of computer forensics can provide assurances not only to an election official's constituents, but each election official can personally receive assurances that the entire system is operating as it should and its integrity remains intact.

Applied Computer Forensics™

Traditionally, forensics has been applied to systems in a post-assessment scenario when the system is idle and a full audit can be deployed. This type of audit takes months and requires substantial resources. It also does not provide an ability to respond to threats and problems as they occur. With the financial stakes so high in the banking and technology sectors of our economy, these industries are applying computer forensics in active environments so these industries can be truly responsive to dynamic threats. Although election officials are not involved with financial transactions, the value in maintaining voter confidence and the realization that elections are a one-time pass/fail event, lends them to a real-time approach with regard to a forensic analysis.

Applied Computer Forensics™ is the systematic approach that governs how data is collected and preserved for use in a legal proceeding and as an overall process improvement model. It is the application of these approaches and methods developed into a solution that works in response to the specific needs of a client. Since a traditional forensic analysis of an electronic voting system can result in an examination of millions of files requiring months of time and resources (two items that are in shorty supply in an elections office) an application of the forensics process is necessary in order to shorten the time and effort required to thoroughly complete an analysis.

Data Defenders has developed a set of automation tools that provide a scalable solution for election jurisdictions to apply computer forensics on a real-time basis. The automation process allows for an expedited review of the election system and a more efficient approach for finding the proverbial "needle in a haystack." If a system anomaly is detected, a full scale incident analysis is conducted which applies the full suite of forensic methods toward that specific incident.

The combination of system automation and full forensic auditing offers the most flexibility for a jurisdiction that is looking to maximize its resources, provide real-time monitoring and shorten the time frame for providing assurances that the operational integrity of the system has remained intact.

The EIFA™ Approach In Practice- Revisiting Cook County

Since 2007, Data Defenders, LLC has implemented its Applied Computer Forensics process, called Election Integrity Forensics Analysis (EIFA)™, in the Cook County Clerk's office as part of its overall election integrity management plan. Cook County's approach for the EIFA™ process focused on the operation of its core voting system. The core services offered under the EIFA™ process include:

Data Acquisition & Imaging: Forensic images are acquired from randomly selected electronic voting system components. Images acquired represent exact duplicates of each voting system component.

High, Medium and Low-Level Data Analysis: Data is analyzed as it is collected; thereby, allowing election officials to address system issues that may threaten ballot integrity before election day. The data analysis stage includes reviewing file behavior within its relative system and detecting changes that may have a negative impact on system performance.

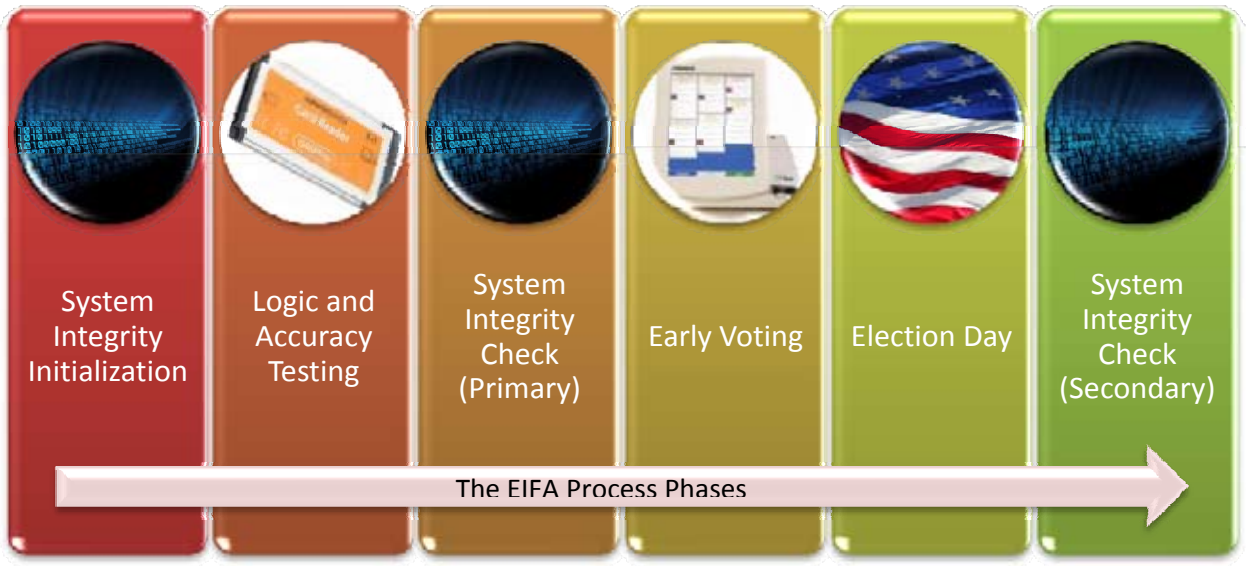
Incident Analysis: Forensic images are analyzed to identify changes made to the file system structure for all critical systems. An analysis is undertaken to identify authorized system changes and operational irregularities as potential indicators of tampering. Should any indications of tampering occur, each instance is reviewed for the root cause(s). If system tampering is detected, all data for the devices involved will be handled according to generally accepted law enforcement rules for criminal evidence.

Data Archiving: All data is stored using an information dispersal algorithm and remains securely preserved for use in any subsequent election contest. The archival process incorporates the same technology use by the Department of Defense and other federal government agencies to store sensitive data.

The EIFA™ process serves as a comprehensive approach for the detection and deterrence of any unauthorized activities which could negatively impact the normal operations of the voting system. By focusing on data at the smallest level possible, the bit level, Data Defenders monitors all system activities to detect system anomalies, those events that fall outside the normal range of expectations. Any anomalies that are detected trigger a full forensic incident analysis, resulting in the creation of an election archive.

Data Defenders assigned project managers to work with the Cook County Clerk's office to integrate the EIFA™ process in a seamless manner with the least amount of disruption to their election operations. As with any scientific approach, Data Defenders incorporated a control set of equipment that reflected basic system readiness as it was received by the election office from the manufacturer. By establishing a baseline from the control, Data Defenders monitored all file changes and system activities as the voting system was prepared for use in the election. Data Defenders used a combination of forensic analysis tools to identify and monitor the integrity of every file in the voting system. Based on the volume of data, automation was incorporated into each phase of the process in order to reduce costs and increase the detection speed of any system anomalies. Ten terabytes of information were collected from Cook

Figure 3: The EIFA™ Process In-Practice



Cook County incorporates the EIFA process into its election management practices. The EIFA process is a methodical approach that analyzes the customer's identified core pieces of election infrastructure and monitors them as they move through each stage of the election process. Each system component is analyzed for system integrity. Should any anomalies be detected, a separate analysis is conducted on each incident. If the analysis indicates potential system tampering, the information is stored and subject to retrieval for subsequent investigation.

County's voting system and a total of over six million files were analyzed.

At the completion of the 2008 Presidential Election Cycle, a full forensic audit report was presented to the Cook County Clerk's office verifying that no evidence was found of malicious code or tampering in its voting system. Although no evidence was found, Cook County has taken the proactive step to manage any type of disaster that arises from the technical operation of their elections. Since 2006, the Cook County Clerk's office has positioned themselves well with their ability to provide positive assurances that its election infrastructure operates with the utmost integrity. Should something happen in the future, Cook County will be able to readily respond by documenting all of the activities that transpired and apply lessons learned as part its process improvement plan.

References

Diamond Management & Technology Consultants (2007). *Report on the Use of Voting Technology in the November 7th Cook County Election*. Report to County Clerk Election Review Panel, Chicago,IL. Retrieved March 17, 2010 from www.suffredin.org.

Election Data Services (2008). National Voting Equipment Report. Retrieved from www.electiondataservices on May 10, 2010.

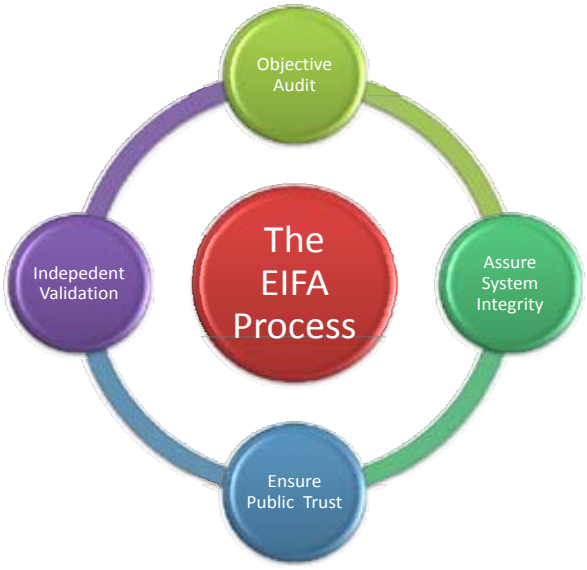
Schweitzer, D. (2003) *Incident Response: Computer Forensics Toolkit*. Indianapolis, IN: Wiley Publishing.

United States Election Assistance Commission (EAC) (2010). "Election Management Guidelines". Washington, DC: Retrieved March 20, 2010 from http://www.eac.gov/election/quick-start-management-guides

Benefits of the EIFA™ Process

Our nation's election officials stand on the frontlines protecting our nation's election infrastructure. With the ongoing move towards more technology in election offices in the form of voting systems, electronic pollbooks, early voting technologies and voter-assistive devices, the potential for denial-of-service attacks or system intrusions remain constant. In an effort to remain diligent, election officials should recognize their role as disaster management specialists and incorporate the core principles of emergency preparedness: mitigation, preparation, response and recovery.

The EIFA™ process is the most comprehensive approach for election officials to incorporate these four principles of emergency preparedness. Data Defenders and its EIFA service allows election officials to proactively respond to election crises and maintain voter confidence without resorting to frenetic attempts at post-election investigations when the ability to respond is at odds with the need to be responsive to the media, candidates and constituents.



For more information contact:
Data Defenders, LLC
10 W. 35th St., Suite 9F5-1
Chicago, IL 60616
Ph: 312.224.8831
sales@data-defenders.com