Cyber security Challenges in Enterprises - A Socio-Organizational Approach -Cybercrime as a model –

Yamina Ghaddab[1]

[1] University of Mohamed Lamine Debaghine – setif 2 (Algeria), minagh87@gmail.com

Abstract:

Cybercrime is one of the most important and attractive topics especially for researchers, scholars, social scientists, and cyber-security specialists, due to its negative impact on individuals as well as institutions, it can also cause significant financial and material loss. This made some institutions allocate large sums of money to establish cyber-security, protect their reputation and its properties and components, maintain their position in the labor market, also their relationship with their customers and suppliers.

Therefore, this research focused on cybercrime because of its spread in both local and international communities posing a threat to the most important and largest economic institutions, and sometimes even to social organizations, as it is carried out by a technocratic group composed of technicians who are capable of computer science and have extensive knowledge in information field. This study came within the framework of theoretical and analytical based on the descriptive approach to suit the analysis, diagnosis, and understanding of the phenomenon and come up with preventive recommendations and other corrective treatment directed to the parties threatened by this type of crime.

Keywords : cybercrime, cybercriminal, information, cyber Security, institutions.

Tob Regul Sci. ™ 2023;9(1): 3047-3065
DOI: doi.org/10.18001/TRS.9.1.212

1. Problematic:

Technological development has led to the emergence of the latest technologies which have become necessities of daily life for the public and private members of society and its institutions due to their high speed in giving information and processing data, which made it the subject of attracting many who need its various advantages, but mastering the use of these techniques and means for some is a curse on others, when they abandon morals and valuable principles in dealing and exploit them unjustly to harm others with various risks and criminal behaviors that threaten their existence as a social entity or Thus, many crimes appeared, including cybercrime, which represents a criminal activity carried out by certain means such as computers and smart phones, to achieve certain goals at the expense of others or to harm them by adopting certain information to facilitate the criminal process, which formed a focus and issue that occupied those interested and researchers, and prompted them to try to find the most important strategies by which to confront this phenomenon.

Cybercrime often represents a risk that causes losses to the economy and institutions that represent the vital infrastructure of countries, as a report (sponsored by McAfee) revealed in 2014 that the annual damage to the global economy was 445 billion$, and nearly 1.5 billion$ was lost in 2012 due to online credit and open credit fraud within the United States. In 2018, a study by the Center for Strategic and International Studies (CSIS), in partnership with McAfee, indicated that 600 billion$, a fraction of global value, is lost to crime annually. (GIRI, 2019, p664)

Studies conducted by the Stand Ford Research Institute show that the new generation of cybercrime professionals are often young people between the ages of 25 and 45 years, and statistics in this area show the following:

25% of cyber fraud or cybercrime are committed by the analyst, 18% of these acts are committed by the programmer, 17% are committed by the user who has ideas for information systems, 12% are committed by a foreigner from the place where the information systems are located, and 11% of these acts are committed by the operating technician.(Momani,2008, p85).

As a result of the spread of this modern criminal phenomenon, the security of the information infrastructure has become one of the major concerns of institutions, whether in the public or private sector, to put technical barriers and take measures to combat harmful content committed through information and communication technologies, especially the Internet, to protect intellectual property rights and personal data, and strengthen electronic transport security.

Through the previous proposal, we put the following questions:

* What is cybercrime?

* What are cybercrime risks to institutions?

* What is cyber-security, and what are the ways to enhance it?

2. Basic Concepts of Study:

2.1 Cybercrime:

There are several names given to this crime, which are as follows:

* Cyber or electronic crime.

* Computer or Internet crimes.

* Internet crimes.

* High-tech crimes.

* Electronic terrorism. (Al-Afifi, 2013, p8)

- The term cybercrime refers to illegal acts where a digital device or information system is either a tool, a target, or a combination of the two. The term cybercrime can be used interchangeably as either cybercrime, cybercrime, high-tech crime, information age crime, cybercrime, computer-related crime, or digital crime. (SABILLON et al, 2016, p166)
- Therefore, it is an act or incident whose physical pillars include cybercrime that involves a computer, network, technology, and new devices, and the computer here may be used as a weapon for crime, or it may be a target in addition to technology and system. Some forms of cybercrime have become prominent, especially those involving piracy, copyright infringement, unjustified mass surveillance, piracy of software packages, possession of outlaw material, false mail, defamation, and grooming of children. (GIRI, 2019, p664)
- Baumard defines it as the use of digital, electronic, or software capabilities to illegally mislead, convert, destroy, or exploit public or private information systems. (Baumard, 2014,p41).
- The Tenth United Nations Congress on the Prevention and Punishment of Offenders, held in Vienna in 2000, defined cybercrime as: "any crime that can be committed on a computer system or network, and in principle includes all crimes that can be committed in an electronic environment". (Abdel Gawad,2020,p393)

2.2. Cyber-security:

One of the main terms in digital knowledge is the term "cybernetic", which is derived from the Greek term kybernetes, which means pilot, helmsman, or ruler, and the modern derivation indicates that the word cyber includes feedback mechanisms that allow command and control functions in closed systems... The study of cyber is associated with many diverse disciplines, but the English word cyber is commonly used in the field of information and communication technologies such as cyberspace. (B. Seel: Warad, 2017, pp21,22)

From the academic point of view, information security means the science that examines theories and strategies to protect information from the dangers that threaten it and from the attack on it, the technical point of view it is the set of means, tools, and procedures necessary to ensure the protection of information from various internal and external dangers.(Yaish Tammam,1st Edition, 2019, p14)

For institutions, the term cybersecurity is referred to a set of modern technologies and systems that aim to protect networks, electronic systems, and modern technological tools for institutions and various sectors to reduce cyber-attacks unjustly. (Belacel.B.N&Amrouche, 2021,p165).

2.3. Information Technology

Information technology focuses on technologies related to the acquisition and transfer of information to obtain the best decisions necessary to introduce new products and services and includes the process of collecting, processing, and distributing appropriate information, especially computer-based technologies. (DeifAllah, 2016-2017, p80)

UNESCO defines information technology (1992) as: "the application of electronic technologies, including computers, satellites and other advanced technologies, to produce, store, retrieve, distribute, and transmit analog and digital information from one place to another". (Badi, 2004-2005,p72).

2.4. Internet:

It is considered an important and necessary element in the implementation of cybercrime due to the advantages it offers, and can be defined as follows:

- **Ahmed Al-Kasibi defined it as:**"A group of information networks that are considered one of the most important and largest information networks in the world; they are a group of networks connected, and allow the free exchange of information between the networks of large institutions and even the smallest private and personal networks.(Deifallah, 2016-2017, p105).
- The Internet is not a network in the traditional sense known, but rather a connection of thematic networks LAN distributed and scattered all over the world, these networks exchange information among themselves through the TCB / IP ceremony, and the TCB / IP ceremony developed in 1992, which was adopted globally as a measure of information exchange, this ceremony was introduced due to its effectiveness mainly in universities and research institutes, through which the different objective networks of origin were linked with the superior computers that were in Over the years, these objective networks have already been linked to each other to be the largest network spread in most parts of the world, which is known to be called the Internet. (Abbas, 2004, p91).
- Skyker defined it as: "It is the Wide World Web that connects a huge number of computers and uses in the process of linking various means of telecommunications such as telephone lines, private lines or satellites, and the Internet extends around the world to form a huge international network for the exchange of information." (Skiker, 2010, p28).

2.5. Information:

- Informatics is the science of logical dealing with information, and it has control rules and governing texts and organization for the use of its systems. Information is a set of symbols, facts, concepts, or instructions that are suitable to be the object of exchange and communication or for interpretation and interpretation or processing, whether it is done by individuals or by electronic systems. Information is flexible so that it can be changed, fragmented, collected, or transferred by different means and forms. (Skiker, 2010,p12)
- It is also defined as: "It is all types of data that have been collected by observation, observation or codification, whether audible or visual, it is characterized by being processable by computer techniques and available information mechanisms, so it turns into a discourse that carries a knowledge connotation that can be changed

and deliberated, ensuring that the parties that use it acquire knowledge and facts that can be invested in various fields of contemporary activities". (Al-Kaabi,nd,p 718)

➢ The term data and information is used interchangeably, but it is important and useful to distinguish between the two terms, data is the raw materials that when processed produce manufactured goods that are information, and on this basis, we can define information as data that has been converted into a meaningful image and usable by the last beneficiary, and data is usually worthless until after it is converted into information and this is done through: Processing it, analyzing its content, and then placing it in a way that enables humans to use it, and therefore we must look at the information as processed data and placed in a way that gives it value to the end user. (Sabbagh, 2000, p19)

2.6. Information System:

The information system is an integrated set of components for collecting, storing, and processing data and delivering information, cards, and digital products. Commercial companies and other institutions rely on information systems to implement and manage their operations, interact with their customers and suppliers, and compete in the market. (Berisha–Shaqiri,2014,p19), All this is done within the institutional and social framework of society, although the general interest in the field of information systems is the development, use, and impact of information systems in institutions and society. However, it is not primarily concerned with the technical and computational aspects of information technology. It's about how technology is customized and created to meet the needs of different actors – such as individuals, groups, or institutions – with the information and requirements that enable them to achieve their specific goals. (Boell & Cecez-Kecmanovic,2015,p4959)

From a social point of view, it is humans who use the information system, interpret the information generated by the system, create meaning and take action, and make IT outputs meaningful and actionable. It is a human activity that enables institutions to deploy information technology to achieve their goals, which are part of future development strategies. What is important in these processes are the sociocultural contexts, social structures, and power structures in which the information system is integrated and in which its output becomes meaningful and used with influences Especially. Thus, the information system, its meanings, and its use are socially determined. (Boell & Cecez-Kecmanovic, 2015, P4962)

* Through these concepts we conclude that:

Cybercrime is a set of illegal behaviors, behaviors and acts that are carried out by a person specialized in the field of information, software and information technology ; it is called the information criminal, relying on a set of modern and advanced technical devices, the most important of which is the computer, where it is equipped with professional programs in sabotage, hacking and hacking the cybersecurity system, and it is connected to the Internet so that it can access the database of any institution wherever it is located Geographer across the world, with the aim of sabotaging its information system and destroying its data in order to cause financial, material and moral damage and losses such as defamation of the institution in question, to achieve the ultimate goal, which constitutes the main starting point in carrying out this cybercrime, whether to achieve a personal purpose or for the benefit of other parties in exchange for large sums of money or other offers that serve the interest of the cybercriminal.

3. The Components of Information Systems in Institutions:

Each system consists of a set of components, and each component plays a key role in support with other components to serve the general goal for which the system was established and established, and the information system in institutions is based on a set of components:

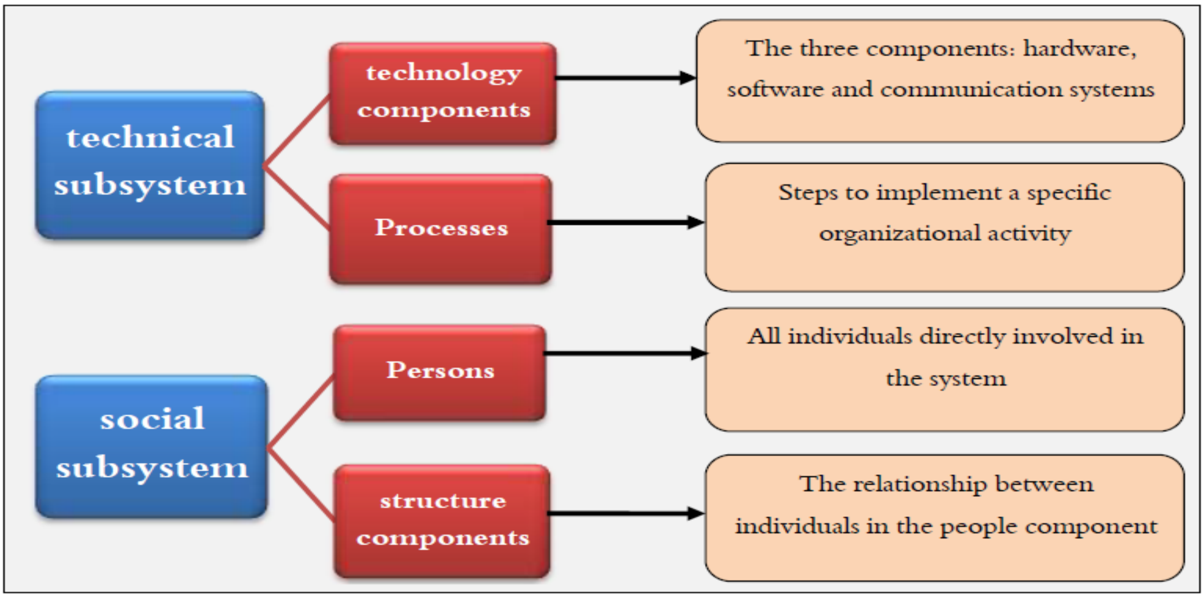
It is defined as: "a socio-technical system comprised of two sub-systems:

- ❖ Technical sub-system and social sub-system. The technical sub-system includes technology components and processes.
- ✓ Information Technology Component: consists of three elements: hardware, software, and communication systems.
- ✓ Processes: It is the set of steps used to carry out a specific institutional activity, by specifying the actions that an individual, group, or institution must perform.
- ❖ Social subsystem: includes people and components of the structure.
- ✓ The structure component (or organizational structure) refers to the relationship between individuals in the people component. (Piccoli & Liu, 2007, pp 20-22)
- ✓ People component: All individuals involved in information systems. From frontline help desk staff to systems analysts, to programmers, to chief information officer (CIO). (Bourgeois,2014, P7)

The following figure illustrates the basic components of the information system and the relationships between them:

Figure (1): Information Systems Components.

Source: (Prepared by the researcher)


technical subsystem
technology components
Processes
The three components: hardware, software and communication systems
Steps to implement a specific organizational activity
social subsystem
Persons
structure components
All individuals directly involved in the system
The relationship between individuals in the people component

Through the diagram shown above, it is clear that the social system is focused on the human resource, whether through its existence as a social entity or through the relationships on which it is based in communication and various interactions to achieve the goal of the economic entity represented in the institution, as it is the one who controls the technical system, manages it, makes adjustments to it or changes parts of it, according to what is commensurate with serving the general goal for which the institution was established, which is often a two-fold goal: A related part to the organizational entity of the institution through the pursuit of expansion, development and domination and another part related to society through the social responsibility of the institution, and the pursuit of achieving the requirements of society and joining the ranks of developed countries, after the establishment of the organizational structure, individuals determine the general objectives and on the basis of which the processes that must be accomplished are determined and according to which information technologies and devices are determined to assist in that of software and communication devices.

4. Elements of Cybercrime in Institutions:

It is not possible to occur any crime in a specific scope or field without the availability of a set of elements, each element has an important complementary role to the other elements, and crimes targeting institutions are directed to inflict specific damage that may be material or moral, and their elements vary according to the type of crime and the specific goal from the beginning, so the elements that cause electronic crime in an institution are:

4.1 Institutions:

The institution is considered an element of cybercrime, there can be no crime without the presence of a victim, and the victim here is the institution on which the criminal act is located to damage its information system and database. Where the enterprise is considered as an abstract product that combines the appropriate factors of production in the industrial economy, seeks to achieve goals, and is subject to market and environmental control, Marcel Capet says the institution as a production group includes: human, autonomy, with heritage, the impact of the environment, and its future depends on the sale of products obtained through its activity.(Khémiri, nd, P12) is "an institution that produces, transforms, and sells goods or services to meet the needs of other institutions, communities, and individuals" (BETTAHAR, 2014,P3). By projecting on Algerian institutions, they must not be limited to simple implementation functions but must become in areas where they serve as a better-equipped and more participatory structure, and an independent decision-making center that determines the objectives of its activity and the means necessary to achieve them.(TCHAM, 2010, p4)

4.2. Cybercriminal:

It is considered directly responsible and the main element in the commission and implementation of criminal behavior and acts related to cybercrimes in institutions. He has technical skills and knowledge of computer system technology, so the personality of the information criminal, whether a natural or legal person and the mechanism of committing the crime makes him a person with special features added to the other qualities that must be available in the ordinary criminal. (Al-Magsodi, 2015, p24), and he is also a technocrat with a deep understanding of the Internet and computers, so technology is his weapon in committing cybercrime. It can take seconds or a few minutes to hack websites or carry out online scams. Cybercrime also does not define any geographical boundaries or distances. This enables a cybercriminal in one corner of the world to commit hacking on a system in another corner of the world. The act of cybercrime from preparation to execution occurs in the information space (cyber), which makes cybercriminals physically exist outside it. (Tubake, 2013, p130) In the different specialists in the definition of electronic crime, a sect focused in its definition of it by focusing on the person of the offender and the extent of technical and technical know-how of information systems, and then defined cybercrime as: "that crime carried out by a person who has special knowledge of computer technologies and information systems." (Abdel Gawad,2020, p392). Due to the superior capabilities and depth of technical knowledge that characterizes the cybercriminal, in contrast to the lack of experience and competence of the security and judicial agencies, this prompted some countries that are unable to deal with electronic crimes to cooperate with some criminals called "hackers": "A person who has skills or knowledge of the tactic used in the electronic computer system and can use this tactic to penetrate the secret code to change information, to implement programs, or to convert from computers by using the computer itself" to uncover the mystery of some crimes. (Baghdadi, 2018, p15)

4.3. The Electronic Device and How to Use it:

One of the characteristics that distinguishes cybercrime from traditional crime is the modernity of the means used to commit it, of which the computer or computer is one of the most important.

The electronic device is the tool of the crime and the means of its implementation, or it is the subject of the crime, such as the destruction or theft of data and information, and here the problem arises, but if the subject of the assault is the device itself, its screen or the physical entities of the computer, here the traditional criminalization texts are sufficient. Practical reality has proven that cybercrimes may be committed through mobile phones, especially after the emergence of smartphones, which are small computers, through which the Internet is connected, where it is easy to store and transfer information.(Al-Afifi,2013,p15). Because of the importance of these devices in committing a criminal act, a group of specialists has focused on them in defining cybercrime as "all types of illegal behavior committed by the computer or with its assistance or to be a major tool in its commission, or has an important positive role in this commission." Illegal, or any act or omission that would infringe on material or moral funds resulting directly or indirectly from the interference of information technology, or advanced technology of development systems. (AbdelGawad, 2020, pp391,392)

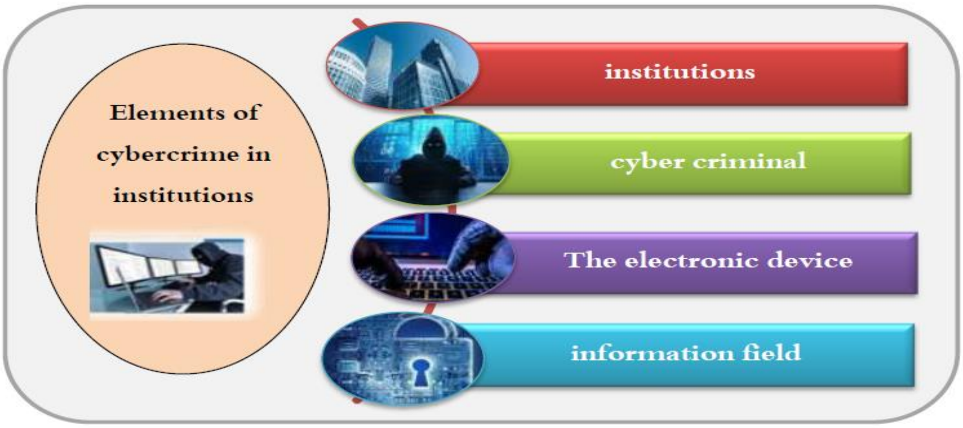
4.4. Information Domain:

It is not possible to say that the crime occurred unless it was done with certain facts, and any crime that occurs cannot be described as a cybercrime unless it takes place in the information field, so some specialists focused on defining it: "Based on the place of the crime, it is very illegal behavior or activity related to copying, changing or deleting data or information stored within the system or accessing it or those that are transferred through it or is every illegal behavior or activity directed to automated data processing or transfer".(Abdel Gawad,2020, p392). Despite the advantages of the computer age in speed, accessibility, and functionality, not being properly controlled enables individuals and institutions to easily spy on or interfere with computer operations from remote locations to serve bad purposes, and to carry out sabotage or fraud (Broadhurst & Chang,2013,p49). The ability of information technology to shorten distances and strengthen the link between different parts of the world has led to a reflection on the nature of criminal acts in which criminals use these technologies in breaking the law, which means that the crime scene is no longer local but global. (Baghdadi, 2018, p12), Cybercrimes are unrestricted crimes linked to a specific geographical area, as they cross borders and distances and are committed by computers and through the information network.(AL-Hawamdeh,2016-2017,p9).

The ease of movement of information through modern technology systems makes it possible to commit a crime through a computer located in a particular country, while the criminal act is achieved in another country, the information society does not recognize the geographical borders of countries, because it is a society of opening through networks that penetrate time and space and are not subject to certain borders that stop them, there are no visible or tangible borders that can stand in front of the huge flow of information through computers and networks, and the place is always not an obstacle to its commission, as the perpetrators of these crimes do not need to obtain entry visas For countries, from multiple places and different countries, the criminal act may be committed (Hasnia,2017,p9), where the criminal is in one country and the victim is in another country, and the damage may have occurred in a third country or in several countries, such as: hacking and destroying devices and sites, and stealing data, information and money, all of which made the fight against cybercrime difficult, due to the multiplicity of places related to crime.(Al-Afifi,2013, pp15,16), In addition to the difficulty of detecting them, and proving their evidence, and this is due to the relationship of this type of crimes with the technical character that gives these crimes a lot of complexity and difficulty in proving, and establishing evidence of who commits them (AL-Hawamdeh,2016-2017, p11), and this confirms the seriousness of this type of crimes on institutions that lack or reduce the percentage of information security, as they are vulnerable to information penetration at any moment when criminals have the opportunity to access their information system or infiltrate their database because pushing A button in a country sufficient to bankrupt institutions and lay off a large percentage of workers in other countries, and this is the essence of the difference from traditional crime in terms of not being affected by the space-time circumstance, traditional crimes can be confronted with human security and defense by means of physical protection, while cybercrime requires protection and immunity of institutions by providing and adopting technical means and tools such as protection programs and information security, and the following figure shows the elements of cybercrime on institutions:

Figure (2): The elements of cybercrime in institutions

Source: (Prepared by the researcher)



5. Types of Cybercrime in Institutions:

Because of cybercriminals 'interests to be achieved, such as embezzlement of huge amounts of funds, destroying the name of the institution and its reputation in the market, achieving other personal interests, or implementing a request or order that serves other parties, in addition to the diversity of gaps that facilitate their implementation, such as the lack of mechanisms to control criminal operations, and the means to combat and eliminate them or address them, this phenomenon has worsened to turn into the most serious obstacle that challenges the existence of institutions and stands in the way of achieving their goals, especially as it is embodied in Several models and forms, the most important of which are:

- **Hacking**: means the unauthorized control or access to the computer system and the act of hacking that destroys data as well as computer software.
- **Password sniffing:** Through programs that monitor and record the name and password of network users when logging in to the site... (Kaur,2018,p437)
- **Phishing:** It is a method of stealing personal data where an authentic-looking email appears as if it is coming from a real company or institution, and the idea is to trick the recipient into sending confidential information such as account information or login data to the fraudster. (Alansari et al. 2019, P10).
- **Denial-of-service attacks:** Attackers target a site or service hosted on high-profile web servers such as banks, credit card payment gateways, and mobile networks..., where denial-of-service attacks are designed to consume resources so that other users cannot use the resources and that is "denial of service".
- **Virus attack:** A computer virus is a malicious program that repeats when executed by inserting copies of it into other computer programs or data files in your hard drive.
- **Email bombing**: refers to sending a large number of emails to the victim to crash the victim's email account or crash the server.(Kaur,2018, p437), in addition to sending spam over the Internet, for advertising, phishing, spreading malware, etc. (Alansari et al. 2019, P10)
- **Salami attack:** These attacks were used to commit financial crimes. The key here is to make the change so small that in one case it goes completely unnoticed, for example, when a bank employee inserts a program into the bank's servers that deducts a small amount from each customer's account.
- **Logic bomb:** A piece of code that is intentionally inserted into a software system that will perform a malicious function when certain conditions are met. For example, a programmer might hide part of the code that starts deleting files if they are terminated from the institutions.
- **Trojans:** Trojans are email viruses that can copy themselves, steal information, or damage a computer system. (Kaur,2018, pp:437-438)

6. Chronology of Cybercrimes in Institutions:

The first recorded cybercrime occurred in 1820, when Joseph-Marie Jacquard, a textile maker in France, produced the loom. This device allowed one to repeat a series of steps in weaving special fabrics. This led to Jacquard staff fearing that their traditional work and livelihoods would be threatened. They committed acts of sabotage to dissuade "Jacquard" from more use of new technology. To be the first recorded cybercrime.(Subha & al, 2015, p351)

With the development of means and techniques and the spread of information that has become the capital of developed countries, the so-called information society has emerged and the type of crimes has evolved with it and has become focused on hacking databases, stealing important information, or damaging devices to damage institutions, and one of the most important cybercrimes that occurred and caused serious losses to institutions, we find as shown according to a chronological sequence in the following table:

Table (1): The most important cybercrimes from 2011 to 2014.

Date	Target	Type of attack	Loss
2011	Citigroup	Hacking the system of the company	2.7 $ million Dollar
			Theft over 200,000 customer sensitive information
2011	Citi Bank	Individual hackers	Over 2.7 $ million Dollar
			customer data Loss
2012	- USDJ (United States Department of Justice) - FBI (Federal Bureau of Investigation) - RIAA (Recording Industry Association of America) - MPAA (Motion Picture Association of America) - IFPI (International Federation of the Phonographic Industry)	Hacking website Defacement	Website downtime
			Loss of reputation
2014	Sony	Attacked by hackers called Guardians of Peace	Caused companywide shutdown of computers
			Leak of corporate information such as: salaries and bonus of executives and the security numbers of employees

Source:(Alansari et al.2019, PP 10,11)

The crimes did not stop there, but they are in continuity, and one of the most important institutions targeted by these cybercrimes not long time ago, according to what was reported on December 29, 2021 on the website of "**The Herjavec Group**" security software company, which dates back to the establishment of "Robert Herjavec"(Herjavec, 2021, December 29)

- 2015: American health insurance company Anthem reported the theft of personal information of up to 78.8 million customers.
- 2017: Wanna Cryis the first known example of ransomware running via (a virus that replicates and distributes itself), targeting a vulnerability in older versions of the Windows operating system**.** Within days, tens of thousands of companies and institutions in 150 countries shut down their systems with WannaCry encryption. The attackers demanded $300 per computer to unlock the code.
- 2019: A telemarketing employee in particular obtained 1.1 million pieces of data, including customer contact information, of Chinese e-commerce company Alibaba and leaked it to a distributor during a singles' shopping festival on November 11.
- 2020: SolarWinds – A cybersecurity company FireEyesays it was the victim of a nation-state attack. The security team reported the theft of their Red Team toolkit, which contains apps used by ethical hackers in penetration tests. The researchers also found evidence that the attackers entered a backdoor in the SolarWinds program. "Trojan" SolarWinds Orion business software updates for malware distribution.
- 2021: Accenture's networks are hacked by the LockBit ransomware gang, which encrypted the files and demanded $50 million to avoid selling their encrypted files on the dark web.
-

7. Cybercrime Risks on Institutions:

"Unless we can secure our information or electronic infrastructure, all a criminal needs to disrupt our economy and put our lives in danger, simple clicks on the computer and connect via the Internet, the mouse can now be more dangerous than a bullet or a bomb," said Lamar Smith, chairman of the subcommittee responsible for crime and the US Congress to demonstrate the economic loss that the United States may suffer as a result of cybercrime. The indicators highlight the increase in the losses of cybercrime, especially in countries that rely heavily on information technology systems. (Momani,2008, p68).

This information technology has also been adopted in various institutions of different activities, due to its advantages in facilitating various transactions, its ability to reduce time, shorten distances, speed of data processing, and its large capacity in storing huge numbers of it and ease of retrieval when needed. However, these technologies carried with them in parallel with the positives a set of negatives that reflected on the institutions that adopt them and the customers and consumers they deal with, and their harm was not limited to countries only, and the following table shows the top 10 consumer countries and the top 10 countries with institutions and companies affected by cybercrime through the number of complaints filed against this type of crime in 2013, according to statistics contained in the Information Economy Report of the United Nations Conference on Trade and Development issued in 2015.

Table 2: complaints number from the top 10 websites of consumers and companies' victims of cybercrime in 2013:

Top Consumer locations	**Number of complaints**	**Top Corporate locations**	**Number of complaints**
United States	13445	United States	4731
Australia	1914	China	3996
France	1100	United Kingdom	1213
United Kingdom	767	India	469
Canada	694	Canada	285
Brazil	555	Australia	264
Israel	448	France	246
Argentina	341	Germany	220
India	311	Mexico	158
Spain	295	Spain	144

Source:(UNITED NATIONS, 2015, P71)

Through this table, we note the high volume of the seriousness of cybercrimes, which is evidenced by the increase in the number of registered complaints. Cybercrimes pose a threat to institutions because their damage is serious and profound, up to disrupting or damaging the institution's database, distorting its reputation, and losing leadership, which leads to the loss of customers and dealers, and the percentage of its profits decreases, and this leads to a decline in its market share, and thus, according to our point of view, the institution finds itself in front of two solutions:

The first solution is: to cover up crimes for fear of a decline in their reputation due to the loss of confidence of their customers in their inability to secure and protect their data, and their information, especially if it comes to some sensitive or important personal data, and financial account numbers, which facilitates their embezzlement, and thus incur the losses of cybercrimes that affected them in addition to bearing the losses of correction and re-standing again or changing the field in which they are active, which requires them to reconstitute a database with new data and information and work to maintain them and make them safer from exposure to cybercrimes.

As for the second solution, some institutions choose it compulsively if the first solution is not valid and does not correspond to their available conditions, which are: to declare their loss, lay off workers, and sell their market share to one of the competitors, thus erasing and disappearing as an economic entity due to its inability to rebuild itself, as well as the lack of financial sources from which other costs such as workers' salaries, raw materials costs, and input transfers are deducted, and then taken out in the form of services. And goods and marketed to customers, thereby completely withdrawing from the labor market. This has made cybercrime a threat that worries all countries with their various institutions and the diversity of sectors in which they operate, as it directly threatens their economy.

8. The Necessity of Cybersecurity in Institutions:

Cybersecurity has become an imperative necessity dictated by the reality of development in the technological and information field to address various cybercrimes that threaten institutions.

Protection is by following an information system that protects the assets, resources, and gains of the institution in legitimate ways, and it is a tool that controls the institutions of relations and communications, without affecting the ability of users of this system to perform or hinder their work in terms of efficiency or timing, and information protection is not prevention from system penetrations, but it limits them if they are strong, effective and accurate, and if these conditions are met and breached, it is:

- ✓ Hard for the hacker.
- ✓ It takes a long time.
- ✓ It is easy to detect before or after success. (Ahmed Messaoud,2012-2013,p17)

Therefore, cybersecurity is a basic strategic priority for the development of institutions, and the information systems and information they process are protected by two means:

First: Technical protection of systems.

Second: The legal protection of these systems by enacting legislation that regulates the crimes that target them by attacking them or using them as a tool to commit other crimes. (Ahmed Messaoud, 2012-2013, p16).

➢ **This protection and cyber security are embodied and required by each part of the institution's information system, as follows:**

1. Information Security: It is related to information that is the basis or objective of the existing information system.

2. Security of access to systems: It includes procedures for securing access control operations for the information system itself, and controlling the applications on which the facility's information system operates.

3. Information systems software security: It is the process of protecting the programs that run or are based on the information system itself.

4. Telecommunications Security: It is the process of securing the means of communication on which the establishment relies in its functional work. (Ahmed Messaoud, 2012-2013, p17)

9. Conclusion:

In conclusion, it can be said that for institutions to achieve their goals in the short and long term, expand their market share, increase their profit rate, spread at the global level, as well as contribute effectively to economic development, they must update their organizational structure, use the best material and technical means and information programs and open up to foreign markets to keep pace with developments at the global level, and in return train employees to use these means and developments to ensure that they benefit from the advantages of these technologies and programs and thus facilitate the various Operations related to the activities assigned to them and the tasks entrusted to them, not forgetting the need to secure the negative side of these technologies that result from the developments of the information field, the most important and most prominent of which is cybercrime, and to avoid its dangers, the study proposes some recommendations, as follows:

- ✓ Work on training the competent authorities in the investigation and inference of modern techniques used by criminals in committing cybercrimes, to be able to detect and confront them.
- ✓ The obligation to report cybercrimes to institutions so that covering them up does not constitute an incentive that encourages cybercriminals to continue their criminal acts, in addition to declaring the percentage of damages and the size of the losses resulting from these crimes so that other institutions can take the necessary measures to guard against exposure to them.
- ✓ The acquisition of the latest technologies and programs capable of providing protection for various information and the database from penetration and piracy, taking into account the updating of each time the developments that occur in this field coinciding with the development of viruses and the methods adopted by criminals to penetrate the components of the information system, to ensure comprehensive and permanent cybersecurity.
- ✓ Coordination between the various authorities and bodies specialized in the field of digitization, and the creation of a strong arsenal of protection programs and encrypted passwords are characterized by the difficulty of dismantling the immunity of the database of institutions from cybercrime and preserving it from piracy or destruction.

- ✓ Not to enable any individual in a particular department o of the institution to identify or view the password of the database of another department of the institution, and make it the monopoly of those who are directly concerned with it, to avoid data sabotage in the event of internal organizational conflicts between employees in various departments.
- ✓ The institution saves a backup copy of the database and stores it in a safe place so that it is easy to refer to it if the first database is damaged by cybercriminals.
- ✓ Organizing training and training courses for individuals working in the institution on how to deal with and control digital data, to shorten the time and effort in correcting the percentage of damage caused to the database and treating it as soon as possible and at the lowest cost.
- ✓ Enacting penal laws to deter perpetrators of cybercrimes, protect the database and data of institutions, and ensure the implementation of penal sentences.

Bibliography:

1. Abbas, Tarek Mahmoud. (2004). Digital Information Society. First Edition. Al-Aseel Center for Printing. Publishing and Distribution. Cairo. Egypt.
2. Abdel Gawad, Amira Mohamed Abdel Azim. (2020). Cyber Risks and Ways to Confront Them in Public International Law. Journal of Sharia and Law. Issue 33, Part 3.
3. Ahmed Messaoud, Mariam. (2012-2013). Mechanisms for Combating ICT Crimes in the Light of Law N° 09/04. Memorandum submitted to obtain a master's degree. specialization: Criminal Law. Faculty of Law and Political Science. Kasdi Merbah University. Ouargla.
4. Al-Afifi, Youssef Khalil Youssef. (2013). the electronic crimes in the Palestinian Law (A comparative analytical study). a memorandum submitted to obtain a master's degree in public law from the Faculty of Sharia and Law at the Islamic University of Gaza. Palestine.
5. Alansari, M. M., Aljazzaf, Z. M., & Sarfraz, M. (2019). On Cyber Crimes and Cyber Security. In M. Sarfraz (Ed.), Developments in Information Security and Cybernetic Wars, pp.1-41. IGI Global, Hershey, PA, USA. doi:10.4018/978-1-5225-8304-2.ch001. .https://www.researchgate.net/publication/331914032_On_Cyber_Crimes_and_Cyber_Securiy
6. AL-Hawamdeh, Lourane Said. (2016-2017). Cybercrimes: Their Pillars and Combating Mechanism -A comparative analytical study-. Al-Meezan for Low and Islamic Studies Journal. International College of Islamic Sciences. Amman. Jordan.
7. Al-Kaabi, Karima Shafi Jabr. (nd). The Information Society in the Arab World -Iraq as a model-. Journal of the Faculty of Arts (98). pp. 715-737. Baghdad. Iraq.
8.Al-Magsodi, Mohammed bin Ahmed bin Ali. (2015). Cybercrimes. their characteristics and how to confront them legally: international integration required to combat them. pp. 21-33. Dar Al-Manzouma. Riyadh. Saudi Arabia.

9. Badi, Souham. 2004-2005. Policies and strategies for employing information technology in education towards a national strategy -for employing information technology in higher education- a field study in the universities of eastern Algeria. a memorandum submitted to the master's degree in library science. Department of Library Science. Faculty of Humanities and Social Sciences. University of Monturi. Constantine.
10. Baghdadi, Adham Bassem Nimr. (2018). Means of Research and Investigation of Cybercrime. a memorandum submitted to obtain a master's degree in public law at the Faculty of Graduate Studies at An-Najah National University. Nablus. Palestine.
11. Baumard, Philippe. (2014, October). La cybercriminalité comportementale: Historique et régulation, RFCDP Revue française de criminologie et de droit pénal, édition Institut pour la justice. (3). pp. 39-75. France.
12. Belacel Bent nabi, Yasmine & Amrouche, Houssine. (2021). Electronic Threats and Cyber security in the Arab World. Numerus Academic Journal. 2(2). pp. 161-180.
13. Berisha-Shaqiri, Afërdita. (2014, July). Management Information System and Decision-Making. Academic Journal of Interdisciplinary Studies MCSER Publishing. 3(2). pp. 19-23. Rome-Italy. E-ISSN 2281-4612. ISSN 2281-3993,
14. BETTAHAR, HAMID. (2014). management des organisations. Alger: El DAR EL OTHMANIA Edition distribution.
15. Boell, Sebastian K. & Cecez-Kecmanovic, Dubravka. (2015). What is an Information System?. 48th Hawaii International Conference on System Sciences(HICSS), PP 4959- 4968. Kauaii. Hawaii: USA: Conference Paper.
16. Bourgeois,T. David, Ph.D. (2014). Information Systems for Business and Beyond. published through the open textbook challenge. SAYLOR ACADEMY.
17. Broadhurst, Roderic & Chang, Lennon Y.C. (2013). Cybercrime in Asia: Trends and Challenges. J.Liu et al. (eds). Handbook of Asian Criminology. Springer Science+Business Media. pp 49-63. New York.
18. Deifallah, Nassima. (2016-2017). The use of information and communication technology and its impact on improving the quality of the educational process - a sample study of Algerian universities. thesis submitted to obtain a doctorate in management sciences Division: Management of Organizations. Department: Management Sciences. Faculty of Economic. Commercial and Management Sciences. University of Hajj Lakhdar. Batna.
19. GIRI, SHAILENDRA. (2019). Cyber Crime. Cyber threat. Cyber Security Strategies and Cyber Law in Nepal. Pramana Research Journal. 9(3). PP. 662-672. ISSN NO: 2249-2976. ISSN NO: 2249-2976. https://pramanaresearch.org.
20. Hasnia, Ahmed Osama. (2017). Cybercrime between Criminal and Procedural Legitimacy. 19. pp. 1-42. Al-Azhar University Journal. Gaza.
21. Herjavec, Robert. (2021, December 29). Cyber CEO: The History Of Cybercrime. From 1834 To Present. Retrieved. 08,15, 2022. from https://robertherjavec.com/cyber-ceo-the-history-of-cybercrime-from-1834-to-present/

22. Kaur, Navneet. (2018, August). INTRODUCTION OF CYBER CRIME AND ITS TYPE. International Research Journal of Computer Science (IRJCS). ISSN: 2393-9842. IRJCS- All Rights Reserved. 5(08). pp. 435-439. www.irjcs.com.
23. Khémiri, Achwak. (n.d). Module :Culture Entrepreneuriale. Institut Supérieur du Sport et de l'Education Physique. Le KEF -Formation continue-. Tunisie.
24. Momani, Nahla Abdul Qadir. (2008). Cybercrime. First Edition. Dar Al-Thaqafa. Head Office. Amman. Jordan.
25. Piccoli, Gabrielle & Liu, Iris. (2007, September). Information Systems. Chapter 2 Achieving Efficiency and Effectiveness through Systems. Global Text Project. the open University of Hong Kong. pp 19-29.
26. Sabbagh, Imad. (2000). Information Systems: What They Are and Components. First Edition. Dar Al-Thaqafa. Amman. Jordan.
27. SABILLON, R & al. (2016, JUNE). Cybercrime and Cybercriminals: A Comprehensive Study, International Journal of Computer Networks and Communications Security. 4(6), 165–176. Available online at: www.ijcncs.org. E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print).
28. Seel, Peter, B. (2017). The Digital Universe: The Global Revolution in Communications, Warad, Zia. Publisher Hindawi CIC. UK.
29. Skiker, Muhammad Ali. (2010). Cybercrime and How to Address It. First Edition. Dar Al-Gomhoria for Press and Publishing. Egypt.
30. Subha, C et al. (2015, Sep–Oct). Cyber Crime – Attacks. Types. and Protection. International Journal of Trend in Research and Development. 2(5). pp351-355. ISSN: 2394-9333. www.ijtrd.com. IJTRD Available Online: www.ijtrd.com.
31. TCHAM, KAMEL. (2010, décembre 13,14). Le management de la qualité et son rôle dans l'amélioration des pratiques des entreprises économiques algériennes. participation au colloque national sur: le management de la qualité totale et le développement de la performance de l'entreprise. l'Université Dr.Tahar Moulley Saida. Algérie.
32. Tubake, Muragendra. (2013, Mar-Apr). Cyber Crimes: An Overview. Online International Interdisciplinary Research Journal. {Bi-Monthly}. 3(2). pp. 129-139. ISSN2249-9598, , http://www.oiirj.org/oiirj/mar-apr2013/18.pdf, ISSN2249 – 9598.
33. UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT (UNCTAD). (2015). INFORMATION ECONOMY REPORT. United Nations publication. ISBN 978-92-1-112887-1. Printed at United Nations. Geneva.
34. Yaish, Tammam Shawki. (2019). Cybercrime – A fundamental comparative study-. First Edition. Rimal Press - El Oued - Algeria.