THE ECONOMIC IMPACT OF CYBER-ATTACKS

[**Issue Number 108 - April 2019**](https://www.lebarmy.gov.lb/en/content/108-d)

**The Economic Impact of Cyber-Attacks**  
Prepared By: B. Gen. Eng. Robert Mansour  
officer in the lebanese army

**Introduction**

The increased use and integration of IT systems and networks in business and commercial entities bring both opportunity and danger. As more companies integrate and incorporate cloud-based systems into their infrastructure to move processes online, the threat of cyber-security breach increases, and the damage it can cause is growing dramatically. Today, all companies are reliant on information technology to a certain extent. Due to this, companies need to make security as a top priority since the threat of such a system being down directly injures the internal work of the company or any agency. Conversely, many organizations count on network infrastructures that are formed of older, out-of-date components that run the vulnerable software, and thus lack cyber resilience.

Cyber-criminal activity is one of the major challenges that humanity will face in the next two decades.

Cyber-terrorism and data breaches are the greatest threat to every individual and any company in the world, and one of the biggest problems with mankind. The impact on society is reflected in the numbers.[[1]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn1" \o ")

The World Wide Web, “www”, was invented in 1989. The first-ever website went live in 1991. Today, there are more than 1.2 billion websites. There are around 3.8 billion internet users in 2017 (i.e. 51% of the world’s population of 7 billion), up from 2 billion in 2015. Cyber-security Ventures predicts that there will be more than 6 billion internet users by 2022, and more than 7.5 billion internet users by 2030.

Microsoft estimates that digital growth, with its evaluation of online data volumes, will be 50 times greater in 2020 than they were in 2016.

"The Big Data Bang" is an IoT[[2]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn2" \o ") (Internet of Things) world that will explode from 2 billion objects (smart devices that communicate wirelessly) in 2006 to a projected 200 billion by 2020, according to Intel.

Gartner[[3]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn3" \o ") estimates that more than half a billion wearable devices will be sold worldwide in 2021, up from roughly 310 million in 2017. Wearables include smartwatches, head-mounted displays, body-worn cameras, Bluetooth headsets and fitness monitors.

Despite the promises from biometrics developers predicting a future with no more passwords, which may, in fact, come to pass at one point in the far out future, a 2017 report mentions that the world will need to cyber protect 300 billion passwords globally by 2020.

Each year, there are 111 billion lines of new software code being produced that introduces a massive number of vulnerabilities that can be exploited.

The world’s digital content is expected to grow tremendously. It is doubling in size every two years, and by 2020 the digital universe, the data that is created and copied annually, will reach 44 zettabytes (ZB), or 44 trillion gigabytes (GB). (This is how big a zettabyte is[[4]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn4" \o ")).

The far corners of the Deep Web, known as the Dark Web, are intentionally hidden, and used to conceal and promote terrible criminal activities. Some estimates put the size of the Deep Web (which isn’t indexed or accessible by search engines) at as much as 5,000 times larger than the surface web and growing rapidly at a rate that defies quantification, according to one report.[[5]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn5" \o ")

ABI, a technology market intelligence company, has forecasted that more than 20 million connected cars will ship with built-in software-based security technology by 2020, and Spanish telecom provider Telefonica states by 2020, 90% of cars will be online, compared with just 2% in 2012.[[6]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn6" \o ")

Hundreds of thousands, and possibly millions, of people can be hacked now via their wirelessly connected and digitally monitored Implantable Medical Devices (IMDs), which include Implantable Cardioverter Defibrillators (ICD), deep brain neurostimulators, pacemakers, insulin pumps, ear tubes and more.

The impact on countries is just as important when it comes to international relations. Just look at the hack of the Democratic Party and the publication of confidential emails during the 2016 US presidential election, which elevated cyber security in the context of international affairs to a new level around the world.

Hackers will target any industry they can profit from, and this is highlighted by the wide range of nations and industries impacted by the ransomware attack last month. Aside from any financial loss the biggest impact can be on reputation and share price.

Right now, cyber-criminals and bad actors are busy stealing data from within corporate networks and listing it for sale on the dark web. Most organizations neither know about it nor are they equipped to detect or do anything about it. Employee names, addresses, logins, and corporate credit card information is readily available, and companies carry on completely unaware of any illegal activity.

Most companies are not doing enough to secure the assets they’re creating. Large organizations can have incredibly complex networks and ‘border-control’ issues as they can struggle to secure their IT infrastructure & supply chain. Smaller organizations find it easier to understand where their system borders are, but may lack resource and expertise to secure them.[[7]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn7" \o ")

However, analysis shows that some sectors are potentially more at risk than others. For example, according to Price water house Coopers’ 2014 “Global Economic Crime Survey”, 39% of financial sector respondents said they had been victims of cyber-crime, compared with only 17% in other industries. Other research from Trend Micro assessed breaches that took place between 2005 and 2015 and showed health care as the most highly targeted industry for data breaches.[[8]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn8" \o ")

The vice president of MEMS and Sensing Solutions at Fairchild Semiconductor, Dr. Janusz Bryzek, predicts that there will be 45 trillion networked sensors 20 years from now. This will be driven by smart systems, including IoT, mobile and wearable market growth, digital health, context computing, global environmental monitoring, and IBM Research’s “5 in 5”, Artificial Intelligence (AI), hyper-imaging, macroscopes, medical “labs on a chip,” and silicon photonics.[[9]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn9" \o ")

Ultimately, businesses need to consider the cost/benefit of investing in better security systems and changes in practice, to reduce the impact on their business-critical processes. Investment in these approaches may be seen as disproportionately high given the likely impact of an attack; but as we’ve seen successful attacks can, and do, negatively impact reputation in significant means, and it is these intangibles that are hard to regain. Rather than an expense, improving security should be viewed as an investment, and insurance against brand damage to help ensure future longevity.

Consequently we came to the big question, are detection and security measures worth the investments?

**Body**

Seldom a day passes without a new media story about hacking schemes, data breaches, or cyber-attacks impacting individuals, companies, and even governmental agencies.

Threats and attacks could be against any sector; healthcare, defense, military, communications, ports, banks, power-plants and grids, critical infrastructures, financial, food and agriculture, transportation, and any database. Consequently, the internet is being weaponized, and cyber-security companies could be considered part of our defense industry.

As a matter of fact and illustration, on February 4th, 2016, due to the cyber-attacks on the Central Bank of Bangladesh, the losses were estimated not less than $81m, in addition to the prevention of another $850 million in transactions from being processed. The Yahoo breach resulted in more than 500 million users having their data stolen. The type, scale, and malicious nature of attacks are becoming more deep and profound. Even with the well documented confrontational or adversarial effects of an attack or hack, many companies have neither sufficient policy in place to be protected against this threat, nor do they possess an adequate response plan for an attack [[10]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn10" \o ").

Fundamentally, companies don’t have full control over the motivations or capabilities of their attackers, but they can make it harder to access their classified information and networks. Attackers include cyber criminals, hacktivists (who are politically motivated to cause damage), and even industry competitors and foreign intelligence services, attempting to gain economic advantage, uncover strategies, or damage reputations.

The consequences or outcomes of an attack have different effects as well, ranging from data theft, data deterioration or damage (deleting or wiping files), and exploring and interrupting systems or services. The information collected can include any number of objects or articles, for example concerning e-commerce platforms, security question answers, which are used by platforms to protect users when resetting passwords and authorizing accounts. Such answers, containing a mother’s maiden name for example, could be the same across multiple services, and are widely used by an extensive variety of other platforms including Apple’s iTunes and Amazon Prime, which can be exploited to access other data. Though companies are becoming more sophisticated in coding and encrypting moving data (i.e., data transmitted between entities) data at rest is often left unsecured and unsafe. Hence, this is therefore not unlike a criminal syndicate following a heavily secured truck to an unsecured warehouse where the cargo is unloaded.

Furthermore, attackers can use ransomware to hold data hostage in return for a massive acquisition. Ransomware provides cyber attackers with an easy method to extract more money directly from users, and Cisco noted, in their 2016 Annual Security Report, that the use of such software is on the rise.

In May, 2017, after the WannaCry attack[[11]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn11" \o "), cyber-security became a top priority in organizations of every type throughout the world. The young cyber-security industry also became a hot topic on Wall Street, and many stocks soared in price. As a result, WannaCry held the title as the most unprecedented cyber-attack of the year because of the incredibly broad impact and how fast the attack spread. Once WannaCry was activated to unleash devastation, it quickly spread to reportedly more than 100 countries in less than 24 hours. And while the Ransomware attackers only received over $140,000 in bitcoin from the operation, a report by CBS News said that the losses due to the ransomware attack were estimated to reach around $4 billion![[12]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn12" \o ")

**A.   Domains of Impact**

Market Research Media, for instance, reports that the cyber spending at the federal level in US rose from $7.5 billion in 2007, and would have to grow at 12% a year just to hit $22 billion in 2022.[[13]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn13" \o ") Even at that level, “the annual cyber-security spending of the U.S. federal government is larger than entire national cyber-security spending of most countries in the world,” the analysts note, adding that the government sector “is under constant pressure to boost investments in cyber-security technologies”[[14]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn14" \o "). Accordingly, the major domains are:

**i- Data Breaches**

A data breach is a security incident or event in which confidential, sensitive, protected data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so. One of the biggest phishing incidents in recent history affected Google and Facebook, which both were scammed out of over $100 million in a sophisticated attack.[[15]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn15" \o ") This is concerning because it affects the supply chain and trade relationships. Trade is driven by trust, and if you can’t trust who you are trading with, it undermines the relationship.

**a. Average Cost of a Data Breach**

• Globally: $3.62 million average cost of a data breach, up 17% since 2013.[[16]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn16" \o ")

• In the U.S. only: $7.35 million average cost of a data breach, up 25% since 2013, as cleared in figures 1 & 2 below.[[17]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn17" \o ")

**b. Average Cost per Record Breached**

• Globally: $141 average cost per record breached.[[18]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn18" \o ")

• In the U.S. only: $225 average cost per record breached.[[19]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn19" \o ")

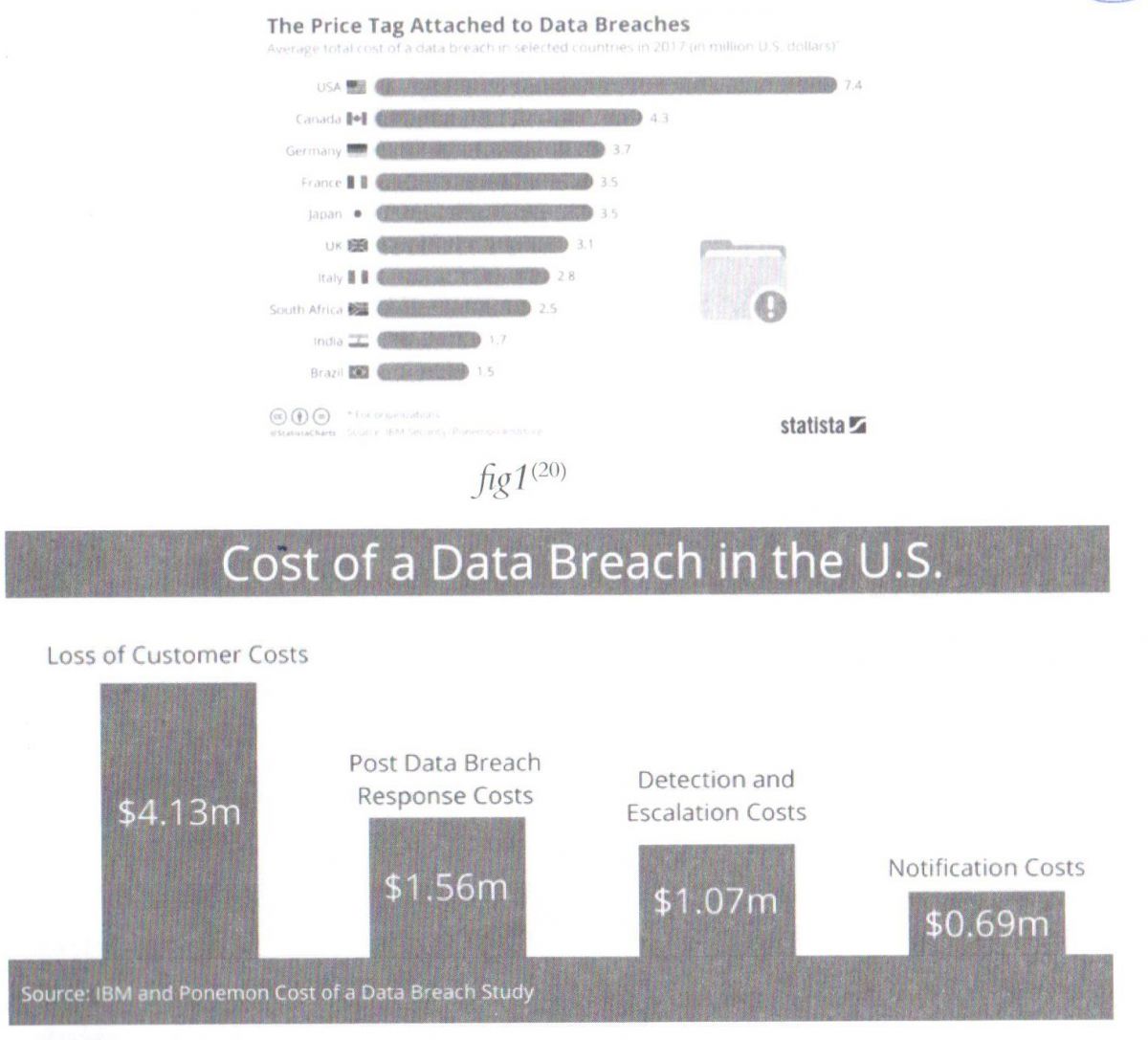


fig1[[20]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn20" \o ")

**ii- Social Sites**

Through online social media, many other competitive organizations attempt to decrease the reputation, regarding the brand, source, field of job, etc. They post or tweet negative propagations against an organization so that it reduces the trust among the people.

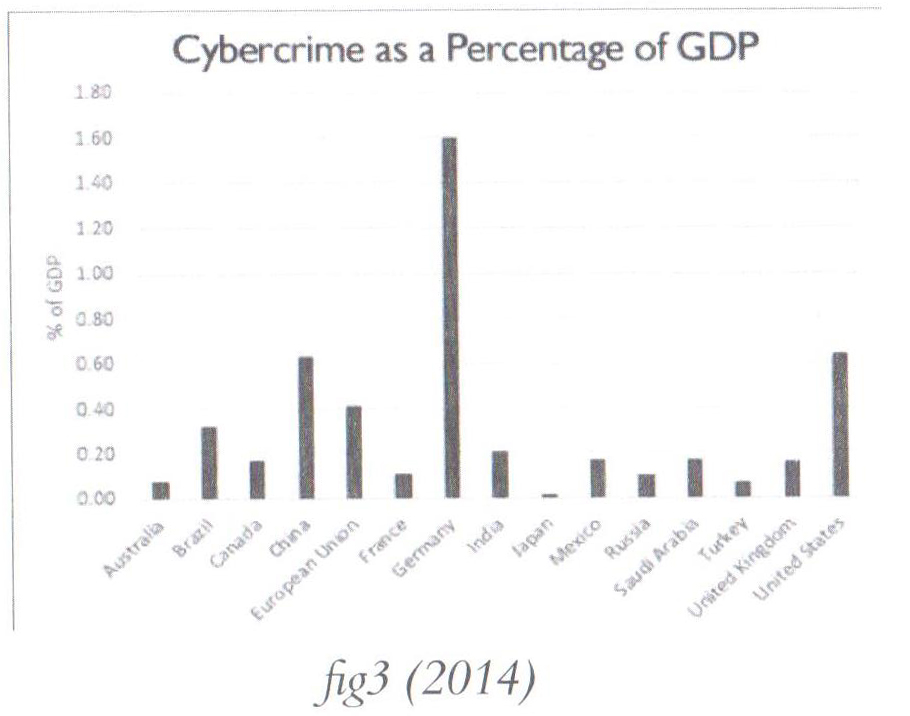
**iii- Cyber-crime**

As crimes with global impact go, a cyber-crime is becoming a world scale issue regarding economy and it ranks third, behind government corruption and narcotics as a global economic scourge.[[21]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn21" \o ") Cyber-crime is harsh, relentless, undiminished, and unlikely to stop. It is just too easy and too rewarding, and the chances of being caught and punished are perceived as being too low. Cyber-criminals, at the high end, are as technologically sophisticated as the most advanced Information Technology (IT) companies, and, similarly, have moved quickly to adopt cloud computing, artificial intelligence, Software-as-a-Service, and encryption. Cyber-crime continues to remain far too easy, as many technology users miss or fail to take the most basic protective actions or measures, and many technology products lack sufficient and suitable defenses, while cyber-criminals use both simple and advanced technology to identify targets, automate software creation and delivery, and legalizing what they steal, converting them into a legal tender.[[22]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn22" \o ")

Cyber-crime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration, deletion of hacked data and systems, and reputational harm.

In 2014, taking into account the full range of costs, cyber-crime costed the world between $345 billion and $445 billion.

As a percentage of global GDP, cyber-crime costed the global economy 0.62% of GDP in 2014. Figure 3 below[[23]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn23" \o "), shows some values of this field.



Using the same analytical methods, the range is now between $445 billion and $600 billion. Our second effort at a global estimate suggests that as a percentage of global GDP, cyber-crime cost the global economy 0.8% in 2016.[[24]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn24" \o ") The global cost of cyber-crime continues to increase; this isn’t a surprise due to the intensification of this kind of illegal practice. According to an analysis conducted by Cyber-security Ventures, the cost of cyber-crime could reach $6 trillion by 2021.[[25]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn25" \o ")

Cyber-crime is no longer driven by the individual acts of basement-dwelling loners. It has grown to become an industry in itself, with vast amounts of money there for the taking for any attacker willing and able to exploit organizations’ weaknesses. As attackers become more ingenious, all major fields of interest to those attackers will become more vulnerable. The growth of the cyber-crime activities will force an increase in the global spending on cyber security products and services. Global spending is expected to exceed $1 trillion cumulatively over the next five years, from 2017 to 2021.[[26]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn26" \o ") The fields of cyber-crime include:

• Financial

• Ransomware

• Tor[[27]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn27" \o ") and Bitcoin

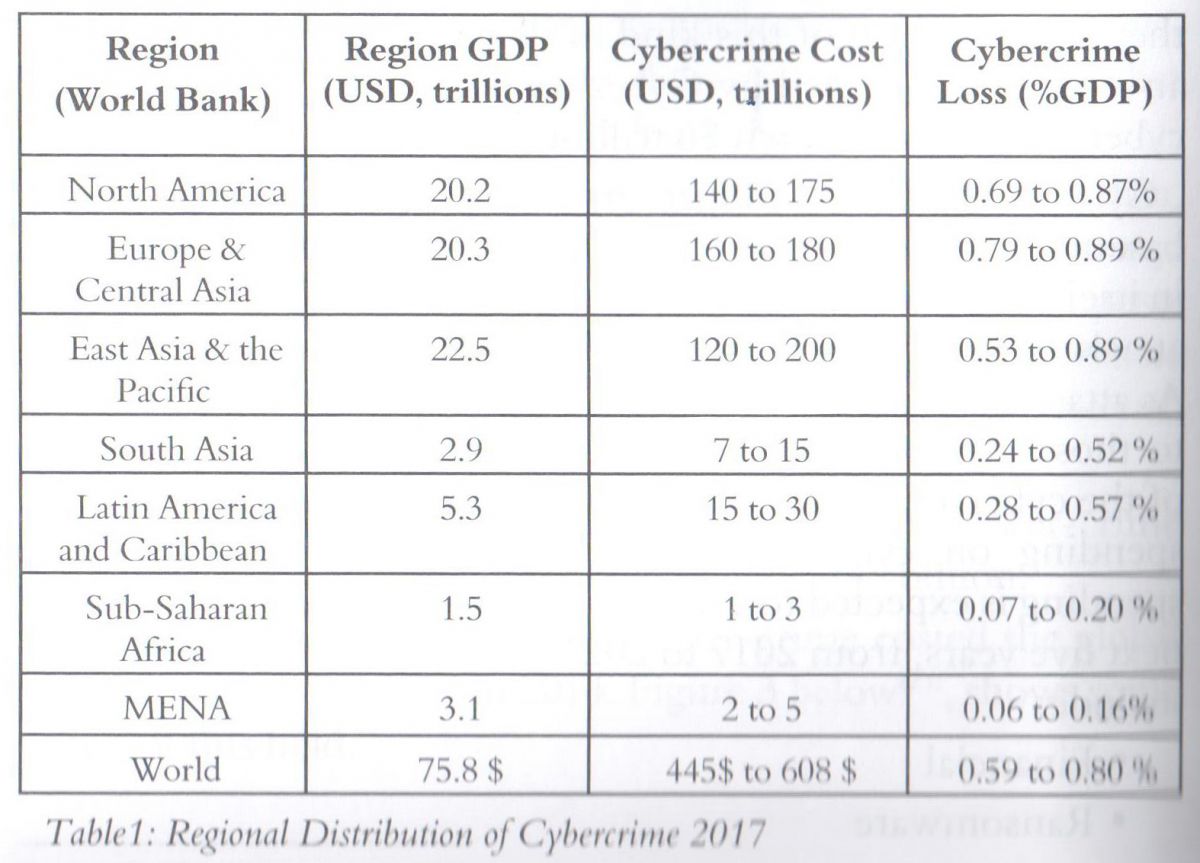
• Intellectual Property Theft

• Identity Theft

At the same time, more stringent regulations are being put in place, such as the EU’s General Data Protection Regulation, GDPR, that will increase the penalty for companies that fail to protect European data from cyber threats.

When this comes into force in 2018, the courts will be able to fine companies up to EUR 20m or 4% of global turnover, whichever is higher, if they fail to comply with the new rules.

The cost of cyber-crime is distributed among all the countries of the world, no one is immune. Table 1 below shows variations by region that are linked to income levels and level of cyber-security maturity, the countries with greater losses are the richest ones.[[28]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn28" \o ")



**iv- Cyber-Terrorism**

The most dangerous cyber-terrorism attacks are those that affect national infrastructure or business systems. Although cyber-terrorism may not be able to generate the same effect as a physical explosion, cyber-terrorism can lead to extensive monetary loss. If cyber terrorists shut down the Amazon.com website, potential customers would buy goods from other online sellers. In this case, only Amazon.com would lose the sale, however other online sellers would benefit from this incident.

However, if the intrusion resulted in the creation of fake or spurious transactions, especially to key financial institutions, such as the national/federal banks, then this could create a panic amongst businesses, which would, in turn, impact the national economy adversely.

Compared with other terrorism approaches, cyber-terrorism requires fewer people and fewer inputs. Cyber-terrorism does not require the cyber terrorists to be physically present. Cyber terrorists can remotely launch attacks, and remain anonymous by using proxy servers and IP-change methods to hide their real addresses. Because cyber terrorists can easily hide their identity, it is difficult for government agents to trace and capture them.[[29]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn29" \o ")

**v- Social Engineering**

It is a method to get the critical information of authentication and identity by social interaction with the intended person. An outside hacker uses socio-psychological tricks on important employee in context to an organization to gain access to their system. So in this technique the needed information is obtained directly from the person rather than breaking into the system without even realizing that they have been manipulated.

**vi- Phishing**

Phishing is an attempt to acquire vital information such as username, password, credit card details, pin code, account number, unique id through deceiving as trust worthy entity. It can be done by SMS, e-mail, telecommunication etc. As RSA Anti-Fraud Command Center reported the total number of fishing attacks was 59% higher than 2011 in 2012.The global losses estimated at $ 1.5 billion in 2012 was 22% higher than 2011.[[30]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn30" \o ")

**vii- Malware**

The malicious software installed in a system is a malware. Dramatically, it has abilities, and it can communicate to its originator in background without the knowledge of the system administrator. It is the most powerful tool to harm an organization. It can be installed by e-mail, downloading attachment, and sometime by USB or other external devices. In public sector, one e-mail out of 72 in public sector, 163 in education, 218 in finance, 235 in marketing, and 236 in accommodation industry contains a malware.[[31]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn31" \o ")

**viii- DDoS- Distributed Denial of Service**

In distributed denial of service attacks, the attackers makes the resources unavailable to the legitimate users. The attacker creates botnets and malware in the networks and create zombie machines that are remotely controlled by the attacker and constantly send request to the server then the server gets so busy to avail the services or resources to the intended users. According to Neustar[[32]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn32" \o ") survey over 300 businesses were targeted by DDoS attacks. Mostly web based industries such as financial services, telecom services, retail, travel, IT were victimized often. When a website goes down it costs up to $10K per hour.[[33]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn33" \o ")

**B.    Cyber Economic Facts/Stats/Results**

**i- Facts**

The cyber security industry is rapidly growing every day. As more specialists join the ranks, more malware is being launched than ever before; 230,000 new malware samples/day. Although more resources are being deployed to counter cyber-attacks, the nature of the industry still has a long way to go before we can, as a whole, catch up with these threats. It’s important for us to define what the current information security and cyber security industry looks like with these alarming cyber security facts and stats[[34]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn34" \o "):

a. There is a hacker attack every 39 seconds, affecting one in three Americans each year.

b. 95% of breached records came from three industries in 2016: Government, retail, and technology.

c. 43% of cyber-attacks target small business. 64% of companies have experienced web-based attacks. 62% experienced phishing & social engineering attacks. 59% of companies experienced malicious code and botnets and 51% experienced denial of service attacks.

d. The average cost of a data breach in 2020 will exceed $150 million, as more business infrastructure gets connected.[[35]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn35" \o ")

e. Since 2013 there are 3,809,448 records stolen from breaches every day, 158,727 per hour, 2,645 per minute and 44 every second of every day.[[36]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn36" \o ")

f. Over 75% of health care industry has been infected with malware over last year.[[37]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn37" \o ")

g.Large-scale DDoS attacks up 140 percent in 2016’s fourth quarter. [[38]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn38" \o ")

h. Approximately $1 trillion is expected to be spent globally on cyber-security from 2017 to 2021.[[39]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn39" \o ")

i. Unfilled cyber-security jobs worldwide will reach 3.5 million by 2021. More than 209,000 cyber-security jobs in the U.S. are unfilled, and postings are up 74% over the past five years.[[40]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn40" \o ")

j. By 2020 there will be roughly 200 billion connected devices. The risk is real with “Internet of Things”-IoT and its growing. According to figures compiled within a recent Symantec Internet Security Threat Report, there are 25 connected devices per 100 inhabitants in the US.[[41]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn41" \o ")

k. Only 38% of global organizations claim they are prepared to handle a sophisticated cyber-attack.[[42]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn42" \o ")

l. Total cost for cyber-crime committed globally has added up to 100 billion dollars. Don’t think that all that money comes from hackers targeting corporations, banks or wealthy celebrities. Individual users like you and me are also targets. As long as you’re connected to the Internet, you can become a victim of cyber-attacks. What does it all mean? Last year, Ginni Rometty[[43]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn43" \o "), said: “Cyber-crime is the greatest threat to every company in the world.” And she was right. During the next five years, cyber-crime might become the greatest threat to every person, place and thing in the world.

**ii- Concerns**

The last years experienced some of the biggest cyber-threats in recent history, with millions of consumers and thousands of businesses affected by everything from major attacks, such as “WannaCry”, to the “Equifax”, and “Uber” data breaches. Gartner reports that worldwide, information security spending will increase tremendously, and the 2017 Cybercrime Report anticipates cyber-crime damages to cost the world trillions annually by 2021.[[44]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn44" \o ")

So, how can businesses and governments protect themselves from falling victim to next year’s most anticipated security attacks?

a. Sophisticated cyber-attacks are the biggest technology concern in 2018. Breaches and cyber- attacks are becoming a daily occurrence. Targeted attacks, by skilled and persistent cyber criminals, are now a business reality. Cyber-attacks have become more sophisticated and attackers use a variety of tactics, such as:

• Social Engineering by manipulation through “SMiShing”, phishing, vishing (voice or VOIP) phishing, etc.

• Malware by malicious software that damages your computer network or information.

• Ransomware, including Petva, WannaCry and NotPetya.[[45]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn45" \o ")

b. In the age of Blockchain and Cryptocurrencies, the crypto-jacking “gold rush” will be the top priority for cybercriminals. Crypto-jacking activity began exploding toward the end of 2017, and it’s suspected that there will be far more activity in 2018, particularly as the value of cryptocurrencies escalates. What makes this kind of activity interesting is how it has created a blurry line between the everyday Internet user and the cybercriminal. An individual mining cryptocurrency could very well be mining for their own wallet, based on visitors to their own web properties. There is also a very likely chance within those circumstances that disclosed crypto-jacking activity could replace advertising on sites to become an entirely new revenue stream. However, the largest portion of crypto-jacking is likely to occur from legitimate websites compromised to mine currency for the criminal wallet.

c. Malicious script-based attacks, specifically PowerShell-based attacks, are incredibly difficult to identify. They can easily evade antivirus engines, making it that much more appealing to cybercriminals. PowerShell is an attacker’s tool of choice for conducting file-less malware attacks.

d. The cybercriminal underground will continue to evolve and grow. While it may seem like we are already overwhelmed by the amount of cyber-attacks occurring daily, this will not slow down in the coming future. In fact, with a recent increase in cybercriminal tools and a lower threshold of knowledge required to carry out attacks, the pool of cybercriminals will only increase. This growth is a likely response to news media and pop culture publicizing the profitability and success that cybercrime has become. Ransomware alone was a $1 billion industry last year. Joining the world of cybercrime is no longer taboo, as the stigma of these activities diminishes in parts of the world. To many, it’s simply a “good” business decision. At the same time, those already established as “top-players” in cybercrime will increase their aggressive defense of their criminal territories, areas of operations and revenue streams.[[46]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn46" \o ")

e. Security software will have a target on its back. By targeting trusted programs, and the software and hardware supply chain, attackers can control devices, and totally manipulate users. Hackers will leverage and exploit security products, either directly subverting the agent on the endpoint, or intercepting and redirecting cloud traffic to achieve their means.

f. Investing in cyber security fields, training and digital skills will be critical and crucial for business leaders if they want investors to increase confidence in their companies.[[47]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn47" \o ")

**iii- Results**

A successful cyber-attack can cause major damage to any business. It can affect your bottom line, as well as your business' standing and consumer trust. What cyber economic numbers can be resulted, gathered, or collected from the massively expanding cyber-attack surface?

a. Cyber-crime damages will cost the world $6 trillion annually by 2021.[[48]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn48" \o ")

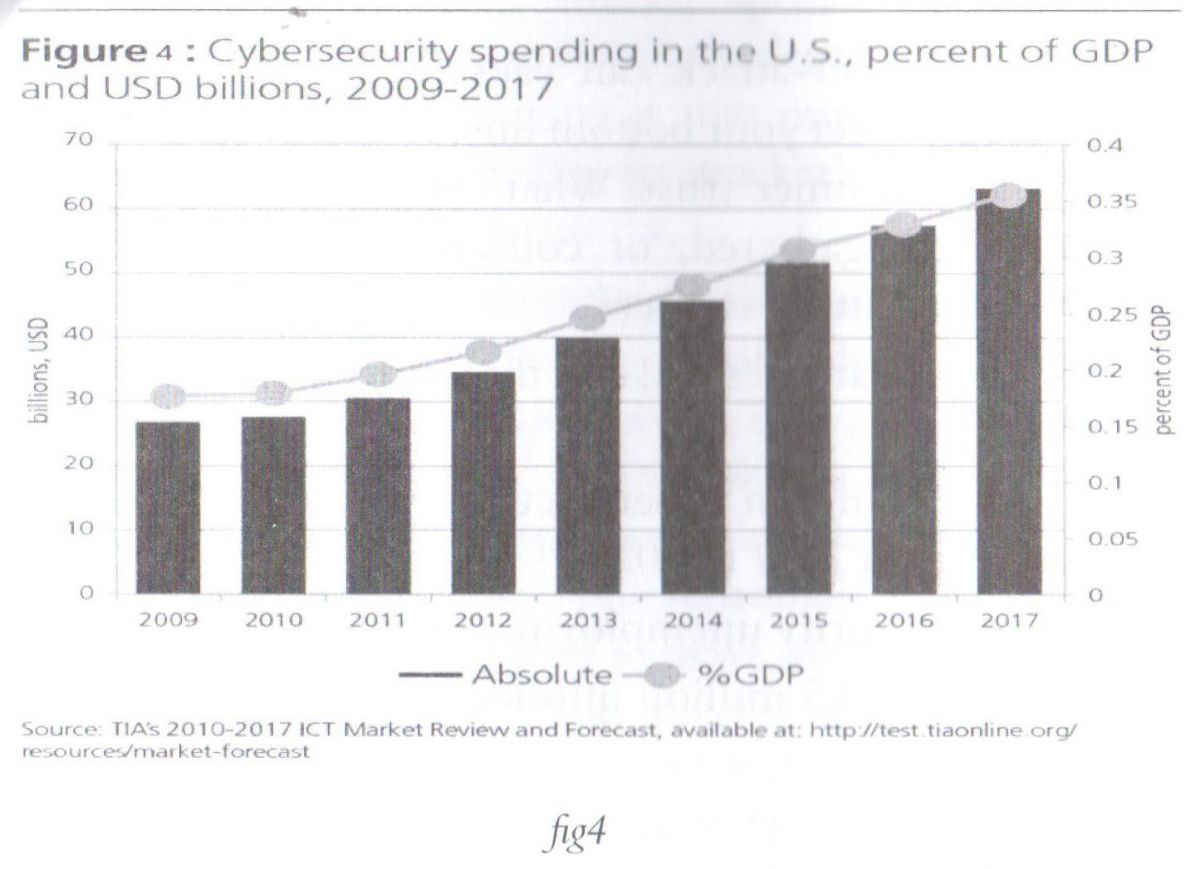
b. Global spending on cyber-security will exceed $1 trillion cumulatively from 2017 to 2021.[[49]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn49" \o ")

c. The cyber-security unemployment rate is 0%.

d. There will be 3.5 million unfilled cyber-security positions by 2021.[[50]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn50" \o ")

e. The demand for cyber-security professionals will increase to approximately 6 million globally by 2019, according to some industry experts cited by the Palo Alto Networks Research Center.[[51]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn51" \o ")

f. Billions of dollars are being pumped into cyber-security startups by Venture Capitals -VCs and corporate investors.[[52]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn52" \o ") Moreover, countries of superpower capabilities are spending tremendously in cyber-security domain with high percentage value of GDP that exceeds some budgets of small countries as in the case of USA, presented figure 4 below.



g. Reputational damage: Cyber-attacks can damage the targeted business reputation, and erode the trust of customers. Potentially, this could lead to:

• Loss of customers

• Loss of sales

• Reduction in profits

h. Legal consequences: Data protection privacy laws require proper management of personal information of costumers, and any breach could result in fines and regulatory sanctions.

i. Loss of IP: Sometimes the Intellectual Property of an organization like patent, copyright trade secret is stolen which causes a huge loss.

j. Loss of sensitive business information: The data that has value in worth of money should be preserved, but loss of such data causes harm to the organization as it can be used by the competitors.

k. Lack of Trust: Once an organization faces a cyber-attack then customers do not feel safe with that organization anymore. It compels its customers to move on to other services.

l. Business Disruption/ Lost Sales: Due do different types of attacks business or sales also affected. In denial of service attack customers cannot get the services and this results in losses to the organization in a very short period of time.

m.  Equipment Loss: Sometimes the malwares destroy the whole networking equipment, and this forces organizations to spend a lot of money to reinstall them.

n. Stock Prices: The attacker may interpret the stock prices of the organization to reduce the value and image of the particular organization by using malwares.

**C.    What can be done?**

However, there are contests to be overcome:

i- Contribute to a stronger security posture, identify critical security tasks, allocate the responsibility for those tasks, and implement successful cyber security programs.

ii- More cyber-security is better cyber security. Governments, companies, and different sectors only really understand the importance of security when they do not have it and something happens.

iii- Invest in capacity building and develop resources, through building knowledge, understanding, and awareness. This can allow for a maximal utilization of the Internet and secure its users against threats and attacks.

iv- Human Resource of an organization should be trained time to time to raise awareness about the latest attacking technique.

v-  Develop cooperation between the private and public sector, as this will be indicated as vital to protect digital assets and improve cybersecurity.

vi- Develop effective information sharing channels to ensure that software vulnerabilities are addressed before hackers can exploit them.

vii-  Establish a cyber-security strategy, with proper action plans.

viii- Implement cyber security standards like ISO 27001, BS 7799, etc. to confirm the security.

ix. Data Loss Prevention (DLP) tools can also be used to monitor the data flow.

x- Conduct regular risk assessments and define vulnerabilities. Organizations must now be information security conscious and must develop and implement proper security controls based on the results of their internal risk assessment and vulnerability assessment.

xi- Concentration on better technology provides better security.

xii. Know your security risks, requirements and capabilities, putting in mind that in this asymmetric battle an attacker only needs to be right once, while organizations need to be successful every time, so can we afford security that’s just “good enough”?

xiii. Detection and prevention are the primary measures of success for security, even though detection rates are only one piece of the puzzle, the better measures of success ought to include:

• Number of incidents resolved.

• Speed of incident resolution.

• Potential business impact of the incident.

xiv- Identify the true costs of ineffective security.

xv-  Invest in Cyber-security for the following reasons:

• Detection and analyzing type and frequency of attacks.

• Cost of attacks, direct and indirect consequences.

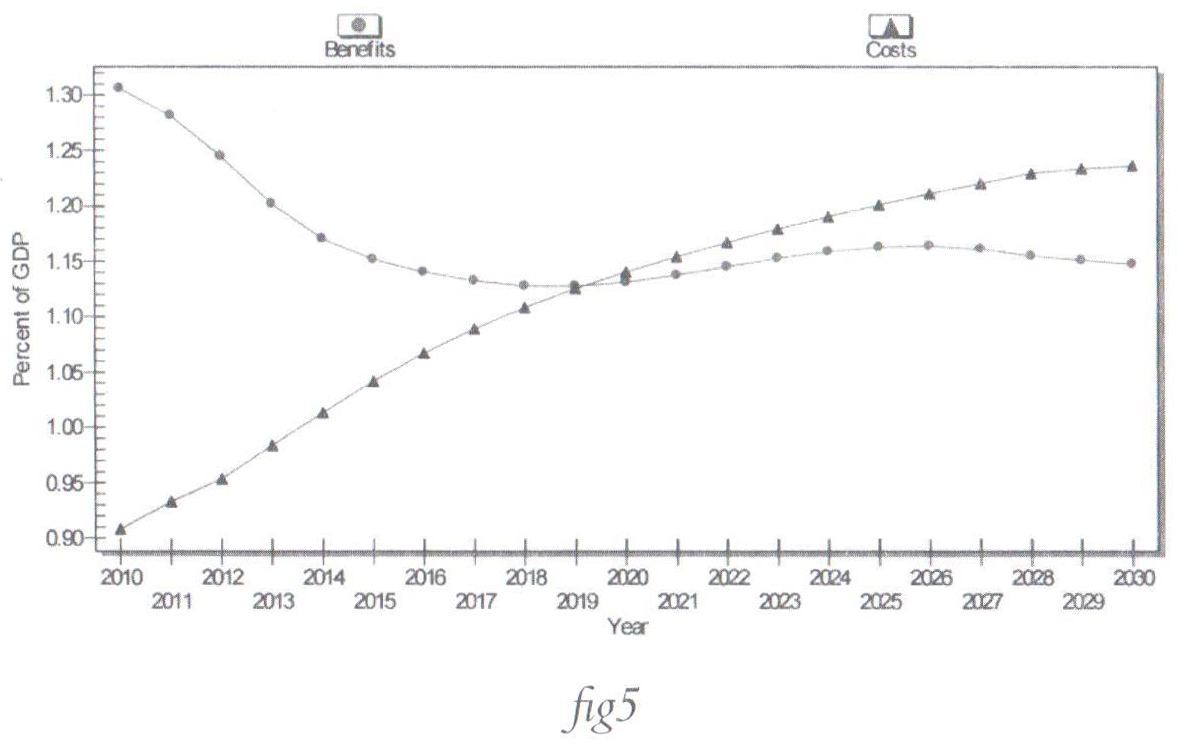
• Cyber-crime focuses on Small to Medium Enterprises (SMEs) as attack targets.

• The number of bad players is expanding rapidly.

• Bad guys are looking for low-hanging fruit, i.e. the employees.

• Better ROI (revenue on investment) on the long term, as

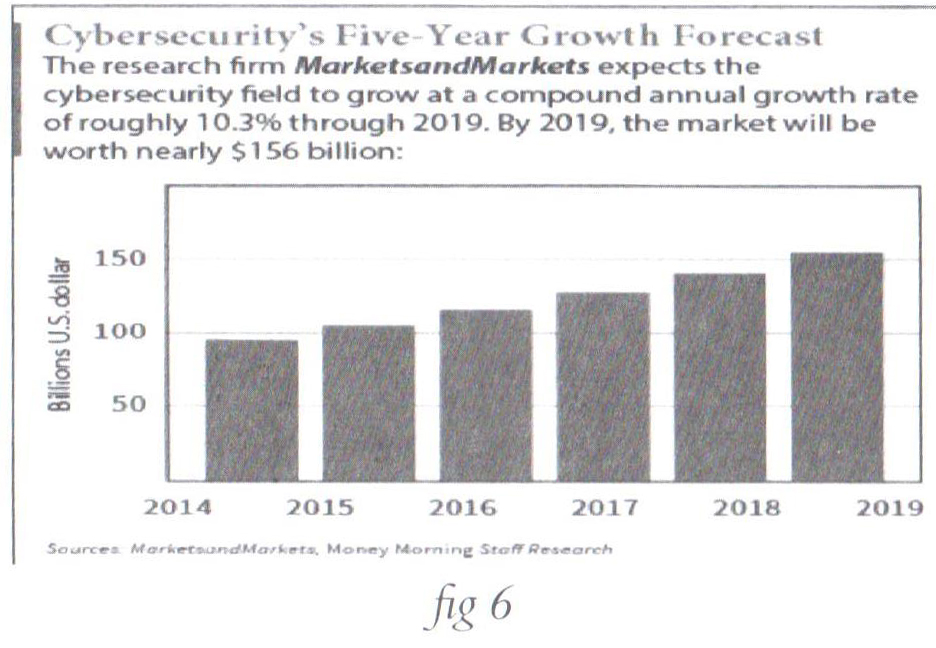
shown in figure 5 below[[53]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn53" \o ").



Comparing the information in both figures, Fig.4 and Fig.5 illustrated earlier, it’s clear that on the long term the investments paid in building security capacities will turn to be an increase on revenues through minimizing the risks and mitigating the threats, though the costs required for an acceptable level of security measures won’t be cheap.

Moreover, there are some countries such as Israel that is ranked among top countries in cyber industry, and as the state is either the owner or the strategic partner in the cyber-security powerhouse; its revenues are increasing tremendously[[54]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn54" \o ").

Not to forget that as the number of cyber-attacks increases, more growth appeared in the market size of security equipment, thus an increase of sales, deals, and development of measures with additional pouring of money in the cyber-security industry as illustrated in figure 6 below[[55]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn55" \o ").



**Conclusion**

The Cyber-attacks through the Internet is a new thing, and new things can appear more alarming and frightening than they really are. Businesses need to take the economic impact of cyber-threats more seriously, as the cost of cyber-attacks is increasing tremendously and massively.

Cyber-attacks posture a very real risk in their potential for crime, and for driving and imposing economic costs far out of proportion compared to the price of launching the attack. When research shows that the number of detected security incidents increased by 38% from 2014-2015, and the cost per breach increased by nearly 20% to $15 million in the same time frame, then it’s necessary to take notice[[56]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftn56" \o ").

Both nations and organizations can take several steps as a way to reduce losses and focuse on the costs of cyber-threats through consistent implementation of key security measures, increase international law enforcement cooperation among nations and the private sector, boost the level of awareness among different generations and types of users, apply different tracks of training and educations of such aspects, investing in more resources for investigation, especially among developing nations.

The costs associated with cyber-attacks, in most cases, are neither clear nor transparent, due to the concern that most of the companies or governmental agencies are often aware and guarded about the extent of their losses from cyber-attacks for fear of reputational damage or legal action.

Moreover, it’s important to focus on the organization risk, but how to manage this risk? How do you identify critical security tasks, allocate the responsibility for those tasks, and implement successful cyber-security programs? We don't need to wait to be breached; we have to start planning now.

 In light of these issues, Cyber connectivity is an important driver of productivity, innovation, and growth for every nation’s economy, but it comes at a cost. Companies, individuals, and governments are vulnerable to malicious cyber activity. Effective public and private-sectors efforts to combat this malicious activity would contribute to domestic GDP growth. However, the ever-evolving nature and scope of cyber threats suggest that additional and continued efforts are critical and necessary, and the cooperation between public and private sectors is the efficient key.

To mitigate the risk of future cyber-attacks, nations, governments, individuals, and corporations need to maintain up-to-date technology, training, and improve information sharing of technical vulnerabilities.

Given the amount of economic damage involved, policymakers and companies need to take proactive measures to prevent cyber-attacks.

**References**

- Anderson, R. (2001), “Why Information Security is Hard- an Economic Perspective”, Proceedings of the 17th Annual Computer Security Applications Conference.

- Grady, M. (2005), “The Law and Economics of Cybersecurity”, Cambridge University Press, 2005.

- Bank Info Security, https://www.bankinfosecurity.com/, “Assessing the Cost of Cybersecurity”, 2015.

- Bloomberg, https://www.bloomberg.com/middleeast, “Cyber Threats Top Concerns for U.K. Investors, Business Leaders”, 2018.

- Center for Strategic and International Studies (2016), “Significant Cyber Incidents since 2006”.

- CSO, from IDG, https://www.csoonline.com/, 2017.

- Cyber Security Ventures, https://cybersecurityventures.com/.

- FireEye, https://www.fireeye.com/, 2017.

- Gartner, https://www.gartner.com/en.

- International Journal of Information & Computation Technology, http://www. irphouse.com, 2014.

- McAfee, “The Economic Impact of Cybercrime and Cyber Espionage”, Jul.,2013

- IMF, “Cyber Risk, Market Failures, and Financial Stability”, Aug., 2017.

- Juniper Research, https://www.juniperresearch.com/home, 2015.

- NASDAQ, “The Best Type of Cybersecurity Companies to Invest in Now”, Feb., 2015.

- PwC Global, www.pwc.com, “Pulling fraud out of the Shadows”, 2018.

- Research Gate, https://www.researchgate.net/publication/, The Journal of Cyber Terrorist Attack, “The Economic Impact of Cyber Terrorism”, 2013.

- Security Affairs, https://securityaffairs.co/wordpress/, “The Global cost of cybercrime jumped up to $600 Billion”, Paganini, 2018.

- Statista, The Statistics Portal, https://www.statista.com/, “The Price Tag Attached to Data Breaches”, Martin Armstrong, 2017.

- The Economist, https://www.economist.com/, “Cyber-boom or cyber-bubble?” 2015.

[[1]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref1" \o ")-   https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/, access date: 02/05/2018.

[[2]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref2" \o ")-   https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT, access date: 03/05/2018.

[[3]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref3" \o ")-   Gartner is the world's leading research and advisory company.

[[4]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref4" \o ")-   One zettabyte equals 270 bytes

[[5]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref5" \o ")-   https://www.csoonline.com/article/3241816/security/cyber-attack-surface-facts-figures-and-statistics-for-2017-to-2022.html, access date: 04/05/2018.

[[6]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref6" \o ")-   Ibid

[[7]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref7" \o ")-   https://www.finance-monthly.com/2017/07/your-thoughts-how-are-cyber-threats-damaging-the-global-economy-markets/

[[8]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref8" \o ")-   https://www.pwc.com/crimesurvey

[[9]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref9" \o ")-   Ibid.

[[10]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref10" \o ")-  https://themarketmogul.com/cyber-security-attacks-effects-role-law/, access date: 29/04/2018.

[[11]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref11" \o ")-  https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack, access date: 10/05/2018.

[[12]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref12" \o ")-  https://www.lbmcinformationsecurity.com/blog/4-of-the-most-expensive-cyber-attacks-of-2017-and-how-they-could-have-been-prevented, access date: 22/07/2018.

[[13]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref13" \o ")-  https://www.fifthdomain.com/civilian/2017/09/01/how-much-does-federal-government-spend-on-cybersecurity/, access date: 08/05/2018.

[[14]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref14" \o ")-  Ibid

[[15]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref15" \o ")-  https://www.theguardian.com/technology/2017/apr/28/facebook-google-conned-100m-phishing-scheme

[[16]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref16" \o ")-  https://www.ibm.com/security/data-breach, access date: 01/10/2018.

[[17]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref17" \o ")-  https://www.statista.com/chart/9918/the-price-tag-attached-to-data-breaches/, access date: 01/10/2018.

[[18]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref18" \o ")-  Ibid.

[[19]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref19" \o ")-  https://blog.dashlane.com/data-breach-statistics-2018-forecast-everything-you-need-to-know/, access date: 27/05/2018.

[[20]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref20" \o ")-  https://www.statista.com/chart/9918/the-price-tag-attached-to-data-breaches/, access date: 28/04/2018.

[[21]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref21" \o ")-  Op. cit., p.5

[[22]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref22" \o ")-  Center for Strategic and International Studies, https://www.csis.org/analysis/economic-impact-cybercrime, access date: 8/5/2018.

[[23]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref23" \o ")-  https://www.financialsense.com/contributors/guild/cybercrime-s-global-costs, access date: 05/05/2018.

[[24]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref24" \o ")-  Op. cit., p.5

[[25]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref25" \o ")-  https://securityaffairs.co/wordpress/50680/cyber-crime/global-cost-of-cybercrime.html, access date: 09/05/2018.

[[26]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref26" \o ")-  Ibid

[[27]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref27" \o ")-  Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy

[[28]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref28" \o ")-  https://securityaffairs.co/wordpress/69401/cyber-crime/cybercrime-cost-2017.html, access date: 24/7/2018.

[[29]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref29" \o ")-  Journal of Strategic Information Systems, https://www.researchgate.net/profile/Jian\_Hua3/publication/261860155\_The\_economic\_impact\_of\_cyber\_terrorism/links/5a9dc896a6fdccff6d1a19b3/The-economic-impact-of-cyber-terrorism.pdf, access date: 08/05/2018.

[[30]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref30" \o ")-  https://www.ripublication.com/irph/ijict\_spl/ijictv4n9spl\_11.pdf, access date: 21/07/2018.

[[31]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref31" \o ")-  Ibid.

[[32]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref32" \o ")-  Neustar, Inc. is an American technology company that provides real-time information and analytics for the Internet, telecommunications, entertainment, and marketing industries.

[[33]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref33" \o ")-  http://www. irphouse.com, access date: 21/07/2018.

[[34]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref34" \o ")-  https://www.cybintsolutions.com/cyber-security-facts-stats/, access date: 21/07/2018.

[[35]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref35" \o ")-  https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

[[36]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref36" \o ")-  Op.cit.

[[37]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref37" \o ")-  https://cdn2.hubspot.net/hubfs/533449/SecurityScorecard\_2016\_Healthcare\_Report\_Final.pdf

[[38]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref38" \o ")-  Ibid.

[[39]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref39" \o ")-  https://cybersecurityventures.com/cybersecurity-market-report/

[[40]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref40" \o ")-  https://www.threatadvice.com/blog/FaceTheFacts

[[41]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref41" \o ")-  https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

[[42]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref42" \o ")-  https://www.tektonikamag.com/wp-content/uploads/2017/05/HP-White-Hat-AI-e-book-04-24.pdf

[[43]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref43" \o ")-  IBM’s chairman, president and CEO

[[44]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref44" \o ")-  https://www.csoonline.com/article/3241766/cyber-attacks-espionage/top-5-cybersecurity-concerns-for-2018.html

[[45]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref45" \o ")-  https://www.itgovernance.co.uk/blog/sophisticated-cyber-attacks-are-biggest-technology-concern-in-2018/

[[46]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref46" \o ")-  Ibid.

[[47]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref47" \o ")-  https://www.bloomberg.com/news/articles/2018-02-26/cyber-threats-top-concerns-for-u-k-investors-business-leaders

[[48]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref48" \o ")-  https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/, access date: 02/10/2018.

[[49]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref49" \o ")-  https://cybersecurityventures.com/cybersecurity-market-report/, access date: 02/10/2018.

[[50]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref50" \o ")-  https://cybersecurityventures.com/jobs/, access date: 02/10/2018.

[[51]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref51" \o ")-  https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf, access date: 22/07/2018.

[[52]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref52" \o ")-  https://www.csoonline.com/article/3241816/security/cyber-attack-surface-facts-figures-and-statistics-for-2017-to-2022.html, access date:  06/05/2018.

[[53]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref53" \o ")-  https://www.bankinfosecurity.com/assessing-cost-cybersecurity-a-8529, access date: 6/05/2018.

[[54]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref54" \o ")-  https://www.economist.com/business/2015/07/30/cyber-boom-or-cyber-bubble, access date: 01/06/2018.

[[55]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref55" \o ")-  https://www.nasdaq.com/article/the-best-type-of-cybersecurity-companies-to-invest-in-now-cm449507, access date: 06/05/2018.

[[56]](https://www.lebarmy.gov.lb/en/content/economic-impact-cyber-attacks" \l "_ftnref56" \o ")-  https://www.fireeye.com/current-threats/what-a-ceo-needs-to-know-about-cyber-security/executive-playbook.html, access date: 07/05/2018.

**التأثير الاقتصادي للهجمات الإلكترونية**

واحدة من أهم المخاطر الإلكترونية تكمن في الاعتقاد بأنّ الهجمات الإلكترونية غير موجودة. أما الخطر الآخر فهو في محاولة معالجة المخاطر المحتملة جميعها.

حاليًا أصبحت الهجمات الإلكترونية أكثر تواترًا، ويمكن أن تستهدف وتؤثّر في أهداف من كل الأحجام حول العالم. ويطرح المجتمع الرقمي أنواع مختلفة من التحديات بأوجهٍ مختلفة ومن بينها الأثر الاقتصادي للهجمات الإلكترونية.

بدأت الدول والشركات والوزارات وغيرها من القطاعات بالاستثمار بشكلٍ كبير في مجال التدابير الأمنية، في محاولة منها لخفض أعداد الهجمات الإلكترونية أو حتى منع حصولها، ولكن هل تُعد كلفة هذه التدابير مقبولة؟

وفقًا إلى تقرير صدر حديثًا عن مؤسسة "Lloyd’s" تبيّن أنّه يمكن لهجومٍ إلكتروني شامل أن يتسبب بخسائر اقتصادية، يمكن أن يصل حجمها إلى 53 مليار دولار، وهي كلفة تفوق حجم الخسائر الناجمة عن إعصار "ساندي" الكارثي الذي ضرب الولايات المتحدة في العام 2012. وأشار التقرير إلى أنّ الخطر الإلكتروني هو تهديد عالمي يتزايد وطأة. التحوّل الرقمي يُحدث ثورة في مجال النماذج التجارية، كما يتسبب بتحوّلاتٍ تطال حياتنا العادية، ويجعل الاقتصاد العالمي أكثر عرضة للهجمات الإلكترونية.

احتساب الأثر الاقتصادي للهجمات الإلكترونية مسألة في غاية الصعوبة لأن المعلومات المجموعة غير مكتملة. بعض البلدان يتمتع بأنظمةٍ قوية معتمدة لجمع المعلومات المتعلقة بحوادث الهجمات الإلكترونية، ولكنّنا نجد في بلدان أخرى أنظمة ضعيفة لنقل المعلومات، وأحيانًا أخرى يمكن أن تكون هذه الأنظمة غير موجودة إطلاقًا.

الهدف من هذا المقال هو تقديم مقاربة تحليلية عن تأثير الخروقات التي تطال المعلومات والجرائم الإلكترونية والإرهاب الإلكتروني من وجهة النظر الاقتصادية. هذا المقال يُبرز أيضًا الأرقام المتعلقة بالكلفة العالمية والنتائج التي تنجم عن مثل هذه الهجمات، ويصف بعض الحلول لمثل هذه التأثيرات.