

# **KEMESA LLC WHITE PAPER: BEST PRACTICES IN RECORDS MANAGEMENT SECURITY**

*Few would argue that we are in the midst of an identity theft epidemic. In 2009 alone 223 million data files were compromised (Source: Identity Theft Resource Center). Worse still the hackers and fraudsters who are reaping the rewards of an estimated \$1 Trillion worldwide are essentially "untouchable" (1 in 700 are successfully prosecuted... Source: FBI). On top of all of this is a growing trend to make the record holders responsible for not just reporting database breaches, but also for the damage caused by them.*

*In the midst of this onslaught an amendment to the Homeland Security Act is under consideration that would require States to collect private information about "beneficial owners" of all companies filing for the legal right to do business. Irrespective of the outcome of this initiative, the operative question is:*

## ***HOW WELL DOES YOUR STATE PROTECT THE INFORMATION IN ITS DATABASES?***

### **PARAMETERS FOR SECURE RECORD MANAGEMENT BEST PRACTICES**

*To help each State answer this question we have provided a summary of what experts recognize as best practices parameters that are essential characteristics of current secure records management systems. These characteristics are viewed as prerequisite to successfully protecting the privacy of sensitive information, repelling database breaches and enhancing law enforcement's efforts to prosecute offenders.*

*If many of these parameters are unfamiliar it is not an indication that you may be behind your peers in protecting the privacy of your constituent's sensitive information. Rather it is an indication that staying ahead of "the bad guys" is a constantly evolving and full time job that requires the involvement of experts who are single minded in their dedication to the security of your data systems.*

#### **Parameter #1: Dynamic Encryption**

*Private data is dynamically encrypted so it is accessible only by those authorized (data owner or qualified third parties). The importance of the encryption being dynamic (i.e. constantly changing) is that there will be more keys than the bad guys can decrypt.*

### **Parameter #2: Fragmentation**

Each data component is separated into small pieces and placed on multiple databases in different random orders. The result is that there is no central database. Even if all the separate servers containing the entire database or all backup tapes were stolen they would not have any coherent information on them for the hackers to steal.

### **Parameter #3: Compartmentalization**

Placing function specific data management services on dedicated resources into separated compartments allows for the implementation of security procedures, protocols, and systems that protect each specific function. This ensures that database functions must be accessed from authorized points, and gives high visibility when unauthorized attempts are made out of the approved access pattern.

### **Parameter #4: Physical Network Separation**

By maintaining fragmented databases on separate networks the likelihood of all the data being breached is reduced. Separate networks also require separate attacks by an offender thereby increasing their exposure and risk of being detected. This also ensures that data cannot be put together except through authorized access points by data owners or assigned owners, and minimizes theft of an entire database.

### **Parameter #5: Multi-factor Authentication**

Multi-factor authentication is something you have (tokens), something you know (passwords), or something you are (biometrics). Having at least two out of three of these provides a higher confidence that the persons accessing data are who they say they are

### **Parameter #6: Repediation**

The act of using an authentication system that bases its tokens upon the history of their use during authentications provides repediation. By looking at the history of tokens it can be determined if the user's account was accessed from their authorized device. This is an algorithm attached to the access verification virtual token method. It provides proof that the chain of accesses has been consistent or evidence that it has been broken. This ensures a log for audit of authorized activities by owners and of data access.

### **Parameter #7: Defragmentation and Decryption Control Point**

By limiting the points where data can be decrypted and defragmented there is a significant reduction in the risk of unauthorized data access. Defragmentation and decryption of data can only be achieved by authorized owners or qualified 3<sup>rd</sup> parties

### **Parameter #8: 24/7 Active & Passive Monitoring**

Monitoring of networks is a full time job. Using a second passive monitoring system that is not directly connected to the active monitoring system creates a "correlation effect" (i.e. if they don't match something is wrong). This increases visibility in the event of network tampering, and even network monitoring systems tampering. The security system should include 24/7 tracking of both the active and passive monitoring.

### **Parameter #9: Real Time Access Denial**

Detecting a single unauthorized access is one thing, denying continued unauthorized access attempts is another. By having an active real time access denial system, the risk of a known offender attempting an attack multiple times is reduced. If the attack is part of known attack signatures (example: those on the CVE database) real time denial will also reduce risk on the first attempt and the access point will be removed for that offender.

**Parameter #10: Data is Useless If Stolen**

*If there is a loss of any and/or all data it should be made useless to the offender, and in no way threaten the privacy of the information. This is greater than encryption and fragmentation. It is a combination of both. This makes the data useless without stealing the entire database as well as both the decryption and defragmentation systems. Otherwise, the stolen data is useless gibberish.*

*(please proceed to the next page)*

## **THE RECORDS PROTECTION REPORT CARD**

To help assess the security of your State's records management system check the box provided with each of the parameter listed if your system provides that parameter; then add-up the number of checks. We suggest you use the following criteria in evaluating your results:

- 8 or more checks... **E** (Effective records management security)
- 5 to 7 checks... **M** (Marginal records management security)
- Less than 5 checks... **V** (Vulnerable records management security)

### **Parameter #1: Dynamic Encryption**

Private data is dynamically encrypted so it is accessible only by those authorized (data owner or qualified third parties).

Your Assessment: [   ]

### **Parameter #2: Fragmentation**

Data is fragmented and placed on multiple databases.

Your Assessment: [   ]

### **Parameter #3: Compartmentalization**

Database components are compartmentalized, with access controls separating each compartment.

Your Assessment: [   ]

### **Parameter #4: Physical Network Separation**

Database servers holding fragmented information are separated physically by independent networks that communicate only to the control points and not with each other.

Your Assessment [   ]

### **Parameter #5: Multi-factor Authentication**

Access to the data is achieved by multi-factor authentication involving ownership verification and authorized devices.

Your Assessment: [   ]

### **Parameter #6: Repediation**

The authentication system employs repediation.

Your Assessment: [   ]

### **Parameter #7: Defragmentation and Decryption Control Point**

Defragmentation and decryption of data can only be achieved by authorized owners or qualified 3<sup>rd</sup> parties.

Your Assessment: [   ]

### **Parameter #8: 24/7 Active & Passive Monitoring**

The security system includes both 24/7 active and 24/7 passive monitoring.

Your Assessment: [   ]

### **Parameter #9: Real Time Access Denial**

Real time and localized deactivation capability in response to unauthorized access attempts.

Your Assessment: [   ]

### **Parameter #10: Data is Useless If Stolen**

If a database breach involving the loss of any or all data on its servers occurs the stolen data contained will be useless and in no way threaten the privacy of the information.

Your Assessment [   ]

### About Kemesa LLC

*Kemesa (acronym for Keeps Me Safe) is a data management company that is single-mindedly focused upon preventing the unnecessary distribution and assuring the safe management of personal identifying and financial information. Its operating, database management and fraud control centers are located in Salt Lake City, Utah*