Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6, 9245-9252
2024
Publisher: Learning Gate
DOI: 10.55214/25768484.v8i6.3980

The impact of cyber-attacks on companies and organisations in developed countries

Ali Khalid Diwan Kazim[1*], Nisreen Riad Shanshul[2]
[1,2]Nahrain University / Faculty of Political Science / Department of International Economic Relations Country/Iraq;
ali.merp22@ced.nahrainuniv.edu.iq (A.K.D.K.) dr.nisren@nahrainuniv.edu.iq (N.R.S.).

Abstract: Cyber-attacks are a growing threat to businesses and organisations in developed countries. They bring about significant financial losses, operational disruptions, and a decline in customer confidence. It is estimated that cybercrime could run up the global economy to $10.5 trillion annually by 2025 in comparison to $3 trillion in 2015. For example, British companies ran into losses estimated at $55 billion during 2018–2023 as a result of these attacks. These attacks go after vital sectors such as financial services, energy, and healthcare. They disrupt daily operations and bring on direct and indirect financial losses. In addition, the loss of sensitive data can bring down corporate reputation and lower customer and investor confidence. To deal with these challenges, it has become necessary to step up cybersecurity investments and work out sophisticated defence strategies.

Keywords: *Cybersecurity, Cyber attacks, Digital economy, Developed countries, Economic impact.*

1. Introduction

Cyber-attacks make up one of the major threats and major challenges facing companies and institutions in developed countries. These attacks bring about a variety of forms such as viruses, malware, and denial of service attacks. They set out to disrupt systems or make off with sensitive information, and are continuously building up in complexity and diversity. In light of the growing reliance on technology and digital systems, these attacks greatly bring down the business environment. They can bring about huge financial losses, reputation damage, and loss of trust by customers. Attacks can shut down business operations and bring down competitiveness. Reputational damage and loss of trust by customers can come up, as attacks can break down business operations and cut down competitiveness. In addition, cybersecurity costs are going up dramatically, forcing companies to put in huge investments and come up with effective strategies to stand up to ongoing risks and deal with these threats. Furthermore, companies may run into legal penalties if they cannot properly look after their customers' data.

1.1. The Importance of Research

The importance of the research comes up from the increasing intensity of cyber attacks, their threats and risks to organizations and companies in developed countries, and their high financial and economic costs. This stands out especially since cyber power has turned into one of the most important forms of power in the world today. This came about after countries stepped up their dependence on computer systems, internet networks and information infrastructures following the technological revolution.

1.2. The Research Problem

The main research problem stems from the negative effects of cyber-attacks on companies and organisations in developed countries. Several sub-questions arise from this, as follows:

* Correspondence: ali.merp22@ced.nahrainuniv.edu.iq

- What is the impact of cyber-attacks on the systems of digital organisations in developed countries?
- Is there an impact of cyber-attacks on the systems of digital companies in developed countries?

1.3. Research Objective

The main objective of this research is to point out the negative effects of cyber-attacks on the economies of developed countries. It also aims to analyse the losses of companies and organizations coming up from cyber-attacks (e.g. remediation costs, loss of revenue, and reputational losses).

1.4. Research Hypothesis

The research sets out on the hypothesis that there is an inverse relationship between cyber attacks and the digital economies of developed countries. As the risks and effects of cyber attacks go up, this brings about the decline and impacts of the digital economy of developed countries. Conversely, the more there is determinants and perceptions of the risks and effects of these attacks, the more it brings about the growth and development of the digital economies of developed countries.

1.5. Research Methodology

For the purpose of forming the objectives of the study and its hypothesis, the inductive method was adopted by following through the part in order to get to the whole by dealing with the molecules by analysis and then generalisation in subsequent stages, and making use of the descriptive-analytical approach to describe and analyse the impact of cyber attacks on institutions and companies in developed countries.

1.6. Research Structure

This research has been broken up into eight sections. Firstly, the increased costs caused by cyber attacks. Secondly, the loss of trust and difficulty in bringing in customers and business partners. Thirdly, the impact on the company's reputation and brand and the drop in the growth rate of its sales. Fourthly, we look into the decrease in the value of shares. Fifthly, the drop in revenue and the increase in the financial burden of the company due to imposing fines and spending additional time and effort to clear up the damage caused by cyber-attacks. Sixthly, we delve into the violation of digital intellectual property rights. Seventhly, we discuss the business interruption and changing work policies causing disruption of services. And eighthly, we delve into the reduction in wages and incentives. As well as reaching conclusions.

1.7. The Impact of Cyber Attacks on Companies and Organizations in Developed Countries

The risk of cyber-attacks comes at the forefront of the risks that threaten commercial organizations and companies of all types and sizes. These attacks bring about serious damage to the brands and reputation of companies and organizations. This often ends up in serious financial damage. The cyber risk cuts into the net profits of each of them. This leads to increased costs and reduced revenues. According to a study carried out by the Institute of Internal Auditors in North America for the year 2022, cybersecurity risks are the leading among 13 other risks affecting business organizations. Another study carried out by the Institute of Internal Auditors in the European Union found that cybersecurity risks are among the top five risks that threaten the business environment. There is also the impact of cyber risk on the ability of commercial organizations and companies to take on and hold on to customers, in addition to cutting down on innovation (Arif, 2022, p. 435). It can be said that the threat of cyber-attacks to companies and organizations of all kinds affects them in various aspects, including the following:

1.7.1. First: Increased Costs

Where the costs taken on by institutions and commercial companies to defend their systems against expected and unexpected cyber risks go up, such as covering the legal expenses resulting from the realization of the cyber risk, or making sure that the company lives up to the legal standards to be

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 9245-9252, 2024
DOI: 10.55214/25768484.v8i6.3980

followed to avoid fines, crisis management costs from communications and lawyers, investigation costs from technical experts and consultants, repair and reconstruction costs, lost data recovery costs, notification fees, and delayed fines resulting from the breach of contracts with customers and operational losses after the occurrence of the cyber risk (Kathuriya, 2022, p. 56).

1.7.2. Second: Loss of Trust and Difficulty in Attracting Customers and Business Partners

The discovery of many violations brought about by cyber risks to commercial organizations and companies, and the difficulty of tracking down the perpetrator, leads up to, in most cases, huge material and moral damages. This brings down trust between business partners and customers and holds back attracting them. This is especially true after commercial companies come to rely on the cyber environment to put out most of their services and the great threats that this brings along (Juma, 2019, p. 11).

Customers, and even suppliers, turn away when they turn over their sensitive information to a company whose IT infrastructure has been broken into at least once before. For example, following the cyber threat to Equifax, an American multinational consumer credit reporting agency based in Atlanta, Georgia. It stands out as one of the three largest, along with Experian and TransUnion (collectively known as the "Big Three").

Equifax takes up and puts together information on more than 800 million individual consumers and more than 88 million businesses worldwide. In addition to credit and demographic data and services to businesses, Equifax puts out credit monitoring and fraud prevention services directly to consumers.

TransUnion is an American consumer credit reporting agency that pulls in information on more than one billion individual consumers in more than thirty countries, including "200 million files featuring virtually every credit-active consumer in the United States". Its clients bring up more than 65,000 businesses. Headquartered in Chicago, Illinois, TransUnion's revenue in 2014 came up to US$1.3 billion. It comes across as the smallest of the Big Three credit agencies, along with Experian and Equifax (known as the "Big Three").

Experian is a multinational data analytics and consumer credit reporting company headquartered in Dublin, Ireland. Experian takes in and works up information on more than one billion people and businesses, including 235 million individual U.S. consumers and more than 25 million U.S. businesses. It shows up on the London Stock Exchange and comes out as a component of the FTSE 100. Experian teams up in validating USPS addresses. It stands out as one of the "Big Three" credit reporting agencies, along with TransUnion and Equifax.

Both TransUnion and Experian, the two largest credit reporting agencies in the United States, ended up being negatively impacted as customers feared that a similar breach could come about again. This brought about a credit freeze at these companies, and regulators brought in stricter measures to keep similar breaches from coming up in the future. For example, one in five French companies pointed out difficulty in bringing back customers after a cyber incident or breach, and 16% of Belgian companies that were broken into lost business partners according to the report of the British company Hisox Internet Risk Insurance for the year 2020 (Banqa, 2019, p. 21). Hiscox is an Anglo-Bermudian insurance company that shows up on the London Stock Exchange. It stands out as a guarantor in Lloyd's of London, with special focus on specific areas of the market, reaching out to companies and high net worth individuals with property and casualty insurance. This company also deals out coverage against risks such as piracy, hijacking and satellite damage. The company features in the London Stock Exchange and makes up part of the FTSE 100 index. Setting up shop in Bermuda, it now is home to more than 3000 employees spread out in 14 countries and 34 bureaus.

1.7.3. Third: The Impact on the Company's Reputation and Brand and the Low Growth Rate of its Sales

The exposure of a commercial company to a cyber risk, or the possibility of exposure to this risk, brings down its commercial reputation. This often makes its customers turn away from investing in it. This leads up to a decrease in the rate of growth of its sales. It comes across as difficult to map out all the effects of cyber risks because it is difficult to pin down and figure out these risks.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 9245-9252, 2024
DOI: 10.55214/25768484.v8i6.3980

In general, companies that come up against one of these risks will step up investment in cyber risk management to cut down its effects. This is because these risks bring about a strong impact on the extent of customer trust in the company and its brand. This brings down its commercial reputation and, consequently, brings about the decline in sales.

From the point of view of Hiscox Insurance, the more the company comes up with good capabilities to pick up cyber risks early, the less impact shows up. This has brought about a rise in cybersecurity spending in the budgets set aside for information technology by commercial companies. Therefore, the more companies put out on cybersecurity, the more their sales growth rate goes up.

Ireland stands out at the top of the list of countries whose companies have taken up specialized cyber coverage. The United States of America and Belgium come after. Meanwhile, the United Kingdom and France came third. (Kamiya et al., 2018).

1.7.4. Fourth: Decrease in the Value of Shares

The vulnerability of commercial companies to cyber risks comes up differently according to the nature of the company's activity and the type of attack. The bringing out of a cyber violation of a commercial company often brings about a significant economic impact on the value of the shares of that company. Because of that, many commercial companies who fell victim to these attacks hold back from reporting or putting out announcements about them. The bringing up of such a violation, especially those involving the giving away of customer information, brings down the company's reputation, on the one hand. It may even lead up to paying out fines to the competent government authorities on the other hand.

There also shows up an adverse effect on the performance of companies. Studies have pointed out a decline in company performance due to falling off in sales following exposure to cyber risk.

Fifth: Lack of revenues and bringing up of the financial burden of the company due to putting forth fines and carrying out additional time and effort to sort out the damages arising from cyber attacks (Tweneboah-Kodua et al., 2018, p. 5).

An example of this comes up in the hacking incident of Home Depot, which carries out business in home appliances in 2014. The data of electronic payment cards for its customers, which came up to about 56 million customer cards, leaked out. In addition to that, 53 million e-mails broke out from the company and its customers. The intermediate attack was brought about by a third party who came across as a seller and put out malware to get hold of POS devices owned by the company. This brought about the company taking on the above loss, figured out at $300 million, spread out among fines payable due to damage from the cyber risk.

Companies usually set out to find the fastest way out of cyber risk effects. They often give in to paying out the ransom, even if the financial burden turns up large and the result doesn't pan out as guaranteed. A recent study that took in 30 companies found that 64% of them came up against a ransomware attack during 2023. It showed that 83% of these companies put up the required ransom. It also brought out that 8% of the companies that paid out the ransom wound up recovering all their data, compared to 63% picking up only half of their data.

Some companies may come across a request to put up a second ransom or perhaps more despite paying the first on time. The problem turns up more complicated when the commercial company puts forth the ransom and can't bring back its data. On the other hand, companies that work out a decision not to pay take on the cost at the level of business interruption and loss of revenues. Meanwhile, companies that are exposed by these attacks and are not backed up with a solid support system or response plan could end up suffering more than everyone. (Banqa, 2019, p. 21).

1.7.5. Sixth: Violation of Digital Intellectual Property Rights

It comes across as a set of rights to stand up for the intellectual creations of people. These rights hand over to the creator an exclusive right to put out his works for a certain period of time and make them show up on cyberspace. These rights bring up creative or innovative works built up in the information technology environment, which started to turn up with the spread of the computer.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 9245-9252, 2024
DOI: 10.55214/25768484.v8i6.3980

Technological development has brought about an expansion in the concept of digital intellectual property rights through bringing up new types of works. These were called digital works that have come to be set up on electronic media. This comes through in supports, files, data, electronic messages or documents that are worked up for the purpose of electronic circulation. They were originally put together in a digital environment or stand in as a digital form.

Data in whatever form, whether written, audio, or in the form of images, symbols or music, when put through modern means of communication, turns up as numbers that the computer works with. These then get passed along through electronic channels tied up with cyberspace.

The digital work appears to be as such since bringing forth a traditional work. The content of copyright in the digital environment displays the same in the field of traditional intellectual property. However, due to modern digital technologies, cyber risks that come up against the author's right in cyberspace prove difficult to keep under control. This results from the lack of legislation that holds up these rights.

These rights take in digital copyrights, neighboring digital rights, digital industrial property rights such as patents, digital industrial designs, and digital commercial property rights such as digital trademarks (Juma, 2019, p. 38).

1.7.6. Seventh: Business Interruption and Change in Work Policies Cause Disruption of Services

Cyber risks can bring about disrupting or temporarily holding off the practice of institutions and companies. This leads up to a decrease in their productivity and holds back providing their services. Each must think over how information is gathered up and laid down to make sure sensitive information doesn't come up at risk.

Many companies hold back from storing financial and personal information for customers such as credit card numbers, social security numbers, and dates of birth. Some shut down their online stores for fear of not being able to put forth adequate protection against cyber risks.

In 2012, a number of banks in the United States of America came up against deactivation attacks (DOSS). This brought about customers not being able to get into their accounts or put through bills online. This happened despite these banks putting out millions of dollars annually on cybersecurity to stand up against cyber risks. Despite the absence of theft of bank data and currencies, the goal of the denial of service attack turns out to be temporarily shutting down the websites of banks. This brings about disruption and putting off of business. This then brings on customer frustration and breaks down their confidence (Tariq, 2018, p. 5).

1.7.7. Eighth: Reducing the Wages and Incentives of Employees of Commercial Companies

Employees of commercial companies are generally hit by cyber attacks and the consequent ramp-up in the financial burdens of the company and the costs of clearing up the damage caused by them in the long term and at a rate of three years from the occurrence of the cyber attack on the company. This leads to employees ending up with much lower amounts than they were getting before the attack was realized. They also pay out much lower rewards than in the past (Kamiya et al., 2018, p. 30).

The table below shows some of the largest cyber attacks that occurred for the period (2013-2023).

Table 1.

Company	Cyber attack
Target (American Company)	In 2013, Target, the third largest US retail chain, was the victim of a severe hacker attack in which 70 million customers had their personal information, including their bank account details, compromised. As a result, the company's reputation took a serious hit. The cyberattack cost Target about US$1 billion and the event reduced the group's profits in the fourth quarter of 2013 by US$440 million.
The American giant company of Ebay	In 2014, the American giant eBay came under a cyberattack that cleared out the data of 140 million customer bank accounts. The stolen data included names, email addresses, postal addresses, phone numbers, dates of birth, and

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 9245-9252, 2024
DOI: 10.55214/25768484.v8i6.3980

	passwords. The passwords of eBay employees were also compromised.
Sony Pictures	In 2014, hackers penetrated Sony Pictures' computer systems at various locations of the company, including its Los Angeles headquarters and the stolen data, including new movies and confidential information, became publicly available on the internet.
Orange	French mobile operator Orange came under two online attacks in 2014, in which millions of customers' personal data was stolen and the cost of these incidents to Orange amounted to more than 24 million euros (29 million US dollars).
TV5 Monde	In 2015, the French channel TV5 Monde came under a large-scale cyber attack as the systems became unable to run on longer and the broadcast was cut off and the amount of the claim is not yet known.
Ryanair	In 2015, the company announced that hackers had stolen about US$5 million following a fraudulent electronic transfer via a Chinese bank. According to the company, the money should have been used to pay kerosene bills.
The issue of influencing the US elections	In 2016, one of the most famous cyber hacks (influencing the U.S. elections) occurred, and researchers at the IBM Institute have observed that the losses incurred by the United States due to this hack amounted to more than 35 million U.S. dollars.
Equifax Hack	In 2017, one of the largest cyber breaches in history occurred. The company announced that 147 million consumers were affected by the data breach, representing 56% of the US population. Hackers gained access to consumers' names, social security numbers, dates of birth, credit card numbers, and even driver's license numbers.
British Airways	In 2018, a group of hackers launched a "sophisticated and criminal attack" on the company's website and the company said that personal and financial data belonging to the company's customers were compromised, and the hack reached about 380,000 ticket purchases, and the value of the shares of IAG, which owns the airline, decreased by about 3%.
SolarWinds	In 2020, hackers believed to be Russian broke into the systems of Solar Winds. Their software is used by large companies and major government agencies in America. This later turned out as one of the largest cyber attacks in history. The hackers managed to sneak in malicious code. This allowed them to slip into the most sensitive systems in the world without detection for months. The company pointed out that this software reached 18,000 customers. This made up more than half of its customers. These consisted of major companies and major government agencies.
Lapsus Group	In 2022, the digital extortion ring Lapsus set up a serious hacking operation, first stealing source code and other valuable data from high-profile and sensitive companies, including Nvidia, Samsung and Ubisoft, and then leaking the data in extortion attempts.
MOVEit Hack	In 2023, more than 200 organizations and up to 17.5 million individuals were affected by the MOVEit mass breach Many federal agencies are among those affected, including the Department of Energy, Agriculture, and Health and Human Services.
WazirX hack	In 2024 WazirX, one of the most popular cryptocurrency trading platforms, went through a cyber breach, after which the platform halted trading and cut off cryptocurrency withdrawals, hackers stole $230 million worth of cryptocurrency from the platform, affecting nearly half of the platform's

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 9245-9252, 2024
DOI: 10.55214/25768484.v8i6.3980

	reserves..

Source: Source prepared by the researcher based on the Egyptian Insurance Federation Bulletin, Electronic Attacks (Cyber) and Insurance, a published article available at the following electronic link: https://www.ifegypt.org/NewsDetails.aspx?Page_ID=1244&PageDetailID=1324

2. Conclusion

To conclude this research, it is clear that cyber-attacks presents themselves as a major challenge for companies and organizations in developed countries, as they widely take over various economic, operational, and reputational aspects. Direct and indirect economic losses from attacks add up to billions of dollars annually, while operational interruption and loss of customer confidence break down the sustainability of business in the digital age. On the other hand, although many companies and organizations have begun to introduce preventive strategies such as relying on advanced technologies and stepping up employee awareness, this effort needs to bring together greater integration between governments. Striking a balance between technological innovation and security protection is key to ensuring a sustainable and secure future for businesses in developed countries.

Through the above, the research came up with a number of conclusions.

1. Cyber attacks deeply break into companies and organizations in developed countries, bringing about financial, operational, and moral damage.
2. The more advanced and electronic the country is, leaning on technology and digital intelligence, the greater the chances of coming under cyber attacks.
3. For the continuation and development of technological technology, technology has worked to break into the economic, political, and social aspects in order to carry on continuous and ongoing interaction.

As for the recommendations, as a result of the rapid growth, progress, and digital technological developments that come about in the global system at the economic, political, and social level, the researcher recommends: -

1. Drawing up cybersecurity strategies and putting forward certain measures to cut down attacks and breaches.
2. Building the digital infrastructure of companies and working on systems that confront attacks.
3. Bringing about international cooperation between governments and companies to hand over information about threats.
4. Introducing periodic training programs for employees to deal with modern fraud and attacks.

References

[1] Banqa, A. E. (2019). The risks of cyber (electronic) attacks and their economic effects: A case study of Gulf Cooperation Council countries. Arab Planning Institute, 63, Kuwait, 21.

[2] Juma, S. (2019). Insurance against risks of digital intellectual property rights violations. Alexandria: New University Press, 38.

[3] Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2018). What is the impact of successful cyberattacks on target firms? Working Paper No. 24409. National Bureau of Economic Research, Cambridge, MA, 12.

[4] Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2018). What is the impact of successful cyberattacks on target firms? Working Paper No. 24409. National Bureau of Economic Research, Cambridge, MA, 30.

[5] Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2018). What is the impact of successful cyberattacks on target firms? (No. w24409). National Bureau of Economic Research.

[6] Ramadan, A. R., & Saleh, A. M. M. (2022). Using agile methodology in improving the performance of internal auditing to address cybersecurity risks. Journal of Financial and Commercial Research, 23(3), 435.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 9245-9252, 2024
DOI: 10.55214/25768484.v8i6.3980

[7] Tariq, N. (2018). Impact of cyberattacks on financial institutions. Journal of Internet Banking and Commerce, 23(2), 5.
[8] Tweneboah-Kodua, S., Atsu, F., & Buchanan, W. (2018). Impact of cyberattacks on stock performance: a comparative study. Information & Computer Security, 26(5), 637-652.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 9245-9252, 2024
DOI: 10.55214/25768484.v8i6.3980