Knowledge Management, Business Intelligence and Databases

Business knowledge

Let's turn our attention to the world of business and how the data and information gathered by and for the business can lead to a sense of business knowledge or business intelligence. First, let's set the foundation for this with a definition of business knowledge, also known as knowledge management (KM) or sometimes business intelligence (BI)

The power of knowledge in business

Knowledge management is the gathering, organizing, sharing, and analyzing of the data and information to which a business has access. The data that is stored in a repository can then be organized, shared, and analyzed. That data comes from many sources, both from within the business itself (organizational memory including experiences and skills of the workforce, documents regarding customers and suppliers, existing designs and processes etc.) and from outside sources (market research and market reports, talking to customers and suppliers, professional associations and trade bodies, trade exhibitions and conferences, and collaboration with associated institutions and businesses) (Knowledge management and business growth, n.d.) However, knowledge management may very well not mean the same thing to different companies.

Sometimes KM is defined or explained in terms of productivity gain. Another description of KM can be couched in terms of data sharing of business intelligence rather than on the sharing of knowledge. Finally, some companies focus on implementation of employee portals (sources where employees will have access to the data needed for their specific jobs). Seiner (2002) posits the following definition and impact of knowledge management:

> *In every case, the intentions of sharing knowledge are good, even if the definition of knowledge management and the definition of knowledge itself varies from place to place. The definition of knowledge management that I use states that KM involves a discipline of spreading knowledge of individuals and groups across the organization in ways that directly impact performance. This impact on performance can take many shapes and forms. The impact can be related to the promotion of "healthy" or smart business activities, the involvement of knowledge stewards in daily activities, the limiting of the risk associated with people leaving the organization, understanding employee needs for knowledge, and making that knowledge, information, and data available to them.*

Why is Knowledge management important for a business?

Here are three key reasons why it is important for a business to generate and manage KM (also called business intelligence or BI):

- KM facilitates decision-making capability. Processing an overwhelming amount of information can get in the way of achieving high-quality decisions. Derbyshire (2011) reports that scientists claim that the amount of data sent to a typical person in

the course of a year is "the equivalent of every person in the world reading 174 newspapers every single day." A knowledge management system that can make sense of all this data can facilitate better, more informed decisions.

- KM builds learning organizations by making learning routine. Simply put, capturing learning from experience builds knowledge that can then be used to streamline operations and improve processes, and
- KM stimulates cultural change and innovation. KM programs can help managers be open to change and fosters an environment open to ideas and insight. This type of environment can lead to innovation, even for owners of businesses regardless of size (Quast, 2012).

All of that data needs to be catalogued, sorted, filtered, and linked in order for intelligent data analysis to occur with results that a business can use. This involves data mining in addition to data analysis. Remember that the goal of KM is to provide the business with output that can be used to address specific business tasks and projects (Rouse, n.d.). In order to understand the basis of this type of business knowledge or business intelligence, let's take a look at the foundations of data storage – databases.

Databases: Basic Concepts

In December 2013, Target, Inc., announced that a security breach had allowed unauthorized individuals to gain access to information about customers who had recently shopped at Target and used a credit card or debit card to make purchases. Then in January 2014, Neiman Marcus reported the same problem: Unauthorized people had accessed its database and taken shoppers' personal information, including names, addresses, phone numbers, and e-mail addresses. Both of these security breaches had grave implications for the personally identifiable information (PII) of the shoppers, with the potential for these unauthorized persons to complete credit card or loan applications, make unauthorized purchases, and potentially impact credit ratings for millions of customers of these two stores.

All of the data about the customers had been stored in databases. What makes it so convenient to simply swipe your credit card or debit card when making a purchase, and to have the purchase approved almost instantaneously, is also what makes these security breaches so potentially devastating. All of the information the store needs for billing—your card numbers, billing address, phone number, e-mail address, and more—is stored in large databases maintained by the store. This collection of data about you is organized in such a way that retrieval of the information can be done in seconds. That is the strength of databases and database software.

Basic Organization of a Database

So, what is a **database**? It is *a computer-based collection of related pieces of data organized so that the data can readily be accessed, managed, and updated*. As you recall, computers work with the binary system where a bit is the smallest entity represented and is either a one (on) or a zero (off). Together eight bits combine to form a byte which represents one character. The characters represented by bytes may be letters, numbers, and/or special symbols. By themselves, characters generally are not meaningful, but they combine to form meaningful data such as your first name. Your first name consists of a set of characters ultimately stored as bits in the computer.

Databases operate by organizing data into meaningful groupings called fields, records, tables, and finally databases.

- **Fields,** which contain one or more characters or an audio, video or image file. Fields can be designed to hold only character data or only numeric data, or they can be designed to hold other types of data, such as images or audio or video files or a hyperlink to a website or other information source. For instance, one field might contain a first name, another field a last name, another the street portion of an address, and so on. Each field is given a specific name. You can visualize fields as being organized in columns of a particular table in the database.
- **Records,** a collection of related fields, usually organized in a row. The record contains all of the information related to a specific entity—a person, a place, a thing, or an event. For example, a record might contain a first name, a last name, and a social security number. You can visualize the records as being organized into rows in a particular table, where all the components of a single row are made up of fields that represent characteristics of a person, place, thing, or event.
- **Tables,** collections of related records. A table contains all the records for a particular group or type of thing or event.
- **Database,** a collection of related tables and other objects such as queries, forms, and reports, that help users view data in meaningful ways.

The overall organization of the database, then, moves from the smallest piece of meaningful information (the field) through records and tables to the database itself which contains tables, queries, forms and reports.

Interacting with a Database

Database software, also called a database management system or DBMS, allows users to interact with the database at all levels of the hierarchy. After a database structure is designed and the structure is implemented by creating the fields and tables, data is entered typically via a **data entry form**, a window on the screen that allows the user to enter data into the fields that make up a record. Data can also be modified via the form.

Database software, also called a database management system or DBMS, allows users to interact with the database at all levels of the hierarchy.

A **query** is a way of retrieving data from the database via specification of criteria that identify exactly what data is to be retrieved and how it might be sorted and displayed. Data can also be modified via the query.

Reports are also used to retrieve data from the database, in which the user can specify how the retrieved data are presented. Reports can be displayed, printed, or shared. Reports can also be used for things like mailing labels.

The term **file maintenance** refers to procedures that keep data current in the database. File maintenance supports adding, modifying, or deleting records, and creating backup copies of the database.

If you are familiar with Microsoft Access, you perhaps have used wizards to help you create required elements of your project. A **wizard** is a software application that is used to create

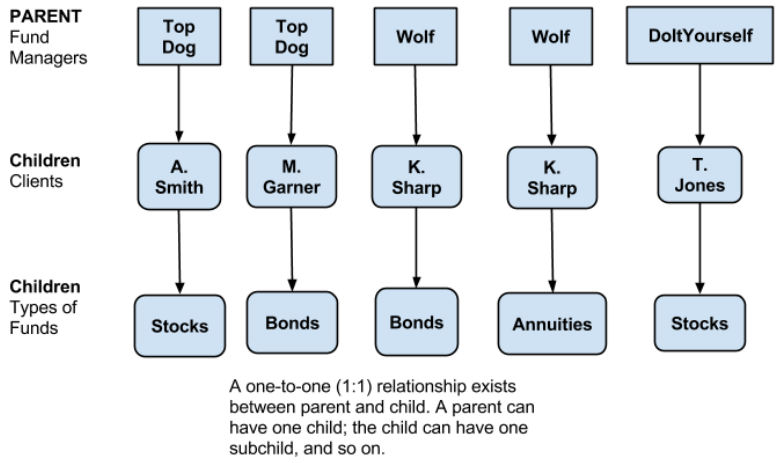
tables, queries, and reports. The wizard itself is not used to enter or modify data in the fields or records.

Different Database Models

All databases are composed of the elements identified above. But the organization of the records and tables can be quite different. What are the various models used for structuring a database? The older, less efficient models were the hierarchical and network models. Both models were restricted in that the organization of data had to be defined up front, making the structure quite inflexible. It was difficult to add new fields or tables to the database.

Hierarchical Model

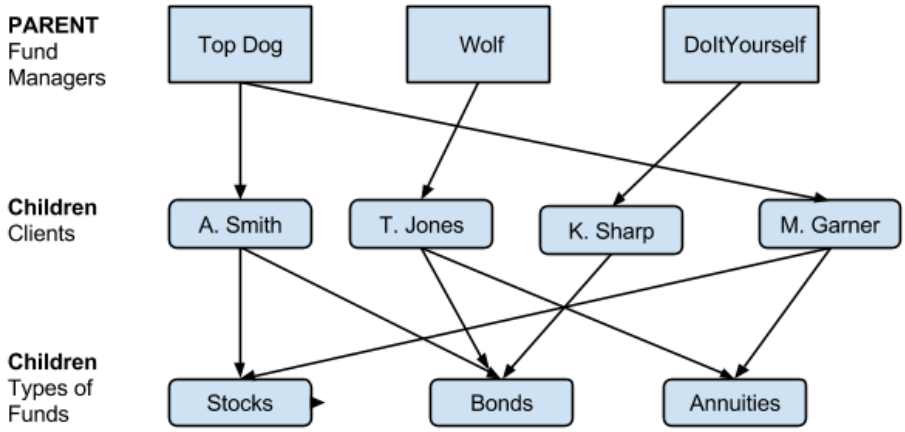
The structure was predefined. If new fields were needed, the entire database had to be redefined. This diagram represents an example of the hierarchical structure:



The top field—in this example, Fund Manager—was called the "parent," and the other fields (clients and types of funds) were called the "children" of that parent. There was no way to relate the children of one parent with the children of another—no common key field. For example, it was impossible to retrieve just a list of the client names (a child field) from all the fund manager records without retrieving all the data for *all* the fund managers. Think about it as an all-or-nothing situation. To enter the data about an item, person, or place, or even to retrieve even one piece of information about that same item, the entire record for that item had to be retrieved or opened up for editing. If you wanted to know what funds Wolf was managing, you had to retrieve the entire record wherever Wolf's name appeared as the Fund Manager; that is, the Fund Manager's name, the client name, and which funds this client was invested in. You can see the inefficiency in this structure and why a newer model quickly developed.

Network Model

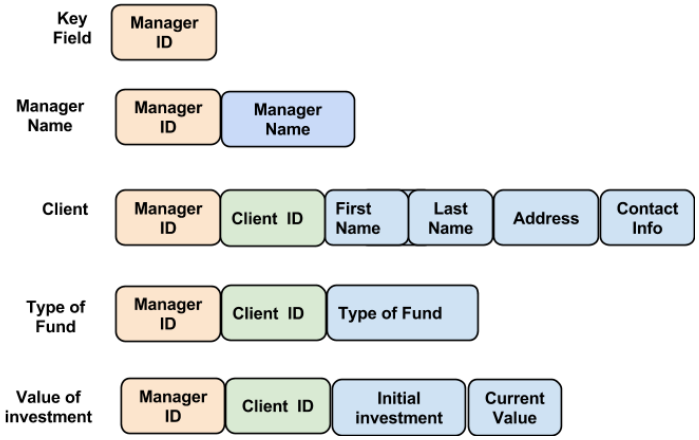
The network database was an extension of the hierarchical model. It allowed a parent record to have more than one child, and child records to be related to more than one subchild record. It was more flexible than the hierarchical structure because new relationships could be established between data. But because the structure still needed to be defined in advance (Williams & Sawyer, 2013), it still was fairly inflexible.



A one-to-many (1:*N*) relationship exists between parent and child records. A parent can have multiple child records; child records can have multiple connections to other subchild records.

Relational Model

The relational database model grew out of this need for greater flexibility in adding new fields and tables, and to retrieve just the information desired for a particular purpose. Instead of each record containing *all* the information about a person, place, event, etc., the information is spread across different tables. But these tables must have some means of connecting the different types of data that are used to describe an individual, place, thing, or event. That is accomplished by inserting a common key field, called the **primary key**, into each record to link the records in separate tables. So if one table contains a fund manager's name, another client information, another fund types, and another the value of investments, a unique field common to each table links the records from the different tables. If an identification (ID) number is the primary key, each record in the various tables that are associated with an individual, for example, will have the same ID number as one of its fields.



This is how the data in the tables might appear:

Manager ID Table

Manager ID
1
2
3

Manager Name Table

Manager ID	Manager Name
1	Top Dog
2	Wolf
3	DoItYourself

Client Table

Manager ID	Client ID	First Name	Last Name	Address	Contact Info
1	AAA	A	Smith	1234 Hemlock Rd. Huntsville, AL	345-555-4321
2	BBB	M	Garner	3608 Pines Blvd. Lauderdale, FL	954-555-9876
3	CCC	K	Sharpe	34 E. Hilltop Ave. San Francisco, CA	846-123-5555

Type of Fund Table

Client ID	Fund type
AAA	Stocks
AAA	Bonds
BBB	Bonds
BBB	Annuities
CCC	Stocks

Value of Investment Table

Manager ID	Client ID	Initial Investment	Current Value
1	AAA	$500	$50,000
2	BBB	$99,000	$2,465,723
3	CCC	$4,500	$495,000

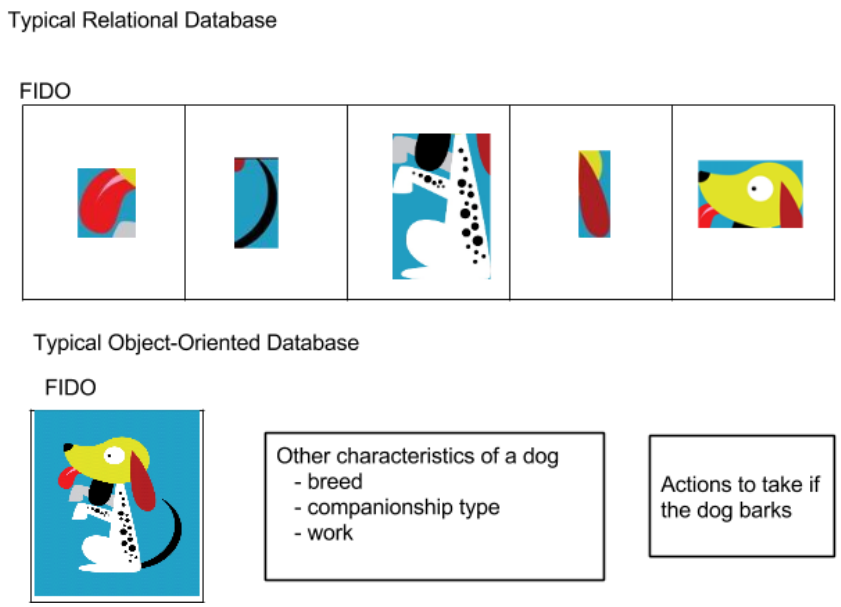
In this case, new fields in the existing tables or even completely new tables can be added—perhaps an e-mail address for the client, or a new fund type. If the Manager ID is maintained as the primary key in each new table and the secondary key for the client in the appropriate tables, then links to the other information in the other tables can be maintained without rebuilding the database.

It is easy to retrieve specific information from the relational database, as there is no need to retrieve all the information spread across different tables with all fields, as was necessary in a hierarchical database. The fields from specified tables are accessed via a special database language called Structured Query Language (SQL). This same language is used

to create, modify, and maintain a relational database. When you use wizards in MS Access to create databases, enter the data, and retrieve data for specified reports, you have used a wizard based on the SQL needed to manipulate the database.

Object-Oriented Model

There are two other database models we will touch on briefly here: the object-oriented database and the multidimensional database. In an object-oriented database, the data itself is conceived of as objects. The object can consist of data (character, numeric, etc.), or it can be instructions on what to do with that data. For example, in a relational database, all the elements that make up a dog—nose, eyes, mouth, ears, body, legs, tail—would be stored in separate fields. In an object-oriented database, all these components would be stored in one "object," the dog.



An object-oriented database is especially useful in areas such as design; scientific experiments; telecommunications; geographical information systems (GIS); and multimedia such as photos, sound files, and video (Williams & Sawyer, 2013). Note that all of these applications rely heavily on the use of images or multimedia. Those types of data cannot as easily be stored in the typical relational database where all the fields are typically character, text, or number-based. In object-oriented databases, the data in various tables are linked to and accessed by the use of pointers instead of common fields as in the relational database.

Multidimensional Model

The final database model is the multidimensional database, built and used optimally for data warehouse and online analytical processing applications. A special type of database language called online analytical processing (OLAP) or multidimensional OLAP (MOLAP) is used to manipulate the data in these types of databases.

Integrity and Validity of the Data

What is common to all database structures, whether hierarchical, relational, object-oriented, or multidimensional, is the support for ease of entry (adding records), retrieving the desired

information, updating or correcting records, and ensuring that the data in the database is accurate. Data **integrity** should ensure that the data can be verified as correct, is up to date or timely, is organized in a way that is useful, is accessible to the user when it is needed, and is cost effective (that is, its value is greater than the cost to produce the data).
Data **validity** is accomplished by comparing data that is being entered to a set of rules to ensure that the entry complies with those rules (Shelly & Vermaat, 2013). For example, if text data is entered into a field which has been set up to accept only numbers, the user entering the data should be alerted immediately to the mismatch.

All of the database models support the following advantages, to some extent, over a file processing system (one in which data is stored in **flat** files—that is, with no connections between the data in the files).

- Reduced data redundancy: Duplicate data is more easily avoided.
- Improved data integrity: Changes are made in one place instead of needing to search through multiple files or spreadsheets to find where changes need to be made.
- Shared data: A single set of data in the database can be shared with multiple users. Security settings define which users can access, add, modify, or delete records.
- Easier access: With appropriate software and access privileges, a nontechnical person can use the database without needing to know the complexity of the underlying structure.
- Reduced development time: The tools available for creating a database can result in an easier and faster development process than would be required for developing and maintaining multiple separate files that have been created and organized for different types of users or departments.

There are some challenges to the creation and use of databases, as well.

- A database system may be more complex than a series of spreadsheets or lists and may require people with special training to design and implement the database.
- A database consumes more memory, storage, and processing power than a file processing system.
- Because a great deal of information is stored in the database, if it is lost or the data become corrupt and unusable, it may affect all those who need to access the data.
- Unauthorized access to a database containing personally identifiable information (PII) could result in harm to those individuals whose information is accessed (Shelly & Vermaat, 2013).

Databases and Security Issues

Would it be possible to store all of the available data (in digital form) in a single database? Most likely not, since the volume of digital data doubles almost every year (Vishen, 2013). One recent estimate lists the total volume of digital data at 4.4 trillion gigabytes (Dartnell, 2014). That data is currently stored in many different databases, and claims of having the largest database by volume are contested. Recent reports agree that the current holder of that title is the World Data Center for Climate (WDCC) operated by the Max Planck Institute for Meteorology and German Climate Computing Center (Vishen, 2013). Also among the world's largest databases:

- National Energy Research Scientific Computer Center (Lawrence Labs)
- AT&T (calling records)
- Google
- Sprint (calling records)
- LexisNexis (legal research)
- YouTube
- Amazon
- the Central Intelligence Agency, and
- Library of Congress (Vishen, 2013)

NSA's surveillance database and PRISM data mining program could contend for the top spot if the number of data records were revealed.

Why Data Security Is Important

It is the confidentiality, integrity, and availability (CIA) of the data in a database that need to be protected. Confidentiality can be lost if an unauthorized person gains entry or access to a database, or if a person who is authorized to view selected records in a database accesses other records he or she should not be able to view. If the data is altered by someone who is unauthorized to do so, the result is a loss of data integrity. And if those who need to have access to the database and its services are blocked from doing so, there is a resulting loss of availability. Security of any database is significantly impacted by any one or more of these basic components of CIA being violated (Nuramn, 2011).

Both businesses and home computer users should be concerned about data security. The information stored in databases—client information, payment information, personal files, bank account details, and more—can be hard to replace, whether the loss results from:

- physical threats such as a fire or a significant power outage
- human error that results in errors in the processing of information or unintended deletion of data, or from erroneous input
- corporate espionage, theft, or malicious activity.

Loss of this data is potentially dangerous if it falls into the wrong hands (Spamlaws, 2016).

It is in these three areas that a risk assessment of the database's security and protection of the data should focus. Is there a backup procedure that would allow access to the data if the primary database is destroyed by a physical threat? That same backup procedure might be important in case the CIA of the database is inadvertently affected by human error. And what safeguards can/should be put in place to prevent incidents of espionage, theft, or other malicious activity? We will look again at risk assessments later on this page.

How Common Are Database Breaches?

Just how prevalent are the threats against databases? Is it worth the time, money, and personnel effort to ensure that the database is safeguarded? Remember the Target and Neiman Marcus problems that surfaced in late 2013? And the continuing saga of Edward Snowden and the NSA leaks? These may have been the most widely publicized data breaches of 2013. But they were definitely just two of many such database breaches. **Database breaches** are the exposure of database records containing personally identifiable information (PII) or other sensitive information to unauthorized viewers. Risk Based Security (RBS), a group of consultants and founders of the Open Security Foundation (OSF), report that 2013 saw a record number of data records exposed via data

breaches. Over 822 million such records were made available to persons who had no authority to view these records ("Risk Based Security," 2014). But remember, the number of reported database breaches does not reflect the total number of breaches that occurred. Some companies do not report breaches in order to protect their reputations or to prevent customers from abandoning the company. The following is a short list of what RBS discovered.

- The business sector accounted for 53.4% of reported incidents, followed by government (19.3%), medical (11.5%), education (8.2%), and unknown (7.6%).
- Hacking was the cause of 59.8% of reported incidents, accounting for 72.0% of exposed records.
- Of the reported incidents, 4.8% were the result of web-related attacks, which amounted to 16.9% of exposed records.
- Four incidents *in 2013 alone* secured a place on the Top 10 All-Time Breaches list:
  - Adobe—152 million records. Customer IDs, encrypted passwords, debit or credit card numbers, and other information relating to customer orders was compromised.
  - Unknown organizations—140 million records. North Korean hackers exposed e-mail addresses and identification numbers of South Korean individuals.
  - Target—110 million records. Information included customer names, addresses, phone numbers, e-mail addresses, credit/debit card numbers, PINs, and security codes.
  - Pinterest—70 million records. A flaw in the site's application programming interface (API) exposed users' e-mail addresses.

Even if you were not impacted by any of the above data breaches, if you have used a credit card, made an airline reservation, subscribed to a magazine, been a patient in a hospital, or shopped at a chain store (supermarket or department store), or if you are a member of an online social media site, your personally identifiable information (PII) is stored in a database. How vulnerable is your PII?

What Are the Most Common Causes of Database Breaches?

As evidenced by the NSA Snowden leaks and the Target breach, no database and no government agency, company, or business is as secure as the owners of that database think. It is difficult for database administrators and security managers to keep pace with the new threats and vulnerabilities that continually emerge. And to compound the issues, every company/business/government has different security issues, making it a particularly hard challenge to standardize any one solution that fits all. However, there are some common threats and vulnerabilities that seem to occur repeatedly.

Threats

Unauthorized Access by Insiders

The malicious insider with approved access to the system is one of the greatest threats to database security.

> *People attack computers because that's where the information is, and in our hyper-competitive, hi-tech business and international environment, information increasingly has great value. Some alienated individuals also gain a sense of*

power, control, and self-importance through successful penetration of computer systems to steal or destroy information or disrupt an organization's activities (JA, 2015).

Another scenario might involve employees affected by a workforce reduction who take customer account lists, financial data, or strategic plans with them when they leave. Proprietary information could end up in the hands of competitors or be widely disseminated online ("Data Loss Prevention: Keeping sensitive data out of the wrong hands," 2008).

Insiders may also be a threat to database security if they are granted database access privileges that go beyond the requirements of their job function, abuse legitimate database privileges for unauthorized purposes, or convert access privileges from those of an ordinary user to those of an administrator.

Accidental Breaches Resulting from Incorrect—but Not Malicious—Usage

The data breach is not always the result of a deliberate attempt to subvert data security; sometimes it is an unintended consequence. For example, employees might export data from the parent database system at work and send it, typically unencrypted, to personal e-mail addresses so they can work from home. The data then might be subsequently compromised on someone's home computer. Or a data mining application might contain flaws that allow a user without the correct access credentials to stumble upon database records inadvertently. (Note: If the user deliberately continues to access the data without permission, this situation becomes a malicious insider threat.)

Unprotected Personal Hardware Collection

It is becoming increasingly common for data to be transferred to other personal mobile devices—USB flash drives, smartphones, tablets, and the like. It is rare now to find an employee who never uses a mobile device—personal or company-supplied—for business purposes. However, mobile devices continue to be a significant source of data breaches, stemming from a range of circumstances, including loss or theft of the devices, failure to install antimalware tools on the devices, or failing to password-protect a device being used for business purposes. Data is at risk if an employee stores any proprietary information on such a device or if that device is used to access a company's network and/or database (Bruemmer, 2014).

Stolen Laptops

Forgetful or careless laptop owners whose equipment is taken expose data on that laptop to persons not authorized to have access to the data. This can also happen if a laptop is replaced and the hard drive on the original machine is not properly erased or destroyed.

Weak Authentication

A legitimate database user typically is required to submit an ID and password in order to gain access to a protected database. Authentication is the process (internal to the database program itself) by which the credentials of the user are verified and access may be granted. If the process of authentication is weak, an attacker can assume the identity of a legitimate user by stealing or obtaining login credentials. Credentials may be illegitimately obtained by various means:

- **Credential theft.** The attacker accesses password files or finds a paper on which the legitimate user has written down the ID and password.

- **Social engineering.** The attacker deceives someone into providing the login ID and password by posing as a supervisor, IT maintenance personnel, or other authority.
- **Brute-force attacks.** Have you ever been locked out of an account after attempting to log in more than three times with an incorrect password? If so, this is the simplest (and perhaps least effective) means of blocking a brute force attack, whether it is an attempt to access files on your machine or to access a database. However, not all password protected systems, databases, or files block you from access after three attempts. For example, if you have put a lock on a file on your computer, you most likely have not set a limit on the number of attempts on that file. A brute-force attack is a password-guessing approach in which the attacker attempts to discover a password by systematically testing every combination of letters, numbers, and symbols until the correct combination is found. Depending upon the password's length and complexity, this can be a very difficult task to complete. However, there are widely available tools that hackers can use to find the password, and it can be difficult to block all the means by which hacker will try to find the password ("Blocking brute force attacks - system administration database," n.d.)

Exploiting Weaknesses in an Operating System or Network

Worms, viruses, or Trojan horses could be introduced into an unprotected or poorly protected operating system or computer network that supports the database, leading to potential unauthorized database access (loss of confidentiality), data corruption (loss of integrity), or denial of service (DOS), a loss of access to legitimate users. A DOS may be achieved by causing a server to stop functioning, or "crash," flooding a network with message traffic or overloading resources on the computer, forcing it to stop handling additional tasks or processing.

Theft of Database Backup Tapes or Hard Drives

Database backups typically do not have the same security measures in place that the primary database employs. These backups may not be encrypted, and the media on which backups are stored are also unprotected. Theft of the backup media may allow the attacker full access to the data stored within the backup (Manes, 2015).

Vulnerabilities

There are other means by which databases are exposed to security breaches, and these are considered vulnerabilities that may subject a database to a security breach. These are more passive, but they can do as much harm as direct threats:

- **Data at rest** (unencrypted information) that is passively residing in storage within the boundaries of company computers, perhaps waiting to be moved to a secure database. Data at rest typically is not as well protected as data that has been entered into the database and enjoys the database security measures.
- **Data in motion** is information that is being electronically transmitted outside the company's protected network via e-mail or other communication mediums. For example, the data might be transferred to a backup facility that is not part of the internal storage media used for daily work. Or if the company uses the cloud for data storage backups, the transfer might take place outside of the company's protected network. This can lead to a loss of sensitive data if there is a malicious attack via malware during the transfer process or during execution of a flawed business process that allows unauthorized persons to view or obtain the data. (This is not the

same as the accidental breach resulting from incorrect but not malicious usage noted above, where the home computer to which the data has been transferred is attacked or breached. That accidental breach occurred without any intention of harm by the employee.)

- **Poor architecture,** in which security was not adequately factored into the design and development of the database structure. This vulnerability may not be discovered until there is an attempted or successful data breach.
- **Vendor bugs**, particularly programming flaws that allow actions to take place within the database and with the data that were not intended or planned. Much like poor application architecture, this vulnerability may not be uncovered until there is an attempted or successful data breach.
- An **unlocked database** is one that has no security measures in place to control access or auditing. This seems counter-intuitive, but many home users employing a database for personal needs, or even for working on company data while at home, may be working with an unlocked database (Nichols, 2007) ("Data Loss Prevention: Keeping sensitive data out of the wrong hands," 2008).

Risk Assessments

In the business environment, it is critical that a thorough risk assessment takes place and be periodically reviewed. The assessment should address:

- who has access to what data
- the circumstances under which access to the database may need to change
- who maintains the passwords needed to access the database
- who uses the company's computers for access to the internet, e-mail programs, etc., and how employees access those resources
- what type of firewalls and antimalware solutions to put in place
- the training of the staff
- who has responsibility for enforcement procedures related to data security (Spamlaws, 2016).

There are identified solutions for each of the threats and vulnerabilities discussed here, including well-defined and enforced access policies, use of strong data encryption, vulnerability assessments, policies related to strong passwords, and installation of firewalls. There are companies that specialize in designing plans, procedures, and software to prevent data loss or data leakage. With **data loss,** the data is lost forever, either by deletion, theft, or data corruption. **Data leakage** allows unauthorized people to get access to the data, either by intentional action or by mistake. So data loss and data leakage can be intentional or unintentional, and both can be malicious or just human errors (VJ, 2013).

How Can You Protect Your PII?

Protecting databases and the data contained within can be a costly and all-consuming activity. But what does this mean for you, the individual who uses that credit card, makes airline reservations, files taxes online, subscribes to a magazine, has been a patient in a hospital, shops at a chain store, or is a member of an online social media site? Your PII is out there, stored in multiple databases. Obviously, you cannot implement security measures for the company, business, or government agency that holds your PII. But are there many

measures you can take to better protect yourself? Here are a few rules of thumb that you can implement:

Keep your passwords to yourself.	Do not leave a slip with a list of passwords under your computer, or anywhere where it can be viewed or taken by someone. Just giving your password to a friend is not a good idea, either.
Use different passwords for different accounts.	Remembering multiple passwords can be a challenge, and it's often convenient to use the same password for multiple accounts, ranging from Facebook and your bank account to your Twitter page. The danger here is that a compromise of any one of these accounts could also result in the compromise of others if the same password is used for multiple accounts.
Use strong passwords.	Many of your user IDs must have strong passwords to gain entry into one or more systems. In those instances when you can choose any password configuration, pick a strong password to protect your information.
Check your credit reports annually.	Sometimes people don't learn that they're victims of identity theft until their credit rating and identity are destroyed. It's proactive to get copies of your credit reports from the credit bureaus and carefully review them for any errors. Be sure to follow-up with the credit bureaus to make any corrections to your reports, if needed. By law, you can get one free credit report from each of the three credit bureaus every year.
Google yourself	Enter your own name in Google, Yahoo or other search engine and see what data comes up. Investigate any postings about yourself in the information that you find. Look for any suggestions that your PII may be compromised.
Remember that people can be a very weak link in security.	No matter how secure you make your passwords and how careful you are with your technology, there is always a human element to protecting your information.
Control physical access to your devices.	It's important to not leave laptops and other mobile devices unattended in public locations, like a coffee shop or other location with free WiFi. An unattended machine is at risk, for both theft and other security threats. When you aren't controlling physical access to your machine, you shouldn't let it out of your sight.
Remember to logout of a	Whether it's your email, bank account, retail store

website when you are finished using it.	shopping account or library account, always remember to logout when you leave the website.
Remember to lock your computer with a password when you are finished using it.	By requiring a password to access your computer (or other electronic device) you are protecting your information. You are also making your computer useless to a thief who cannot break password locks.

Let's Summarize

In this unit we have been looking at databases—their purpose, structure, uses, and security applications in the business arena. First, a **database** is a computer-based collection of related pieces of data organized so that the data can readily be accessed, managed, and updated.

Basic Organization of a Database

A database is composed of tables (and the queries, reports and other forms that are generated from data in the tables). The tables are composed of records, and the records contain fields.

Interacting with a Database

Database software, also called a database management system or DBMS, allows users to interact with the database at all levels of the hierarchy. Some of the interactions are characterized as **data entry forms, queries, reports, file maintenance, and wizards.**

Different Database Models

All databases are composed of the elements identified above. But the organization of the records and tables can be quite different. We briefly looked at several models.

Hierarchical and **network models** are less flexible, not allowing for easy changes to the structure of the database. In the **relational** model, *all* the information about a person, place, event, etc., is stored in related records, but the information is spread across different tables. The different types of data that are used to describe an individual, place, thing, or event are linked by a common key field, called the **primary key**. In the **object-oriented database** model, the data itself is conceived of as objects. The object can consist of data (character, numeric, etc.), or it can be instructions on what to do with that data. The objects are joined by the use of pointers. The final database model is the **multidimensional** database model, built and used optimally for data warehouse and online analytical processing applications.

Integrity and Validity of the Data

Data **integrity** means that the data is verified as correct, up to date or timely, organized in a way that is useful, and accessible to the user when it is needed. Data **validity** is satisfied by comparing data being entered to a set of rules to ensure that the entry complies with those rules (Shelly & Vermaat, 2013).

Databases and Security Issues

It is the confidentiality, integrity, and availability (CIA) of the data in a database that need to be protected. Confidentiality can be lost if an unauthorized person gains entry or access to a database, or if a person who is authorized to view selected records in a database accesses other records he or she should not be able to view. If the data is altered by

someone who is unauthorized to do so, the result is a loss of data integrity. And if those who need to have access to the database and its services are blocked from doing so, there is a resulting loss of availability.

Security of any database is significantly impacted by any one or more of these basic components of CIA being violated. CIA can be compromised by threats or vulnerabilities.

Risk Assessments

In the business environment, it is critical that a thorough risk assessment take place and be periodically reviewed. The assessment should address who has access to and control of the database, database security software, and training.

How Can You Protect Your PII?

Protecting databases and the data contained within can be a costly and all-consuming activity. Obviously, you cannot implement security measures for the company, business, or government agency that holds your PII. But there are measures you can take to better protect yourself.

References

Blocking brute force attacks - system administration database. Retrieved from System Administration Database UVA Computer Science: http://www.cs.virginia.edu/~csadmin/gen_support/brute_force.php

Bruemmer, M. (2014, January 21). *How mobile devices can imperil your organization's Cyber security*. Retrieved from Experian: http://www.experian.com/blogs/data-breach/2014/01/21/how-mobile-devices-can-imperil-your-organizations-cyber-security/

Dartnell, J. (2014, April 20). *EMC: Digital universe data to grow tenfold by 2020*. Retrieved from CNME: computer news middle east: http://www.cnmeonline.com/news/emc-digital-universe-data-to-grow-tenfold-by-2020/

Data Loss Prevention: Keeping sensitive data out of the wrong hands. (2008, July). Retrieved from Advisory Services: http://www.pwc.com/us/en/increasing-it-effectiveness/assets/data_loss_prevention.pdf

JA, A. (2015, June 8). *Insider vs. Outsider threats: Identify and prevent - InfoSec resources*. Retrieved from Forensics: http://resources.infosecinstitute.com/insider-vs-outsider-threats-identify-and-prevent/.

Knowledge management and business growth. (n.d.). Retrieved from NIBusinessInfro.co.uk: https://www.nibusinessinfo.co.uk/content/basic-sources-knowledge

Manes, C. (2015, September 23). *If you keep it, encrypt it*. Retrieved from IT Security: http://www.gfi.com/blog/if-you-keep-it-encrypt-it/.

Nichols, R. (2007). *Eleven specific solutions to today's most common database security threats and vulnerabilities*. Retrieved from University of Oregon: Applied Information Management: http://aim.uoregon.edu/news/ebriefing/eleven_solutions_to_database_security_threats.php.

Nuramn, A. (2011). *Database security*. Retrieved August 18, 2016, from Brighthub: http://www.brighthub.com/computing/smb-security/articles/61400.aspx.

Quast, L. (2012). *Why knowledge management is important to the success of your company*. Retrieved from Forbes.com: https://www.forbes.com/sites/lisaquast/2012/08/20/why-knowledge-management-is-important-to-the-success-of-your-company/#36b146103681

Risk Based Security. (2014, February 18). *Data Breach QuickView.* Retrieved from Risk Based Security: https://www.riskbasedsecurity.com/reports/2013-DataBreachQuickView.pdf

Rouse, M. (n.d.). *Knowledge management (KM)*. Retrieved from techtarget: http://searchdomino.techtarget.com/definition/knowledge-management

Seiner, R. (2002). *Business Impact of Knowledge Management*. Retrieved from The data administration newsletter: http://tdan.com/business-impact-of-knowledge-management/4943

Shelly, G. B., & Vermaat, M. E. (2013). *Discovering Computers 2013.* Boston: Course Technology

Spamlaws. (2016). *Why data security is of paramount Importance*. Retrieved from http://www.spamlaws.com/data-security-importance.html

Vishen, N. (2013, April 20). *Largest databases of the world*. Retrieved from http://neeraj-dba.blogspot.com/2013/04/largest-databases-of-world.html.

VJ (2013, April 2). *Is There a Difference Between Data LOSS and Data LEAKAGE Prevention?.* Retrieved from Rational Survivability:http://www.rationalsurvivability.com/blog/2008/06/is-there-a-difference-between-data-loss-and-data-leakage-prevention/.

Williams, B. K., & Sawyer, S. C. (2013). *Using Information Technology.* New York: McGraw-Hill