المعهد القومى للملكية الفكرية
The National Institute of Intellectual Property
Helwan University, Egypt

المجلة العلمية للملكية الفكرية وإدارة الابتكار

دورية نصف سنوية محكمة يصدرها

المعهد القومي للملكية الفكرية

جامعة حلوان

العدد الثالث
يوليو٢٠٢٠

الهدف من المجلة:

تهدف المجلة العلمية للملكية الفكرية وإدارة الابتكار إلى نشر البحوث والدراسات النظرية والتطبيقية فى مجال الملكية الفكرية بشقيها الصناعي والأدبي والفني وعلاقتها بإدارة الابتكار والتنمية المستدامة من كافة النواحي القانونية والاقتصادية والادارية والعلمية والأدبية والفنية.

ضوابط عامة:

- تعبر كافة الدراسات والبحوث والمقالات عن رأى مؤلفيها ويأتي ترتيبها بالمجلة وفقا لإعتبارات فنية لا علاقة لها بالقيمة العلمية لأى منها.
- تنشر المقالات غير المحكمة (أوراق العمل) فى زاوية خاصة في المجلة.
- تنشر المجلة مراجعات وعروض الكتب الجديدة والدوريات.
- تنشر المجلة التقارير والبحوث والدراسات الملقاه في مؤتمرات ومنتديات علمية والنشاطات الأكاديمية في مجال تخصصها دونما تحكيم في أعداد خاصة من المجلة.
- يمكن الاقتباس من بعض مواد المجلة بشرط الاشارة إلى المصدر.
- تنشر المجلة الأوراق البحثية للطلاب المسجلين لدرجتى الماجستير والدكتوراه.
- تصدر المجلة محكمة ودورية نصف سنوية.

ألية النشر فى المجلة:

- تقبل المجلة كافة البحوث والدراسات التطبيقية والأكاديمية في مجال حقوق الملكية الفكرية بكافة جوانبها القانونية والتقنية والاقتصادية والادارية والاجتماعية والثقافية والفنية.
- تقبل البحوث باللغات (العربية والانجليزية والفرنسية).
- تنشر المجلة ملخصات الرسائل العلمية الجديدة، وتعامل معاملة أوراق العمل.
- يجب أن يلتزم الباحث بعدم إرسال بحثه إلى جهة أخرى حتى يأتيه رد المجلة.
- يجب أن يلتزم الباحث بإتباع الأسس العلمية السليمة في بحثه.
- يجب أن يرسل الباحث بحثه إلى المجلة من ثلاثة نسخ مطبوعة، وملخص باللغة العربية أو الانجليزية أو الفرنسية، فى حدود ٨ ـ ١٢ سطر، ويجب أن تكون الرسوم البيانية والإيضاحية مطبوعة وواضحة، بالإضافة إلى نسخة إلكترونية Soft Copy، ونوع الخط Romanes Times New ١٤ للعربى، و١٢ للانجليزي على B5 (ورق نصف ثمانيات) على البريد الالكتروني: ymgad@niip.edi.eg
- ترسل البحوث إلى محكمين متخصصين وتحكم بسرية تامة.
- في حالة قبول البحث للنشر، يلتزم الباحث بتعديله ليتناسب مع مقترحات المحكمين، وأسلوب النشر بالمجلة.

مجلس إدارة تحرير المجلة	
أ.د. ياسر محمد جاد الله محمود	أستاذ الاقتصاد والملكية الفكرية وعميد المعهد القومي للملكية الفكرية (بالتكليف) - رئيس تحرير المجلة
أ.د. أحمد عبد الكريم سلامة	أستاذ القانون الدولي الخاص بكلية الحقوق بجامعة حلوان والمستشار العلمي للمعهد - عضو مجلس إدارة تحرير المجلة
أ.د. وكيل المعهد للدراسات العليا والبحوث	سكرتير تحرير المجلة
أ.د. جلال عبد الحميد عبد اللاه	أستاذ الهندسة الانشائية بكلية الهندسة بالمطرية بجامعة حلوان - عضو مجلس إدارة تحرير المجلة
أ.د. هناء محمد الحسيني	أستاذ علوم الأطعمة بكلية الاقتصاد المنزلي بجامعة حلوان - عضو مجلس إدارة تحرير المجلة
أ.د. وزير مفوض/ مها بخيت محمد زكي	مدير إدارة الملكية الفكرية والتنافسية بجامعة الدول العربية - عضو مجلس إدارة تحرير المجلة
اللواء أ.د. عبد القدوس عبد الرزاق العبيدلي	رئيس مجلس إدارة جمعية الامارات للملكية الفكرية - عضو مجلس إدارة تحرير المجلة
Prof Dr. Alexander Peukert	أستاذ القانون المدنى بجامعة جوته فرانكفورت أم ماين – ألمانيا - عضو مجلس إدارة تحرير المجلة
Prof Dr. Andrew Griffiths	أستاذ القانون التجارى بجامعة نيو كاسل - بريطانيا - عضو مجلس إدارة تحرير المجلة

المراسلات

ترسل البحوث إلى رئيس تحرير المجلة العلمية للملكية الفكرية وإدارة الابتكار بجامعة حلوان
جامعة حلوان - ٤ شارع كمال الدين صلاح - أمام السفارة الأمريكية بالقاهرة -جاردن سيتى
ص.ب: ١١٤٦١ جاردن سيتي
ت: ٠٢ ٢٥٤٨١٠٥٠ + ٢٠ محمول: ٢٠١٠٠٠٣٠٠٥٤٨ + ف: ٠٢ ٢٧٩٤٩٢٣٠ +
http://www.helwan.edu.eg/niip/
ymgad@niip.edu.eg

Effect of cybercrime on the pharmaceutical industry

Nahla Elaraby Abd Elazeem

Effect of cybercrime on the pharmaceutical industry

Nahla Elaraby Abd Elazeem

The abstract:

The pharmaceutical industry has became particularly vulnerable to cybercrime, as the counterfeit pharmaceuticals are a growing and profitable business for fraudsters, who perform these cyber attacks for money, fame or for the politics, eventually it may lead to brand damage or reputational damage, since once a pharmaceutical organization is exposed in the media for breaching data, it can be difficult to recover public trust.

In America, cybercriminals stole 8.3 million patient records from the Virginia Prescription Monitoring Program and demanded a $10m (approximately £6m) ransom.

There is a persistent need to protect drug recipes and researches as those companies are rich in IP, but first they should know where their data is, as the data is often scattered across unstructured sources, having processes and procedures to identify, report and remediate that data and also diminish data sharing, via electronic health records, personal health records, insurance portals and prescription sites, it comprises personal and sensitive information, as well as drug recipes and research data.

Detica (an international business and technology consulting firm owned by BAE Systems) have developed five steps for cybercrime risk appraisal:

1. Establish potential attackers and threats;

2. Assess the likely target of attacks (i.e. IP, customer databases, etc.);
3. Determine the purpose of the attack;
4. Assess the impact of an attack on the organization; and finally,
5. Identify which assets are high impacts and require prioritizing in terms of protection.

The pharmaceutical company Roche has affirmed that it was hit by a Winnti cyber-attack in 2019, thought to be supported by the Chinese government; The Company has stated that no sensitive information has been lost.

Bayer was also targeted by Winnti attacks last year, in 2017; Merck & Co has its active pharmaceutical ingredients (API) production and some R&D systems seriously disrupted by the NotPetya attack, highlighting the need for cyber-security for pharmaceutical companies.

A range of other German companies were also affected by the attack.

The introduction:

Pharmaceutical industry have been changed enormously from past until now, there is huge exchanges occur generally in the international economy, drug discovery and development strategies for new drugs have changed in the past two decades.

The pharmaceutical industry discovers, develops, produces, and markets drugs for use as medications to be administrated to patients, to cure, vaccinate them or to alleviate the symptoms.

Pharmaceutical companies may deal in generic or brand medications and medical devices. They are subject to a variety of laws and regulations that govern the patenting, testing, safety, efficacy and marketing of drugs.

A pharmaceutical company, or drug company, is a commercial business licensed to research, develop, market and/or distribute drugs, most commonly in the context of healthcare. They can deal in generic and/or brand medications. They are subject to a variety of laws and regulations regarding the patenting, testing and marketing of drugs, particularly prescription drugs.

The roots of the pharmaceutical industry lie back with the apothecaries and pharmacies that offered traditional remedies as far back as the middle ages, based on centuries of folk knowledge. But the industry as we understand it today really has its origins in the second half of the 19th century. The scientific revolution of the 17th century had spread ideas of rationalism and experimentation, and the industrial revolution had transformed the production of goods in the late 18th century.

The earliest company to move in this direction was Merck in Germany. Originating as a pharmacy founded in Darmstadt in 1668, it was in 1827 that Heinrich Emanuel Merck began the transition towards an industrial and scientific concern, by manufacturing and selling alkaloids.[1]

Other examples, Hoffmann-La Roche in Switzerland; Burroughs Wellcome in England; Etienne Poulenc in France; and Abbott, Smith Kline, Parke-Davis, Eli Lilly, Squibb, and Upjohn in the U.S. all started as apothecaries and drug suppliers between the early 1830s and late 1890s. Other firms whose names carry recognition today began with the production of organic chemicals (especially dyestuffs) before moving into pharmaceuticals. These include Agfa, Bayer, and Hoechst in Germany; Ciba, Geigy, and Sandoz in Switzerland; Imperial Chemical Industries in England; and Pfizer in the U.S.[2]

In the past most drugs have been discovered either by identifying the active ingredient from traditional remedies or by accidental discovery. A newer approach has been to understand how disease and infection are controlled at the molecular and physiology level and to target specific entities based on this knowledge. New technologies and Data Management/Informatics systems are now employed to speed up this process.

---

[1] Walsh, robin (2010) A history of the pharmaceutical industry, **https://pharmaphorum.com/articles/a_history_of_the_pharmaceutical_industry/**
April 2020

[2] **https://pubsapp.acs.org/cen/coverstory/83/8325/8325emergence.html** April 2020

Drug development is considered a costly and intensive process. Of all compounds investigated for use in humans only a small fraction is eventually approved, and only after heavy investment in pre-clinical development, clinical trials, and safety monitoring to determine the safety and efficacy of a compound.

Drug discovery is the process by which drugs are discovered and/or designed. An early discovery requiring the combinative chemistry to synthesize the library of new chemical entities and to further optimize the structures to identify the targets for treatment of life threatening diseases, are new patterns in the modern drug development process. In vitro and in vivo screenings of small and large molecules against biological targets, proteins and enzymes for diseases like cancers, anti-inflammatory and rare diseases to identify the lead candidates, supplemented with molecular modeling and collaborative research, have opened the avenues for modern therapies and yielded the opportunities for licensing new molecules and formulation technologies.

The pharmaceutical industry aimed to meet unmet needs in multiple areas of therapy such as anti-body directed therapy, CAR-T cell therapy {A type of treatment in which a patient's T cells (a type of immune system cell) are changed in the laboratory so they will attack cancer cells}, immune-oncology drug delivery, siRNA technology (It interferes with the expression of specific genes with complementary nucleotide sequences by degrading mRNA after transcription), gene therapy among others.[1]

[1] Ali, shaukat (2018) A 20 Year Retrospective: The Pharmaceutical Industry Then and Now, https://www.americanpharmaceuticalreview.com/Featured-Articles/354573-A-20-Year-Retrospective-The-Pharmaceutical-Industry-Then-and-Now/ April 2020

Here are some facts about how pharmaceutical industry changed over the last 10 years:

1. The major fact is about the increase in Research and Development. There is a huge competition between companies to produce a new product and achieve innovation.
2. Protecting Intellectual property got more important because of Market Exclusivity.
3. It became harder to get the approval from the authority in contrary to past.
4. The numbers and types of audits for the facilities have changed, there needs became different and hard to satisfy.
5. Quality of the products improved, so it became difficult to make a higher and better quality.
6. Number of products for wellness, which affect the human life quality, increased.
7. Improvements in biotechnology changed the industry a lot. Many biologic products have been launched for rare and chronic diseases.
8. Technology transfers began.
9. There has been a rise in generic production.
10. Import and export for pharmaceuticals grew around the world.[1]

[1] Boran, Pelin (2015) How has the Pharmaceutical Industry Changed over the past 10 years? **https://www.linkedin.com/pulse/how-has-pharmaceutical-industry-changed-over-past-10-years-boran** April 2020

The research methodology:

Chapter one: Protecting pharmaceutical industry
Chapter two: The emergence of cybercrime
Chapter three: The impact of cybercrime on pharmaceutical industry
Chapter four: Pharmaceutical companies' procedures to confront cybercrime

Chapter one
Protecting pharmaceutical industry

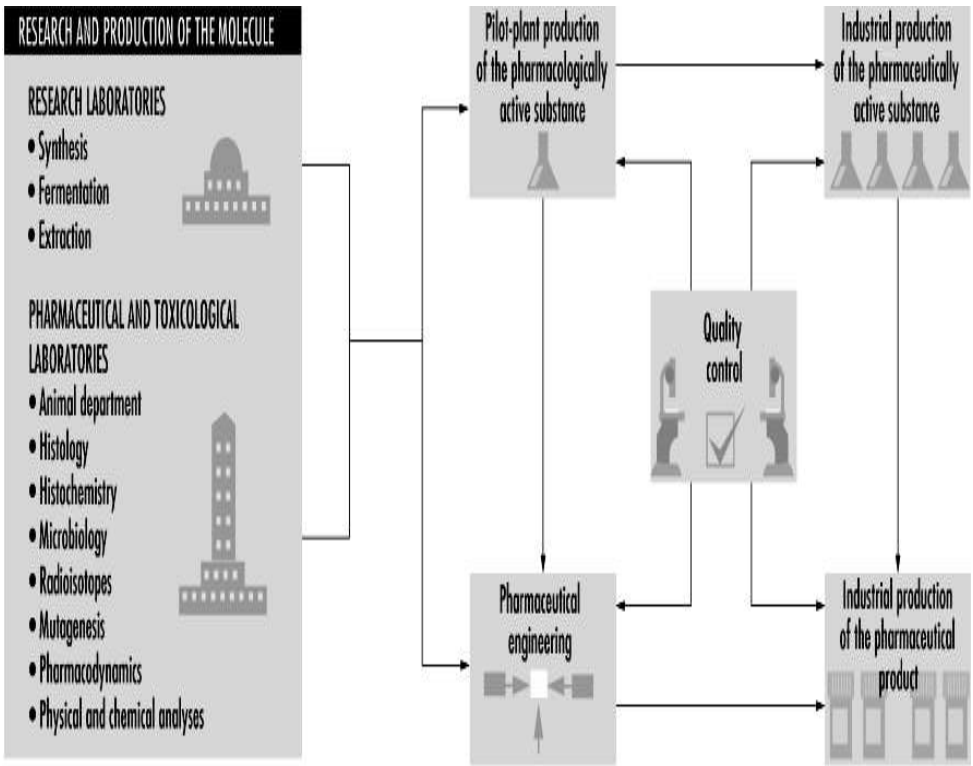
The pharmaceutical industry is an important component of health care systems throughout the world; it is comprised of many public and private organizations that discover, develop, manufacture and market medicines for human and animal health. The pharmaceutical industry is based primarily upon the scientific research and development (R&D) of medicines that prevent or treat diseases and disorders.

With the cost of bringing a new drug to market now exceeding $2.5B, it should come as no surprise that pharmaceutical companies are increasingly targeted for their Intellectual Property (IP).

Intellectual Property protections are the laws that enable people and organizations to make the investments necessary to develop new technologies and to defend their proprietary inventions or products. (IP) is a pharmaceutical or Biotech Company's most valuable resource, and its protection is a key to that company's future success.

Pharmaceuticals companies must face the daily challenge of creating value through the exploitation of IP rights, but avoiding considerable reputational harm. This situation was well illustrated in South Africa during the late 1990s when the balance between IP protection and the urgent needs of patients were not aligned. Since then, companies have become more aware of the potential damage that can be caused by too strict an interpretation of IP rights.

The pharmaceutical industry is largely driven by scientific discovery and development, in conjunction with toxicological and clinical experience.[1]



[1] D. Tait, keith (2004) Encyclopedia of occupational health and safety. Ed.4. International labour office. chapter 79

The management of IP and IPR is a multidimensional task; it became influenced by market needs. It is no longer driven purely by a national perspective, so there is a need to align it with national laws and international treaties and practices.[1]

During the last century, before the existence of any international convention in the field of industrial property, it was difficult to obtain protection for industrial property rights in the various countries of the world because of the diversity of their laws. These practical problems created a strong desire to overcome such difficulties. During the second half of the last century the development of a more internationally oriented flow of technology and the increase of international trade made harmonization of industrial property laws urgent in both the patent and the trademark field. Then there was a final draft proposing an international "union" for the protection of industrial property was prepared in France and was sent by the French Government to a number of other countries, together with an invitation to attend the 1880 International Conference in Paris (Paris Convention).

If the effects of strong drug patenting regimes are fiercely debated in industrialized countries, it is hardly surprising that the signing of the TRIPS agreement in 1994, extending to southern countries the same type of IPR regime that was designed in the north.[2]

[1] Nath Saha, Chandra and Bhattacharya, Sanjib Intellectual property rights: An overview and implications in pharmaceutical industry (Journal of advanced Pharmaceutical Technology & Res**earch**). No.2011 Apr-Jun; p. 88–93.

[2]Cimoli, Mario. et. al. (2014) Intellectual Property Rights: Legal and Economic Challenges for Development. Ed.1. oxford university press. p. 229

The main rule relating to patentability is that patents shall be available for any invention, whether a product or process, in all fields of technology without discrimination, where those inventions meet the standard substantive criteria for patentability (novelty, inventive step and industrial applicability).

IP and its associated rights are seriously influenced by the market needs, market response, cost involved in translating IP into commercial venture and so on. Different forms of IPR demand different treatment, handling, planning, strategies and engagement of persons with different knowledge such as science, engineering, medicines, law, finance, marketing, and economics.

Each industry should evolve its own IP policies, management style, strategies, etc. depending on its area of specialty.

The relevant patent rights are not only recognized and protected under the 2002 IP Law in Egypt, but are also protected under the Egyptian Constitution and Egyptian Trade Law. As the Egyptian legislature appreciated that R&D projects can only occur if stakeholders are entitled to claim exclusivity over the benefits of the results of the of funding of such projects.

With the ongoing attention given to the protection of IP rights nowadays, the general policy in Egypt is to create a safer and more secure environment for the growth of investment and trade. Under the present law governing the protection of IP rights, pharmaceutical companies are reassured. These laws have increased investors' confidence in that the returns on their capital

investments in the R&D of new drugs and products will enjoy legal protection in Egypt.[1]

Chapter two
The emergence of cybercrime

Cyber Crime is technology-based crime committed by technocrats. A hacker is someone who seeks and exploits weaknesses in a computer system or computer network it was first adopted by MIT's computer culture, referring to a person who was an excited programmer. Hacking is a process of breaking into Systems, networks and Websites with the owner's permission and trying to find out vulnerabilities.

Cyber Crime is growing due to dependence on computers in modern life. It can be simply defined as "unlawful acts wherein the computer is either a tool or a target or both". Defining cyber crimes, as "acts that are punishable by the information Technology Act" would be unsuitable, Cyber crime is now the burning issue for all countries to handle because most of data is transferred online even governmental data also. It also include traditional crime in which computer are used.[2]

Cyber crime mainly consists of unauthorized access to Data and data alteration, data destruction, theft of funds or intellectual

[1] Helmi, Abdelrahman (2017) Protection of Patents in the pharmaceutical industry under Egyptian Laws Cairo https://www.tamimi.com/law-update-articles/protection-of-patents-in-the-pharmaceutical-industry-under-egyptian-laws/ April 2020

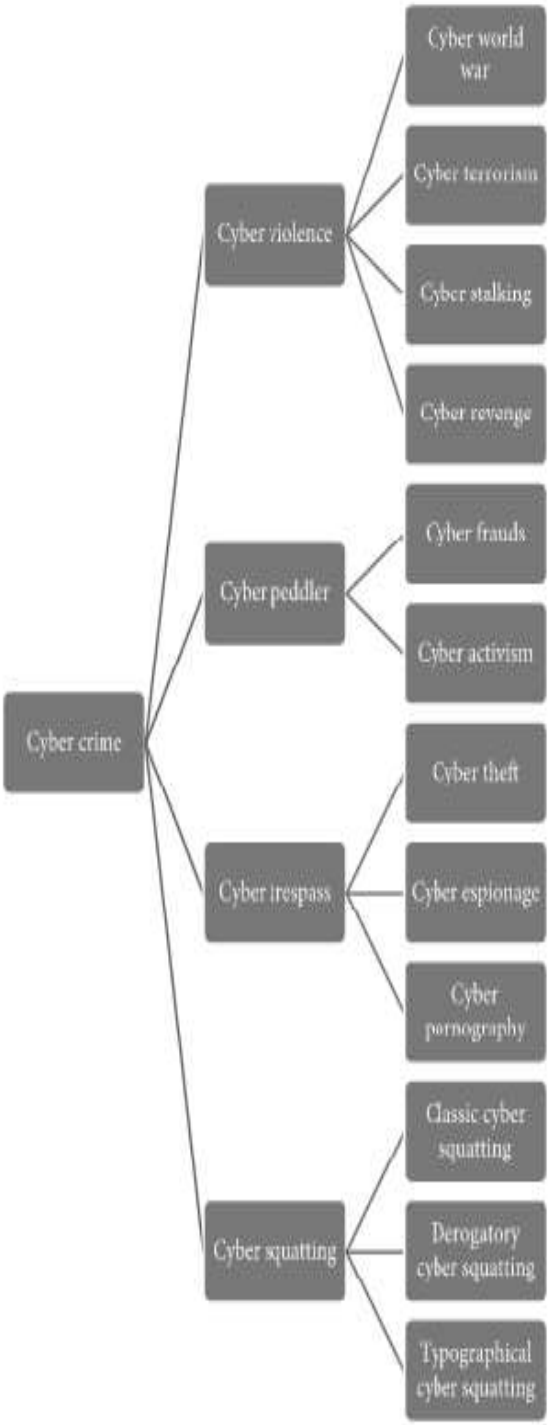
[2] Sharma, Deepanshu. Vinay Prakash (2014) Emergence of Cybercrime: An Overview. (M.S) B.Tech CS TMU. College of Computing Sciences and Information Technology (CCSIT) . Teerthanker Mahaveer University, Moradabad. P.423.

property. The Information security requires sufficient number of skilled professionals to deal with variety of domain specific actions.

The first recorded cyber crime took place in the year 1820, JosephMarie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology.[1]

In the existing world of Internet, we can find a huge volume and a variety of cyberattacks. From the history of cyberattacks on the Internet, it is concluded that trends of attacks are continuously changing day by day. So, the various types of cybercrimes occurring in today's world are shown in Figure below.

[1] http://www.inf.tsu.ru/WebDesign/libra3.nsf/317094d25b4410c6c62571f5001deba4/3b47f7a6821452fdc62572040016d843/$FILE/cybercrime.pdf April 2020


Cyber crime
Cyber violence
Cyber world war
Cyber terrorism
Cyber stalking
Cyber revenge
Cyber peddler
Cyber frauds
Cyber activism
Cyber trespass
Cyber theft
Cyber espionage
Cyber pornography
Cyber squatting
Classic cyber squatting
Derogatory cyber squatting
Typographical cyber squatting

١

The objective of cyberattackers may be to gain money, respect, revenge, or any other. Here are the most common objectives of cyberattackers:

1. Entertainment: Some cybercriminals perform their activities of cyberattack to test their hacking abilities. They feel proud and joy in their successful attempts. They are willing to get fame in the world of cybercriminal.
2. Hacktivists: These cyberattackers are motivated by political, religious, and social ends. The latest example is Ashley Madison dating whose users list was exposed by attackers in public domain.
3. Financial gain: Most of the cyberattackers perform the cyberattacks for financial gain. They desire to become rich.
4. Spying: These types of cybercriminals attack the networks to steal the confidential information of specific country, organization, or individual.
5. Revenge: These types of cybercriminals knew the policies, secrets, and weak points of their company, organization, or country. They perform their activities of cyberattacks under the emotion of hate to take their revenge in the form of financial loss, tarnishing their social image, reputation, and so on.

[1] Singh brar, harmandeep. Gulshan kumar Cybercrimes: A Proposed Taxonomy and Challenges (**journal of computer networks and communications**) vol.2018 p.5.

Due to easily exploitable laws, cybercriminals use developing countries in order to evade detection and prosecution from law enforcement. In developing countries, such as the Philippines, laws against cybercrime are weak or sometimes nonexistent.

These weak laws allow cybercriminals to strike from international borders and remain undetected. Even when identified, these criminals avoid being punished or extradited to a country, such as the United States, that has developed laws that allow for prosecution.[1]

The police and law enforcement agencies should be empowered with power of Information Technology by providing the needed training so that they may discharge their duties effectively.

Since cybercrime is a global problem, the need also arise for law enforcement agencies including every countries police to collaborate in the area of information sharing, such as the Central Bureau of Investigation (CBI), Federal Bureau of Investigation (FBI), National Technical Research Organization (NTRO), Cert-In and INTERPOL to crack-down on cyber criminals.

For personal protection against cybercrime there are 5 critical steps to protect you from cybercrime:

[1] Kshetri, Nir. Diffusion and Effects of Cyber Crime in Developing Countries http://web.a.ebscohost.com/ehost/detail/detail?vid=3&sid=21efdb54-ad43-447f-ab46-ce7fa854a98f%40sessionmgr4003&hid=4109&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=buh&AN=55328703/ April 2020

1. Keep everything up to date.
2. Use strong, unique passwords.
3. Enable multifactor authentication.
4. Encrypt and backup your most important data.
5. Be careful using public Wi-Fi.

Chapter three
The impact of cybercrime on pharmaceutical industry

Biotech and pharmaceutical firms hold vast amounts of critically important data and information. Valuable data and information making them prime targets for cyber-attacks.

Obvious categories include data arising from the development and testing of pharmaceutical products, the sophisticated nature of medical devices and their connectivity raises additional risks, the commercially sensitive information about products and their pricing and promotion.

Since data inside the IT systems of pharma companies and healthcare organizations are highly valued, the industry is the focus of a wide range of cybercriminals. Insiders are a common threat. IBM Managed Security Services data indicates that 68% of attacks on the healthcare sector in 2016 were perpetrated by insiders. Of these, more than 33% were carried out by malicious individuals.[1]

The need for pharmaceutical companies to fortify their security systems has become essential in recent years. The best method of protection is to prevent cyberattacks from happening, or

[1] Alvarez, Michelle. (2017). Security trends in the healthcare industry. IBM security. P.5,7.

at least reduce the risk of a hack. One way to do this is to ensure that all software is updated.

In the case of the WannaCry ransomware attack, the security patch for the malware was available in more recent versions of Microsoft. However, older versions of the software were vulnerable, and users received the free patch only after the attack had occurred.[1]

Another important line of defense is training employees on the latest methods of keeping security documents safe.

So far, most of the examples in Canada and the US, where hospital networks are attacked and a bitcoin (cryptocurrency) ransom are demanded. There is a potential loss of data, and a risk that hackers have gained access to potentially significant personal health information.

In Europe and elsewhere, cyber-attacks are increasing thanks to the growing volume of electronic data and the rising use of electronic storage to keep data.

Pharmaceutical companies are concerned about cyber security threats in three key areas:

- Data relating to clinical trials, and particularly patient data generated during clinical trials,

[1] Low, Aloysios (2017) Microsoft held back a free WannaCry patch, report says. https://www.cnet.com/au/news/microsoft-reportedly-held-back-wannacry-patch-for-older-windows-versions/ April 2020

- Corporate know-how and confidential information relating to the manufacture of biologic drugs
- Day-to-day commercially sensitive information regarding drug pricing and promotion. [1]

Unlicensed pharmaceuticals are perhaps the goods most widely promoted using criminal advertising. Pfizer sells a genuine Viagra pill for several dollars while factories in India will provide a generic version to consumers for a way less price.[2]

Looking at the direct risks to consumers, unregulated Internet pharmaceutical sales pose two potential liabilities: first, there is a risk of fraud (that a customer might order a drug and either not receive it or suffer subsequent charges to their credit card); and second there could be health risks due to poor quality and adulterated drugs. [3]

We can estimate that UK consumers provided roughly $400,000 to the top counterfeit pharmaceutical programs in 2010 and perhaps as much as $1.2 million per-month overall.[4]

[1] Norman, john. Patrick duxbury (2017) Why combatting cybercrime is critical for life science companies https://www.europeanpharmaceuticalreview.com/article/50778/combatting-cybercrime-critical-life-science-companies/ April 2020

[2] Böhme, Rainer. et.al. (2012) the economics of information security and privacy. research gate. P.12.

[3] Kanich, C. et. al. (2011) Show me the money: characterizing spam-advertised revenue. (conference paper) Department of Computer Science and Engineering. University of California.

[4] McCoy, Damon. et.al. (2012) PharmaLeaks: understanding the business of online pharmaceutical affiliate program https://dl.acm.org/doi/10.5555/2362793.2362794 April 2020

There are three massive healthcare data breaches:

1. Atrium Health notified 2.65 million patients that their data was breached due to a hack on its third-party billing vendor, AccuDoc. Patient data was compromised for more than a week in what is the biggest healthcare data breach of 2018.
2. A HealthEquity email hack potentially breached the data of 190,000 customers. Two employee email accounts were hacked over the course of a month. It's the second breach notification for HealthEquity this year.
3. The data of about 128,000 New York Oncology Hematology patients was breached after 15 employees fell victim to targeted phishing attacks in April. The first hack occurred on April 20 and a second attack on one employee account occurred for about six days on April 26.[1]

Cyberattacks also affected huge pharmaceutical companies; Cybersecurity is a pressing issue to pharmaceutical businesses in particular, for a significant number of reasons.

Roche one of Switzerland's largest drug makers was a victim, apparently of hackers supported by the Chinese government. Other companies targeted in the same attack were Siemens, BASF, Henkel, Marriott, Lion Air, Shin-Etsu and Sumitomo.

German pharmaceutical giant Bayer, reported that it was also attacked by Chinese hackers.

[1] Davis, Jessica (2018) Data of 7,000 Tandigm Health Patients Exposed by Site Vulnerability https://healthitsecurity.com/news/data-of-7000-tandigm-health-patients-exposed-by-site-vulnerability April 2020

The companies all reported that no sensitive information was lost.

In June of 2017, Merck was just one of more than a dozen businesses that were hit with a massive cyberattack that ultimately ended up affecting organizations all over the world, the organization suffered a total worldwide disruption of its operations, It was estimated in October of 2017 that insurers could be forced to pay out as much as $275 million to cover the insured portion of the drug maker's loss from the cyberattack.[1]

Chapter four
Pharmaceutical companies' procedures to confront cybercrime

If we make a list of some of the most pressing issues that we're facing as a society, cybersecurity would be right at the top. Cybersecurity is a pressing issue to pharmaceutical businesses in particular, for a significant number of reasons.

In 2017, one study revealed that about 54% of companies experienced one or more successful attacks that compromised data and/or their larger IT infrastructure at some point in the year. A massive 77% of those attacks utilized file-less techniques—meaning that instead of tricking someone into downloading and installing a virus, the attacks were executed using vulnerabilities that were already there. [2]

[1] https://www.reuters.com/article/us-merck-co-cyber-insurance/merck-cyber-attack-may-cost-insurers-275-million-verisks-pcs-idUSKBN1CO2NP April 2020
[2] https://www.barkly.com/ponemon-2018-endpoint-security-statistics-trends April 2020

According to another study conducted by Deloitte, the pharmaceutical sector is regularly the number one target of cyber criminals around the world, particularly when it comes to stealing intellectual property.

In the UK, for example, total damages from IP theft amounted for 9.2 billion pounds during 2017. A significant 1.8 billion of that was attributed to pharmaceutical, biotechnology, and healthcare organizations.[1]

As we mention above, one of the biggest attacks in recent memory struck Merck & Company. If this type of attack can hit a company as large and as old as Merck, it can happen to anyone, which is why learning from situations like these is always of paramount importance.

Pharmaceutical companies need to be willing to learn from each other's mistakes and act accordingly. This isn't something that affects one organization more than others based on size or location—this type of attack can hit any company at any time, and everyone needs to be ready.

All employees and key stakeholders must take the situation equally seriously and they must engage in cybersecurity best practices every day to help the organization as a whole avoid these types of incidents in the future.

[1]Moris, matt. (2017) Industrial Cybersecurity Defenses Essential for Pharma Companies https://www.pharmamanufacturing.com/articles/2017/industrial-cybersecurity-defenses-essential-for-pharma-companies/ April 2020

As Merck showed, a total disruption of an entire business is likely if you become the target of this type of significant breach—but that's not the end of the story. Additional factors to consider include losses stemming from things like:

- Stolen intellectual property
- Being forced to repeat costly and time-consuming clinical trials
- Litigation stemming from the breach itself
- Lost revenue
- Damages to products that are already in development or production
- Significant production shortages in the supply chain

This includes elements like clinical data, IP, formulas for compounds, and in some cases patient or employee personal data as well. The amount of money that a hacker can get for a stolen proprietary formula on the black market significantly eclipses what they might be able to get for something like stolen credit card information.

Merck's problem was that they had systems, partners, contractors, and subcontractors that were not secure and patched in the ways that they should have been, Pharmaceutical businesses in particular need to understand that all of these systems are connected. If any link in the chain is broken, the entire chain becomes compromised.

One of the issues with "Big Pharma" from an IT perspective is that oftentimes organizations are dealing with infrastructures that are a collection of legacy systems, multiple systems that are

difficult to properly integrate (and secure), Excel spreadsheets, purpose-built cloud systems, and more. Gaining the level of visibility, one would need to adequately secure these resources in an ongoing and reactive process that requires the coordination of your vendors, operational methodologies, and company culture. Merck's breach could have arguably been attributed solely to a cultural flaw that they silenced IT and overlooked it.

Legacy systems, for example, often lack the vendor support needed to update them against the latest threats. That alone will leave an organization like Merck exposed, regardless of how large they are.[1]

In the end, the most important thing for pharmaceutical companies, regardless of their size, to understand is that getting hit with this type of cyber attack is no longer a question of "if," but "when?" You can invest in all of the cybersecurity measures that you want—it still won't prevent you from one day becoming the *target* of hackers with malicious intention. That insight will act as your first line of defense against these types of cyber criminals in the future.

Conclusion:

The data collected by pharmaceutical companies, including proprietary information about patented drugs, data related to pharmaceutical advances and technologies, and patient information

[1] Souza, Chris. (2018) What Has Pharma Learned from the Merck Cyber Attack http://www.pharmexec.com/what-has-pharma-learned-merck-cyber-attack April 2020

are all sensitive and valuable, which means that losing control over that data can have catastrophic consequences and affect patient and consumer trust.

Having a comprehensive cybersecurity strategy in place to safeguard those digital assets has become an essential part of any company's security protocols.

5 Facts about Cyber Security for Pharmaceutical Companies:

1. Cyber Attacks Are Already Here:

Individuals or companies having anything of value, should take in consideration that they will be targeted by cyberattackers. Pharmaceutical companies are a prime target given the importance and prevalence of the intellectual property they possess.

2. Attack Vectors are Different:

You should put yourself in the place of the attackers and try to Know how attackers operate within your industry that you will be able to strengthen your cyber security posture.

In pharma, foreign state actors' pursuit of intellectual property remains a significant threat to these companies.

3. Start with Data Classification:

Marketing and labeling what is sensitive more than other and ordering them so that you are alerted to who's accessing it and where it's being sent, it will be an important step to protect these data.

4. Trying to lower Insider Threats with Privileged Account Management:

As we said before insider attacks to pharmaceutical companies is real. The challenge is in detecting and mitigating the risks posed by an insider attack.

5. Unite Your Cyber Protection:

Lines of business in pharmaceutical companies are vastly different, but cyber protection shouldn't be. It may be the job of a CISO to develop security processes and protocols to protect the firm from cyber attacks, but threat awareness is everyone's job. [1]

[1] Klubenspies,Lou. 5 Facts about Cyber Security for Pharmaceutical Companies https://www.coursehero.com/file/36910066/5-facts-about-cyber-and-pharmapdf/ April 2020

References

Walsh, robin (2010) A history of the pharmaceutical industry, https://pharmaphorum.com/articles/a_history_of_the_pharmaceutical_industry/ April 2020

https://pubsapp.acs.org/cen/coverstory/83/8325/8325emergence.html April 2020

Ali, shaukat (2018) A 20 Year Retrospective: The Pharmaceutical Industry Then and Now, https://www.americanpharmaceuticalreview.com/Featured-Articles/354573-A-20-Year-Retrospective-The-Pharmaceutical-Industry-Then-and-Now/ April 2020

Boran, Pelin (2015) How has the Pharmaceutical Industry Changed over the past 10 years? https://www.linkedin.com/pulse/how-has-pharmaceutical-industry-changed-over-past-10-years-boran April 2020

D. Tait, keith (2004) Encyclopedia of occupational health and safety. Ed.4. International labour office. chapter 79

Nath Saha, Chandra and Bhattacharya, Sanjib Intellectual property rights: An overview and implications in pharmaceutical industry (**Journal of advanced Pharmaceutical Technology & Research**). No.2011 Apr-Jun.

Cimoli, Mario. et. al. (2014) Intellectual Property Rights: Legal and Economic Challenges for Development. Ed.1. oxford university press.

Helmi, Abdelrahman (2017) Protection of Patents in the pharmaceutical industry under Egyptian Laws, Cairo https://www.tamimi.com/law-update-articles/protection-of-patents-in-the-pharmaceutical-industry-under-egyptian-laws/ April 2020

Sharma, Deepanshu. Vinay Prakash (2014) Emergence of Cybercrime: An Overview. (M.S) B.Tech CS TMU. College of Computing Sciences and Information Technology (CCSIT) . Teerthanker Mahaveer University, Moradabad.

http://www.inf.tsu.ru/WebDesign/libra3.nsf/317094d25b4410c6c62571f5001deba4/3b47f7a6821452fdc62572040016d843/$FILE/cybercrime.pdf April 2020

Singh brar, harmandeep. Gulshan kumar Cybercrimes: A Proposed Taxonomy and Challenges (**journal of computer networks and communications**) vol.2018.

Kshetri, Nir. Diffusion and Effects of Cyber Crime in Developing Countries http://web.a.ebscohost.com/ehost/detail/detail?vid=3&sid=21efdb54-ad43-447f-ab46-ce7fa854a98f%40sessionmgr4003&hid=4109&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=buh&AN=55328703/ April 2020

Alvarez, Michelle. (2017). Security trends in the healthcare industry. IBM security.

Low, Aloysios (2017) Microsoft held back a free WannaCry patch, report says. https://www.cnet.com/au/news/microsoft-reportedly-held-back-wannacry-patch-for-older-windows-versions/ April 2020

Norman, john. Patrick duxbury (2017) Why combatting cybercrime is critical for life science companies https://www.europeanpharmaceuticalreview.com/article/50778/combatting-cybercrime-critical-life-science-companies/ April 2020

Böhme, Rainer. et.al. (2012) the economics of information security and privacy. research gate.

Kanich, C. et. al. (2011) Show me the money: characterizing spam-advertised revenue. (conference paper) Department of Computer Science and Engineering. University of California.

McCoy, Damon. et.al. (2012) PharmaLeaks: understanding the business of online pharmaceutical affiliate program https://dl.acm.org/doi/10.5555/2362793.2362794 April 2020

Davis, Jessica (2018) Data of 7,000 Tandigm Health Patients Exposed by Site Vulnerability https://healthitsecurity.com/news/data-of-7000-tandigm-health-patients-exposed-by-site-vulnerability April 2020

https://www.reuters.com/article/us-merck-co-cyber-insurance/merck-cyber-attack-may-cost-insurers-275-million-verisks-pcs-idUSKBN1CO2NP April 2020

https://www.barkly.com/ponemon-2018-endpoint-security-statistics-trends April 2020

Moris, matt. (2017) Industrial Cybersecurity Defenses Essential for Pharma Companies https://www.pharmamanufacturing.com/articles/2017/industrial-cybersecurity-defenses-essential-for-pharma-companies/ April 2020

Souza, Chris. (2018) What Has Pharma Learned from the Merck Cyber Attack http://www.pharmexec.com/what-has-pharma-learned-merck-cyber-attack April 2020

Klubenspies,Lou. 5 Facts about Cyber Security for Pharmaceutical Companies https://www.coursehero.com/file/36910066/5-facts-about-cyber-and-pharmapdf/ April 2020