Course Title: - Management Information Systems **Course No: - MCA-209-EA**

UNIT 111

Knowledge management

This is a knowledge management site covering the theories, frameworks, models, tools, and supporting disciplines that are relevant to both the student and the practitioner. The goal of this site is to provide a comprehensive overview of knowledge management by examining its objectives, scope, strategy, best practices, knowledge management tools, and so on.

Introducing Knowledge Management

Knowledge management is essentially about getting the right knowledge to the right person at the right time. This in itself may not seem so complex, but it implies a strong tie to corporate strategy, understanding of where and in what forms knowledge exists, creating processes that span organizational functions, and ensuring that initiatives are accepted and supported by organizational members. Knowledge management may also include new knowledge creation, or it may solely focus on knowledge sharing, storage, and refinement. For a more comprehensive discussion and definition, see my knowledge management definition.

It is important to remember that knowledge management is not about managing knowledge for knowledge's sake.

The overall objective is to create value and to leverage, improve, and refine the firm's competences and knowledge assets to meet organizational goals and targets. Implementing knowledge management thus has several dimensions including:

- **KM Strategy:** Knowledge management strategy must be dependent on corporate strategy. The objective is to manage, share, and create *relevant* knowledge assets that will help meet tactical and strategic requirements.
- **Organizational Culture:** The organizational culture influences the way people interact, the context within which knowledge is created, the resistance they will have towards certain changes, and ultimately the way they share (or the way they do not share) knowledge.
- **Organizational Processes:** The right processes, environments, and systems that enable KM to be implemented in the organization.
- **Management & Leadership:** KM requires competent and experienced leadership at all levels. There are a wide variety of KM-related roles that an organization may or may not need to implement, including a CKO, knowledge managers, knowledge brokers and so on. More on this in the section on KM positions and roles.
- **Technology:** The systems, tools, and technologies that fit the organization's requirements - properly designed and implemented.
- **Politics:** The long-term support to implement and sustain initiatives that involve virtually all organizational functions, which may be costly to implement (both from the perspective of time and money), and which often do not have a directly visible return on investment.

Typically, failed initiatives have often placed an undue focus on knowledge management tools and systems while neglecting the other aspects. This issue will also be addressed throughout the site, and particularly in the knowledge management strategy section.

At this point, the articles presented on this site focus on the first five dimensions. Originally, I had deemed the political dimension to be beyond the scope of this site, since it is not something that is commonly tackled in KM literature. However, I will add a section on the political aspect of KM in the future.

Throughout the site, I will explain and discuss known theories, occasionally contributing with some of my own frameworks. I will also discuss the potential role of knowledge management systems from a broad perspective, and in the section on KM tools I will provide specific advice on this topic. I have tried to organize the site as logically as possible, moving from a general introduction to knowledge and KM to introducing key subjects like organizational memory, learning, and culture. The later sections discuss several models and frameworks as well as knowledge management initiatives, strategy, and systems, before finally presenting an overview of various tools and techniques.

E-governance

1.A concept and emerging practice, seeking to realise processes and structures for harnessing the potentialities of information and communication technologies at various levels of government and the public sector and beyond, for the purposes of enhancing good governance.

2.

In the public sector context governance refers to coordination, interaction, and institutional arrangements which are needed to pursue collective interest in policy-making, development and service processes in the context of nonhierarchically organized stakeholder relations. Electronic governance or **e-governance** is technologically mediated communication, coordination, and interaction in governance processes.

3.

A dynamic process enhancing interactions between citizens, consumers, public administration, private sector, and third sector. It applies electronic means to foster such interaction between these actors.

4.

Governance refers to the exercise of political, economic and administrative authority in the management of a country's affairs, including citizens' articulation of their interests and exercise of their legal rights and obligations. **E-governance** may be understood as the performance of this governance via the electronic medium in order to facilitate an efficient, speedy and transparent process of disseminating information to the public, and other agencies, and for performing government administration activities. **E-governance** is generally considered as a wider concept than e-government, since it can bring about a change in the way how citizens relate to governments and to each other.

5.

The use of emerging information and communication technologies (ICT) to facilitate the processes of government and public administration. It is about providing citizens with the ability to choose the manner in which they wish to interact with their governments. And it is about the choices governments make about how ICT will be deployed to support citizen choices.

6.

Communication by electronic means to place power in the hands of citizens to determine what laws need to be made and how these laws should be written.

7.

Is "the application of electronic means in (1) the interaction between government and citizens and government and businesses, as well as (2) in internal government operations to simplify and improve democratic, government and business aspects of Governance?

8.

The use of ICTs such as the internet and mobile phone as a platform for exchanging information, providing services and transacting with citizens, businesses, and other arms of government

9.

E-Governance is defined as that stage of e-government that inculcates digital democracy, online citizen participation, and online public discussion along with the aspects of online public service delivery.

10.

Conceptual study of utilizing digital technologies in governance at all levels.

11.
Refers to the use of ICTs by government, civil society, and political institutions to engage citizens in political processes and to the promote greater participation of citizens in the public sphere.
12.
Governance (the exercise of political authority and the use of institutional resources to manage society's problems and affairs) of information and communication technologies and their use
13.
Electronic Governance is the application of Information and Communication Technologies (ICTs) for delivering government services through integration of various stand-alone systems between Government-to-Citizens (G2C), Government-to-Business (G2B), and Government-to-Government(G2G) services. It is often linked with back office processes and interactions within the entire government framework. Through **e-Governance**, the government services are made available to the citizens in a convenient, efficient, and transparent manner.
14.
ICT-enabled management of an SES whose domain is limited to a national/federal one, including e-government as one component, and not necessarily including the executive (strategic) management

15.
It is a network of organizations to include government, non-profit, and private-sector entities; in **e-governance** there are no distinct boundaries
16.
E-Governance is a network of organizations to include government, nonprofit, and private-sector entities
17.
e-Governance is the public sector's use of the most innovative information and communication technologies, like the Internet, in order to deliver citizens with improved services, reliable information and greater knowledge in order to facilitate access to the governing process and encourage deeper participation (UNESCO). It is a generic term that refers to any government functions or processes that are carried out in digital form over the Internet. Local, state and federal governments essentially set up central websites from which the public (both private citizens and businesses) can find public information, download government forms and contact government representatives.

Ethical Responsibilities of Business Professionals

12 Ethical Principles for Business Executives

Ethical values, translated into active language establishing standards or rules describing the kind of behavior an ethical person should and should not engage in, are ethical principles. The following list of principles incorporate the characteristics and values that most people associate with ethical behavior.

***1*. HONESTY.** Ethical executives are honest and truthful in all their dealings and they do not deliberately mislead or deceive others by misrepresentations, overstatements, partial truths, selective omissions, or any other means.

2. INTEGRITY. Ethical executives demonstrate personal integrity and the courage of their convictions by doing what they think is right even when there is great pressure to do otherwise; they are principled, honorable and upright; they will fight for their beliefs. They will not sacrifice principle for expediency, be hypocritical, or unscrupulous.

3. PROMISE-KEEPING & TRUSTWORTHINESS. Ethical executives are worthy of trust. They are candid and forthcoming in supplying relevant information and correcting misapprehensions of fact, and they make every reasonable effort to fulfill the letter and spirit of their promises and commitments. They do not interpret agreements in an unreasonably technical or legalistic manner in order to rationalize non-compliance or create justifications for escaping their commitments.

4. LOYALTY. Ethical executives are worthy of trust, demonstrate fidelity and loyalty to persons and institutions by friendship in adversity, support and devotion to duty; they do not use or disclose information learned in confidence for personal advantage. They safeguard the ability to make independent professional judgments by scrupulously avoiding undue influences and conflicts of interest. They are loyal to their companies and colleagues and if they decide to accept other employment, they provide reasonable notice, respect the proprietary information of their former employer, and refuse to engage in any activities that take undue advantage of their previous positions.

5. FAIRNESS. Ethical executives and fair and just in all dealings; they do not exercise power arbitrarily, and do not use overreaching nor indecent means to gain or maintain any advantage nor take undue advantage of another's mistakes or difficulties. Fair persons manifest a commitment to justice, the equal treatment of individuals, tolerance for and acceptance of diversity, the they are open-minded; they are willing to admit they are wrong and, where appropriate, change their positions and beliefs.

6. CONCERN FOR OTHERS. Ethical executives are caring, compassionate, benevolent and kind; they like the Golden Rule, help those in need, and seek to accomplish their business objectives in a manner that causes the least harm and the greatest positive good.

7. RESPECT FOR OTHERS. Ethical executives demonstrate respect for the human dignity, autonomy, privacy, rights, and interests of all those who have a stake in their decisions; they are courteous and treat all people with equal respect and dignity regardless of sex, race or national origin.

8. LAW ABIDING. Ethical executives abide by laws, rules and regulations relating to their business activities.

9. COMMITMENT TO EXCELLENCE. Ethical executives pursue excellence in performing their duties, are well informed and prepared, and constantly endeavor to increase their proficiency in all areas of responsibility.

10. LEADERSHIP. Ethical executives are conscious of the responsibilities and opportunities of their position of leadership and seek to be positive ethical role models by their own conduct and by helping to create an environment in which principled reasoning and ethical decision making are highly prized.

11. REPUTATION AND MORALE. Ethical executives seek to protect and build the company's good reputation and the morale of its employees by engaging in no conduct that might undermine respect and by taking whatever actions are necessary to correct or prevent inappropriate conduct of others.

12. ACCOUNTABILITY. Ethical executives acknowledge and accept personal accountability for the ethical quality of their decisions and omissions to themselves, their colleagues, their companies, and their communities.

Computer Crime

Alternatively referred to as **cyber crime**, **e-crime**, **electronic crime**, or **hi-tech crime. Computer crime** is an act performed by a knowledgeable computer user, sometimes referred to as a hacker that illegally browses or steals a company's or individual's private information. In some cases, this person or group of individuals may be malicious and destroy or otherwise corrupt the computer or data files.

Examples of computer crimes

Below is a listing of the different types of computer crimes today. Clicking on any of the links below gives further information about each crime.

- **Child pornography** - Making or distributing child pornography.
- **Cyber terrorism** - Hacking, threats, and blackmailing towards a business or person.
- **Cyberbully or Cyberstalking** - Harassing others online.
- **Creating Malware** - Writing, creating, or distributing malware (e.g. viruses and spyware.)
- **Denial of Service attack** - Overloading a system with so many requests it cannot serve normal requests.
- **Espionage** - Spying on a person or business.
- **Fraud** - Manipulating data, e.g. changing banking records to transfer money to an account.
- **Harvesting** - Collect account or other account related information on other people.
- **Identity theft** - Pretending to be someone you are not.
- **Intellectual property theft** - Stealing another persons or companies intellectual property.
- **Phishing** - Deceiving individuals to gain private or personal information about that person.
- **Salami slicing** - Stealing tiny amounts of money from each transaction.
- **Scam** - Tricking people into believing something that is not true.
- **Spamming** - Distributed unsolicited e-mail to dozens or hundreds of different addresses.

- **Spoofing** - Deceiving a system into thinking you are someone you really are not.
- **Unauthorized access** - Gaining access to systems you have no permission to access.
- **Wiretapping** - Connecting a device to a phone line to listen to conversations.

Hacking

Computer hacking refers to the practice of modifying or altering computer software and hardware to accomplish a goal that is considered to be outside of the creator's original objective. Those individuals who engage in computer hacking activities are typically referred to as "hackers."

The majority of hackers possess an advanced understanding of computer technology. The typical computer hacker will possess an expert level in a particular computer program and will have advanced abilities in regards to computer programming.

Unlike the majority of computer crimes which are regarded as clear cut in terms of legality issues, computer hacking is somewhat ambiguous and difficult to define. In all forms, however, computer hacking will involve some degree of infringement on the privacy of others or the damaging of a computer-based property such as web pages, software, or files.

As a result of this loaded definition, the impact of computer hacking will vary from a simple invasive procedure to an illegal extraction of confidential or personal information.

Definitions of Hacking

The New Hacker's Dictionary, a resource used to elucidate upon the art of computer hacking, has defined the practice through an assortment of definitions:

A hacker may be defined as any person who enjoys exploring the intricacies of programmable systems and how to stretch their capabilities. This definition is held in contrast to a generic computer user, who prefers to access a computer's minimal functions;

One who programs or who enjoys programming, as opposed to those individuals who simply theorize about programming;

An individual who possesses exceptional skill regarding computer programming;

A malicious meddler who attempts to discover and subsequently tamper with sensitive information through poking around computer-based technologies. These individuals are commonly referred to as "network hackers" or "password hackers."

Regardless of the definition, there are unwritten rules or principles that a hacker will ultimately live by. The belief that information sharing is a powerful exercise and that is the ethical duty of hackers to share their expertise through the creation of free software and through facilitating access to information and to computing resources is a fundamental code for which the majority of hackers follow. In addition, computer hacking as a practice revolves around the belief that system-cracking as a hobby or for fun is ethically okay so long as the hacker commits no vandalism, theft, or a breach of confidentiality.

Issues of Computer Hacking

Computer hacking possesses a mixed perception. Due to our reliance on computer technologies and the critical information shared on networks, the art of computer hacking has been skeptically viewed. That being said, there is also a "Robin Hood" mentality attached to the practice, where free programs or facilitated measures have been awarded to the average computer user.

The primary issue attached to computer hacking stems from an individual's ability to access crucial or personal information that is found on a computer network. The ability to retrieve and subsequently tamper with such information will give way to the potential to commit heinous criminal acts.

Ways to Prevent Computer Hacking
Educational institutions must clearly establish use policies and delineate appropriate and inappropriate actions to all individuals who access information via a computer. The use of filters or firewalls may be considered to reduce access to unauthorized software serial numbers and other hacking-related materials.

Cyber Crimes

Cyber-crimes are any crimes that involve a computer and a network. In some cases, the computer may have been used in order to commit the crime, and in other cases, the computer may have been the target of the crime.

Computer Viruses

Computer viruses are computer programs that, when opened, put copies of themselves into other computers' hard drives without the users' consent. Creating a computer virus and disseminating it is a cyber-crime. The virus may steal disk space, access personal information, ruin data on the computer or send information out to the other computer user's personal contacts.

The most common way for a virus to infect a computer is by way of an email attachment. An example would be if you received an email with an attachment. You open this attachment, and the virus immediately spreads through your computer system. In some cases, if the virus is opened by a computer on a system network, such as your place of employment, the virus can immediately be spread throughout the network without needing to be sent via email.

There are numerous reasons that a person would create a virus to send out to another computer or computers. It may be to steal information or money, to sabotage that system or to demonstrate the flaws that the other computer system has. In some cases these viruses are able to be removed from the user's computer system, and in some cases they are not. Therefore, it is easy for us to understand how these viruses cause significant financial harm every year. The punishment for those who damage or gain unauthorized access to a protected computer can be prison time and the repayment of financial losses.

Cyberstalking

Cyberstalking is the use of the Internet or electronics to stalk or harass an individual, an organization or a specific group. There are many ways in which cyberstalking becomes a cyber crime. Cyberstalking can include monitoring someone's activity **realtime**, or while on the computer or device in the current moment, or while they are **offline**, or not on the computer or

electronic device. Cyberstalking becomes a crime because of the repeated threatening, harassing or monitoring of someone with whom the stalker has, or no longer has, a relationship.

Cyberstalking can include harassment of the victim, the obtaining of financial information of the victim or threatening the victim in order to frighten them. An example of cyberstalking would be to put a recording or monitoring device on a victim's computer or smartphone in order to save every keystroke they make so that the stalker can obtain information. Another example would be repeatedly posting derogatory or personal information about a victim on web pages or social media despite being warned not to do so. Cyberstalking has the potential punishment of a prison sentence.

Identity Theft

Identity theft is a form of stealing someone's personal information and pretending to be that person in order to obtain financial resources or other benefits in that person's name without their consent. Identity theft is considered a cyber crime. The personal information stolen can include the person's name, social security number, birth date or credit card numbers. This stolen information is then used to obtain new credit cards, access bank accounts or obtain other benefits, such as a driver's license.

Identity theft is completed by using breaches in the victim's browser security or through **spyware**, which is software placed unknowingly on a person's computer in order to obtain information. Identity theft can also be performed by hacking into computer networks to obtain personal data - sometimes in large amounts. For example, an individual could get your password and obtain your personal information that you entered into *Amazon.com* when you made a purchase in the past. He could then use your birth date and social security number in order to apply for a new driver's license in your name with his picture on it! Identity theft is punishable by a prison sanction.

Ergonomics

Ergonomics (from the Greek word *ergon* meaning *work*, and *nomoi* meaning *natural laws*), is the science of refining the design of products to optimize them for human use. Human characteristics, such as height, weight, and proportions are considered, as well as information about human hearing, sight, temperature preferences, and so on. Ergonomics is sometimes known as human factors engineering.

Computers and related products, such as computer desks and chairs, are frequently the focus of ergonomic design. A great number of people use these products for extended periods of time -- such as the typical work day. If these products are poorly designed or improperly adjusted for human use, the person using them may suffer unnecessary fatigue, stress, and even injury.

Cyber terrorism

What is Cyber-terrorism?

In the wake of the recent computer attacks, many have been quick to jump to conclusions that a new breed of terrorism is on the rise and our country must defend itself with all possible means.

As a society we have a vast operational and legal experience and proved techniques to combat terrorism, but are we ready to fight terrorism in the new arena – cyber space?

A strategic plan of a combat operation includes characterization of the enemy's goals, operational techniques, resources, and agents. Prior to taking combative actions on the legislative and operational front, one has to precisely define the enemy. That is, it is imperative to expand the definition of terrorism to include cyber-terrorism.

As a society that prides itself on impartiality of justice, we must provide clear and definitive legislative guidelines for dealing with new breed of terrorism. As things stand now, justice cannot be served as we have yet to provide a clear definition of the term. In this light, I propose to re-examine our understanding of cyber-terrorism.

There is a lot of misinterpretation in the definition cyber-terrorism, the word consisting of familiar "cyber" and less familiar "terrorism". While "cyber" is anything related to our tool of trade, terrorism by nature is difficult to define. Even the U.S. government cannot agree on one single definition. The old maxim, "One man's terrorist is another man's freedom fighter" is still alive and well.

The ambiguity in the definition brings indistinctness in action, as D. Denning pointed in her work Activism, Hactivism and Cyberterrorism, "an e-mail bomb may be considered hacktivism by some and cyber-terrorism by others"

It follows that there is a degree of "understanding" of the meanings of cyber-terrorism, either from the popular media, other secondary sources, or personal experience; however, the specialists' use different definitions of the meaning. Cyber-terrorism as well as other contemporary "terrorisms" (bioterrorism, chemical terrorism, etc.) appeared as a mixture of words terrorism and a meaning of an area of application. Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California, who in 1997 was attributed for creation of the term "Cyberterrorism", defined cyber-terrorism as the convergence of cybernetics and terrorism. In the same year Mark Pollitt, special agent for the FBI, offers a working definition: "Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub national groups or clandestine agents."

Since that time the word cyber-terrorism has entered into the lexicon of IT security specialists and terrorist experts and the word list of mass media "professionals". One of the experts, a police chief, offers his version of definition: "Cyber-terrorism – attacking sabotage-prone targets by computer – poses potentially disastrous consequences for our incredibly computer-dependent society."

The media often use cyber-terrorism term quite deliberately: "Canadian boy admits cyberterrorism of his family: "Emeryville, Ontario (Reuter) - A 15-year-old Canadian boy has admitted he was responsible for months of notorious high-tech pranks that terrorized his own family, police said Monday"

A renowned expert Dorothy Denning defined cyber-terrorism as "unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives". R. Stark from the SMS University defines cyber-terrorism as " any attack against an information function, regardless of the means"

Under the above-mentioned definitions of cyber-terrorism one can only point to the fact that any telecommunications infrastructure attack, including site defacing and other computer pranks, constitute terrorism. It means that cyber-terrorism has already occurred and we "live " in the epoch of cyber terror.

However, another expert, James Christy the law enforcement and counterintelligence coordinator for the DIAP (Defense-wide Information Assurance Program), which is steered by the office of the assistant secretary of defense for command, control, communications and intelligence, states that cyber-terrorism has never been waged against the United States. "Rather, recent hacking events – including a 1998 web page set up by a supporter of the Mexican Zapatistas rebel group, which led to attacks on the U.S. military from 1,500 locations in 50 different countries – constitute computer crime. William Church, a former U.S. Army Intelligence officer, who founded the Center for Infrastructural Warfare Studies (CIWARS) agrees that the United States has not seen a cyber terrorist threat from terrorists using information warfare techniques. "None of the groups that are conventionally defined as terrorist groups have used information weapons against the infrastructure" Richard Clarke, national co-ordinator for security, infrastructure protection and counterterrorism at the National Security Council offered to stop using "cyberterrorism" and use "information warfare " instead

The above-mentioned observations drive a clear line between cyber-terrorism and cybercrime and allow us to define cyber-terrorism as: **Use of information technology and means by terrorist groups and agents.**

In defining the cyber terrorist activity it is necessary to segment of action and motivation. There is no doubt that acts of hacking can have the same consequences as acts of terrorism but in the legal sense the intentional abuse of the information cyberspace must be a part of the terrorist campaign or an action.

Examples of cyber terrorist activity may include use of information technology to organize and carry out attacks, support groups activities and perception-management campaigns. Experts agree that many terrorist groups such as Osama bin Ladenn organization and the Islamic militant group Hamas have adopted new information technology as a means to conduct operations without being detected by counter terrorist officials.

Thus, use of information technology and means by terrorist groups and agents constitute cyber-terrorism. Other activities, so richly glamorized by the media, should be defined as cybercrime.