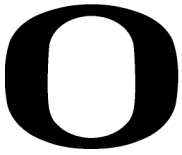

UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Presented to the Interdisciplinary Studies Program:
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

Database Security: An Inventory of Threats, Vulnerabilities, and Security Solutions

CAPSTONE REPORT

Ryan Nichols,
Project Leader Systems Database Administrator,
HBO

University of Oregon
Applied Information Management Program

June 2007

722 SW Second Avenue
Suite 230
Portland, OR 97204
(800) 824-2714

Approved By

_____

Dr. Linda F. Ettinger
Academic Director, AIM Program

ABSTRACT

for

Database Security: An Inventory of Threats, Vulnerabilities, and Security Solutions

Databases are being compromised today at an alarming rate (Britt 2007). This content analysis study provides database administrators and security managers with an inventory of five common threats to and six common vulnerabilities of databases of large corporations when more than 1000 devices require security management (Whitman and Mattord 2004), aligning these threats with potential security solutions. As noted by Vizard (2007), while companies are becoming adept at fighting data breaches, attacks are gaining in sophistication.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER I – PURPOSE OF STUDY

Brief Purpose

The purpose of this study is to identify common threats and vulnerabilities to databases of large corporations when more than 1000 devices require security management (Whitman and Mattord 2004). The research goal is to be able to recommend basic security policies to address those threats and vulnerabilities. In this study, the concept of a threat refers to an object, person or other entity that represents a risk of loss to an asset (Whitman and Mattord 2004). The concept of a vulnerability refers to a weakness or fault in a system or protection mechanism that exposes information to attack or damage (Whitman and Mattord 2004). The assumption underlying this study is that by understanding the weaknesses and the threats facing them, a database administrator can then begin to create a security plan to better protect their databases (Whitman and Mattord 2004).

Corporations today are capturing more information and doing more with that information than ever before. Nearly twenty years ago, Corman (1988) wrote "Security features of a data base are severely threatened as more end users access the centralized corporate data base" (p. 2). The topic of database security continues to be a top priority. Just this year, Britt (2007) states "Security breaches at organizations with large databases continue to monopolize the headlines" (p. 1). The gravity of the situation becomes more clear with the following statistic from Luftman (2004) who writes ". . . based on a recent survey of businesses, a majority of them did not have a company-wide security policy" (p. 166),

not to mention a database security policy. And although the terms 'enterprise security policies' (Whitman and Mattord 2004), 'vulnerability management' (Rath 2006) and 'database security' (Curtain 2007) are being discussed within business periodicals, general standards have yet to be developed.

A wide range of professionals have a stake in a study of database security, however, this study is focused on the needs of the database administrator and the IT Security Manager These two groups of professionals have an immediate need for security recommendations to the database due to the nature of their responsibilities. The information security management team, led by the IT Security Manager, needs to be able to balance the trade-offs between information system utility and security (Whitman and Mattord 2004). A core responsibility of the database administrator (DBA) has always been and continues to be to maintain data integrity and security within the corporate database (Corman, 1998).

This study is designed as a literature review (Leedy and Ormrod 2005) wherein literature is collected that both frames the larger study and forms the data set for content analysis (Palmquist, Busch et al. 2005). In this case, literature is collected that addresses concepts regarding database security, published between 1990 and today. Conceptual analysis is applied as a data analysis strategy, in order to identify common threats and vulnerabilities to large corporate databases, as these are described throughout the various texts (Palmquist, Busch et al. 2005). Additionally, content analysis is applied to identify recommendations for ways to address each of the identified threats and vulnerabilities. Good results of the content analysis are presented in the form of several lists: 1) a list of

identified threats; 2) a list of identified vulnerabilities; and 3) a list of recommendations described in the literature.

The primary outcome of this study is presented as an inventory of potential threats and vulnerabilities common to databases in large corporations. This inventory is designed to better aid database administrators and security managers in not only identifying but also addressing potential threats and vulnerabilities to their corporate databases. To this end, one part of the inventory includes a list of recommendations, excerpted from the literature, that have been or might be used to address each identified threat and vulnerability.

Full Purpose

Due to recent developments and innovations in technology, many business areas have moved all of their data and applications onto the computer (Thuraisingham 2005). Thuraisingham (2005) predicts the risk of moving data onto the computer by saying, "Data has become a critical resource in many organizations, and therefore, efficient access to data, sharing the data, extracting information from the data, and making use of the information has become an urgent need" (p.1). However, due to this urgent need for efficient access to the data, the security features of corporate database have become severely threatened (Corman 1998). This study focuses on the threats and vulnerabilities of large corporate databases when more than 1000 devices require security management (Whitman and Mattord 2004). The objective of the research is to provide security measures that will align with the identified threats and vulnerabilities revealed in the study. Threats can come in the form of an object, person, or other entity that represents a

risk of loss to an asset (Whitman and Mattord 2004). These manifest in a wide range of possibilities, for example, an angry employee using their own access to gather data, a high ranking executive who misplaces their notebook, or even a malicious employee who steals information to sell to the highest bidder (Scheier 2006). A vulnerability refers to a weakness or fault in a system or protection mechanism that exposes information to attack or damage (Whitman and Mattord 2004). Microsoft distributes service packs and patches to their customers, designed to lock down potential vulnerabilities in the software, such as buffer overflows and other programming errors (2007). This kind of response to vulnerabilities is common to database software as well (Newman 2005).

IBM conducted a survey, in late 2006, which stated 83 percent of U.S. organizations believe they have taken significant measures to secure their databases. However in reality over 100 million records containing sensitive, personal information were involved in security breaches since February 2005 according to the Privacy Rights Clearinghouse, a nonprofit consumer information and advocacy program that keeps an up-to-date list of data breaches (2007). Even with much discussion on tightening security of large corporate enterprises, security breaches against those databases continue to dominate the headlines (Britt 2007). This is illustrated clearly by the recent incident at the University of California in which the personal information of more than 800,000 people (located in just one of their databases) was breached from October, 2005 to November, 2006 (Britt 2007).

More than 2,400 years ago, in “The Art of War”, general Sun Tzu made some observations about warfare that are relevant today to the discussion of information security (Whitman and Mattord 2004). According to Sun Tzu, an organization must know itself and know its enemy if it is to reduce risk to the organization through the creation of a layered defense (Whitman and Mattord 2004). Expanding upon this philosophy, the database administrator, who is the keeper or protector of the database, must evaluate the current level of security against the database and establish a baseline for future evaluations (Newman 2005). And for the database administrator to evaluate the vulnerabilities and threats to their database, he or she must be aware of the different kinds of vulnerabilities and threats (Newman 2005).

The security of the database has been a concern for a large number of individuals and groups in large corporations for quite some time (Dutta and McCrohan 2002). Any single application or mechanism that holds the majority of any organization’s data from financial records to human resource information has the eyes and ears of many individuals from the CEO to the Human Resource Director (Dutta and McCrohan 2002). However, it has always been and continues to be the responsibility of the database administrator (DBA) to maintain the data security within the corporate database (Corman 1998). The DBA is tasked with managing the database system which includes determining how a corporation handles its data and enforcing appropriate policies and procedures for managing the corporate data (Thuraisingham 2005). Statements made by Davidson (1995) more than ten years ago still ring true today to describe the job of the DBA in relation to database security:

> Basic requirements for system security are evaluation of the data at risk, assessment of the vulnerabilities of the data, and evaluation of the methods that can be used to reduce the threat to data to an acceptable level of risk. This process results in a written security policy (i.e., the set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information).

Therefore, since it is one of the tasks of the DBA and security manager to create a security policy for the corporate data and database, this study focuses on the DBA and the IT Security Manager whose core responsibilities would be most affected by these threats and vulnerabilities.

This study is designed as a literature review of various articles, books and other research related to large corporate database vulnerabilities and threats. A qualitative research approach is taken in order to focus on the phenomenon of database security (Leedy and Ormrod 2005). By examining the various articles and research material, the study frames new insight into the numerous threats and vulnerabilities affecting corporate databases today. For example, vulnerabilities could be made up from a number of possibilities including vendor bugs, poor architecture, misconfigurations of databases and incorrect usage of application code against the database (Newman 2005). Threats could come not only from outside forces, but internal factors as well. Disgruntled employees, forgetful users who may misplace or lose notebooks with sensitive information on them or even dishonest employees who sell corporate information are all considered internal threats

(Scheier 2006). The study also notes strategies reported in the literature to address these threats and vulnerabilities. Knowing that there is not a single, ultimate security policy to be discovered, the goal of this study is to recommend several potential solutions in relation to an identified set of vulnerabilities and threats. This is due to the variety of environmental factors that drive information security, such as contractual obligations, regulation requirements and even risk to corporate branding (Curtin 2007). While these factors may be similar across different corporations none will be the same.

Content analysis, specifically conceptual analysis (Palmquist, Busch et al. 2005) is chosen as the approach to data analysis in this study. The rationale behind this approach is to determine the kinds of threats and vulnerabilities impacting databases in large corporations, as well as reports of solutions to these dangers. Sixteen pieces of literature are selected from the larger set of materials collected for this study, to form the data set for conceptual analysis. Coding proceeds in three phases, to identify database threats and vulnerabilities along with suggested security measures to counter-act or close up the threats or vulnerabilities. By tallying the presence of these threats and vulnerabilities during the coding process in relation to solutions reported within the collected material, conceptual analysis enables further analysis of the concepts identified (Palmquist, Busch et al. 2005).

The results of the content analysis are presented in the form of three lists. The first list presents threats which represent a risk of loss to the data held within the databases (Whitman and Mattord 2004). The risk of loss could come from a wide range of

possibilities such as a virus or worm (Rath 2006) to confidentiality violations where confidential data is compromised (Thuraisingham 2005). An example of a threat in the form of a worm happened in late January, 2003 when the Slammer worm crippled the Internet and ripped through unprotected systems running Microsoft SQL Server (Fonseca 2004). The damage to the unprotected databases was quite severe by denying Internet activity and severely slowing Internet traffic (Curtin 2007). Perhaps more serious was the fact that it exposed many vulnerabilities within database software (Fonseca 2004). The second list presents vulnerabilities, which are essentially features that allow unintended and unanticipated behaviors that are contrary to the original intention of the database (Curtin 2007). Vulnerabilities can be seen as vendor bugs in the database software, poor architecture of the application that accesses the database by not designing security into the system, and misconfigurations within the database parameters that may have been overlooked, but allow for remote access (Newman 2005). Examples of these vulnerabilities are rampant in the literature collected from sites such as the various Universities that have had their student information stolen to large corporations including CitiFinacials, Ford Motor Company and Time Warner that have all lost data (Schultz 2006). The third list presents reports of ways to address these threats and vulnerabilities with a potential security solution. A solution is presented for each vulnerability and threat identified in this study. The lists can be used in a stand-alone fashion, which will aid the DBA or security manager in either identifying vulnerabilities or threats in their own system based on entries and descriptions in the lists or by recommending a security solution that will potentially resolve an identified threat or vulnerability.

Once the results of the conceptual analysis are formed, the data is used to build two final outcomes of the study, designed for database administrators. The first outcome is framed as an inventory of potential vulnerabilities and threats to large corporate databases. The inventory presents a listing of various vulnerabilities and threats that have appeared or have been experienced in other large corporate databases as reported in the literature. The inventory is designed to give DBAs and security managers a warning sign for items to investigate within their own databases. The inventory is documented in a spreadsheet, listing the vulnerability or threat along with a brief explanation. The format of the inventory can be seen below in Figure 1: Vulnerability and Threat Inventory Template.

Database Vulnerabilities		
	Vulnerability	**Description**
1		
2		
3		
4		

Database Threats		
	Threats	**Description**
1		
2		
3		
4		

Figure 1: Vulnerability and Threat Inventory Template

Along with the inventory of threats and vulnerabilities is a second outcome of study, which is a list of recommendations the DBA and security manager can implement in an effort to thwart a threat to their corporate database. The security solutions are aligned with the threats and vulnerabilities in a spreadsheet. This allows the DBA to quickly examine a threat or vulnerability within the inventory that is present in their environment and arrive at a potential security solution for the issue. A format for the table is found below in Figure 2: Database Security Solutions Template

Database Vulnerabilities & Security Solutions			
	Vulnerability	Security Solution	Solution Description
1			
2			
3			
4			

Database Threats & Security Solutions			
	Threats	Security Solution	Solution Description
1			
2			
3			
4			

Figure 2: Database Security Solutions Template

Limitations

Databases, as they are used in today's corporate world, did not evolve into the sophistication and size they are now until the early 1990s. And it wasn't until the mid-90s that database security started to become a real concern to organizations as more end users gained access to the centralized corporate database (Corman 1998). Therefore, literature collected for use in this study ranges in publication dates from 1990 to 2007.

The literature for this study is gathered from sources such as online databases from the University of Oregon, the New York Public Library, the Science, Industry, and Business Library (SIBL) branch of the New York Public Library, as well as the World Wide Web (WWW). The types of literature retrieved range from online articles, books and journals to conference discussions. Because focus is on corporate databases, the majority of the resources are selected from articles found in industry publications such as magazines and online articles.

This study does not create a security policy. Instead common vulnerabilities and threats to the corporate database are identified and aligned with suggested recommendations, framing a new perspective on options for consideration by the DBA and Information Security Manager. This list can be used by the DBA and security manager to aid in creation of a threats and vulnerabilities assessment tool (Schultz, 2006), but should not be used in place of a larger security policy. Because each corporation's environment is unique, the threats and vulnerabilities noted in this study should not be viewed as a comprehensive list for all.

Literature review, as defined by Leedy and Ormrod (2005), is selected as the basis for construction of the overall research design. The method allows this researcher to collect and study diverse viewpoints and research conclusions on the larger topic of database security and to synthesize these into an organized whole to present as an outcome (Leedy and Ormrod 2005).

To help narrow the focus of the study, emphasis is placed on large corporate databases. This choice is made because the majority of the data breaches as of late have been against large organizations and therefore much of the available literature is framed within this context. Also, focus is on database security as opposed to a more holistic enterprise security.

There are many potential topics that could be examined related to the larger concept of database security. In this study focus is on 'threats' (Whitman and Mattord 2004) and

'vulnerabilities' (Whitman and Mattord 2004) because these are the most immediate and severe affects to the integrity of the database as well as the most commonly overlooked component (2007). Greenemeier (2006) clearly articulates the issue by stating, "databases are becoming more vulnerable to the outside world as Web-facing apps demand faster access to information and databases move closer to the network perimeter, opening them to network-based attacks." (p. 1)

Problem Area & Significance of Study

The use of database systems is an established, effective and efficient method of managing and storing information for large corporations (Curtain 2007). Curtin (2007) articulates the potential vulnerability of the database when he says:

> While the benefits of using a database system are numerous, people rightly wonder about the potential risk of using such systems to contain sensitive financial information. In the same way that a database can make your job more efficient, it can also make an attacker's job easier – by providing a wealth of sensitive information in one place. (p. 26)

A survey conducted in 2001 found that a majority of businesses did not have a company-wide security policy (Luftman 2004). Perhaps it should not be surprising that five years later, the personal information of more than 55 million individuals was compromised due to database breaches between Feb. 15, 2005 and May 7, 2006, according to the Privacy Rights Clearing house, a nonprofit consumer advocacy group in San Diego (Schultz 2006).

Databases are becoming more vulnerable due to Web-facing applications that demand faster access to information. As databases move closer to the network perimeter, the potential is increased for network based attacks (Greenemeier 2006). The economic impact of an attack on one computer in a large corporation can be devastating. By stealing just one computer, hackers can now retrieve a large cache of potentially sensitive information without going to the effort of breaking into any other system. Because of this, hackers have concentrated their efforts on databases (Curtin 2007). And while the large database vendors have increased the sophistication of their native security features, products still only meet basic security requirements (Schultz 2006).

Database threats have always been viewed from an outside-in mindset (2007). But today, this leaves far too much room for error or malfeasance (2007). Not all threats emerge from the outside. Many overlooked (and sometimes the most damaging) breaches occur within the organization (Scheier 2006).

According to a November 2005 report from Forrester Research "all enterprises should implement database vulnerability assessment, data-at-rest encryption, intrusion detection and in-depth auditing" (Schultz 2006). Security leaders all over corporate America are demanding that corporations implement stricter security policies against their databases. Aaron Newman, the Chief Technology Officer of Applications Security Inc, states that though it is important for organizations to be wary of sensationalism in the media, "it is also important to ensure you are implementing the best security practices to ensure that your databases are kept safe and secure" (Newman 2005, p. 32).

CHAPTER II – REVIEW OF THE LITERATURE

This chapter provides a review of references that were used to conduct this study. The review is organized into three main sections. The first section consists of material used to guide the significance of the study and the purpose. These resources were not used in the data analysis. They are more focused at describing the big picture of database vulnerabilities and threats. The second section consists of resources used to conduct the data analysis of this study. These recourses may have been used to guide the purpose of the study, but were also integral in the data analysis of the study and made up a large portion of the literature review. The final section consists of resources used to describe the methodology used to conduct this study.

Each section is presented in alphabetical order. The entries address how the resource relates to the study and the rationale for selecting it.

Section one: References that guide the purpose

(2007). Data security still at risk. Communications News. Retrieved April 1, 2007 from http://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=24036077&loginpage=login.asp

This article examines the prevalence of security issues in regards to database breaches. The author strengthens the argument by providing real world examples. The piece most useful in this study is the reference to an IBM survey stating that organizations feel they have done a good job implementing security measures, but in reality security measures

are being compromised and breached ever more frequently based on a study from the Privacy Rights Clearinghouse.

This reference supports both the purpose and significance area of this study. The issue of the lack of security against databases and examples speak to the heart of this study. It is chosen as a reliable source due to publication in The Communication News -- a publication that has been around since 1964 and one that is well respected within the Information Technology industry.

Corman, L. (1998). Data integrity and security of the corporate data base: the dilemma of end user computing. The ACM Digital Library. Retrieved March 22, 2007 from http://portal.acm.org/citation.cfm?id=65767&jmp=citings&coll=portal&dl=ACM&CFID=18001597&CFTOKEN=65428580#citings

This paper discusses early issues in database security, at a time when "end user computing" (Corman 1998) became more prevalent in the late 1990s. The paper focuses on data integrity in the database as more users are directly modifying data, as opposed to direct outside security features. However, the paper describes the task of a DBA quite clearly and is still relevant today.

This paper aided in the development of the purpose of the study as well as helping define a DBA. The paper cites many credible authors in the database industry. As well, the author himself and his paper are cited in other material that is chosen for this study.

Fonseca, B., (2004). DBA Boundaries Blurring. eWeek. Retrieved April 11, 2007 from http://web.ebscohost.com/ehost/detail?vid=14&hid=103&sid=ce7ef31a-6690-48da-9e6a-e85908765943%40SRCSM2

This article discusses how the responsibilities of the DBA are ever increasing due to increased security threats. It is in a similar vein to Corman's paper with an updated focus. It discusses how the responsibilities of the DBA have grown to include locking down application access, due to recent legislation and exposure of existing vulnerabilities from viruses. This article explains the current responsibility of the DBA and how the increased tasks have stressed the workload of the individuals.

This article supports the purpose of the study by exposing the increased workload of the DBA and therefore the need for an aid to aspects of their work. It also indirectly helped in defining what a DBA does in a day-to-day environment. The publication, eWeek, which published the article, is highly regarded in the Information Technology field.

Section two: References that provide core material for data analysis.

Britt, P. (2007, February). Tightening Security in 2007. InformationToday. Retrieved March 23, 2007 from http://0-search.ebscohost.com.janus.uoregon.edu:80/login.aspx?direct=true&db=buh&AN=23878734&loginpage=login.asp&site=ehost-live

Britt focuses the majority of his discussion in the article on the problem of database security by providing examples. By examining the current threats and vulnerabilities Britt is able to explore security solutions to selected issues. In providing the security solution, Britt also explains the rationale behind the solution and what security vulnerabilities will be rectified by the solution. A solution discussion is exemplified when Britt says

"Encrypting data "at rest" also helps prevent data breaches in the event of lost or stolen media, such as tapes, laptops, floppies, etc." (p. 2).

This article served as a major inspiration for the purpose and significance sections of this study. By providing solutions and context for those solutions it was easy to tie the purpose through to the significance and the data analysis. The author, Phillip Britt, is president and CEO of S&P Enterprises. He is also a business writer who often covers key topics in the information industry field.

Curtain, M. (2007, February 26). Database Security: Solve the right problem now, for fewer headaches tomorrow. Accounting Today. Retrieved March 23, 2007 from http://0-web.ebscohost.com.janus.uoregon.edu/ehost/results?vid=2&hid=6&sid=3fa2b3cc-7f02-4b8a-98db-7fa6ae0a52ea%40sessionmgr7

This article discusses the increased necessity to lock down corporate databases due to the fact that systems today are now "globally interconnected" (Curtain, 2007, p. 26). Curtain briefly touches on understanding how a compromise of a database takes place. This content helps form part of the purpose of the study. He then proceeds to profile three common mistakes in security and how the database is involved. Upon profiling the three common mistakes he also provides potential solutions.

This resource provides input for the purpose of the study by touching on how a breach of the database takes place. However, its true significance in this study is as one item in the data set for coding in the data analysis phase by adding potential solutions to the vulnerabilities.

Matthew Curtain is the founder of Interhack Corp, which is a professional services firm with practices in information assurance and forensic computing. He is also the author of Brute Force: Cracking the Data Encryption Standard.

Newman, A. (2005). Database Security Best Practices. Security. Retrieved April 1, 2007 from Business Source Premier database.

This article is a key source in the data set for coding, for the data analysis section of the study. Like other articles Newman supports his text by giving recent data breach examples, but then goes into further detail than the other articles on understanding the vulnerabilities and threats. After detailing the vulnerabilities and threats Newman explains several possible solutions to these threats and vulnerabilities. He provides a detailed description of each solution given in his article.

The article is used both in the purpose and data analysis sections of this study. It helps build the case for the study by providing insight on how to understand vulnerabilities. At the same time Newman provides valuable data for analysis in the practices listed in the article.

Aaron Newman is the co-founder and Chief Technology Officer of Application Security Inc. He is also the co-author of the Oracle Security Handbook. He is cited in several publications used in this study.

Scheier, R. (2006, August 28). Protecting the corporate database. Computerworld. Retrieved March 23, 2007 from http://0-web.ebscohost.com.janus.uoregon.edu/ehost/results?vid=5&hid=6&sid=3fa2b3cc-7f02-4b8a-98db-7fa6ae0a52ea%40sessionmgr7

This article focuses on identifying the internal threat to corporate databases as opposed to external threats. It touches on external threats as well, but it is the internal threat that is the main focus. Upon identifying the internal threat, Scheier provides four key security solutions to the threats that will make the corporate database much safer. The four key defenses are a major source of data for the analysis of the study. Scheier discusses database protection vendors, which is not pertinent to this study, but comes back to the underlying four defenses.

This article provides support for the purpose of this study by examining threats and where they originate. Scheier then discusses four key defenses which provide data for the analysis phase as potential solutions to the existing threats. Robert Scheier's article "Protecting the corporate database" is published in several industry standard publications.

Whitman, M., Mattord, H. (2004). *Management of Information Security.* Canada. Course Technology.

This book provides definitions for a large number of the key terms for this study. At the same time the text provides information identifying who the audience is for security issues regarding the information infrastructure. The text also discusses in depth about threat identification and risk management.

The information from this source supports the entire study by defining the key terms. Also, the text provides data to aid in identifying the audience of the study as well as data for analysis of vulnerabilities and threats. The book is used as a course text in the Information Security course for the AIM Program.

Vijayan, J. (2007). Six Ways To Stop Data Leaks. Computerworld. Retrieved April 1, 2007 from Business Source Premier database.

Vijayan jumps right into discussing six potential solutions to shutting down data leaks. The source is included as part of the data set for coding for data analysis, and these suggestions are a great source of data for the analysis phase of the study. Upon introducing the solutions, Vijayan provides an explanation to the threat or vulnerability the solution is resolving and then a description of the resolution itself. Like other articles he uses a real world example of a data breach for his basis.

The data within the article provides a plethora of information for the data analysis section of the study. The six solutions are a key source of information for the final outcome of the data analysis. Jaikumar Vijayan has been published several times in the Computerworld publication. Computerworld is a well known publication in the information technology industry.

Section three: References pertaining to literature reviews and the methodology of content analysis

Leedy, P., Ormond, J. (2005). *Practical Research: Planning and Design* (8th ed.). Upper Saddle River, NJ. Pearson Education, Inc.

This text provides a description of both qualitative and quantitative research methodologies. The section regarding the qualitative method provides support for determining the approach chosen for this study. This text is used as the primary reference for the Research Methods course in the AIM Program.

Palmquist, M., Busch, C., De Maret, P., Flynn, T., Kellum, R., Le, S., Meyers, B., Saunders, M., White, R. (2005). Content Analysis. Retrieved April 1, 2007 from Colorado Statue University Department of English Web site: http://writing.colostate.edu/guides/research/content/.

This reference is used to help guide the method of this study. The site is the primary resource used to help design and perform the content analysis plan used in this study. It provides a straight forward process to follow with examples and links for additional resources. The AIM Program recommends this resource for a research procedure for conceptual analysis.

CHAPTER III – METHOD

The research methodology selected for this study is a literature review (Leedy and Ormrod 2005). Database breaches in large corporations regularly dominate the news headlines (Britt 2007). Due to the numerous articles written about these breaches, there is ample material from which to collect literature for this study. Literature review (Leedy and Ormrod 2005) is selected as the overall method of study due to the fact that it supports the collection of written materials that examine the larger topic of security threats and vulnerabilities within large corporate databases.

This study uses content analysis and more specifically conceptual analysis (Palmquist, Busch et al. 2005) for the data analysis strategy. This strategy focuses on identifying the existence of selected terms and concepts within a particular text-based resources (Palmquist, Busch et al. 2005). This fits into the larger method of literature review because it provides a process for identification of threats and vulnerabilities to large corporate databases as these are reported in the literature selected to form the data set for coding.

Literature Collection

Literature collection in this study is focused on materials that address the security of large corporate databases. This begins by identifying several key terms and searching library and online databases, library indexes and also the World Wide Web (WWW). After

several initial pieces of literature are identified and reviewed the key terms are modified as needed and the process is then repeated.

The following key terms are used to direct searching:

1. Security > Enterprise Security > Database Security > Tightening Security > Security Threats
2. Database > Corporate Database
3. Encryption > Cryptology > Personally Identifiable Information (PII)
4. Database Management > Database Vulnerability

The following criteria are used to collect literature related to the key terms in this study.

1. The literature is printed between the dates of 1990 and 2007.
2. The literature contains aspects that are pertinent to database threats and vulnerabilities in a large corporate database.
3. The literature is from a trusted source. A trusted source is one that is from a professional publication, the author is known in the field, and/or the work is cited in other publications.
4. The literature is available online in full-text or in hard-copy print.

Searches to locate the research material are conducted in a number of ways. Online databases from the University of Oregon and the New York Public Library are a great asset. Some of the online databases being utilized are ACM Digital Library, Academic Index, Academic Search Premier, Business Company Resource Center, Business Source

Premier, Computer Source, and Google Scholar. Physical Library searches take place in the Science, Industry & Business Library (SIBL) branch of the New York Public Library. Finally, searches are conducted against the World Wide Web (WWW) on websites such as Google, Information Week, SANS Institute, CIO, and eWeek. Several key samples of literature identified by these searches are;

1. Database and Applications Security by Bhavani Thuraisingham (2005)
2. DBA Boundaries Blurring by Brian Fonseca (2004)
3. Tightening Security in 2007 by Phillip Britt; and
4. Protecting the Corporate Database by Robert Scheier (2006).

Data Analysis

Ten pieces of literature are selected for use as the 'data set' for the content analysis. Key pieces of literature that make up the data set are;

1. Britt, P. (2007, February). Tightening Security in 2007.
2. Corman, L. (1998). Data integrity and security of the corporate data base: the dilemma of end user computing.
3. Curtain, M. (2007). Database Security: Solve the right problem now, for fewer headaches tomorrow.
4. Davidson, M.A. (1995). Security in an Oracle data base environment.
5. Newman, A. (2005). Database Security Best Practices.
6. Scheier, R. (2006). Protecting the corporate database.
7. Schultz, B. (2006). The hacker-resistant database.
8. Thuraisingham, B. (2005). Database and Applications Security: Integrating Information Security and Data Management.
9. Vijayan, J. (2007). Six Ways to Stop Data Leaks.

10. Whitman, M. and Mattord, H. (2004). Management of Information Security.

Conceptual analysis (Palmquist, Busch et al. 2005) is chosen as the guide to analysis of the research material for this study. The following eight steps, as outlined in the Colorado State University Writing Guide, are used to conduct the conceptual Analysis (Palmquist, Busch et al. 2005).

1. Decide the level of analysis

This study codes for sets of words and phrases such as database security, database vulnerabilities, and corporate databases. However, single words such as threats and vulnerabilities are coded as well.

2. Decide how many concepts to code for

By creating a pre-defined set of concepts to code for, the focus of the study is narrowed. A list of three pre-defined concepts is;

A. Database Security, defined in this study as Handling complex security policies, granting access to data based on roles and functions, and also both positive and negative authorization policies (Thuraisingham, 2005).
B. Database Vulnerability, defined in this study as a weakness or fault in a system or protection mechanism that exposes information to attack or damage (Whitman and Mattord 2004).
C. Corporate Databases, defined in this study as databases of large corporations when more than 1000 devices require security management (Whitman and Mattord 2004).

The study, however, is open to the discovery of related and new concepts as these might emerge during the coding process, for coding flexibility. A related concept might address vulnerability management, for example.

3. Decide whether to code for existence or frequency of a concept

This study focuses on the existence of the concept when coding to indicate the broadest range of topics that are reported within the selected literature.

4. Decide on how you will distinguish among concepts

Concepts are broken down into three subgroups, including threats, vulnerabilities and security. While the majority of the concepts are explicitly coded, several terms, due to the differences in technical wording need to be implicitly coded. Examples of this are 'discretionary security' (Thuraisingham 2005) and 'security' (Newman 2005) in regards to the database. Both concepts imply handling security policies and granting access to the database. Two other examples are 'compromised' (Curtin 2007) and 'breached' (Newman 2005), both of which both refer to an unauthorized penetration of a database.

5. Develop rules for coding texts

The following rules are set in place to insure the consistency of the concepts throughout the data analysis process:

A. If the term is explicitly analyzed it is listed in the pre-defined table.

B. Each occurrence of the implicit phrase is evaluated against similar pre-analyzed terms and against the pre-defined set of concepts.

6. Decide what to do with "irrelevant" information

Irrelevant information is defined as information not pertaining to this study or contributing to the focus of the terms and concepts. Irrelevant information is therefore discarded since it is of no use to this study.

7. Code the texts

Coding the concepts is done manually by examining the text and relevant context for the existence of the pre-defined or emergent terms and concepts. Upon identification the terms are placed into the appropriate list held in a spreadsheet for each of the three subgroups. A sample of the recording format is found below in Figure 3:

Database Threats and Vulnerabilities and potential Security Solutions			
	Threats	Vulnerabilities	Security Solutions
1			
2			
3			
4			
5			
6			

Figure 3: Coding Spreadsheet Template

8. Analyze Your Results

After the coding is complete the data are reviewed and formulated into two tables which present 1) a listing of the threats (see Appendix C – Database Threats) and 2) a listing of vulnerabilities (see Appendix C – Database Vulnerabilities). Each list is designed to be used as a stand-alone aid by the database administrator (Whitman and Mattord 2004). Based on these results, an inventory is generated into a table format to create the final outcome (see Appendix D – Security Solutions Inventory). The final outcome of the study is described in the Data Presentation section of this chapter.

Data Presentation

The inventory generated from the results of the conceptual analysis process is a compiled listing of the vulnerabilities and threats, presented in two tables. Each table includes a brief description of the threat and vulnerability. Along with the two tables of threats and vulnerabilities are another two tables aligning a security solution with each threat and vulnerability. Templates for all of these tables are shown below in Figure 4.

Database Vulnerabilities & Potential Security Solutions			
	Vulnerability	**Security Solution**	**Solution Description**
1			
2			
3			
4			

Database Threats & Potential Security Solutions			
	Threats	**Security Solution**	**Solution Description**
1			
2			
3			
4			

Figure 4: Security Solutions Inventory Template

The outcome is designed to serve several purposes for the DBA or security manager. One task the DBA performs is to create a database environment from scratch upon the development of a new application. After the database is created in the new environment the security manager and DBA typically conduct a vulnerability assessment to insure the security of the new database. The security manager and DBA could use the inventory of threats and vulnerabilities along with the descriptions to assess the database. By reviewing the description of the threats and vulnerabilities, the DBA should be able to accurately confirm if all of the potential threats and vulnerabilities listed in the inventory have been addressed.

Another scenario where the inventory, created from the results of the data analysis, might be utilized happens when a threat or vulnerability is identified in an existing database environment. A DBA often gets a request to extract data from a database and occasionally the information being requested is personally identifiable information (PII). A vulnerability occurs if the PII being extracted is in plaintext format. Upon the identification of the vulnerability the DBA could examine the inventory for this particular vulnerability to discover a potential security solution to be put in place. It should be noted that if the DBA implements the security solution, thereby eliminating the vulnerability. In this case, the data needs to be encrypted in order to prevent plaintext extraction.

CHAPTER IV – DATA ANALYSIS

This chapter details the results of the content analysis of ten pieces of literature. The references comprising the data set for coding are collected through the search process detailed in Chapter 3: Method. The ten references are listed below in alphabetical order:

1. Britt, P. (2007, February). Tightening Security in 2007.
2. Corman, L. (1998). Data integrity and security of the corporate data base: the dilemma of end user computing.
3. Curtain, M. (2007). Database Security: Solve the right problem now, for fewer headaches tomorrow.
4. Davidson, M.A. (1995). Security in an Oracle data base environment.
5. Newman, A. (2005). Database Security Best Practices.
6. Scheier, R. (2006). Protecting the corporate database.
7. Schultz, B. (2006). The hacker-resistant database.
8. Thuraisingham, B. (2005). Database and Applications Security: Integrating Information Security and Data Management.
9. Vijayan, J. (2007). Six Ways to Stop Data Leaks.
10. Whitman, M. and Mattord, H. (2004). Management of Information Security.

Each of the references is analyzed using the three pre-defined set of concepts described in the Data Analysis section of Chapter 3: Method. These concepts are 1) Database Security, 2) Database Vulnerability, and 3) Corporate Databases. The references are coded using key terms that are derived from a set of definitions, one per concept. The coding process is designed to be flexible, in order to allow for the discovery of related and new concepts as they might emerge.

Raw Results

Appendix B – Report of Raw Coding Results presents the raw results of the coding process, and details four categories of information: Source, Threats, Vulnerabilites, and Security Solutions. Once the coding is complete the terms and concepts are transferred to this coding. Special care is taken to maintain the true meaning of the phrase or concept as it was transferred to the spreadsheet. Concepts are recorded in the spreadsheet in the order they emerged from the text.

The manual coding is done by highlighting predefined terms within the text. The pre-defined terms are only coded when they reference database security. For example references describing security policies for portable electronic devices (Whitman and Mattord 2004) are not coded. However, a reference describing unauthorized access to a corporate database (Corman 1998) is coded.

As the coding process progresses concepts are translated to include variations of the original concepts. Terms such as “database breach” are identified to equal the term “compromised database”. It is found that many of these terms and concepts are used interchangeably throughout the references. Along with the concept translations comes identification of emergent concepts within each reference. These are coded along with the pre-defined concepts and actually comprise the majority of the total coded concepts. An example of an emergent concept can be seen in Britt’s discussion on password management when he says “One common way to secure data and limit access is to require a password” (Britt 2007, p. 2). This concept is emergent because it is not pre-

defined, however, it directly relates to database security by controlling unauthorized access to the system. As the emergent concepts and the pre-defined concepts are discovered they fall into larger "umbrella" concepts. For example, "database breach", "compromised database" and the emergent concept of passwords discussed by Britt (2007) all fall under the "umbrella" concept of "Access Control". Nine umbrella concepts are discovered with a total of 117 concepts (21 – Threats, 26 – Vulnerabilities, & 70 Security Solutions) coded in all.

Final Inventories

The raw results of the coding are then reframed to create a set of two inventory tables, presented in Appendix C and D, which are designed to highlight the key concepts that emerged from the analysis. Key concepts are defined as those that identified in more than two sources. An exception is made if the concept identified is considered to be critical to the nature of database security. For example, the "brute force" attack against the database as described by Curtin (2007) is a highly critical and plausible threat to any corporate database. This type of threat needs to have an immediate security solution implemented. Appendix C – Threat and Vulnerability Inventory presents a final formulation of six database vulnerabilities and five database threats. Each of these is then aligned with an identified solution, presented in Appendix D. A discussion of the content in these inventories is presented in the Conclusion chapter of this paper.

The reframing process proceeds as described here. As the raw data is reviewed at this stage, common themes emerge among all of the references in the data set. For example

“data-at-rest” is a common concept found throughout the references. This concept is usually followed by the security solution of encryption. The inventories began to take form through identification of these common themes. By consolidating the concepts into one common phrase they are moved into one of the inventories based on which pre-defined concept they fall under (i.e. threat, vulnerability, or security solution). Once identified and transferred to the inventory a description of the phrase is taken from a single source that best represents the common theme. The threats and vulnerabilities are then moved to a second set of inventories that align them with a security solution. Again, the solution is consolidated among the common themes found throughout the references, and a single description is identified among the references that best represent the security solution.

CHAPTER V – CONCLUSION

The purpose of this study is to identify common threats and vulnerabilities to large corporate databases. The goal upon identifying the common threats and vulnerabilities is to recommend basic security solutions to address the threats and vulnerabilities. By understanding the weaknesses and threats facing corporate databases a DBA can begin to create a security plan in order to protect the database.

Ten references are used as the data-set for this study. They were all published between 1995 and 2007. The literature that makes up the data-set for this study is gathered from various places such as online databases from the University of Oregon, physical libraries such as the Science, Industry, and Business Library (SIBL) branch of the New York Public Library, and the World Wide Web (WWW). The types of literature range from online articles, books and journals, and conference discussions. The study is conducted as a literature review (Leedy and Ormrod 2005) and utilizes conceptual analysis for its coding strategy (Palmquist, Busch et al. 2005).

There are three outcomes of this study: (1) a database vulnerability inventory of six common vulnerabilities, as seen in Appendix C – Threat and Vulnerability Inventory, (2) a database threat inventory of five common threats, as seen in Appendix C – Threat and Vulnerability Inventory, and (3) a set of two potential security solutions inventories to these eleven common threats and vulnerabilities, as seen in Appendix D – Security Solutions Inventories.

The five common threats identified in this study are: 1) Unauthorized access by insiders, 2) “Brute Force” attacks, 3) Incorrect Usage, 4) Stolen laptops, and 5) personal hardware collection. All of the threats can be combined under one form or another of an attack. These acts are all deliberate acts against a corporate database in order to compromise the data that resides within the database. For example, insiders to a company may try to access certain information using their legitimate access rights in the database that would be quite valuable to a rival corporation. Another example would be the “brute force” attack where an attacker from the outside, using sophisticated equipment, would attempt to break into a database using a password sniffer, which “sniffs” or looks for unencrypted passwords on the network that will allow the attacker access to the corporate database. Once inside the database the attacker could download sensitive information to sell to a rival organization.

The six common vulnerabilities identified in this study are: 1) data-at-rest, 2) sensitive data, 3) poor application architecture, 4) password vulnerability, 5) unlocked database, and 6) vendor bugs. Unlike threats, which represent various potential attacks against a database, vulnerabilities identify areas of the database, which if exposed, could pose a risk to the security of a corporation’s data assets. For example most data when transmitted from one location to another is encrypted along the network by means of a virtual private network (VPN) or secure socket layer (SSL) connection. However, data-at-rest is not encrypted and therefore could be stolen and compromised while not in a transmitted state. And if the data was of a sensitive nature the corporation is now at risk of losing confidentiality of its data assets. Poor architecture is a vulnerability that could

allow access to sensitive, at-rest data, by making the entry point through an application that has poor security controls.

Eleven different security solutions are identified in this study – one aligned to each identified vulnerability or threat. Solutions to the six identified common vulnerabilities include a range of responses, from incorporation of ever improved encryption strategies to constantly updating patches. All of the potential solutions are intended with securing certain aspects of the database. The solutions are also complimentary to each other and when combined can make a database practically impenetrable to outside risks. For instance, the firewall will be a first line of defense which will keep most unauthorized access at bay. A complex password policy will prevent most attackers from falsely obtaining passwords if they were able to make it past a firewall. And finally, data encryption will make sensitive data useless to anyone other than the individuals who own the encryption key.

Solutions to the five common threats include a range of responses, from strict access policies to auditing and monitoring access to the database. Unlike security solutions to vulnerabilities, which are designed to close up the vulnerable aspects of the database, solutions for threats are more designed as guardians of the database and what it contains. For instance by constantly auditing and monitoring access to the database a database administrator can view when a user may violate their access control spelled out in the access policy. By actively monitoring the database the database administrator can then take swift action to lock down the database and deny access to the user violating the

policy. At the same time, by encrypting the sensitive data, any information leaked during the breach in security will be secure without access to the encryption key.

By using the inventories a DBA or Security Manager will have the tools they need to help perform a vulnerability assessment or tackle an existing security breach. The inventories are designed to be easy to read problems and their descriptions are aligned with a solution and an explanation of the solution. These inventories represent a compilation of common threats and vulnerabilities experienced by large corporations throughout the country. Security solutions are those recommended by experts in the fields in response to the ongoing threat of attacks by hackers outside of the organization and from users within the enterprise. Several of the security solutions can be used to help solve more than one threat or vulnerability. For example, encryption can be used to secure sensitive data, data-at-rest, and data compromised inside a stolen laptop. Another example of a vulnerability assessment is a good security measure to prevent poor application architecture or incorrect usage of an application due to poor application architecture. These inventories should be an essential piece in the security arsenal of the DBA and Security Manager – at least for the short term.

The state of database security affairs is likely to get worse before it gets better (Vizard 2007), therefore the need for a set of tools like the inventories produced from this study becomes ever more critical. The good news is that companies are getting better and more adept at fighting attacks from viruses, worms and other forms of data breaches; the bad news is the bad guys are becoming more sophisticated (Vizard 2007). In the past security

was looked at in the outside-in mindset, however today's reality leaves to much room for error or malfeasance with that mindset (2007). There needs to be an inside-out security mindset starting with the database (2007).

As databases continue to grow and become more accessible, so do the responsibilities of the DBA to keep the databases available to all applications but at the same time maintain the security of the database to attacks and breaches (Fonseca 2004). While many organizations have given more control and authority to the DBAs to enact security controls due to new federal legislation such as the US Patriot Act and Sarbanes-Oxley, the criticality of the database's security has also increased (Fonseca 2004). Though the inventories derived from this study are not presented as a complete security solution they are intended to help relieve some of the burden of the DBA during a vulnerability assessment or threat control. Newman (2005) states it well when he says "In order to understand vulnerabilities, it is important to be aware of the different kinds" (p. 32).

APPENDICIES

Appendix A - Definitions

Architecture: Design of how an application works (Newman 2005).

Database: A set of dictionary tables and user tables that are treated as a unit. One or more operating system files in which the database software stores tables, views and other objects (Loney 2004).

Database Administrator (DBA): someone who is responsible to define the various schemas ad mappings of the database as well as auditing the database and implementing the appropriate backup & recovery procedures (Thuraisingham 2005) and ensuring the security and data integrity of the database (Corman 1998).

Database Security: Handling complex security policies, granting access to data based on roles and functions, and also both positive and negative authorization policies (Thuraisingham 2005).

Electronic Commerce (EC): the conduct of an organization's activities with increasingly heavy reliance on contemporary computing and telecommunications technologies across its entire value chain (Dutta and McCrohan 2002).

Inventory: identified information and listing about vulnerabilities, threats and security solutions to an environment (Whitman and Mattord 2004).

Large Corporation: more than 1000 devices requiring security management. (Whitman and Mattord 2004).

Medium Corporation: between 100 and 1000 devices requiring security management. (Whitman and Mattord 2004).

Security: To be protected from the threat of loss; protection from that which would do harm, intentionally or otherwise. (Whitman and Mattord 2004).

Security Policy: set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information (Davidson 1995).

Sensitive: Important information that could embarrass the organization or cause loss of market share if compromised (Whitman and Mattord 2004)

Small Corporation: less than 100 devices requiring security management. (Whitman and Mattord 2004).

Security Solution: A series of steps, practices, and/or implementations designed to mitigate the risks of threats and vulnerabilities (Vijayan 2007).

Threat: An object, person or other entity that represents a risk of loss to an asset. (Whitman and Mattord 2004)

Vulnerability: A weakness or fault in a system or protection mechanism that exposes information to attack or damage. (Whitman and Mattord 2004).

Vulnerability Assessment: The process of identifying and documenting specific and provable flaws in the organization's information asset environment (Whitman and Mattord 2004).

Appendix B – Report of Raw Coding Results

Database Threats and Vulnerabilities and potential Security Solutions				
	Source	**Threats**	**Vulnerabilities**	**Security Solutions**
1	Britt (2007)	Access Control • data compromised • unauthorized access • people attempt to hack into database.	Access Control • compromised database • liability risk if data is compromised.	Access Control • monitor access • "One common way to secure data and limit access is to require a password." • passwords be at least 12 characters long. • firewalls & access control systems • layered security Poor Architecture • patches Data Sensitivity • Encryption • mask personal information • shredders Vulnerability Assessment • third party firms to review security procedures
2	Corman (1998)	Lack of Control • "Security features of a data base are severely threatened as more end users access the centralized corporate database." Data flow control • end users downloading information straight to their microcomputer	Data Sensitivity • data integrity to corporate database. Poor Architecture • faulty modeling design • errors in data retrieval and analysis • lack of documentation	Access Control • keep end users "in the dark" • segregation of duties • limit authorized personnel • password tiering • offsite backup facility Data Sensitivity • encryption techniques • database recovery procedures Monitoring • security logging

Database Threats and Vulnerabilities and potential Security Solutions				
	Source	**Threats**	**Vulnerabilities**	**Security Solutions**
		.		
3	Curtin (2007)	Attacks • attackers can do serious damage to corporate database • "brute force" attacks against authentication mechanisms	Access Control • compromised system • interconnected systems Data Sensitivity • loss of control over data on laptops • back-up media that has been lost, typically in transit. Poor Architecture • poorly designed application code living on top of the database.	Access Control • session authentication is an important control. • database behind a firewall • granular access to the data from the application. Data Sensitivity • encryption of "data-at-rest"
4	Davidson (1995)	Access Control • users can access and manipulate data. Outside Control • network snooping	Data Sensitivity • organizations are placing valuable corporate information and sensitive data in their computer systems. • information sensitivity • sensitive corporate data. Poor Architecture • data modification or replay of transactions Access Control	Vulnerability Assessment • managing corporate information • assessment of the vulnerabilities of the data • security policy Access Control • locking computers • discretionary access control is an important security mechanism in controlling initial access to information. • mandatory access control addresses the limitations of discretionary access control by controlling access to data based on its sensitivity.

Database Threats and Vulnerabilities and potential Security Solutions				
	Source	**Threats**	**Vulnerabilities**	**Security Solutions**
			• widespread accessibility to open computer systems • establishing user identification across a network • passwords are vulnerable to compromise	• Oracle password protocol • configure roles for user access <u>Monitoring</u> • "critical aspect of any security policy is maintaining a record of system activity" • limit the readability of the database files in the operating system <u>Data Sensitivity</u> • full data base encryption • partial data base encryption • network encryption
5	Newman (2005)	<u>Attacks and Poor Architecture</u> • SQL Injection where a hacker injects code into the application to retrieve information from the database.	<u>Poor Architecture</u> • vendor bugs • not properly locking down the database	<u>Vulnerability Assessment</u> • establish a baseline of current security procedures • conduct regular audits to ensure security policies are in check and being followed. • utilize security auditing tools <u>Monitoring</u> • monitor progress to ensure baseline compliance <u>Poor Architecture</u> • keep database patched <u>Data Sensitivity</u> • encryption <u>Access Control</u> • maintain perimeter security by using a firewall

Database Threats and Vulnerabilities and potential Security Solutions				
	Source	**Threats**	**Vulnerabilities**	**Security Solutions**
				• insulate the database from threat sources like default passwords • implement a real-time intrusion detection application
6	Scheier (2006)	Access Control • disgruntled employees using legitimate access rights to prowl for data Data Sensitivity • forgetful users whose data-rich notebooks are stolen Access Control • dishonest employees who sell information to the highest bidder	Data Sensitivity • data-at-rest	Data Sensitivity • encryption Access Control • separation of duties • access control and authentication products Vulnerability Assessment • vulnerability scanners Monitoring • database access monitoring tools
7	Schultz (2006)	Access Control • data breaches		Vulnerability Assessment • basic security requirements • database vulnerability assessment Data Sensitivity • data-at-rest encryption Monitoring • intrusion detection • in-depth auditing
8	Thuraisingham (2005)	Access Control • unauthorized access	Access Control • poor password management.	Access Control • access Control Policies • authorization policies • role-based access control

Database Threats and Vulnerabilities and potential Security Solutions				
	Source	**Threats**	**Vulnerabilities**	**Security Solutions**
				• Identification and authentication Monitoring • auditing the database system Poor Architecture • SQL Extensions for security • query modification
9	Vijayan (2007)	Data Flow Control • risks can be challenging, especially in large corporations • users walking away with information downloaded onto personal hardware (i.e. laptop, usb memory)	Data Sensitivity • not knowing where sensitive and proprietary information resides in the database Data Flow Control • what data is flowing over the network from the database.	Data Sensitivity • get an understanding where sensitive data lives • encrypt sensitive data • categorize data and choose the most appropriate set of controls for each data class. Monitoring • monitor content in motion. Access Control • know who is accessing the database • limit user privilege • create access policies
10	Whitman & Mattord (2004)	Attacks • deliberate attacks Data Sensitivity • acts of human error or failure • laptop stolen Access Control • unauthorized access by insiders	Attacks • database vulnerable to a denial of service attack • employees or contractors may cause a failure in system	Vulnerability Assessment • vulnerability assessment • threat identification

Appendix C – Threat and Vulnerability Inventories

Database Vulnerabilities		
	Vulnerability	**Description**
1	Data-at-rest	Information that is stored, even temporarily, as opposed to data in transit over a network (Scheier 2006).
2	Sensitive data	Data that is important to the organization and is widely distributed throughout the database (Whitman and Mattord 2004).
3	Poor application architecture	Not properly factoring security into the design of how an application works (Newman 2005).
4	Password vulnerability	Hackers breaking into user ids by compromising passwords and masquerading as the victim user (Thuraisingham 2005)
5	Unlocked Database	Database completely wide open for users to access without any auditing or controls (Davidson 1995).
6	Vendor Bugs	Buffer overflows and other programming errors that result in users executing the commands that are typically not allowed to run (Newman 2005).

Database Threats		
	Threats	**Description**
1	Unauthorized access by insiders	Threats may come from disgruntled employees using legitimate access rights to prowl for data or dishonest employees who sell information to the highest bidder (Scheier 2006).
2	“Brute Force” attacks	Attackers write a program that tries every word in the dictionary as a password, along with every common username (Curtin 2007).
3	Incorrect usage	Building an application utilizing developer tools in ways that can be used to break into a database (Newman 2005).
4	Stolen laptops	Forgetful users whose data-rich laptops are stolen or misplaced (Scheier 2006)
5	Personal hardware collection	Users downloading information from the database to their personal hardware (i.e. laptop, PDA, USB memory stick, etc…) (Vijayan 2007).

Appendix D – Security Solutions Inventories

Database Vulnerabilities & Potential Security Solutions			
	Vulnerability	**Security Solution**	**Solution Description**
1	Data-at-rest	Encryption	The process of combining data ("plaintext" or "cleartext") with a small set of secret data ("key") with an algorithm to produce ciphertext. This way data written to a disk, tape or other medium can be stored without fear of it being compromised (Curtin 2007).
2	Sensitive data	• Encryption • Auditing	• The process of combining data ("plaintext" or "cleartext") with a small set of secret data ("key") with an algorithm to produce ciphertext (Curtin 2007). • Monitoring user access to mission-critical data and detecting unauthorized access to high-risk data (Vijayan 2007).
3	Poor application architecture	Vulnerability Assessments	Monitoring and recording what is happening within the database and alert any suspicious or abnormal activity (Newman 2005).
4	Password vulnerability	Password Policy	Passwords be at least 12 characters in length and include uppercase and lowercase letters as well as numbers (Britt 2007).
5	Unlocked database	Firewall	Will remotely control access and allow only known and authorized machines to connect to the database (Curtin 2007).

Database Vulnerabilities & Potential Security Solutions			
	Vulnerability	**Security Solution**	**Solution Description**
6	Vendor bugs	Patches	Staying up-to-date with all vendor patches and monitoring any known vulnerabilities that could affect security efforts (Newman 2005).

Database Threats & Potential Security Solutions			
	Threats	**Security Solution**	**Solution Description**
1	Unauthorized access by insiders	Access Policies	Policies that limit users' database privileges strictly to what is required for their job and set controls for enforcing those policies (Vijayan 2007).
2	"Brute Force" attacks	Firewall	Will remotely control access and allow only known and authorized machines to connect to the database (Curtin 2007).
3	Incorrect usage	Vulnerability Assessment	Monitoring and recording what is happening within the database and alert any suspicious or abnormal activity (Newman 2005).
4	Stolen laptops	Encryption	The process of combining data ("plaintext" or "cleartext") with a small set of secret data ("key") with an algorithm to produce ciphertext (Curtin 2007).
5	Personal hardware collection	Auditing & Monitoring	Monitoring user access to mission-critical data and detecting unauthorized access to high-risk data (Vijayan 2007).

REFERENCES

(2007). Data security still at risk. Communications News. Retrieved April 1, 2007 from http://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=24036077&loginpage=login.asp

Andresen, E. (2002, March 8). Conducting a security audit of an Oracle database. Retrieved March 21, 2007 from http://www.sans.org/reading_room/whitepapers/auditing/19.php

Britt, P. (2007, February). Tightening Security in 2007. InformationToday. Retrieved March 23, 2007 from http://0-search.ebscohost.com.janus.uoregon.edu:80/login.aspx?direct=true&db=buh&AN=23878734&loginpage=login.asp&site=ehost-live

Corman, L. (1998). Data integrity and security of the corporate data base: the dilemma of end user computing. The ACM Digital Library. Retrieved March 22, 2007 from http://portal.acm.org/citation.cfm?id=65767&jmp=citings&coll=portal&dl=ACM&CFID=18001597&CFTOKEN=65428580#citings

Curtain, M. (2007, February 26). Database Security: Solve the right problem now, for fewer headaches tomorrow. Accounting Today. Retrieved March 23, 2007 from http://0-web.ebscohost.com.janus.uoregon.edu/ehost/results?vid=2&hid=6&sid=3fa2b3cc-7f02-4b8a-98db-7fa6ae0a52ea%40sessionmgr7

Davidson, M.A. (1995). Security in an Oracle data base environment. Information Systems Security. Retrieved April 1, 2007 from Business Source Premier database.

Dutta, A. and McCrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. California Management Review. Retrieved April 1, 2007 from Business Source Premier database.

Fonseca, B., (2004) DBA Boundaries Blurring. eWeek. Retrieved April 11, 2007 from http://web.ebscohost.com/ehost/detail?vid=14&hid=103&sid=ce7ef31a-6690-48da-9e6a-e85908765943%40SRCSM2

Krippendorff, K. (2004). *Content Analysis: An Introduction to Its Methodology* (2nd ed.). Thousand Oaks, CA. Sage Publications.

Leedy, P., Ormond, J. (2005). *Practical Research: Planning and Design* (8th ed.). Upper Saddle River, NJ. Pearson Education, Inc.

Loney, K. (2004). *Oracle Database 10g: The Complete Reference*. Emeryville, CA. McGraw-Hill/Osborne.

Luftman, J., (2004). *Managing the Information Technology Resource: Leadership in the Information Age.* Upper Saddle River, NJ. Pearson Education, Inc.

Newman, A. (2005). Database Security Best Practices. Security. Retrieved April 1, 2007 from Business Source Premier database.

Palmquist, M., Busch, C., De Maret, P., Flynn, T., Kellum, R., Le, S., Meyers, B., Saunders, M., White, R. (2005). Content Analysis. Retrieved April 1, 2007 from Colorado Statue University Department of English Web site: http://writing.colostate.edu/guides/research/content/.

Protect Your Computer. (2007). Microsoft. Retrieved April 20, 2007, from http://www.microsoft.com/athome/security/computer/default.mspx

Scheier, R. (2006, August 28). Protecting the corporate database. Computerworld. Retrieved March 23, 2007 from http://0-web.ebscohost.com.janus.uoregon.edu/ehost/results?vid=5&hid=6&sid=3fa2b3cc-7f02-4b8a-98db-7fa6ae0a52ea%40sessionmgr7

Schultz, B. (2006, May 22). The hacker-resistant database. Network World. Retrieved March 22, 2007 from http://0-web.ebscohost.com.janus.uoregon.edu/ehost/results?vid=3&hid=6&sid=3fa2b3cc-7f02-4b8a-98db-7fa6ae0a52ea%40sessionmgr7

Thuraisingham, B. (2005). *Database and Applications Security: Integrating Information Security and Data Management.* Boca Raton, FL: Auerbach Publications.

Vijayan, J. (2007). Six Ways To Stop Data Leaks. Computerworld. Retrieved April 1, 2007 from Business Source Premier database.

Whitman, M., Mattord, H. (2004). *Management of Information Security.* Canada. Course Technology.

BIBLIOGRAPHY

(2007). Data security still at risk. Communications News. Retrieved April 1, 2007 from http://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=24036077&loginpage=login.asp

Andresen, E. (2002, March 8). Conducting a security audit of an Oracle database. Retrieved March 21, 2007 from http://www.sans.org/reading_room/whitepapers/auditing/19.php

Ashendon, D. (2007). BCS group aims to spread lessons of information assurance to the masses. Computer Weekly. Retrieved April 1, 2007 from Business Source Premier database.

Blaze, M. (2004, March 6). Toward a Broader View of Security Protocols. Department of Computer and Information Science. Retrieved March 23, 2007 from http://www.crypto.com/papers/humancambridgepreproc.pdf

Boyce, Robert (2001) Vulnerability Assessments: The Pro-active Steps to Secure Your Organization [On-Line] Accessed May 7, 2005 http://www.sans.org/rr/whitepapers/threats/453.php

Brackin, Cathleen (October 15, 2003) Vulnerability Management: Tools, Challenges and Best Practices [On-Line] Accessed May 7, 2005 http://www.sans.org/rr/whitepapers/threats/1267.php

Britt, P. (2007, February). Tightening Security in 2007. InformationToday. Retrieved March 23, 2007 from http://0-search.ebscohost.com.janus.uoregon.edu:80/login.aspx?direct=true&db=buh&AN=23878734&loginpage=login.asp&site=ehost-live

Chuanxue, B., Nenad, J. (1999). A Security paradigm for Web databases. The ACM Digital Library. Retrieved March 21, 2007 from http://portal.acm.org/citation.cfm?id=306420&jmp=cit&coll=portal&dl=ACM&CFID=18001597&CFTOKEN=65428580#CIT

Corman, L. (1998). Data integrity and security of the corporate data base: the dilemma of end user computing. The ACM Digital Library. Retrieved March 22, 2007 from http://portal.acm.org/citation.cfm?id=65767&jmp=citings&coll=portal&dl=ACM&CFID=18001597&CFTOKEN=65428580#citings

Crossman, P. (2007). The Less-Than-Obvious Costs of Ignoring Data Architectures. Wall Street & Technology. Retrieved April 1, 2007 from Business Source Premier database.

Curtain, M. (2007, February 26). Database Security: Solve the right problem now, for fewer headaches tomorrow. Accounting Today. Retrieved March 23, 2007 from http://0-web.ebscohost.com.janus.uoregon.edu/ehost/results?vid=2&hid=6&sid=3fa2b3cc-7f02-4b8a-98db-7fa6ae0a52ea%40sessionmgr7

Database Vulnerabilities in the Spotlight. (2003, Feb 20). eWeek. pNA Retrieved April 1, 2007 from http://galenet.galegroup.com/servlet/BCRC?vrsn=157&locID=nysl_me_tnypl&srchtp=glb&c=2&ste=25&tab=2&tbst=tsAS&mst=Database+Vulnerabilities&docNum=A97912866&bConts=0

Davidson, M.A. (1995). Security in an Oracle data base environment. Information Systems Security. Retrieved April 1, 2007 from Business Source Premier database.

Doorn, J., Rivero, L. (2002). *Database Integrity: Challenges & Solutions.* Hershey, PA: Idea Group Publishing.

Dutta, A. and McCrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. California Management Review. Retrieved April 1, 2007 from Business Source Premier database.

Fernandez, E., Lunt, T. (1990) Database Security. The ACM Digital Library. Retrieved March 21, 2007 from http://portal.acm.org/citation.cfm?id=122069&coll=portal&dl=ACM&CFID=18001597&CFTOKEN=65428580

Fonseca, B., (2004) DBA Boundaries Blurring. eWeek. Retrieved April 11, 2007 from http://web.ebscohost.com/ehost/detail?vid=14&hid=103&sid=ce7ef31a-6690-48da-9e6a-e85908765943%40SRCSM2

Greenemeier, L. (2006, March 6). Oracle Security Under Scrutiny. Information Week. Retrieved March 22, 2007 from http://0-web.ebscohost.com.janus.uoregon.edu/ehost/detail?vid=5&hid=16&sid=c1ab8d14-705f-4b14-9b84-8052722be23d%40sessionmgr9

Hoffman, T. (2007). The Conversation. Computerworld. Retrieved April 1, 2007 from Business Source Premier database.

Huber, N. (2004). Poor back-up management can create database risk. *Computer Weekly*, Retrieved Friday, March 23, 2007 from the Business Source Premier database.

Jepson, K. (2006). Data Security Getting Better All the Time, Experts Say. Credit Union Journal. Retrieved April 1, 2007 from Business Source Premier database.

Jonker, W., Petkovic, M. (Eds.). (2004). Secure Data Management. In VLDB 2004 Workshop Proceedings. Toronto, Canada.

Kelly, C.J. (2005, July 25). Getting started on database security. Computerworld. v39 i30 p32(1). Retrieved April 1, 2007 from http://galenet.galegroup.com/servlet/BCRC?vrsn=157&locID=nysl_me_tnypl&sgcmd=MAIN&srchtp=glba&c=1&sub=%2522Implementing+Database+Security+and+Auditing+%28Book%29%2522&ste=20&tbst=tsAS&mst=Database+Security

Krippendorff, K. (2004). *Content Analysis: An Introduction to Its Methodology* (2nd ed.). Thousand Oaks, CA. Sage Publications.

Landergren, Pia. "Hacker Vigilantes Strike Back." June 20, 2001. URL: http://archives.cnn.com/2001/TECH/internet/06/20/hacker.vigilantes.idg/index.html. (May 6, 2005)

Laurent, W. (2006). Corporate Governance and Data Security and Privacy. DM Review. Retrieved April 1, 2007 from Business Source Premier database.

Leedy, P., Ormond, J. (2005). *Practical Research: Planning and Design* (8th ed.). Upper Saddle River, NJ. Pearson Education, Inc.

Loney, K. (2004). *Oracle Database 10g: The Complete Reference*. Emeryville, CA. McGraw-Hill/Osborne.

Luftman, J., (2004). *Managing the Information Technology Resource: Leadership in the Information Age.* Upper Saddle River, NJ. Pearson Education, Inc.

Miklau, G. and Suciu, D. (2007). A Formal Analysis of Information Disclosure in Data Exchange. Journal of Computer & Systems Sciences. Retrieved April 1, 2007 from Business Source Premier database.

Newman, A. (2005). Database Security Best Practices. Security. Retrieved April 1, 2007 from Business Source Premier database.

Oracle Database Security Checklist. (2007, January). Oracle Retrieved March 21, 2007 from http://www.oracle.com/technology/deploy/security/pdf/twp_security_checklist_db_database.pdf

Palmquist, M., Busch, C., De Maret, P., Flynn, T., Kellum, R., Le, S., Meyers, B., Saunders, M., White, R. (2005). Content Analysis. Retrieved April 1, 2007 from Colorado Statue University Department of English Web site: http://writing.colostate.edu/guides/research/content/.

Phillip, B. (2007, February). Tightening Security in 2007. Information Today. Retrieved March 22, 2007 from http://0-web.ebscohost.com.janus.uoregon.edu/ehost/results?vid=6&hid=6&sid=3fa2b3cc-7f02-4b8a-98db-7fa6ae0a52ea%40sessionmgr7

Polk, T., Bassham III, L. (1993, August). *Security Issues in the Database Language SQL* (NIST Special Publication 800-8). Gaithersburg, MD: National Institute of Standards and Technology.

Protect Your Computer. (2007). Microsoft. Retrieved April 20, 2007, from http://www.microsoft.com/athome/security/computer/default.mspx

Rath, V. (2006, December). Threat and Vulnerability Management Plan. ComputerWorld. Retrieved March 23, 2007 from http://www.computerworld.com/action/whitepapers.do?command=viewWhitePaperDetail&contentId=9013095&source=rss_topic85

Rubenking, N.J. (2007). Security Super Guide. PC Magazine. Retrieved April 1, 2007 from Business Source Premier database.

Scheier, R. (2006, August 28). Protecting the corporate database. Computerworld. Retrieved March 23, 2007 from http://0-web.ebscohost.com.janus.uoregon.edu/ehost/results?vid=5&hid=6&sid=3fa2b3cc-7f02-4b8a-98db-7fa6ae0a52ea%40sessionmgr7

Schultz, B. (2006, May 22). The hacker-resistant database. Network World. Retrieved March 22, 2007 from http://0-web.ebscohost.com.janus.uoregon.edu/ehost/results?vid=3&hid=6&sid=3fa2b3cc-7f02-4b8a-98db-7fa6ae0a52ea%40sessionmgr7

Scheier, R. (2006, August 28). Building Up Database Defenses. Computerworld. Retrieved March 23, 2007 from http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9002761

Thuraisingham, B. (2005). *Database and Applications Security: Integrating Information Security and Data Management.* Boca Raton, FL: Auerbach Publications.

Vijayan, J. (2007). Six Ways To Stop Data Leaks. Computerworld. Retrieved April 1, 2007 from Business Source Premier database.

Vizard, M. (2007). TIME TO GET TOUGH ON SECURITY THREATS. Baseline. Retrieved April 1, 2007 from Business Source Premier database.

Whitman, M., Mattord, H. (2004). *Management of Information Security.* Canada. Course Technology.

Wiederhold, G. (2000). Protecting Information when Access is Granted for Collaboration. Department of Computer Science, Stanford University. Retrieved March 22, 2007 from Google Scholar.