Presented to the Interdisciplinary Studies Program:

UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Applied Information Management and the Graduate School of the University of Oregon
In partial fulfillment of the requirement for the degree of Master of Science

Data-at-Rest (DAR): Protecting Sensitive Information in Mobile Information Systems (ISs)

CAPSTONE REPORT

Jeffery S. McLean
Information Security Systems Engineer (ISSE)
Harris Corporation

University of Oregon
Applied Information Management
Program

February 2011

Continuing Education
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-2714

Approved by

_____

Dr. Linda F. Ettinger
Senior Academic Director, AIM Program

Data-at-Rest (DAR): Protecting Sensitive Information in Mobile Information Systems (ISs)

Jeffery S. McLean

Harris Corporation

Abstract

As the number of mobile information systems (ISs) increases, so does the amount of data-at-rest (DAR) susceptible to attacks. Literature published from 2001 to 2010 is examined to describe (a) 13 selected standards, regulations, and policies requiring DAR security solutions; and (b) currently available DAR security solutions of two types: hardware (encryption) and applications. Focus is on affordability and interoperability. Solutions are presented as a guide to help curb loss of DAR and identity theft.

Keywords: data-at-rest, mobile information system, encryption, identity theft, national institute of standards and technology, federal information processing standard, advanced encryption standard

Table of Contents

List of Tables

List of Figures

Introduction to the Literature Review

Purpose

In today's technology driven world, laptops, cell phones, Personal Digital Assistants (PDAs), and thumb drives have become a necessity in life (Waring, 2008, p.38). People are able to store data (i.e. personal, organizational) in numerous mobile information systems (ISs) that even include some cars (Bradley, 2010, p.37).

Once data is stored on any storage device, it is deemed data-at-rest (DAR) (Identity Finder, 2009, p.2). Failing to protect DAR places both individuals and organizations at risk (Gibson, 2007, p.35). Individuals face the risk of identity theft, which can result in thieves draining personal bank accounts, purchasing cars, taking out a home loan, and even going as far as assuming the victim's identity all together (USDOJ, n.d.). Organizations face the risk of serious financial repercussions, which include losing their reputation, paying fines, and spending large amounts of money to regain their reputation (Vamosi, 2010, p.41).

According to McNamara (2008), simply password protecting DAR is no longer considered in keeping with best security practices. The problem is that mobile information systems are magnets to thieves and it only takes a moment for a mobile IS to vanish (FTC, 2007, p.1).

The purpose of this study is to identify a set of security feature options that individuals and SMBs can use to protect DAR in mobile ISs. The intent is to present ways to mitigate attacks on information referred to as DAR; attacks are often perpetrated on lost or stolen mobile ISs (Hall, 2008, p.12). Security features that include the implementation of such things as firewalls, Intrusion Protection Systems (IPS), and Virtual Private Networks (VPN) aim to protect the perimeter of the network (SNIA, 2009, p.6). However, these security features do not sufficiently

secure DAR. DAR is traditionally stored in *cleartext*, which means the data is not encrypted and remains vulnerable (SNIA, 2009, p.6).

According to RSA Security, Inc. (2002), protecting DAR requires a minimum of two things: "secure encryption technology to protect confidential data and careful management of access to the cryptographic keys that unlock encrypted data" (p.2). The concept of secure encryption technology refers to making sensitive data unreadable by unauthorized readers; it requires adherence to encryption standards like the Advanced Encryption Standard (AES), which is in keeping with best security practices (EMC^2, 2008, p.6). The concept of careful management of access pertains to ensuring only the individuals that need access to the encrypted data have access to the encryption key that is used to encrypt and decrypt the data (RSA Security, Inc. 2002, p.3).

When secure encryption technology and management of access are not followed to protect DAR on mobile ISs, there are several threats to organizations that are present, which include:

- Additional systems can be compromised when a mobile IS tries to access data from another system,
- Entire networks can be compromised when a mobile IS gets attached,
- Network storage devices can become compromised when a mobile IS gets attached, and
- The control of organizational data storage can be lost (SNIA, 2009, p.7).

However, encryption and key management are not the only ways to protect DAR on mobile ISs. According to Kandra, Aquino, and Brandt (2004) another DAR security solution includes applications that locate lost or stolen mobile ISs. Waring (2008) describes applications

that can wipe data from a lost or stolen mobile ISs through the subscription of third party services once the loss is reported (p. 38).

Problem/Significance

In order to satisfy DAR due diligence, secure encryption technologies must be utilized and access to cryptographic keys must be managed (RSA Security, Inc., 2002, p.2). Cryptographic keys are a set of truly random numbers and letters used in conjunction with an algorithm to encrypt data to make it unreadable unless the reader has the algorithm and key used to encrypt the data (EMC^2, 2008, p.6). Organizations that are looking ahead are developing security strategies (i.e. encryption, access management, security auditing and event logging) aimed at protecting sensitive stored data, defined as data-at-rest (DAR) (RSA Security, Inc., 2002, p.2).

The workplace is changing as the mobile environment becomes more complex and new technologies emerge on the market, which allows the current workforce to become more reliant on mobile ISs (INPUT, 2007, p.1). As the number of mobile ISs increases, the amount of DAR increases along with the likelihood of DAR exposure (INPUT, 2007, p.1). In order to implement DAR security solutions, the DAR solution must be proactive and corrective to allow for securing data at the source (Identity Finder, 2009, p.3).

Security professionals are guided by government policies and legislation (Harris, 2010, p.124). The Department of Defense (DoD) (2007) provides guidelines to constituents that may be of use in other contexts. In this case, the DoD states:

> All unclassified DoD data-at-rest that has not been approved for public release and is stored on mobile computing devices such as laptops and personal digital assistants

> (PDAs), or removable storage media such as thumb drives and compact disks, shall be treated as sensitive data and encrypted using commercially available encryption technology. (p.2)

Additionally, the DoD (2007) further states that the encryption requirement at a minimum:

> . . . shall be National Institute of Standards and Technology (NIST) Federal Information Processing Standard 140-2 (FIPS 140-2) compliant and a mechanism shall be established to ensure encrypted data can be recovered in the event the primary encryption system fails or to support other mission or regulatory requirements. (p.2)

Each of these guidelines points to the need to implement some form of data protection on any device that stores sensitive data, and together they help to drive the technology industry in implementing DAR security solutions that are recognized and standardized (NIST SP 800-53, 2009, p. F-4).

A case example can be used to document the risks involved when not protecting DAR. In 2006, the Veterans' Affairs (VA) had a laptop stolen from one of its employee's residence, which had the personal and service information of 26.5 million veterans and service members. The information was not encrypted and the incident resulted in termination of the employee, the resignation of the employee's superiors, and the resignation of other senior VA officials (INPUT, 2007, p.5). Since the 2006 VA incident, the VA has encrypted DAR on over 18,000 of its laptops and is rolling out software that disables the use of thumb drives and any other storage device the VA deems as unauthorized (Gross, 2007, p.11).

In 2006, the Federal Bureau of Investigation (FBI) estimated that the total cost to U.S. companies of all lost corporate data was $26.5 billion and the average cost to a large company with one incident in data loss was estimated at $4.8 million (Iron Port, 2007, p.16). According to

the Ponemon Institute (as cited by Iron Port, 2002), the average data loss to an organization costs approximately $182 per record, which averages approximately $4.8 million per total incident (p.7). According to Iron Port Systems (2007), "today's strict regulatory and ultra-conservative environment" pertaining to security means that "data loss prevention (DLP) is one of the most critical issues facing Chief Information Officers (CIO), Chief Security Officers (CSO) and Chief Information Security Officers (CISO)" today (p.9).

In the case of risk to individuals, according to the Federal Trade Commission (FTC), approximately nine million Americans have their online identities stolen every year due to stolen or compromised personal information (Identity Finder, LLC, 2009, p.2). In 2001, a computer crime survey of 699 anonymous organizations, performed by the Computer Security Institute (CSI) with participation from the FBI's Computer Crime Squad (as cited by RSA Security, Inc., 2002), reported that one company had a $50 million dollar loss due to exploitation of sensitive data (p.1). According to the CSI/FBI Computer Crime and Security Survey (2005), the total financial losses among 639 survey respondents from anonymous organizations, including laptop theft and unauthorized access, came to over $130 million (p.15). Lost/stolen laptops constitute the most risks associated with sensitive data being compromised (Gibson, 2007, p.43). The following list comprises some of the most notable incidents pertaining to stolen mobile ISs:

- September 28, 2007, Gap has laptop stolen with 800,000 names and Social Security numbers of people who applied for jobs at the Gap,
- October 3, 2007, Adminstaff has a laptop stolen containing the names, addresses, and Social Security numbers of 159,000 current and past employees, and
- October 17, 2007, Office Depot has a single laptop stolen that contains 10,000 employee names, addresses, and Social Security numbers (Gibson, 2007, p.43).

Audience/Outcome

As an information security professional, this researcher is increasingly interested in ensuring that threats related to DAR are mitigated industry wide. Information Security Systems Engineers (ISSE) frequently work with several engineering disciplines (i.e., mechanical, electrical, systems, etc.) and must constantly balance best security practices against implementation costs (i.e. affordability) and risks, with government and commercial customers (Harris, 2010, p.63). Recommending security products, processes, procedures, and architectures driven by governmental and contractual requirements is within this researcher's area of responsibility. The implementation of DAR security solutions is just one area of concern on projects requiring security measures.

The intended audience for this study is CIOs, CSOs, CISOs of small businesses and individuals seeking to protect DAR. These individuals must consider user needs, organizational needs (e.g. interoperability), what security policies, procedures, and implementations are needed to access particular data, and who needs access and when (INPUT, 2007, p.3).

The outcome of this study is formatted as a guide, designed to present: (a) the standards and regulatory protection policies behind the need to push towards DAR security solutions and (b) the potential security options that are available when it comes to protecting DAR in a mobile IS. Selection of elements to include in the guide is limited to those that are commercially and governmentally viable and currently available from leading vendors and experts specializing in DAR security solutions, which include companies like RSA Security, Inc., that specialize in security solutions. This outcome is intended to report elements that go beyond the basic well-known DAR security solutions that include: (a) keeping the mobile IS locked when not in use; (b) keeping the mobile IS away from the floor; (c) protecting usernames and passwords; (d)

staying away from obvious carrying cases since distinctive cases place a target on the mobile IS; (e) never leaving a mobile IS visible in an unoccupied car; (f) keeping eyes on the mobile IS; (g) paying more attention in airports; and (h) not leaving a mobile IS in an unoccupied hotel/motel room (FTC, 2007, p.2).

Security options are framed within two pre-selected criteria: affordability (SNIA, 2009, p.10) and interoperability (DoD, 2007, Attachment 2). According to SNIA (2009), affordability is a key driving factor in determining the right DAR security solution. DAR security solutions must adhere to best security practices and best security practices must ensure that the security solution does not out-weight the information it is intended to protect (p.2). Per DoD (2007), interoperability is another key driving factor in determining the right DAR security solution since the intent of protecting DAR is to ensure that only the people with a need to view the information are permitted (p.3). Interoperability ensures that the selected DAR security solution is compatible on the mobile ISs and other systems it attaches to (DoD, 2007, Attachment 2). For example, a DAR security solution that only works on a laptop would not be a good choice for implementation if the same laptop were intended to synchronize with a particular smart phone (DoD, 2007, Attachment 2).

Delimitations

Study focus. This study focuses on three areas of literature: (a) policy and legislature driving DAR solutions in mobile ISs (INPUT, 2007); (b) standards that DAR solutions must meet (DoA, 2006); and (c) current DAR protection solutions (i.e. encryption and applications) (Identity Finder, LLC, 2009, p.2).

It is reported that 12,000 laptops are lost each week in airports and 65 percent of business travelers do nothing to protect the data on their mobile IS (Ferguson, 2008, p.22). These numbers show that individuals and organizations are not familiar with policies and legislature trying to curb the loss of sensitive data and protect the general public (Ferguson, 2008, p.22). When trying to come up with a DAR security solution, it is important to know what standards must be met to ensure best security practices are followed or recognized since policies and legislature are enforcing some sort of DAR security solution like encryption technologies (NRS 597.970, 2008).

Classification of data. The phrase "classification of data" refers to associating the proper level of protection to information (EMA, 2008, p.6). One of the most challenging aspects associated with DAR is the classification of data since data classification adds a level of complexity and presents a means to minimize unnecessary cost (EMA, 2008, p.6). Data classification and the implementation of security solutions are primarily performed concurrently as a means of ensuring best security practices (EMA, 2008, p.6); however, this study assumes that encryption is not the only viable solution when it comes to DAR security solutions.

Literature selection. The selected literature indicates DAR security solutions vary from hardware implementations, software implementations, security policies and procedures, and a combination of the three (Hall, 2006, p.12). However, this study does not define a single solution for all mobile ISs. Rather, it provides an overview of applicable options to assist individuals and organizations in determining what DAR security solutions may best suit them.

Coding focus. The security solutions identified during coding are framed in the outcome in relation to two pre-selected criteria: affordability (SNIA, 2009, p.10) and interoperability (DoD, 2007, Attachment 2). As stated in the *Audience/Outcome* section, affordability ensures

that the DAR security solution does not cost more than the cost of losing the information and interoperability ensures that the DAR security solution functions as intended between systems.

Time frame. In 2001, it is estimated that more than 600,000 laptops, PDAs, and cell phones were either lost or stolen throughout the United States (U.S.) (Kandra, Aquino, & Brandt, 2004, p.49) and in 2008, almost 10 million people had their identities stolen in the U.S., which is up almost 22% from 2007 (Harris, 2010, p.xviii). In order to ensure that the most accepted technologies are reviewed, this study does not use references that are over ten years old, which places a restriction of 2001 or newer on references for this literature review.

Preview of Data Analysis and Writing Plans

Data analysis plan preview. Creswell states (2009) that "the process of data analysis involves making sense out of text and image data" (p.183). Creswell (2009) further states that data analysis "is an ongoing process involving continual reflection about the data" and "is conducted concurrently with gathering data, making interpretations, and writing reports" (p.184). Material collected to support this study addresses the questions and sub-questions presented in the *Research Parameters* section of this paper but as Creswell (2009) states, "data analysis follows steps from the specific to the general and involves multiple levels of analysis" (p.184). This means that more data collection may transpire as materials are analyzed.

The observational protocol is used in this study to record the information from the references that meet the evaluation criteria (Creswell, 2010, p.181). This is done by taking handwritten notes (while collecting and performing a document analysis on selected references), which consist of notes from analysis, recording key concepts, links, perceptions, and ideas written in the margins of printed full-text references and note cards. Information is then divided

into two sections, which consists of key reference material and supporting key reference material.

Writing plan preview. In order to identify potential security solutions pertaining to DAR in mobile ISs, this study examines a wide range of scholarly and professional references that are collected, scanned, and read (Obenzinger, 2005, p.6). The objective is to locate and present commercially and governmentally viable solutions that are recognized as cost effective (i.e. affordability) and proven in real-world environments (i.e. interoperability). The presentation follows the rhetorical pattern known as *Battlebots*, which presents specific trends in the field of DAR security solutions and positions those trends towards answering the questions and sub-questions presented in the *Research Parameters* section (Obenzinger, 2009, p.5).

Trends are described in relation to the two larger themes examined in this study: (a) relevant standards and policies that provide a security information framework, and (b) security solutions that provide protection options for DAR in mobile ISs. Once combined, the data presented in these two themes form the outcome of the study, which is designed as a guide to help small businesses and individuals select viable security solutions to protect DAR in mobile ISs. Emphasis in the guide is placed on affordability and interoperability.

Definitions

The terminology used in this study comes from selected literature presented as well as additional reference materials. The terms include security industry terminology, such as data-at-rest (DAR) that is a security concern for organizations trying to protect organizational data (Identity Finder, 2009). Although some of the terminology is defined within the body of the text, many more terms are only presented in this formal set of definitions. This section provides definitions to ensure that the specific meaning of terms and phrases, as used within this review, are clear to the audience. Following the list of terms is a separate list of acronyms used in this study.

Terms

Advanced Encryption Standard (AES) – This standard is the federally recognized industry-standard algorithm within the United States and the most common implemented algorithm in current encryption methods (EMC^2, 2008, p.6).

Best Security Practices – This term pertains to providing the maximum protection when dealing with organizations most important asset(s) (RSA Security, Inc., 2002, p.2).

California (CA) 1798 – This was put into place in the state of California in 2003 and mandates that if any organization in California has a computer security breach where the disclosure of confidential resident information arises, the organization must disclose it (Iron Port Systems, 2007, p.32).

Cleartext – This term pertains to data or information that is not encrypted or protected in a system or saved to a storage device (SNIA, 2009, p.6).

Confidential data – Any data that is not deemed as public information and could potentially cause harm to an organization if it is released to the public (RSA Security, Inc., 2002, p.2).

Cryptographic keys – Very specific and mathematical pieces of data that are used in conjunction with encryption algorithms to encrypt data (EMC^2, Inc., 2008, p.6).

Damaging attack – This pertains to vulnerability within an organization that has the potential to diminish the reputation or financials of an organization (RSA Security, Inc., 2002, p.1).

Data classification – Associating the proper level of protection to the information that is to be protected (EMA, 2008, p.6)

Data-at-Rest (DAR) – This term pertains to any data that is stored on a computer, storage device (i.e., hard drive, smart phone, PDA, etc.) but it excludes any data that is traversing a network (Identity Finder, 2009, p.2).

Data-at-Rest Solution – Any solution used to protect data-at-rest within an organization and part of the security strategy to ensure due diligence (Identity Finder, 2009, p.2).

Data-in-Motion – This term pertains to any data that is traversing the network and can be considered secure if both ends are capable of protecting the data so that a third party cannot intercept the data and read it (Identity Finder, 2009, p.2).

Data Loss Prevention (DLP) – A technical solution used to prevent data loss, enforcing compliance, and the protection of an organizations value and reputation (Iron Port Systems, 2007, p.9).

Due diligence – The process of systematically evaluating information to identify vulnerabilities, threats, and issues relating to an organization's overall risk (Harris, 2010, p.1151).

Encrypted data – Data that is protected by utilizing an encryption algorithm and encryption key (RSA Security, Inc., 2002, p.4).

Federal Information Processing Standard (FIPS) – The federally recognized encryption policy to ensure encryption standardization (DoD, 2007).

Gramm-Leach-Bliley Act – This act is also known as the Financial Modernization Act, which is intended to protect all private financial data and applies to numerous financial institutions and any organization that stores personal information that is not considered public record of their customers (Iron Port Systems, 2007, p.30).

Health Insurance Portability and Accountability Act (HIPAA) – HIPAA was put in place in 1996 and institutes numerous requirements on the health care industry's personal information handling procedures and practices by leveraging strict fines for improper handling and directly impacts the operations of messaging systems (Iron Port Systems, 2007, p.31).

Information centric security – This manages the relationship that is between data and people who use the data, which can be considered the livelihood of an organization (EMC^2, 2008, p.4).

Interoperability – The ability of diverse systems to work together (DoD, 2007, Attachment 2).

Mobile Information System (IS) – Any device that includes laptops, portable notebooks, tablet Personal Computers, PDAs, smart phones, etc. that can be taken by an individual outside an organization (DoA, 2006).

National Institute of Standards and Technology (NIST) - A governing organization that oversees the standards and provides policies and security requirements to ensure best security practices (Harris, 2010, p.711).

Personal information – Any information that can be linked to an individual, which includes information pertaining to a person's social security number, medical history or information, and any information about a person that is not deemed as public information (DoA, 2006).

Personal Information Protection Act – The regulation enacted in Japan that protects personal information privacy (EMC^2, 2008, p.10).

Primary encryption system – The main encryption technology used to protect data stored to a specific location (DoD, 2007).

Privacy – This is "the right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others" (EMC^2, 2008, p.5).

Sarbanes-Oxley Act – The "legislation enacted in response to the high-profile Enron, WorldCom, and other financial scandals, to protect shareholders and the general public from accounting misdeeds and fraudulent practices in publicly owned companies" (Harris, 2010, p.35).

Secure encryption technology – An industry recognized encryption technology that is employed to protect data (RSA Security, Inc., 2002, p.2).

Acronyms

Acronyms used throughout this study are presented in Table 1 (see below) along with their respective meaning.

Table 1

Acronyms and meanings

Acronym	**Acronym meaning**
3DES	Triple Data Encryption Standard
AC	Access Control
AES	Advanced Encryption Standard
AIM	Applied Information Management
APA	American Physiological Association
AT	Awareness and Training
AU	Audit and Accountability
CA	California
CBC	Cipher Block Chaining
CBC-MAC	Cipher Block Chaining-Message Authentication Code
CBI	Canadian Back Institute
CD	Compact Disk
CFB	Cipher Feedback
CMAC	cipher-based Message Authentication Code
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CMS	Charlotte-Mecklenburg Schools
CSI	Computer Security Institute
CSO	Chief Security Officer
CTO	Chief Technical Officer
CTR	Counter
DAR	Data-at-Rest
DES	Data Encryption Standard
DIACAP	Department of Defense Information Assurance Certification and Accreditation Process
DLP	Data Loss Prevention
DoA	Department of the Army
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DVD	Digital Versatile Disc
ECB	Electronic Codebook
EMA	Enterprise Management Associates
EMC	Electromagnetic Compatibility
EMC^2	Egan and Marino Company
EMI	Electromagnetic Interference
EU	European Union
FBI	Federal Bureau of Investigation
FDE	Full-Disk Encryption
FIPS	Federal Information Processing Standard

Acronym	Acronym meaning
FISMA	Federal Information Security Management Act
FTC	Federal Trade Commission
GCM	Galois/Counter Mode
GPS	Global Positioning System
HDD	Hard Disk Drive
HIPAA	Health Insurance Portability Accountability Act
IA	Identification and Authentication
IBM	International Business Machines
IPS	Intrusion Protection System
IS	Information System
ISSE	Information Security Systems Engineer
IT	Information Technology
LLC	Limited Liability Company
MD-5	Message Digest algorithm 5
MP	Media Protection
n.d.	No Date
NIST	National Institute of Standards and Technology
NRS	Nevada Revised Statute
OFB	Output Feedback
OMB	Office of Management and Budget
OR	Oregon
PC	Personal Computer
PDA	Personal Digital Assistant
PDF	Portable Document Format
PL	Planning
P.L.	Public Law
RA	Risk Assessment
RSA	Rivest, Shamir, and Adleman
SC	System and Communications Protection
SHA-1	Signature Hashing Algorithm 1
SMB	Small and Medium Business
SNIA	Storage Networking Industry Association
SP	Special Publication
UO	University of Oregon
URL	Uniform Resource Locator
U.S.	United States
USB	Universal Serial Bus
USC	United States Congress
USDOJ	United States Department of Justice
VA	Veterans Administration
VPN	Virtual Private Network
WWW	World Wide Web
XTS	Exclusive Or Encrypt Exclusive Or Tweakable Block Cipher with Ciphertext Stealing

Research Parameters

This section provides the approach used to structure the research design of this study. Based on the results from preliminary searching of literature pertaining to protecting DAR in mobile ISs, a strategy is ascertained to guide additional searches. Search criteria are presented that are used to determine the relevance of information sources, usability, and credibility of the reference. References that are deemed relevant and creditable are recorded, categorized and analyzed for use within this study. Key references, such as the material from RSA Security, Inc., are selected to be included in the data set for coding. Other references listed here are used for focusing the study, providing direction, and supporting and framing the information provided through coding.

Research Questions and Sub-questions

To determine the direction of this study, a set of guiding questions and sub-questions are developed to ensure that the focus of this study stays on track, within scope, and to assist in identifying key search terms and phrases such as *data-at-rest protection*. Each question and sub-question is designed to examine at least one of two main areas of this study (i.e., (a) standards and policies; and (b) security protection solution options. Once policies and solutions are identified, they are presented in the outcome of the study in relation to two pre-selected criteria: (a) affordability (SNIA, 2009, p.10), and (b) interoperability (DoD, 2007, Attachment 2). When combined, it is assumed that the set of questions provides the foundation for answering the overarching research question: *How can individuals and small businesses better ensure protection from attacks regarding DAR in mobile information systems*? Table 2 documents the guiding questions and includes the specific area to which each question pertains.

Table 2

Research questions and areas

Research questions	**Research area**
1. What is driving individuals to protect DAR besides the obvious reason of data loss due to lost or stolen mobile devices? 2. What is driving organizations to protect DAR besides the obvious reason of data loss due to lost or stolen mobile devices?	Standards and Policies
3. What sorts of options are available when it comes to security solutions for mobile devices? a. Why should the solution be hardware based? b. Why should the solution be software based?	Protection Options
4. What costs are associated with DAR protection standardizations? a. How can encryption be an affordable option?	Affordability/Interoperability

Search Report

Search strategy. References are identified through a search of the term DAR combined with additional terms identified from this researcher's guiding questions such as *protection* and *encryption* via the Ebsco database by way of the University of Oregon (UO) Library portal (OnseSearch) and the World Wide Web (WWW) using Google as the search engine. In order to expand the search of protecting mobile ISs, additional keyword terms include adding *laptop* or *phone* to the term *stolen*. In order to define terms and provide additional keyword searches, supplementary references such as the Certified Information Systems Security Professional (CISSP) All-in-One Exam guide, which is recognized as one of the primary texts used in educating security professionals (Harris, 2009, p.1) and standards already in this researcher's

possession, such as FIPS 140-2, which is required to implement governmental compliant encryption (DoD, 2007, p.2) are used.

Protecting DAR and implementing DAR security solutions goes beyond mobile ISs (RSA Security, Inc., 2002, p.2), and therefore these two areas are excluded from the literature search. Excluded DAR security solutions include: (a) database encryption strategies; (b) cryptographic key management; (c) risk assessments; and (d) system monitoring and reporting (Iron Port Systems, 2007, p.18). However, references that pertain to these areas are still reviewed on a secondary basis due to their applicability to encryption standards that apply to DAR in mobile ISs (EMC^2, 2008, p.6).

Evaluation criteria. In order to develop a guide that can be used to determine the right DAR security solution, the material selected for this study is captured from numerous sources. Most of the information used in this study is pulled from the WWW using the Google search engine by utilizing keyword searches of terms located within selected materials addressing DAR. However, additional searches using the same keywords are used within the Ebsco database via OneSearch, which provides students and staff access to search across several document databases and indexes.

Before conducting any keyword searches, the results are limited to materials published no earlier than 2001. Limiting searches by time ensures that results are current and address protecting DAR with industry standards, since NIST FIPS Publication 140-2 sets the encryption standards for protecting DAR (NIST FIPS 140-2, 2002, p.1). The elimination of references prior to 2001 is vital to ensuring that this study conveys the current market trends when it comes to protecting DAR and possibly giving some insight into what is to come. By setting a limiting date prior to performing searches reduces the amount of time required to evaluate search results.

While keeping the limiting date in mind during keyword searches, the results of each search is examined to identify if the material is relevant to: (a) policy and legislature driving DAR solutions in mobile ISs (INPUT, 2007); (b) standards that DAR solutions must meet (DoA, 2006); and (c) current DAR protection solutions (i.e. encryption) (Identity Finder, LLC, 2009, p.2). Abstracts, overviews, and introductions are reviewed for the search results that present information that may be pertinent to each keyword search. If search results return material that is not relevant within the first page of results, the keyword used in the search is revised and the search is repeated.

Once material is deemed relevant to this study, the credibility of each document is evaluated to ensure that the quality of the material is sufficient for this literature review (Hewitt, 2002, p.21). Multiple factors are used to determine the credibility of located material, which include the use of references, details, and if the material appears to have been peer reviewed (Hewitt, 2002, pp.21-22). Preference is given to material written by industry leaders, published policies, standards, legislature, and organizations that specialize in information security.

Documentation approach. Potential electronic references are stored in a folder named with the search term used to locate them and stored in their native format (i.e. .pdf). The Uniform Resource Locator (URL) is copied into a text file with the date it was located and the search term(s) used to find it are recorded. Each potential reference is reviewed for applicability to the overarching topic and direction, focus of the literature review, and overall goal. Key terms within located documentation are recorded during the review process for additional searches, viable references are marked up with comments, and the commented references are cataloged per guiding questions and sub-questions.

Once the reference is cataloged per guiding question and sub-questions, electronic copies of the reference are filed in a folder with the keyword or words comprising the file title, the URL is recorded in a text file corresponding to the references file folder, the date the reference was retrieved is recorded in the text file, and the full American Psychological Association (APA) citation is placed in a Microsoft Word document with the references published abstract (if one is published). If an abstract is not available, a note is placed with the citation stating that one needs to be created.

The hard copy references, with notes, are saved to a physical file folder that holds all analyzed references. If the reference does not meet the guiding questions or sub-questions, the same process is followed but the URL is recorded in the text file with *Not_Relevant* appended to the end of the URL, the full APA citation and subsequent abstract are not recorded, and the reference is not printed out.

Preferred references for this literature review specifically address DAR solutions, standards, and policies. Additional references, such as the Creswell text and CISSP text, are used to provide the framework for this literature review, which includes presenting background information and key-term definitions of terms associated with best security practices encompassing DAR security solutions.

Data analysis plan. Performing a conceptual analysis requires selection of a specific approach to coding. In this paper, the following eight specific steps related to the coding process are utilized, in search of key concepts (Busch, De Maret, Flynn, Kellum, Le, Meyers, Saunders & White, 2005). Key concepts for coding in this study include data-at-rest protection, data-at-rest security, stolen laptops, and stolen cell phones; these concepts are coded in the literature presented in the *Annotated Bibliography*. Coding results are analyzed and synthesized in order to

provide small and medium sized businesses and individuals a means to develop a DAR security solution that protects against the threat of having sensitive data released. In order to accomplish this, data analysis is conducted on the material listed for coding in the *Annotated Bibliography*, which is in accordance with the eight coding steps defined on the Colorado State University Writing Lab website, as follows.

1. Level of analysis – Coding is conducted for key words and key phrases that include data-at-rest, data-at-rest protection, data-at-rest security, DAR standards, DAR policies, identity theft, stolen laptops, and stolen cell phones.
2. Number of concepts to code for – Coding begins for the eight concepts noted in Step 1. Additional concepts are noted as they emerge through the coding process since some of the concepts come by synthesizing the data.
3. Code for existence or frequency – Key words and phrases are coded for existence instead of frequency. For example, the key word *data-at-rest* is coded only once regardless of the number of times it appears in a reference. Varied relevant descriptions of the concept of data-at-rest, determined through contextual reading, are coded separately.
4. Distinguish between concepts – Similar meaning key words and phrases are coded as they appear. For example, *data-at-rest* and *DAR* are coded as the same concept; however the related concepts of *security protection* and *encryption* are coded as distinct and separate concepts.
5. Translation rules for coding references – Rules for coding references ensure that key words or phrases are categorized consistently. For example, *laptops* and *cell phones* are coded under *stolen*, while *protection*, *security*, *standards*, and *polices* are coded under *data-at-rest*.

6. Dealing with irrelevant information – If information does not support this study, it is deemed irrelevant and not coded.
7. Code the texts – The coding process utilizes an iterative process. Key words, phrases, and translation rules are recorded in a text file and saved electronically, while hand written notes are written on printed full-text references and index cards. The results are constantly reviewed as a way to inform coding subsequent references. The results are then combined into a tabular Word document.
8. Analyze results – The Word document is reviewed for additional research direction, emerging concepts, and conclusions through a process described in the Writing Plan.

Writing plan. Iron Port Systems (2007) explains that today's workforce experiences a larger amount of flexibility in their work locations and in their work hours than any of the previous generations (p.14). In 2006, the United States Chamber of Commerce reported that nearly 20 million people in America telecommute, which means that electronic information is the lifeline to organizations and increases the possibility of sensitive data traveling through cyberspace (Iron Port Systems, 2007, p.14). The assumption of this study is that sensitive data is just about everywhere and people must be vigilant in taking the necessary measures to protect sensitive information, which is known as data-at-rest (DAR) (Bradley, 2010, p.37). There are numerous security solutions that are available to organizations and individuals to protect sensitive information and the possibility of identity theft (Waring, 2008, p.38).

The Writing Plan describes how the results of the data analysis are presented in this paper. This writing plan is intended to look at DAR security solution strategies that individuals and small to medium sized business need to understand when implementing DAR security solutions in order to thwart the threat of releasing sensitive information accidentally and by way

of malicious measures such as stolen mobile ISs. Waiting until a news story breaks about a stolen laptop disclosing sensitive information or becoming the victim of identity theft is too late, when looking at DAR security solution strategies (Gibson, 2007, p.35). This study is focused on two pre-selected themes, which include (a) standards and policies behind protecting DAR and (b) the security protection options that are available, with an emphasis on encryption and application(s). An outline of the presentation format follows:

Topic. Protecting Data-at-Rest (DAR) in Mobile Information Systems (ISs) to Curtail Identity Theft

1. Theme one: The need for DAR security solutions
    a. Standards and policies that enforce DAR security solutions
2. Theme two: Two key options for DAR security solution strategies, including the potential benefits of each
    a. Encryption
    b. Application

Coding results are then framed in the final outcome of the study (a guide) in relation to two pre-selected criteria: affordability (SNIA, 2009, p.10) and interoperability (DoD, 2007, Attachment 2). By keeping affordability and interoperability in mind, this ensures that DAR security solutions costs are kept to a minimum and best security practices are followed when implementing the desired DAR security solution.

Annotated Bibliography

All selected references for this study are evaluated, prioritized and categorized. Only references that are determined central to utilizing best security practices for protecting DAR in mobile ISs are identified in this section (Creswell, 2009, p.45). This annotated bibliography provides citations of literature determined foundational data used for analysis (Creswell, 2009, p.175). The annotated bibliography provides a listing of each selected reference with an abstract of its content, an assessment of each citation for validity, and a brief description of the relevancy to this study.

Bradley, T. (2010). Keep your personal data off the market. *PC World, 28*(6), 37-38. Retrieved from Ebsco Academic Search Elite database.

Abstract. The author discusses the importance for keeping one's personal data off their hard drives. The author explains that to ensure that one's data is removed beyond anyone's practical ability to recover it; one must remove or scramble the data itself, not just the market pointing to it, which means having to use a wiping or erasing utility. He adds that neither deleting files nor reformatting the hard drive will be enough to permanently delete data, since both processes just remove the information that the hard drive needs to find the data.

Comments. This article assists in framing the need for protecting DAR in mobile ISs, presented in the Problem/Significance of this study. It presents steps to be performed in order to protect sensitive information, possible DAR protection solutions, and cites a study done by Kessler International on the number of hard drives purchased on eBay

containing unprotected personal information. This article is deemed credible because it is published in a peer-reviewed magazine and cites research performed in DAR protection.

Department of the Army. (2006, September 28). *Army data-at-rest (DAR) protection strategy*. (Department of the Army Memorandum).

Abstract. This memorandum presents the Army's protection strategy for DAR by identifying the problems with not protecting DAR and to ensure that the reputation of the Army is negatively impacted by an incident involved with not taking the necessary actions to protect such information. Information systems are being targeted and designated as mobile to ensure a DAR encryption solution is implemented. DAR implementations will also be evaluated and the results of the evaluation will be used to help drive the requirements for further implementations.

Comments. This memorandum assists in presenting a guiding policy on the government mandate to protect DAR in mobile ISs, as described in the Problem/Significance section of this study. It also provides input into the options that are available to the U.S. Army and the additional steps necessary that go beyond encryption. This memorandum is deemed credible because it is a government published document that references Army best practices and additional documentation that the U.S. Army follows.

Dworkin, M. (2001, December). *Recommendation for block cipher modes of operation: Methods and techniques*. (NIST Special Publication 800-38A).

Abstract. This recommendation defines five confidentiality modes of operation for use with an underlying symmetric key block cipher algorithm: Electronic Codebook (ECB),

Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR). Used with an underlying block cipher algorithm that is approved in a Federal Information Processing Standard (FIPS), these modes can provide cryptographic protection for sensitive, but unclassified, computer data.

Comments. This document provides additional insight into encryption modes that are used with encryption algorithms that are recognized by the government and commercial industry when implementing encryption strategies. It also presents additional options pertaining to functionality and performance measures that are to be considered when implementing encryption for DAR. This document is deemed credible because it is an industry recognized standardization document used by security professionals to implement encryption strategies.

Enterprise Management Associates. (2008, September). *Security for data at rest: critical challenges and IBM information infrastructure solutions*. (Enterprise Management Associates White Paper). Retrieved from http://www.fdesecurityleaders.com/downloads/pdf/security_for_data_at_rest.pdf

Abstract. This White Paper provides some of the risk management challenges pertaining to availability, security, compliance, and retention. The paper also focuses on encryption, why it is important, and the advantages of drive encryption. Finally, the paper discusses some of the solutions that are available for different needs.

Comments. This paper provides the choices for encrypting DAR today that can be used to present the current DAR protection solutions. It also presents one of the critical questions that needs answered when selecting a DAR protection strategy that is right for a

given situation. This paper is deemed usable within this study since the paper comes from one of the industry leaders in information technology.

EMC^2. (2008, January). *Approaches for encryption of data-at-rest in the enterprise: A detailed review*. (White Paper). Retrieved from http://www.emc.com/collateral/hardware/white-papers/h4173-approaches-encryption-data-at-rest-enterprise-wp.pdf

Abstract. This white paper discusses the motivations for and approaches to encrypting data-at-rest in the enterprise. Justification for deployment and tradeoffs between different methods of encryption are also discussed. In addition this paper provides standards that are used to determine the types of encryption to use and how encryption functions.

Comments. This White Paper assists in framing DAR protection solutions using encryption that is compliant with industry standards. It also presents how encryption basically works, areas to consider when implanting encryption, and frames what items are considered DAR. This White Paper is deemed credible because it utilizes security references that are recognized as industry standards and policies.

Ferguson, S. (2008). Securing the laptop. *EWeek, 25*(21), 22-23. Retrieved from Ebsco Academic Search Elite database.

Abstract. The article reports on the determination of Dell Computer Corp. to give business travelers and information technology (IT) managers a better way to protect laptops. It is stated that Dell offered a group of services for its business laptops on June 30, 2008 with a range of security features that can remotely erase company data from hard disk drive (HDD). Dell provided its laptop with a global positioning system (GPS)

device to help guide a user or police to a missing or stolen laptop. It also offered a service called Remote Data Delete Service which provides a remote poison pill (i.e., a form of anti-theft technology) that can wipe a hard drive clean upon request.

Comments. This article helps frame the need for DAR protection and solutions by presenting the results of studies performed by the Ponemon Institute. It also presents possible DAR solutions that are tied to different scenarios and the different possibilities that are available for protecting DAR. This article is deemed credible because it comes from a peer-reviewed magazine that circulates in the information technology industry.

Gibson, S. (2007). Securing the laptop: Mission impossible? *EWeek, 24*(36), 35-43. Retrieved from Ebsco Academic Search Elite database.

Abstract. The article offers insights relevant to laptop security. It discusses the threats that a stolen laptop poses to corporations. According to the author, a lost laptop exposes critical data of companies to the hands of thieves. Laptop hard drive encryption, a response by information technology professionals to the problem of laptop data security, is discussed. Industry analysts John Girard states that multiple encryption entails broader management tools. The author emphasizes that user education is still the key component to laptop security problem.

Comments. This article identifies ways in which DAR can be protected and some of the repercussions that can occur from not protecting DAR. It also goes further by presenting areas to consider when implanting DAR protection and identifying additional DAR solutions. The credibility of this author is assured as a recognized speaker on securing

DAR; and the article is in a peer-reviewed magazine that circulates widely in the information technology industry.

Greenwood, B. (2009). Stolen laptop leads police to identity theft ring. *Information Today, 26*(8), 44. Retrieved from Ebsco Academic Search Elite database.

Abstract. The article reports on the uncovering of evidence of alleged identity theft ring by police officers and Absolute Software following the recovery of a stolen laptop computer from one of the portable trailers at the Charlotte-Mecklenburg Schools (CMS) in North Carolina. It is noted that forensic tools were used by the theft recovery team of Absolute Software to learn about the users of the stolen computer. The trailer was raided by agents of the Immigration and Customs Enforcement and CMS law enforcement.

Comments. This article presents the worst case when DAR protection is not implemented. It presents a real story that happened to personal information that was stored on school laptops and presents the DAR protection solutions used to help thwart the criminal ring that stole school laptops. This article is credible because it comes from a peer-reviewed magazine that circulates widely in the information technology industry.

Identity Finder, LLC. (2009). *Data loss prevention: Data-at-rest vs. data-in-motion*. (White Paper). Retrieved from http://www.identityfinder.com/Software/Docs/WhitePaper.pdf

Abstract. This paper compares the two primary prevention strategies to demonstrate the strength and value in securing Data-at-Rest and Data-in-Motion. The paper also analyzes historical research to highlight the true nature of data breaches and helps to determine which strategy is right best suited for different scenarios.

Comments. This paper presents the key factors to consider when selecting a DAR protection strategy. It also provides information on DAR protection from government agencies that track identity theft. This article is deemed credible due to the company being composed of a group of security experts that specialize in privacy technologies.

INPUT. (2007, June). *Securing data at rest in a mobile environment*. (White Paper). Retrieved from http://www.federalnewsradio.com/pdfs/Securingdataatrestinamobileenvironment.pdf

Abstract. This White Paper provides policies and legislation behind the need for protecting DAR in the mobile ISs. The paper also provides examples of incidents that have caused the push behind protecting DAR and provides possible solutions that can be taken to include additional actions to complement DAR protection.

Comments. This paper provides policies and legislature behind protecting DAR as being within best security practices. It also presents what happens when DAR in not protected and who is driving DAR protection. Finally, it presents a comprehensive list of policies, regulations, and standards that are to be followed when selecting and implementing a DAR protection strategy. This paper is deemed credible since it is peer-reviewed and cites specific policies, regulations, and standards that are used by security professionals to implement security technologies and features.

Johnson III, C. (2006, June 23). *Protection of sensitive agency information*. (Office of Management and Budget Memorandum-06-16).

Abstract. This memorandum recommends that the National Institute of Standards and Technology (NIST) checklist provides the necessary protection of information. The checklist referenced by this memorandum provides a means of compensating for a lack in physical security controls when information is removed from a location and becomes mobile. Steps are provided to assist in determining best security practices and illustrate the process when protecting personal information. Procedures are additionally presented to assist in providing the framework and additional references to effectively protect personal information.

Comments. This memorandum is one of the key policies referenced when implementing security features and points to additional standards that must be followed by government agencies and companies working with the government. This memorandum is viewed as credible since it is referenced by additional government policies and standards.

Kandra, A., Aquino, G., & Brandt, A. (2004). Keep your hands on your handhelds. *PC World, 22*(8), 49-51. Retrieved from Ebsco Academic Search Elite database.

Abstract. This article discusses the measures that can be employed to prevent laptop and other portable devices from being stolen or lost. Researchers estimate that more than 600,000 laptop PC, personal digital assistants (PDA) and mobile phones were lost or stolen in the U.S. in 2001 and other search suggests that the number could double every year as portable devices become more commonplace. It is important to register devices with their manufacturers. In addition, receipts, warranty details and other documentation pertaining to each device must be kept, that way, if a person loses something, any necessary paperwork can be provided for insurance claims, police reports or other follow

up. A variety of robust third-party applications for both handheld and laptop PC will provide security enhancements. PDA Defense Professional is an efficient encryption tool for Palm devices. Extra physical protection such as a lock and cable or an alarm can also be used. Cable systems can secure a notebook at a cost of $50 or less. Alarms which use motion sensors typically run $100 and up. Safeware, an insurance agency that specializes in covering computer equipment, reports that more claims result from accidental damage than from loss or theft and that in many cases, a sturdy protective carrying case could have prevented the damage.

Comments. This article identifies current DAR solutions used to assist in determining a DAR protection strategy in mobile ISs. It also provides current solutions on the market that should be considered to ensure that the right protection solution matches the goals of the user. This article is viewed as credible since it comes from a peer-reviewed magazine and the authors are either contributing editors or senior associate editors for the magazine.

Mearian, L. (2009). Firms take steps to head off encryption dangers. *Computerworld, 43*(6), 10. Retrieved from Ebsco Academic Search Elite database.

Abstract. The article discusses ways on how U.S. firms are taking steps to prevent encryption dangers. AdaptaSoft Inc. uses the self-encrypting software from Seagate to boost customer protection. On the other hand, CBI Health, a company based in Toronto uses Seagate Momentus drives in their laptops to protect sensitive data of their patients. According to analyst Dave Hill from Mesabi Group, disk encryption ensures that stolen data cannot be accessed and that companies comply with data-breach notification laws.

Comments. This article presents additional DAR protection solutions that are currently deployed and introduces the notion that additional standards would better assist the drive to push DAR protection to the next level, which would no longer make it an option. The article also presents what the minimum protection is to be compliant with state and data-breach notification laws. This article is viewed as credible since it is peer-reviewed, published in a magazine that circulates the information technology industry, and cites current standards.

National Institute of Standards and Technology. (2001, November 26). *Announcing the advanced encryption standard (AES).* (Federal Information Processing Standards Publication 197).

Abstract. This standard provides Federal departments and agencies with a specific encryption standard for sensitive (unclassified) information that requires cryptographic protection. In addition to providing a standard, the document provides implementation guidance, when this standard came into effect and what are the drivers behind AES becoming a standard encryption algorithm. The standard presents options for modes of operation and allows for this standard to be carried over to be used by non-Federal Government organizations along with encouraging commercial and private use.

Comments. This standard introduces the federal minimum requirement to use a specific algorithm for recognized encryption and must be adhered to when implementing encryption as a DAR protection solution. The standard presents the exact algorithm that encryption must use in order to be in compliance when implanting encryption. This standard is viewed as credible since it is published by the U.S. government, referenced in

security documentation, and used as a standard for security professionals when implanting encryption technologies.

National Institute of Standards and Technology. (2002, December 3). *Security requirements for cryptographic modules*. (Federal Information Processing Standards Publication 140-2).

Abstract. The selective application of technological and related procedural safeguards is an important responsibility of every Federal organization in providing adequate security in its computer and telecommunication systems. This publication provides a standard that will be used by Federal organizations when these organizations specify that cryptographic-based security systems are to be used to provide protection for sensitive or valuable data. Protection of a cryptographic module within a security system is necessary to maintain the confidentiality and integrity of the information protected by the module. This standard specifies the security requirements that will be satisfied by a cryptographic module. The standard provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

Comments. This standard is primary standard that encryption technologies must meet to be in compliance with if encryption is to be used to protect sensitive information. This

standard presents key areas to consider when selecting encryption as part of a data protection solution. This standard is viewed as credible since it is a federally enforced standard that must be followed if encryption is to be used in any federal system and is a key standard for security professionals to follow.

National Institute of Standards and Technology. (2006, March). *Minimum security requirements for federal information and information systems*. (Federal Information Processing Standards Publication 200).

Abstract. This publication specifies the minimum security requirements for federal information and information systems in 17 security-related areas. Federal agencies must meet the minimum security requirements as defined in this document through the use of security controls in accordance with NIST SP 800-53, as amended.

Comments. This standard bridges the requirement to follow FISMA and NIST security controls in order to be in compliance with best security practices. This standard is viewed as credible since it references other standards that must be followed and comes from the leading organization behind certification and accreditation of information systems.

National Institute of Standards and Technology. (2009, August). *Recommended security controls for federal information systems and organizations*. (NIST Special Publication 800-53, Revision 3).

Abstract. This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. NIST is responsible for developing information security

standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in Circular A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in Circular A-130, Appendix III.

Comments. This document presents the security controls that must be followed in order for a system to be approved for use within numerous federal and commercial agencies. It presents the requirement that protecting sensitive information is a mandate and helps to ensure that best security practices are continuously followed. FISMA is the standard that all certification and accreditation methods reference. This document is viewed as credible since it is constantly used to certify and accredit systems that are federally used or owned and is continually referenced in other documentation.

RSA Security, Inc. (2002*). Securing data at rest: Developing a database encryption strategy*. (White Paper). Retrieved from http://www.rsa.com/products/bsafe/whitepapers/DDES_WP_0702.pdf

Abstract. This paper examines the issues of implementing encryption and makes recommendations that will help a company develop a strategy that will meet the company's needs. The paper also provides basics behind encryption and what to consider when selecting an encryption type.

Comments. This paper provides the key considerations for implementing encryption as part of the DAR protection solution. It also presents encryption strategies to consider when implementing encryption. This paper is considered credible since it is peer-reviewed and is provided by one of the key security solution providers today.

Shipley, G. (2009). Full disk encryption evolves. *InformationWeek*, 47-49. Retrieved from Factiva.

Abstract. This article presents data breaches that were well recognized in that a large number of people were affected. FDE is presented in two ways, which include software solutions and hardware solutions. The pros and cons are also presented for both and what the recommended solution is when encrypting storage media.

Comments. This article provides a deeper look into encryption and breaks it up into hardware and software solutions. It also presents the pros and cons for each and provides insight into how the new Trusted Computing Group standard impacts DAR solutions. This author is deemed credible since he is the CTO of a company that specializes in information security and risk management.

Storage Networking Industry Association. (2009). *Solutions guide for data-at-rest*. (Storage security Industry Forum). Retrieved from http://www.trustedcomputinggroup.org/files/resource_files/147231E7-1D09-3519-AD9B37F37D183748/SSIF_Solutions_Guide_for_Data-at-Rest.pdf

Abstract. This document provides guidance into some of the factors that should be considered when evaluating storage security technology and solutions. In addition, the

guide provides background information describing various storage security threats related to loss of physical control of storage media.

Comments. This guide provides input into the strengths of encryption and the choices that are available when implementing encryption into ISs. It presents different areas within a system that encryption can be implanted and what the impacts are when deciding on an encryption implantation strategy. The guide goes further by comparing vendor solutions and determining how each compares to the other. This guide is viewed as credible since it is peer reviewed and prepared by security experts from around the security industry.

Strohmeyer, R. (2010). Lost! *PC World*, *28*(5), 85-91. Retrieved from Ebsco Academic Search Elite database.

Abstract. The article offers tips for improving the odds of recovering a lost cell phone, laptop or other electronic gear. The author recommends taking some precautions to easily recover a lost phone and safeguard one's data. To improve the odds of getting back a stolen laptop, the author advises running a tracking and recovery application such as zTrace or LoJack for laptops. They can be used to initiate a remote data wipe that erases everything on the hard drive. To recover other mobile devices such as e-book readers, media players, GPS devices, portable hard drives and thumb drives, the author suggests printing one's name and phone number on a return address label and affixing it to the device. The author also presents four habits that help avoid losing one's things.

Comments. This article provides current technologies that are available and presents product capabilities. This article is key to presenting DAR protection solutions for mobile

phones that get overlooked when DAR protection strategies are being implemented. This article is viewed as credible since it is from a peer-reviewed magazine that circulates widely the information technology industry.

The case of the 12,000 lost laptops. (2008). *Communications News*, *45*(8), 6. Retrieved from Ebsco Academic Search Elite database.

Abstract. The article reports on the research study conducted by the Ponemon Institute sponsored by Dell Computers Corp. on the case of frequent laptop loss at U.S. airports, and its impact to businesses' information security since these laptops are owned mostly by business travelers. Based on the study, business travelers are losing more than 12,000 laptops per week in different U.S. airports yet only one-third of these laptops are reclaimed. The study also shows that 53 percent of surveyed business travelers admitted that their laptops contain confidential and sensitive information, while 65 percent said they do not take steps to protect or secure the information on it. With these results, companies are threatened of having a data breach if a stolen laptop contains sensitive information.

Comments. This article presents data from studies performed on the amount of mobile ISs are lost in the United States. It also provides insight into the weak areas that DAR is intended to protect. This article is viewed as credible since it presents data from additional studies and comes from a peer-reviewed magazine.

Review of the Literature

This literature review presents a discussion of two major areas in data-at-rest (DAR) security solutions, which include (a) the standards and policies behind protecting DAR in mobile ISs and (b) the two main security options that are available to organization and individuals, with an emphasis on affordability and interoperability. Keyword and key phrase searches through the World Wide Web (WWW) and the UO Libraries OneSearch indicate that there are numerous publications on the topic of protecting DAR and the potential risks inherent when not protecting DAR. And while the material selected reveals a variety of ways to protect DAR in mobile ISs, it is apparent that DAR security solution strategies are not being fully implemented (Ferguson, 2008, p.22). For example, it is estimated that 50 percent of all laptops contain sensitive data and that 65 percent of all business travelers do not either encrypt their laptops or implement some sort of DAR security solution (Ferguson, 2008, p.22).

In order to identify information pertinent to the research questions addressed in this study, a conceptual analysis is performed on the selected literature. Coding consists of broad searches on data-at-rest protection, data-at-rest security, stolen laptops, and stolen cell phones.

EMA (2008), EMC^2 (2008), RSA Security, Inc. (2002), and Shipley (2010) focus on the use of standardized encryption technologies, which means using NIST FIPS 140-2 compliance, to implement DAR security solutions. This includes how to manage encryption and where to best utilize encryption technologies. Johnson (2006) suggests following NIST checklists for DAR encryption; while Dworkin (2001) takes the matter of encryption further by discussing the different modes that standardized encryption must follow in order to be complaint with industry standards. Mearian (2009) and Bradley (2010) look past encryption and focus on applications that track and potentially wipe sensitive information once the mobile IS has been reported lost.

Factors Driving the Need for DAR Protection

Lost or stolen devices. The need for a data-at-rest (DAR) security solution is ever present with the number of companies dependant on a mobile workforce that requires traveling with laptops, smart phones, personal digital assistants (PDA), and other electronic devices holding sensitive information (12,000 lost laptops, 2008, p.6). Out of all the laptops carried through an airport each year, it is reported that more than 12,000 laptops are lost and 53 percent of business travelers say they have sensitive information stored on their laptops. This potential risk of a lost or stolen mobile information system (IS) is leveraged against organizations that depend on their mobile workforce and is driving organizations to take action in order to mitigate the risk (12,000 lost laptops, 2008, p.6).

Regulations and policies. EMC^2 (2008) says that regulations mandate the use of protection measures to secure DAR and some of these regulations include:

- Sarbanes-Oxley Act
- California (CA) 1798
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Personal Information Protection Act
- Gramm-Leach-Bliley Act
- European Union (EU) Data Protection Directive
- National Data Privacy laws (p.10).

INPUT (2007) also says that the following government policies and legislation are either helping pass additional regulations or lay the groundwork for other regulations that are intended to protect sensitive information. These government policies and legislation include:

- The Office of Management and Budget's (OMB) Memorandum M-06-16

- The Office of Management and Budget's (OMB) Memorandum M-07-16
- The Federal Information Security Management Act (FISMA) of 2002
- The Federal Agency Data Breach Protection Act
- The Notification of Risk to Personal Data Act
- The Personal Data Privacy and Security Act of 2007
- Telework Enhancement Act of 2007 (pp.5-6)

Understanding what to protect. According to Identity Finder, LLC (2009), understanding unsecured files on mobile ISs containing sensitive data is an ever-increasing risk. Data-at-rest (DAR) security solutions, when properly implemented, are intended to mitigate risk when appropriately aligned with the organizational needs (p.2). Identity Finder, LLC (2009) points out that 44 percent of all data breaches occur from lost or stolen digital media and 22 percent of data breaches occur from hackers gaining access to the data source. This means that 66 percent of all data breaches could have been prevented by securing data at the source. Also, the costs associated with implementing a DAR security solution is less than the costs associated with data breaches that cause damage to reputation or require credit monitoring services for affected individuals (pp.2-4).

Identify theft. Greenwood (2009) states that lost and/or stolen laptops can lead to larger scale crimes by giving the means to criminals to carry out identity theft rings when they obtain mobile ISs that are not protected by DAR security solutions. However, when DAR security solutions are implemented, they can assist in preventing identity theft, which in turn assists law enforcement by preventing potential additional crimes (p.44). Greenwood (2009) mentions one instance where a laptop was stolen from a school system in North Carolina; an application had been installed to satisfy state regulations on protecting sensitive information (also known as data-

at-rest (DAR)). When the school realized that the laptop was missing, they notified the application vendor and the vendor was able to locate the laptop via Global Positioning System (GPS). Once the location was recorded, the information was passed to law enforcement, which raided the address and discovered an identity theft ring with all the materials needed to create phony identification for illegal immigrants (p.44).

DAR Standards and Policies

The National Institute of Standards and Technology (NIST) (2009) provides standards and requirements for implementing security measures mandated by the Federal Information Security Management Act (FISMA) of 2002 to ensure that best security practices are utilized when implementing security solutions on information systems (p. iv). Acts such as FISMA and others mentioned in this *Review of the Literature* section are all designed to ensure compliance and reduce security risks towards individuals and organizations (U.S. Government, 2002, Sec. 301).

Minimum security requirements. NIST (2006) recommends a set of minimum security requirements when security solutions are being implemented and the Federal Information Processing Standards Publication 200 (FIPS Pub 200) is one of the two standards required to meet FISMA legislation (p.1). When it comes to protecting data-at-rest, NIST (2006) points out that specifications need to be considered to ensure the solution is implemented correctly and aligns with the needs of the individual and organization. The baseline specifications include:

- Access Control (AC): Limits access to information systems to only those that are authorized users.

- Awareness and Training (AT): Ensures that individuals are aware of security risks associated with their activities.
- Audit and Accountability (AU): Protects and retains information about attempts to access unauthorized information or unauthorized activity.
- Identification and Authentication (IA): Identifies and verifies system users prior to allowing access.
- Media Protection (MP): Protects information, limits access, and destroys media before disposal or release for reuse.
- Planning (PL): Provides the documentation and updates of security plans.
- Risk Assessment (RA): Provides a periodic risk assessment to operations.
- System and Communications Protection (SC): Allows an organization to monitor, control, and protect their communications (NIST, 2006, pp.2-4).

Protection guidance. Clay (2006) references NIST and the NIST checklists that are available to ensure that additional protection is applied to sensitive information that is moved outside of an organization's current physical protection. The checklists also provide specific actions to be taken to ensure that each specification is covered when implementing a DAR security solution (pp.1-2). Clay (2006) also mentions that each organization should go through a protection process prior to utilizing NIST checklists to ensure all related security controls are implemented. This protection process provides insight into what steps the organization or individual needs to take to successfully implement a security measure and determines the best action to take towards protecting sensitive information (p.3). Figure 1 outlines the protection process.

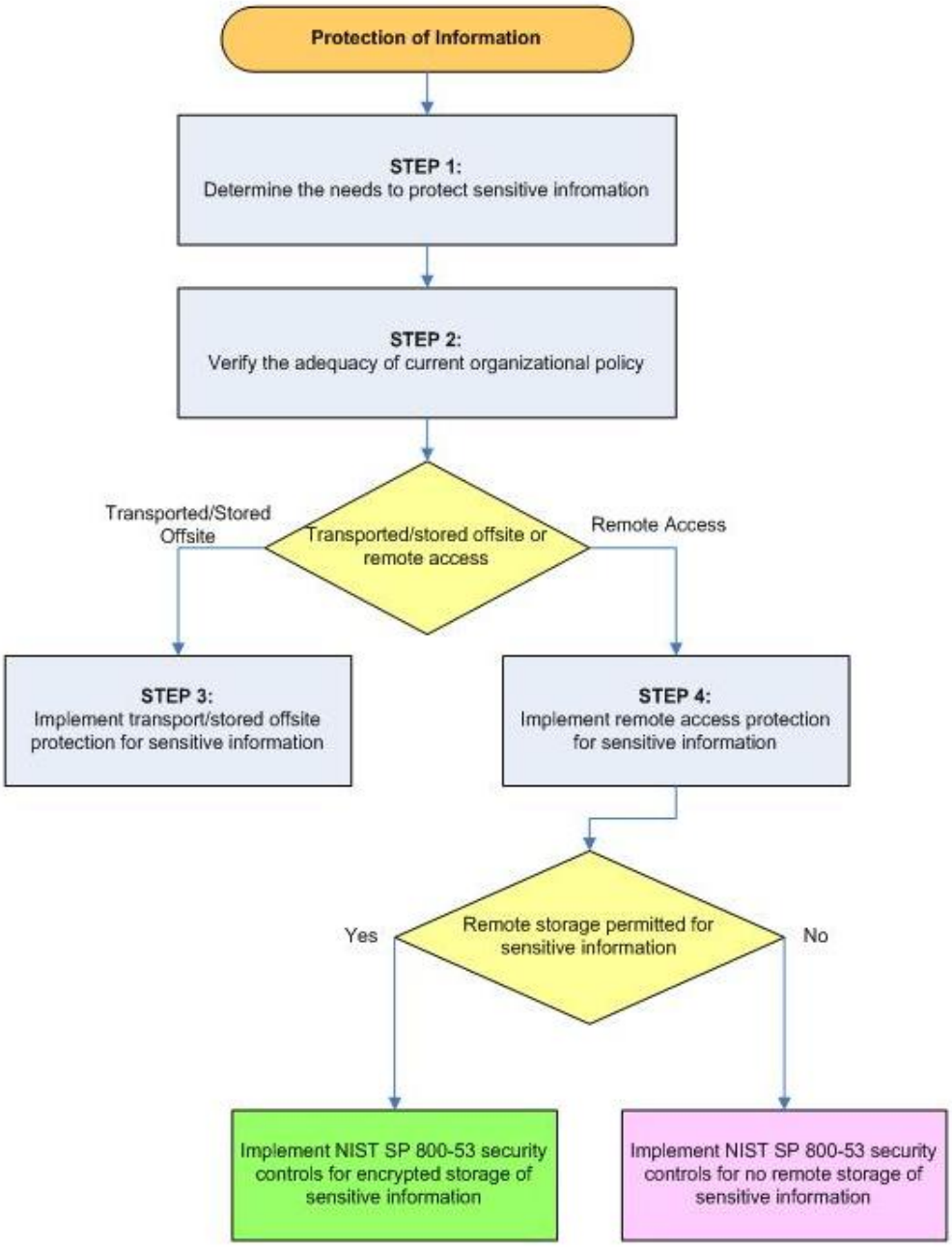

Figure 1. Process for protecting sensitive information. Adapted from "Protection of Sensitive Information Process," by J. Clay, 2006 *Protection of sensitive agency information.* (Office of Management and Budget Memorandum-06-16).

The Department of the Army (2006) provides specific documentation on how DAR security solutions are to be implemented. They utilize a series of guidance documents that align with Army best practices to ensure that affordability and interoperability are maintained throughout all mobile ISs that are under the control of the Army (p.1). The Department of the Army (2006) also provides procedures that assist in identifying, labeling, and accounting for all of its mobile ISs and removable media. They take protecting sensitive information a step further by limiting the amount of sensitive information transported out of facilities to ensure that the minimum amount of sensitive information is transported on mobile ISs (p.2). The final step that the Army takes to protect its sensitive information on mobile ISs is that they provide extensive training to individuals that transport sensitive information to help reduce their risk of having a data breach encompassing sensitive information (DoA, 2006, p.2).

Best security practice guidance. According to NIST (2009), the way to ensure that due diligence is met is by utilizing best security practices when implementing security requirements or controls (p.2). NIST (2009) lays out an industry recognized process for ensuring that systems meet best practices and that risk is mitigated to an acceptable level. The NIST process utilizes risk management to best understand where the sensitive information is, what the organization or individual needs to consider when selecting a security solution, and the steps necessary in order to meet the needs of the organization or individual (p.17). After managing risk, NIST (2009) states that information systems must be categorized to determine the impact of sensitive information being lost. Once the categorization is completed, the security controls must be selected so that the controls correspond to the categorization and risk. After controls are selected, they are implemented and monitored to ensure that the security posture for the security solution stays inline with the needs of the organization or individual (pp.18-21).

DAR Protection Solutions via Encryption

EMA (2008) says that encryption is gaining favorability again in today's market due to the increasingly urgent need to protect greater amounts of transported sensitive information (p.2). EMA (2006) states that encryption must be able to answer several questions if it is to be effectively deployed in information systems that store sensitive information; questions include:

- Can availability of encryption be assured if data is lost due to inadequate encryption management or decryption keys?
- Can encryption keys be secured and available without exposing the encryption strategy to risk?
- Can costs and performance impacts associated with encryption be reduced or eliminated?
- Can encryption assure security without adding additional complexity? (p.1).

Common encryption algorithms. SNIA (2009) says that there are a few different encryption algorithms that can be used when an encryption strategy is desired. These algorithms include the Data Encryption Standard (DES), triple DES (3DES), Signature Hashing Algorithm 1 (SHA-1), Message Digest algorithm 5 (MD-5), and the Advanced Encryption Standard (AES). AES is the preferred algorithm for use today, and is recommended throughout the security industry because it is one of the most dependable (p.9). The AES algorithm is a symmetric block cipher, which is the recommended cipher for protecting DAR via encryption (NIST, 2001). This algorithm's been approved industry wide to be implemented in software, firmware, hardware, or in any combination thereof. The algorithm, which gets stronger as the number of bits increases, is available in key lengths of 128, 192, or 256 bits. However, to ensure that the algorithm is implemented correctly and effectively, it should be implemented with a Federal Information

Processing Standard 197 (FIPS 197) or National Industry Standards and Technology (NIST) mode (pp.ii-5).

Dworkin (2001-2007) says that there are eight modes of operation that are federally approved to be used with the AES algorithm. The algorithm modes of operation work in conjunction with the algorithm and encryption key to encrypt the information in a specific way. The modes of operation include block cipher-based Message Authentication Code (CMAC), Galois/Counter Mode (GCM), Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), Counter (CTR), and CTR combined with Cipher Block Chaining-Message Authentication Code (CBC-MAC). It is important to know if an algorithm is using a specific mode to ensure that all the pieces are available to decrypt information that has already been encrypted (pp.1-2).

Full-disk encryption. Shipley (2009) says that full-disk encryption (FDE) is the preferred way to encrypt data once it is stored since it addresses the threat of data breaches by encrypting the entire hard drive with a single encryption/decryption key, algorithm, and algorithm mode. It is also the preferred way to use encryption on mobile ISs due to reduced costs associated with implementation, reduced management costs associated with encryption key management, and reduced complexity added to the IT environment (p.1).

Mearian (2009) believes that the Trusted Computing Group standard will eventually force all manufacturers to include FDE in every hard drive or solid state drive that is produced within the next five years. This is because FDE ensures that any mobile device that is lost or stolen cannot be accessed by an individual that finds it or steals it. Also, FDE is the surest way to ensure that companies and individuals are in accordance with most state laws pertaining to keeping sensitive information secure (p.10).

EMC^2 (2008) says that encryption is only as good as the management, generation, and protection of the encryption/decryption keys used in the encryption/decryption process. Since FDE reduces the management, generation, and protection of encryption/decryption keys, many organizations and individuals are turning to FDE to help solve their data-at-rest (DAR) security needs in mobile ISs (p.6). However, Gibson (2007) cautions that encryption must be present from time of inception through destruction (p.44).

DAR Protection Solutions via Application

Ferguson (2008) points out that companies like Dell, Lenovo, and Intel have begun including security application tools on certain equipment models that include protection, recovery, and security applications as a standard practice (p.23). Encryption only solves part of the problem of protecting DAR, which is ensuring that sensitive information cannot be seen by someone who does not need to see it. Kandra et al. (2004) say that while encryption is the surest way to protect sensitive data on a mobile IS (i.e., laptop, cell phone, and/or PDA), the device also needs to be retrievable if it is lost or stolen. In order to recover a lost or stolen mobile information system, applications are needed to locate the device or to possibly take an additional step in protecting sensitive information by remotely erasing the data no matter who has the device (p.50).

Available applications. Strohmeyer (2010) says that before any application or encryption is used to protect a mobile information system (IS), it should be made recoverable or replaceable and utilize the password protection feature. In order for the mobile IS to be recoverable, back-ups of the information stored on the mobile IS should be done on a regular

occurrence. To make the mobile IS replaceable, a mobile IS insurance policy option should be in place to allow the back-up information to be easily transferred to the replaced mobile IS (p.87).

Strohmeyer (2010) says that there are three primary protection factors on a mobile IS, which include hardware, the data on the hardware, and the security that is maintained with control over the data. However, the hardware aspect can impact an individual more visibly than an organization due to replacement costs if an insurance policy is not in place (p.87). In order to protect the hardware, insurance policies primarily allow for the replacement hardware to be obtained at a lower cost and can be replaced in a matter of days depending on the insurance policy if the lost/stolen hardware cannot be located. The data on the hardware is protected with back-ups, encryption, and applications to help secure sensitive information. Finally, hardware insurance policies, back-ups, and security applications all work together to assist in maintaining control over the data and allows organizations/individuals get back up and running in a shorter amount of time and at lower costs to the organization/individual (Strohmeyer, 2010, p.87).

Strohmeyer (2010) provides some options on available DAR protection applications for mobile ISs. These include the following:

- Where's My Droid – Free application that helps locate an Android customers phone remotely via another phone by emitting a load ring.
- Where's My Phone – Free application version helps Blackberry customers locate their phone remotely via email and emits a load alarm but the $4.00 version adds a GPS locator option as well.
- Beep My Cell – $0.99 application that helps iPhone customers locate their phone remotely through a Web site, send a beeping noise to the phone and send a custom message to whoever finds the phone.

- Phone Finder With Google Maps – $1.50 application for Windows based phones that sends a beep to the phone and sends the GPS location to the phone that triggered the beep.
- WaveSecure – $20.00 per month application for Android, Blackberry, Symbian S60, and Windows phones that allows the customer to remotely log into a Web browser to locate the phone, detect tampering, back-up, and wipe the phone all remotely.
- MobileMe - $99.00 per year application (there is also a free version) for iPhone customers that allows a customer to log into a Web site and remotely wipe, locate, lock, and send the phone a custom message remotely (pp.88-89).

Kandra et al (2004) points to a software application called LapTrack that utilizes a third party to remotely locate a lost or stolen laptop once it is reported missing. The company also ensures that the data remains secure once the laptop is reported (p.50). Strohmeyer (2010) points to two software applications called zTrace and LoJack for laptops, which cost around $60.00 per year. The applications track the location by way of the service provider, who also works with law enforcement to recover the laptop. The applications immediately start wiping the hard drive in a way that cannot be stopped once started (p.92). Strohmeyer (2010) also mentions an open-source application called TrueCrypt that encrypts information on computer hard drives and universal serial bus (USB) thumb drives by creating a secure volume and encrypting data as it is read and written (p.92).

Bradley (2010) states that there are applications that exist to ensure sensitive data is completely gone prior to disposing of a computer. One such application is called CyberCide and costs $30.00. However, consumers need to be aware that the application ensures that there is no

recoverable information; it goes beyond the standard wipe, which simply over writes memory space with ones and zeros (p.38).

Conclusions

This literature review is intended to assist small and medium sized businesses (SMBs) in selecting data-at-rest (DAR) security solutions to avoid attacks and assist individuals in mitigating the threat of identity theft. The study presents information that is readily available to the general public in references that are either written or endorsed by industry experts. Information is generalized for the intended audience, formatted as a guide, and designed to summarize (a) the standards and regulatory protection policies behind the need to push towards DAR security solutions (see Table 3) and (b) the security options that are available when it comes to protecting DAR in a mobile information system (IS) (see Table 4).

The need for DAR security solutions is ever increasing with the amount of digital information that is available (USC, 2010, pp.2-4). Many organizations and individuals are not doing enough to protect themselves from a having sensitive information either stolen or lost. Due to the amount of mobile ISs used by individuals and the amount of digital information that is available, it is important to review the best security options for protecting sensitive information.

The United States government has started to put into place policies and regulations intended to give the general public guidance on protecting sensitive information (see Table 3). The DoD (2002) utilizes processes and defined roles to help ensure that policies are enforced and current (pp.4-7). The DoD (2003) also utilizes an implementation plan to ensure that each information system follows a documented procedure for best security practices (pp.7-10).

Table 3

Summary of 13 DAR standards, regulations, and policies

Standards, regulations, and polices
• Sarbanes-Oxley Act • California (CA) 1798 • Health Insurance Portability and Accountability Act (HIPAA) of 1996 • Personal Information Protection Act • Gramm-Leach-Bliley Act • European Union (EU) Data Protection Directive • National Data Privacy laws • OMB Memorandum M-06-16 • OMB Memorandum M-06-17 • Federal Information Security Management Act (FISMA) of 2002 • Federal Agency Data Breach Protection Act • Personal Data Privacy and Security Act of 2007 • Telework Enhancement Act of 2007

It is understood that not every organization or individual can mitigate every security risk associated with protecting data-at-rest (DAR). However, to ensure that an organization or an individual is in compliance with policies, regulations, and/or laws governing them, some sort of protection needs to be put into place to ensure that everything that can be done is being done (see Table 4) (SNIA, 2009, p. 3). Applications may be the quickest way to implement some sort of security measures and are normally lower in cost than other solutions (Strohmeyer, 2010, p. 87). Encryption is the best route to take when trying to protect information and it is the preferred method of policies and regulations (NRS 597.970, 2008). Utilizing an application and/or encryption that is greater than 128 bits is in keeping with best security practices and gives a

means of trying to locate the lost/stolen device and provides a deterrent for criminals (Greenwood, 2009, p.26).

Table 4

Summary of DAR security solutions

Solution type	**Protection measure**
Hardware	1. Insurance policy 2. AES 256 bit full-disk encryption a. AES modes i. CMAC, ii. GCM, iii. ECB, iv. CBC, v. CFB, vi. OFB, vii. CTR, or viii. CBC-MAC
Application	1. Where's My Droid 2. Where's My Phone 3. Beep My Cell 4. Phone Finder with Google Maps 5. WaveSecure 6. MobileMe 7. LapTrack 8. zTrace 9. LoJack 10. TrueCrypt 11. CyberCide

Prior to selecting a particular DAR security solution, Strohmeyer (2010) suggests that a holistic review should be performed to determine the exact needs of the organization and/or individual (pp. 86-88). While the review of needs is transpiring, DoD (2009) recommends that the review should incorporate critical planning to ensure performance is not impacted by the security solution (p.2). When any security solution (i.e. DAR) is implemented, it is best to ensure that the security solution fits within specific needs in relation to two driving factors, including (a) affordability, which means it must not cost more than the data is worth (SNIA, 2009, p.10) and (b) interoperability, which means it works within the intended mobile IS and system (DoD, 2007, Attachment 2).

Encryption solutions - affordability and interoperability

RSA Security, Inc. (2002) states the encryption strategies for DAR can become very expensive and may increase the complexity to the network quickly depending on the encryption technology that is selected. Encryption strategies normally require attention in two areas in order for encryption to be successful. The first is the encryption technology itself and the second is the management of the keys used to encrypt and decrypt the information they assist in protecting (p.2).

According to RSA Security, Inc. (2002), best security practices are implemented when an encryption strategy reduces the amount of support required by IT staff, takes the responsibility of protecting sensitive information off of the data owner, compliments the environment it is deployed in, and does not add complexity to the IT environment, which in turn reduces user utilization. One way to ensure that best security practices are met is by using encryption that is industry supported and provided by a cryptographic provider that is reputable (p.3). NIST (2008)

states that the best way to ensure that encryption is industry supported is to ensure that it complies with the Federal Information Processing Standards Publication 140-2 (FIPS 140-2), because the standard is federally recognized and all federal systems that utilize encryption must meet or exceed this standard. The NIST encryption standard is also encouraged to be used by any organization or individual that is interested in implementing an encryption strategy (p.1).

When it comes to encryption, NIST (2008) reports that the best route to take is to use the Advanced Encryption Standard (AES) and to utilize a key that is 256 bits in length for security reasons (pp.2-5). Along with utilizing AES, Dworkin (2010) recommends selecting a block cipher mode that is compatible with AES and falls within the guidelines that have been put in place by industry standards (p.3). However, the safest bet is to select encryption that is backed by an industry leader in providing encryption solutions (RSA Security, Inc. 2002, p.5).

Gibson (2007) says that in order to ensure affordability, interoperability, and early regulation compliance some organizations are ordering and purchasing systems that already have their hard drives pre-encrypted. This includes utilizing operating systems like Windows Vista Ultimate that utilize Microsoft's BitLocker encryption algorithm to help reduce costs associated with encryption and data-at-rest security solutions (p.38).

Application solutions - affordability and interoperability

When it comes to selecting an application as part of the security solution, it is important to purchase an application that is supported by the mobile IS that it is to be installed on (Stroymeyer, 2010, p.87). This means that standardizing mobile ISs within an organization can help in lowering the overall cost of a DAR security solution (Strohmeyer, 2010, pp.86-90). This

standardization will not only assist in the application process but also in selecting the appropriate encryption solution and overall security measure(s) that is sought after.

Providing an encryption solution to protect sensitive information in a mobile IS protects the data and satisfies standards, policies, and regulations. However, it does not provide a holistic approach to an overall DAR security solution (Bradley, 2010). In order to provide a well rounded DAR security solution, applications need to be incorporated into the protection measure(s) to locate the mobile IS in order to ensure replacement costs can be reduced and to ensure that sensitive data that is no longer needed is properly disposed of (Bradley, 2010).

Strohmeyer (2010) recommends applications that utilize GPS to assist in tracking mobile ISs because of the interoperability of the technology and its ease of use (p.86). Most mobile ISs are capable of utilizing the GPS technology and it provides the quickest way to pin-point a lost/stolen item since security applications are capable of ensuring that GPS is not disabled (Strohmeyer, 2010). If the mobile information system is simply lost, a GPS capable application can reduce the amount of time required to locate it and if the mobile IS is stolen, the location can be turned over to law enforcement for retrieval (Strohmeyer, 2010).

Gibson (2007) presents the notion that DAR security solutions need to look past hard drives and realize that Universal Serial Bus (USB) drives, Compact Disc (CD), and Digital Versatile Disc (DVD) drives present security risks as well. This means that the DAR security solution needs to do more than simply protect hard drives with encryption. Attention needs to be made at every location sensitive information can be stored and the DAR security solution must protect multiple storage areas in order to be affordable and ensure that interoperability issues do not arise (p.37).

In order to deploy a well-rounded DAR security solution to curtail identity theft, organizations/individuals must surpass security standards, regulations, and policies that call for encryption, which provides only half of the overall solution. The other half of the DAR security solution must utilize applications that satisfy organizational/individual needs and mitigate the risk (Bradley, 2010).

References

Bradley, T. (2010). Keep your personal data off the market. *PC World, 28*(6), 37-38. Retrieved from Ebsco Academic Search Elite database.

Busch, C., De Maret, P., Flynn, T., Kellum, R., Le, S., Meyers, B., Saunders, M., & White, R., (2005). *Content analysis*. Retrieved from http://writing.colostate.edu/guides/research/content

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). Thousand Oaks, California: SAGE

Department of Defense. (2002, October 24). *Information assurance (IA)*. (Department of Defense Directive 8500.1).

Department of Defense. (2003, February 6). *Information assurance (IA) implementation*. (Department of Defense Instruction 8500.2).

Department of Defense. (2007, July 3). *Encryption of sensitive unclassified data at rest on mobile computing devices and removable storage media*. (Department of Defense Memorandum). Retrieved from http://iase.disa.mil/policy-guidance/dod-dar-tpm-decree07-03-07.pdf

Department of Defense. (2007, November 28). *DoD information assurance certification and accreditation process (DIACAP)*. (Department of Defense Instruction 8510.01).

Department of Defense. (2009, February 10). *Management of the Department of Defense information enterprise*. (Department of Defense Directive 8000.01).

Department of the Army. (2006, September 28). *Army data-at-rest (DAR) protection strategy*. (Department of the Army Memorandum).

Department of the Army. (2006, October 31). *Guidance on protecting data-at-rest (DAR)*. (Department of the Army Memorandum). Retrieved from http://www.tradoc.army.mil/tpubs/misc/DAR/31%20Oct%2006%20-%20DAR%20Memo.PDF

Dworkin, M. (2001, December). *Recommendation for block cipher modes of operation: Methods and techniques*. (NIST Special Publication 800-38A).

Dworkin, M. (2005, May). *Recommendation for block cipher modes of operation: The GMAC mode for authentication*. (NIST Special Publication 800-38B).

Dworkin, M. (2007, July 20). *Recommendation for block cipher modes of operation: The CCM mode for authentication and confidentiality*. (NIST Special Publication 800-38C).

Dworkin, M. (2007, November). *Recommendation for block cipher modes of operation: Galois/counter mode (GCM) and GMAC*. (NIST Special Publication 800-38D).

Dworkin, M. (2010, January). *Recommendation for block cipher modes of operation: The XTS-AES mode for confidentiality on storage devices*. (Addendum to NIST Special Publication 800-38E).

Dworkin, M. (2010, October). *Recommendation for block cipher modes of operation: Three variants of ciphertext stealing for CBC mode*. (NIST Special Publication 800-38A).

Enterprise Management Associates. (2008, September). *Security for data at rest: Critical challenges and IBM information infrastructure solutions*. (Enterprise Management Associates White Paper). Retrieved from http://www.fdesecurityleaders.com/downloads/pdf/security_for_data_at_rest.pdf

EMC^2. (2008, January). *Approaches for encryption of data-at-rest in the enterprise: A detailed review*. (White Paper). Retrieved from http://www.emc.com/collateral/hardware/white-papers/h4173-approaches-encryption-data-at-rest-enterprise-wp.pdf

Federal Trade Commission. (2007). *Keeping laptops from getting lost or stolen*. (White Paper). Retrieved from Ebsco Academic Search Elite database.

Ferguson, S. (2008). Securing the laptop. *EWeek, 25*(21), 22-23. Retrieved from Ebsco Academic Search Elite database.

Gibson, S. (2007). Securing the laptop: mission impossible? *EWeek, 24*(36), 35-43. Retrieved from Ebsco Academic Search Elite database.

Greenwood, B. (2009). Stolen laptop leads police to identity theft ring. *Information Today, 26*(8), 44. Retrieved from Ebsco Academic Search Elite database.

Gross, G. (2007). VA still looking for light at end of it security tunnel. *Computerworld, 41*(39), 11. Retrieved from Ebsco Academic Search Elite database.

Hall, M. (2006). Cell phone security nightmare.... *Computerworld, 40*(23), 12. Retrieved from Ebsco Academic Search Elite database.

Harris, S. (2009). *CISSP all-in-one exam guide* (5th ed). New York: McGraw-Hill Companies.

Hewitt, M. (2002). *Carrying out a literature review* (p.21-22). Trent Focus Group. Retrieved from University of Oregon Blackboard, Terminal Project course page.

Identity Finder, LLC. (2009). *Data loss prevention: Data-at-rest vs. data-in-motion*. (White Paper). Retrieved from http://www.identityfinder.com/Software/Docs/WhitePaper.pdf

INPUT. (2007, June). *Securing data at rest in a mobile environment*. (White Paper). Retrieved from http://www.federalnewsradio.com/pdfs/Securingdataatrestinamobileenvironment.pdf

Iron Port Systems. (2007). *Data loss prevention best practices: Managing sensitive data in the enterprise*. Retrieved from http://www.ironport.com/pdf/ironport_dlp_booklet.pdf

Johnson III, C. (2006, June 23). *Protection of sensitive agency information.* (Office of Management and Budget Memorandum-06-16).

Kandra, A., Aquino, G., & Brandt, A. (2004). Keep your hands on your handhelds. *PC World, 22*(8), 49-51. Retrieved from Ebsco Academic Search Elite database.

Lawrence, G. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005) *CSI/FBI computer crime and security survey*. Retrieved from http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf

McNamara, P. (2008). AT&T manager on laptop loss: "It is pathetic". *Network World, 25*(24), 50-47. Retrieved November 12, 2010, from Ebsco Academic Search Elite database.

Mearian, L. (2009). Firms take steps to head off encryption dangers. *Computerworld, 43*(6), 10. . Retrieved from Ebsco Academic Search Elite database.

National Institute of Standards and Technology. (2001, November 26). *Announcing the advanced encryption standard (AES).* (Federal Information Processing Standards Publication 197).

National Institute of Standards and Technology. (2002, December 3). *Security requirements for cryptographic modules*. (Federal Information Processing Standards Publication 140-2).

National Institute of Standards and Technology. (2006, March). *Minimum security requirements for federal information and information systems*. (Federal Information Processing Standards Publication 200).

National Institute of Standards and Technology. (2009, August). *Recommended security controls for federal information systems and organizations*. (NIST Special Publication 800-53, Revision 3).

National Institute of Standards and Technology Communications Security Establishment (2008, January 24). *Implementation guidance for FIPS PUB 140-2 and the cryptographic module validation program*. (Federal Information Processing Standards Publication 140-2IG).

NRS 597.970. (2008, October 1). *Restrictions on transfer of personal information through electronic transmission*. (Nevada State Law). Retrieved November 5, 2010, from http://www.westernreportingservices.com/NRS597.970.pdf

Obenzinger, H. (2005). *What can a literature review do for me? How to research, write, and survive a literature review* (pp. 1-9). Stanford University. Retrieved from University of Oregon Blackboard, Terminal Project course page.

RSA Security, Inc. (2002*). Securing data at rest: Developing a database encryption strategy*. (White Paper). Retrieved from http://www.rsa.com/products/bsafe/whitepapers/DDES_WP_0702.pdf

Shipley, G. (2009). Full disk encryption evolves. *InformationWeek*, 47-49. Retrieved from Ebsco Academic Search Elite database.

Storage Networking Industry Association. (2009). *Solutions guide for data-at-rest*. (Storage security Industry Forum). Retrieved from http://www.trustedcomputinggroup.org/files/resource_files/147231E7-1D09-3519-AD9B37F37D183748/SSIF_Solutions_Guide_for_Data-at-Rest.pdf

Strohmeyer, R. (2010). Lost! *PC World*, *28*(5), 85-91. Retrieved from Ebsco Academic Search Elite database.

The case of the 12,000 lost laptops. (2008). *Communications News*, *45*(8), 6. Retrieved from Ebsco Academic Search Elite database.

The United States Department of Justice. (n.d.) What are identity theft and identity fraud? Identity Theft. Retrieved November 26, 2010, from http://www.justice.gov/criminal/fraud/websites/idtheft.html

United States Congress. Senate Committee on Homeland Security and Governmental Affairs. (2010). *Protecting personal information: Is the federal government doing enough?*. (Hearing before the committee on homeland security and governmental affairs, United States Senate, one hundred tenth congress, second session, June 18, 2008). Retrieved from Ebsco Academic Search Elite database.

United States Government. (2002). *Title III: Information security.* (Federal Information Security Management Act of 2002). Sec. 301.

Vamosi, R. (2010). Big headaches from little data breaches. *PC World, 28*(9), 41-42. Retrieved November 14, 2010, from Ebsco Academic Search Elite database.

Waring, B. (2008). Keep your laptops (and your data) out of harm's way. *PC World, 26*(4), 38. Retrieved November 12, 2010, from Ebsco Academic Search Elite database.