History, Present 2021 and Future of Cyber Attacks

Mohammed. I. Alghamdi
Department Engineering and Computer Sciences, Al-Baha University, KSA
Email: mialmushilah@bu.edu.sa

Abstract

Cyber-attacks are the attacks that target organizations and individuals either as a tool for other activities like identity theft, stalking, etc. or with a computer as a crime object like phishing, hacking, and spamming. Cyber-attacks are rapidly increasing and making cyber security a major concern currently. When launched successfully, cyber-attacks can cause massive damage to individuals and businesses. Hence, immediate response is mandatory to contain the situation in case cyber-attacks occur. In this paper, we will discuss the history, present and future of cyber-attacks and measures for organizations to prevent those attacks in future. The ever-elusive strategies and suspicious nature of criminals should also be identified. We have outlined some of the practices to prevent those attacks while recommending incidence response measures and updates in enterprises.

Keywords – cyber security, cyber-attacks, cyber criminals, cyber security practices, incidence response

1. Introduction

Cyber-attacks have been ranked 5th among top rated security risks in the year 2020 and became the new normal in private and public sectors. Cyber-attacks in IoT alone are projected to rise up by 200% by 2025 and this risky business is going to grow in the year 2021. In addition, Global Risk report 2020 released by World Economic Forum (2020) claimed that there is only 0.05% of detection in the US. The landscape of cyber security is changing rapidly, and several changes have been made in 2020 alone. Almost all kinds of businesses, whether small or large, had been affected by global pandemic, which amplified cybercrime because of uncertainties related to business security and remote working.

From data theft to data breach and ransomware, there is around 600% rise in cybercrime due to COVID-19 pandemic. Almost every industry needs to look for new solutions and adapt faster. Considering these threats, this article will help businesses to explore the types of security threats and cyber-attacks that have ever happened, present trends, and might happen in future and scholars to look for the ways to ensure cyber security in future.

1.1 Background

DOI: https://doi.org/10.54216/JCIM.080204
Received May 21, 2021 Accepted: November 01, 2021

COVID-19 took the healthcare system by storm but 2020 also brought a cyber pandemic (Lohrmann, 2021). Later on, top experts in the cyber security industry predicted 2021 to be even worse in terms of cyber security outcomes in comparison to 2020 (Lohrmann, 2021). The Orion vulnerability in SolarWinds was one of the worst data breaches ever made in December 2020 and it is still affecting over 18000 companies (Vaughan-Nichols, 2021). Microsoft recently reported vulnerabilities in its Calendar program and Exchange Server mail for government and corporate data centers. Chinese hackers were involved in causing vulnerabilities since January 2021, as per the reports of CNBC (Novet, 2021).
These are a few examples of modern cyber-attacks that have increased recently. In this article, we are going to discuss the genesis of cyber-attacks and their evolution to the present day as well as future trends of these attacks to be aware of. This research will open further research paths for academicians to explore more in this area and find more security vulnerabilities which should be addressed.

1.2 Literature Reviews

Irrespective of the impulsive changes which have taken place in the international politics, North Korea never stops posing threat to global stability by constantly advancing its "long-range ballistic missiles" and nukes. North Korea wants to make huge impact with cyber terrorism at relatively low costs of cyber offenses. **Hwang & Choi (2021)** shares the perspectives of explicit experts in cyber terrorism ever happened in South Korea to focus attention to these scenarios. At the same time, the authors claim to put emphasis on cybercrime and cyber terrorism practices and current academic trend. They adopt criminological theories and perspectives as well as network frameworks of asymmetrical and multifaceted cyber terrorism in post-modern global politics. To do this, they conducted a qualitative analysis of existing trends, forms, objectives, and characteristics of cyber-attacks by North Korea and suggest how to progress for global policy response successfully.

A huge range of cyber-attacks have been observed since the 1980s on "Industrial Control Systems" and some of them affected "critical national infrastructure". There are limitations to access data about industrial communication networks related to cyber-attacks, especially in the context of national security, Miller et al (2021) explains the publicly reported cyber-attacks despite the limitations on accessing details about cyber-attacks targeting industrial communication systems. They analysed and identified earlier cyber-attacks targeted those systems and documented their evolution. They provide great understanding to cyber-security experts about threat actors, attack vectors, targeted locations and sectors, and impact, etc. for the constant improvements in cyber security risk management plans.

COVID-19 was an unexpected and a huge event which changed the lives of billions of people across the world and changed societal norms and the way people used to live and work. Apart from the unprecedented impact on businesses and society as a whole, COVID-19 pandemic has caused a set of unique situations related to cybercrime which affected both businesses and society. The pandemic has already caused a heightened fear with the risks of cyber-attacks along with the rise in range and number of cyber-attacks. **Lallie et al (2021)** analyse the effect of pandemic in the context of cyber-attacks which have happened across the world during COVID-19. They considered and analysed cyber-attacks in major global events to explore the modus operandi of attackers. They explored the gaps between the initial

DOI: https://doi.org/10.54216/JCIM.080204
Received May 21, 2021 Accepted: November 01, 2021

COVID-19 outbreak from China and the first cyber-attack followed by a pandemic. They used the case study of the UK to show how those crooks make the most of government announcements and major events to design and execute their activities carefully.

Currently, the majority of commercial, economic, social and government interactions of different countries are conducted in cyberspace. A lot of government organizations and private players worldwide are suffering the risks of cyber-attacks on their wireless networks. Modern world relies heavily on digital technology and it is still challenging to protect data from cyber-attacks. Cyber-attacks are basically aimed to cause financial harm to the companies. Some of the common attack vectors are malware, DoS, viruses, etc. Organizations use different techniques to avoid cyber-attacks. Researchers across the world have proposed a lot of methods to avoid cyber-attacks and control the damage. **Li and Liu (2021)** conducted a comprehensive review and survey on latest advances in cyber security and investigated the strengths, weaknesses, and challenges of methods proposed. They also discussed usual security practices with the early-generation methods and history of cyber security. They also explored the latest advancements and trends in cyber threats and security along with presenting challenges.

Since the late 1960s, research on cyber security has constantly evolved as information security or computer security. **McShane et al (2021)** briefly discuss the history while focusing on latest cyber risk management strategies including both economic and technical dimensions. They are aimed to discuss major steps involved in the cyber risk control process to focus on the gaps and determine research paths. Cyber risk is not easy to be covered in the overall process of risk management on enterprise level and it is important to approach cyber resilience.

1.3 Research Gap

Cyber-attacks have been more prevalent especially since 2020. In order to deal with those attacks, it has become more important than ever to understand the root cause behind those attacks. There are so many studies related to different kinds of cyber-attacks and policy recommendations. But there is still a lack of study regarding the past, present and future of cyber-attacks. This study is aimed to fill this gap and find out the right solutions to prevent those attacks in future and financial and other losses to companies and governments.

1.4 Research Question

- What is the history of cyber-attacks?
- What are the cyber-attack trends in 2021?
- How are cyber-attacks going to be in future?

1.5 Importance of the Study

Considering the increasing instances of cyber-attacks, it becomes very important to understand how cyber attackers work and how they target organizations and individuals for cyber-attacks. It is even more important to know the origin of cyber-attacks and present scenarios. This way, we can predict how intense cyber-attacks are going to be in the near future.

DOI: https://doi.org/10.54216/JCIM.080204
Received May 21, 2021 Accepted: November 01, 2021

1.6 Research Objectives

- To know the evolution of cyber-attacks from 1990s to present
- To know the current cyber-attack trends and how to ensure cyber security
- To find out how intense cyber-attacks are going to be in future

2. Research Methodology

2.1

2.2 Research Method & Design

To address the above research questions and fulfil research objectives, we have adopted a secondary research method through desktop search and collected recent resources, when it comes to know about existing cyber-attack trends and future predictions. However, we also needed to use earlier studies to explore the history of cyber-attacks and how they evolved over time. We have found relevant evidence based on our research questions. This way, researchers can study and synthesize the results of this study to find out the right policy, practices, and future directions. We used literary studies for getting credible resources so that researchers can critically analyze limitations, assumptions, and findings. Hence, this study is aimed to pay more scientific contributions to future studies in the field of cyber security.

2.3 Research Approach

We have drawn studies on cyber threats and attacks during the pandemic since December 2019, i.e., the onset of COVID-19 and various types of cyber-attacks to different organizations across the world. We considered cybercrimes, cyber security, cyber threats, and cyber-attacks as the inclusion criteria for this research during the COVID-19 outbreak. We conducted a comprehensive search on several online portals, literature, journals, and other databases to search the specific information. We searched for relevant studies through Google Scholar as per our research questions. We chose some of the best online databases like Science Direct, IEEE Xplore, Google Scholar, SpringerLink, ACM Digital Library, and other databases as they are centralized sources for studies based on cyber security and technology.

2.4 Research Limitation

Though we have found some data from credible sources on the internet, there are some limitations of systematic research study. It has captured trends and focus areas in the literature, but there is a need to dig deeper into details and primary studies are required in this topic to assure the quality of results. In addition, more focused review of studies is required so that we can get more detailed information so that policymakers can make more informed decisions in future towards mitigation of cyber-attacks.

3. Analysis of Data

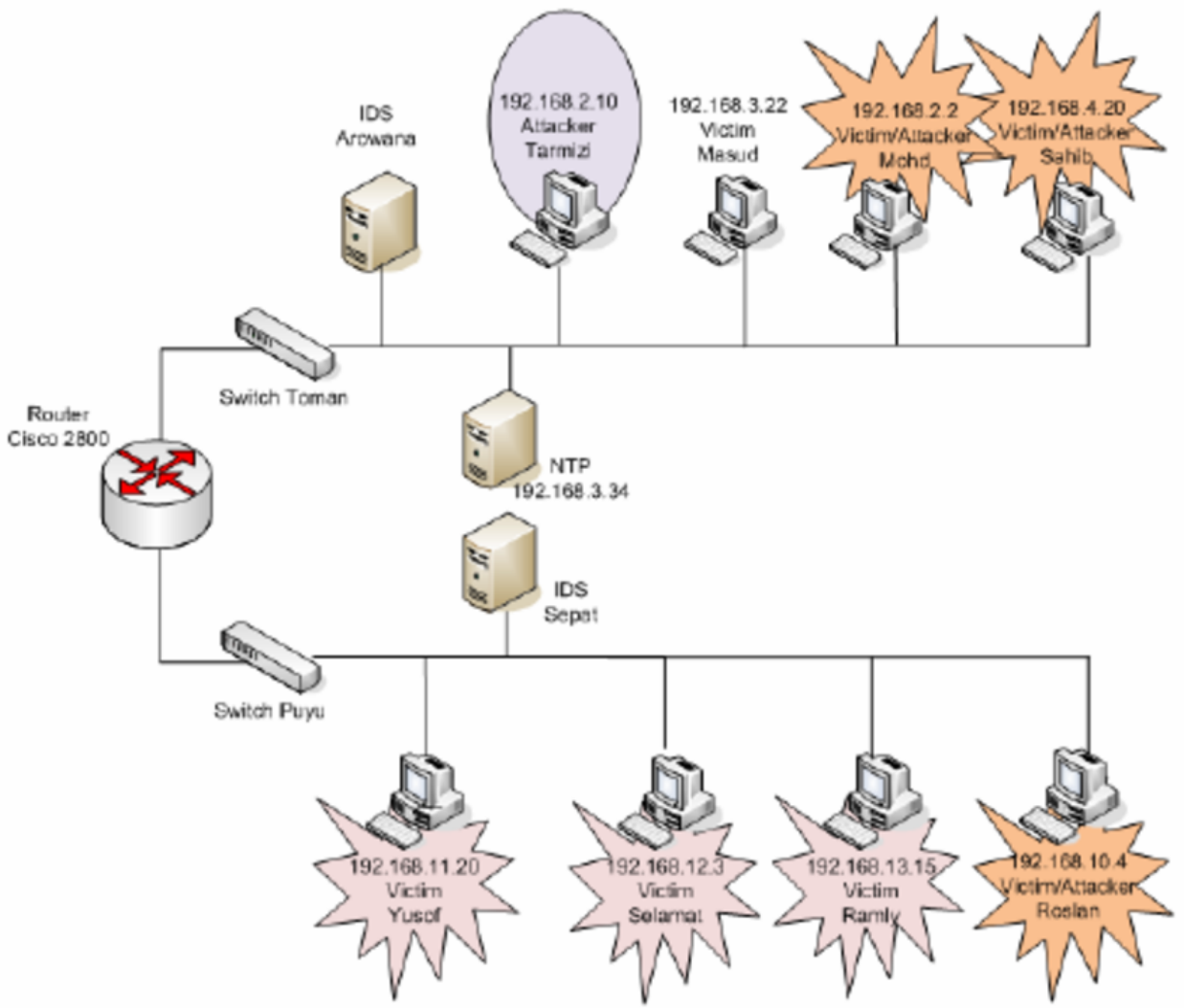
Be it Yahoo data breach, Equifax hack, Ashley Madison incident, or Exatis data leak, Cyber-attacks are constantly evolving day by day and becoming even more sophisticated (Cook, 2000; The Wired, 2018; Mindsight, 2017; Hackett, 2021). When it comes to data breaches or hacking, shady figures under the hoods stealing data for profit are the first that come in mind. But governments are also involved in cyber

DOI: https://doi.org/10.54216/JCIM.080204
Received May 21, 2021 Accepted: November 01, 2021

warfare to spy on enemy nation states. Nations may sway ideology, discourse, or voters and hackers can have a huge sum for selling electronic records of people. We have always wondered how it all started at some point. Before going any further, here are some of the most common cyber-attacks taking place these days –

- **Worms** – They simply copy themselves on other computers and deliver a payload of malicious virus or cause network overloads. Such viruses may steal valuable data like passwords, delete files, and encrypt files (in case of ransomware attack). They deliver a payload to put a backdoor, so that computers can be controlled as hackers' botnets. They remain hidden in a system and wreak havoc (Figure 1).

Figure 1 – A Diagram of Multi-step Worm Attack



Source – Robiah et al (2010)

- **Botnet Attack** – A botnet is used to attempt a Distributed Denial of Service (DDoS) attack, conduct eavesdropping, and spread malware on a network or introduce a phishing attack. There is always a botmaster to control the botnets (Figure 2). The DDoS attack vectors manipulate the networks being legitimate traffic coming through the servers and they cause major slowdowns and outages by overloading the system. These attacks target financial institutions or even businesses.

DOI: https://doi.org/10.54216/JCIM.080204
Received May 21, 2021 Accepted: November 01, 2021

Figure 2 – A Sample of Botnet Attacks

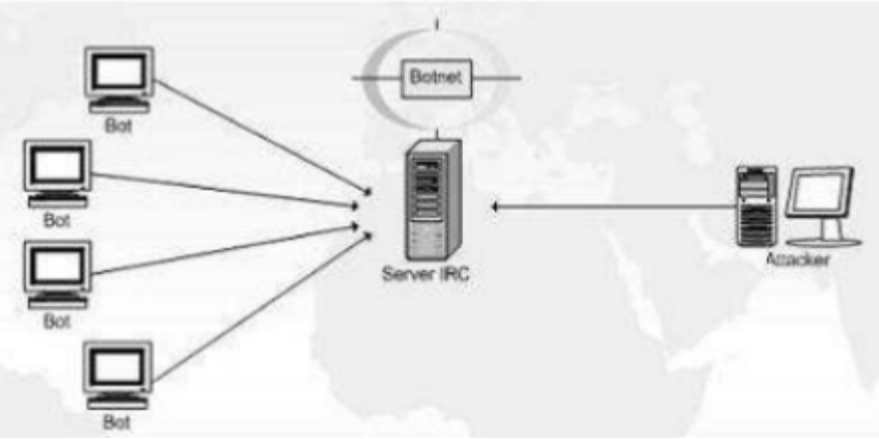


Figure 2 – Botnet attack

- **Phishing** – As the name suggests, a hacker fishes mobile and internet users for data through email, text message, or even a letter sent from a source that seems too good to be true. A representative will either lure or scare the users to share their personal data like passwords, user names, account numbers, UPI pin code, ATM pin, and other sensitive information. They can retrieve all the details they need with this attempt.
- **Trojan Horses** – Once it enters the system, it downloads the threats from the internet secretly like malware, spyware, and other computer viruses, without letting the system know about the infection.

Q. What is the history of cyber-attacks?

Hundreds of thousands of cyber-attacks have been recorded in history over the years. Here's the brief overview of some of the major cyber-attacks ever happened –

Table 1 – History of Cyber Attacks

Year	Cyber Attack Incident	Description
1988	The Morris Worm	It was done basically for good intent, but it went wrong surprisingly. Robert Tappan Morris, a student in Cornell University developed a program to determine internet size. It used to crawl over the web, get installed on other systems, and count its copies. It was done to figure out the numbers of connected systems. The problem arose when it was installed on each computer multiple times. The infected computers crashed and deliberated with each attempt. It was the first ever DDoS attack, though it was done by accident. **Damage** – Over 6000 computers were damaged by the worm (i.e., 10% of the whole internet

DOI: https://doi.org/10.54216/JCIM.080204
Received May 21, 2021 Accepted: November 01, 2021

		network of that time). Considering inflation, the damage cost from $100,000 to $1 million for restoration.
1995	Porsche Giveaway by LA KIIS FM	The 102th caller was supposed to win a Porsche by LA KIIS FM and Kevin Paulson definitely wanted to win. He used his hacking ability to block their calls and hacked the phone network to assure the slot of the 102nd caller. However, he got caught for this attempt and was booked for five years of imprisonment.
2002	DNS Attack	It was the first cyber-attack in history when the internet was targeted directly. The entire internet was assaulted by a DDoS attack for an hour by hitting 13 root servers of Domain Name System.
2008	DDoS Attack on "The Church of Scientology"	Anonymous, a famous hacker group, unleashed a DDoS Attack on "The Church of Scientology" as part of "Project Chaology" a political movement against them. Over 500 DoS attacks were made to get the Scientology website down. A teenager from New Jersey was involved who was charged heavy fines and sentenced to probation for two years.
2013	Yahoo	A state-sponsored attack was made in 2014 until Verizon declared its deal with Yahoo. It got worse because it led to compromising over 500 million accounts. Another breach took place in 2016 and over 1 billion accounts were compromised. **Damage** – According to Yahoo's valuations, the value of the company was down to around $300 million and over 3 billion accounts might be affected.
2014	JP Morgan Chase	During the summer of 2014, more than 7 million accounts of small businesses and 76 million households were hacked and hackers got their names, phone numbers, addresses, and emails.
2016	Adult Friend Finder	In October 2016, over 412.2 million account holders' names, passwords, and email accounts for over 20 years were leaked online. Poor SHA-

DOI: https://doi.org/10.54216/JCIM.080204
Received May 21, 2021 Accepted: November 01, 2021

		1 hashing algorithm was used to protect the passwords.
2017	Equifax	One of the leading credit bureaus based in the US, Equifax exposes over 143 million accounts and the data was highly valuable and sensitive. For example, driver's license, birth dates, social security numbers, and even credit card details.
2018	Exactis	An unknown Florida-based marketing firm leaked over 340 million records. Some of the major parts of the leak include name, phone number, address, number of children (even their genders and ages), habits, interests, and even whether users follow a specific religion or smoke.

Source – Mindsight (Climer, 2018)

Q. What are the cyber-attack trends in 2021?

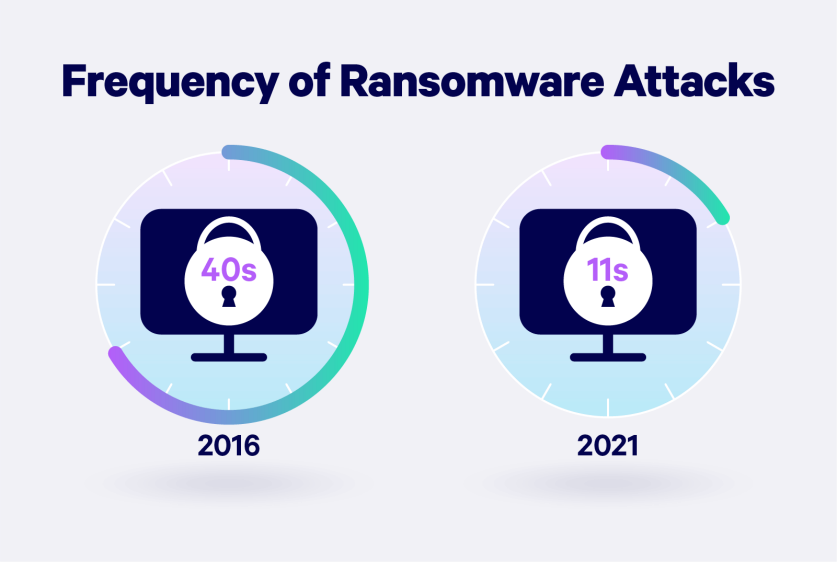
In this day and age, small and medium businesses are getting more targeted by cyber-attacks which are more frequent and complex. According to a study, small businesses are on the radar of 43% of cyber attackers and only 14% are prepared with proper cyber security measures (Accenture, 2019). Along with normal operations, cyber-attack disrupts major IT infrastructure and assets which cannot be recovered without proper resources or budget. Due to this reason, small businesses are unable to cope up with this. Here are some of the recent events happened to small and medium businesses worldwide, according to "State of Cyber Security Report" (Keeper Security, 2021) –

- 45% of small businesses are not prepared to mitigate security attacks due to insufficient measures.
- 66% of them had a cyber-attack over the past year.
- Cyber-attacks have been more targeted in 69% of cases.
- 57% of small businesses suffer phishing attacks, 30% face data theft, and 33% have stolen or compromised devices.

There are different ways cyber attackers can target an organization, i.e., by causing small disruptions to huge fiscal losses. There is some kind of cost involved in every consequence, be it monetary or otherwise, irrespective of cyber-attacks. Reputation damage, financial losses, declined productivity, legal trouble, and continuity issues are some of the consequences of cyber-attacks.

Figure 3 – Ransomware Attacks – Frequency of Cases

DOI: https://doi.org/10.54216/JCIM.080204
Received May 21, 2021 Accepted: November 01, 2021



Source – Embroker (2021)

Ransomware attacks are becoming more frequent and a common security concern. Ransomware attacks used to target businesses every 40 seconds in 2016. In 2021, it rises up to every 11 seconds (Cybersecurity Ventures). A malicious program is used in this attack to encrypt important files in a computer system and a ransom amount is demanded from the victim to decrypt the same.

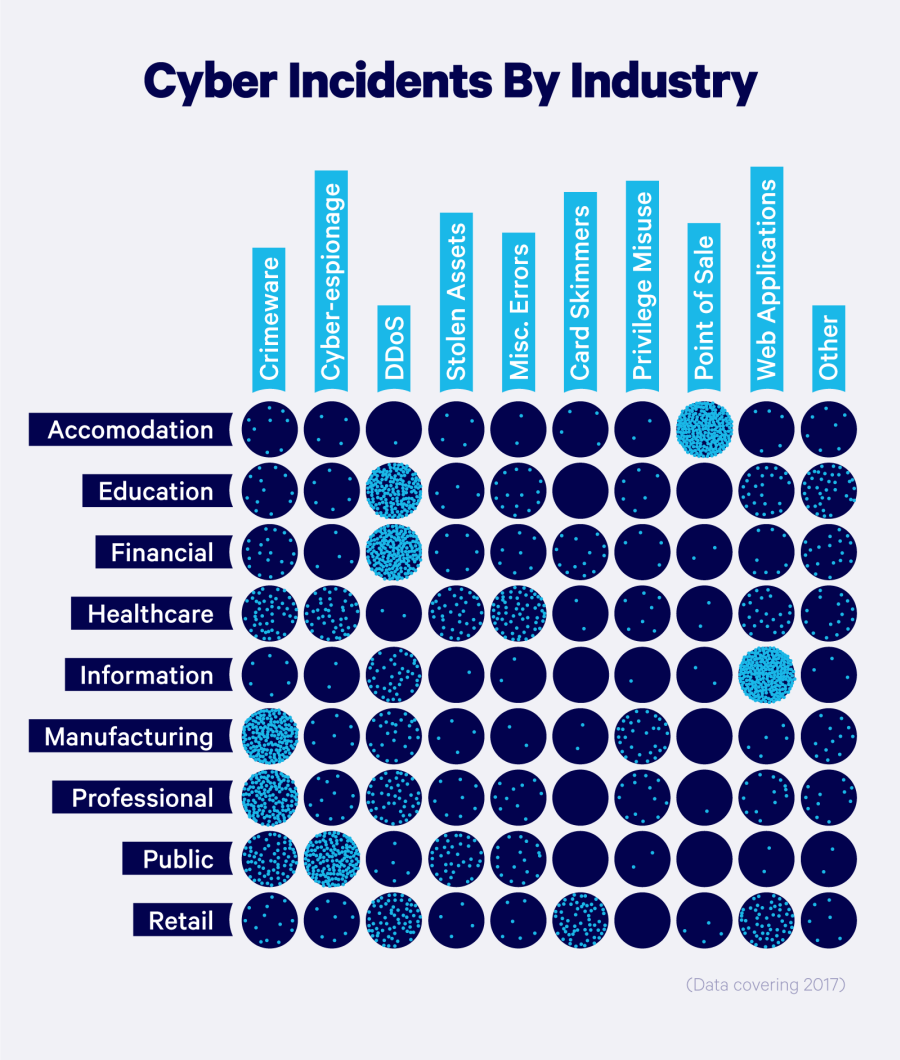
Q. How are cyber-attacks going to be in future?

Cyber-attacks target some industries even more, especially because of the kind of operations they perform. Though data breach could affect any industry, attackers usually target those who are closely related to the daily lives of people. They commonly target companies which hold personal information or sensitive data of clients. Here are some of the highly vulnerable organizations that should be very careful and be vigilant from future cyber-attacks –

- **FinTech and Banks** – They have bank details, card information, and personal data of clients or customers.
- **Healthcare** – They hold clinical research data, electronic health records (EHR), and patients' data, including billing information, social security numbers, and insurance claims.
- **Educational institutions** – They hold students' records, such as academic research, financial records, enrolment, and personal information like addresses, names, etc.
- **Companies** – They have inside information like trade secrets, product concepts, employee and client databases, intellectual property, contract deals, etc.

Figure 4 – Industries highly vulnerable to cyber attacks

DOI: https://doi.org/10.54216/JCIM.080204
Received May 21, 2021 Accepted: November 01, 2021



Source - Embroker (2021)

It is estimated that cybercrime had cost around $3 trillion to companies globally in 2015, which is projected to rise up by $10.5 trillion in 2025 annually (Intrusion Inc, 2020). According to Cybersecurity Ventures, cybercrime is increasing at around 15% per year of growth rate and greatest economic wealth transfer ever has been recorded in cybercrime.

4. Results & Findings

In a business or company, breach is discovered only when any major incident occurs. A breach is discovered after around 197 days on average in a company and it is usually contained around 69 days later, according to IBM. Companies which contained a breach after 30 days spent over $1 million as compared to those which took within 30 days. A company suffers even more trouble when they are slow to respond to a data breach. It can cause a lack of productivity, customer trust, or hefty fines.

One can be prepared in case of data breach with a proactive response plan. A risk management strategy is highly recommended to deal with incidents like breaches to mitigate the impact on the bottom line of the company. For example, a response plan can guide the team in the stages of detection, investigation, containment, recovery, and remediation. Company database might be a bunch of boring files for an average individual, but it is a goldmine for hackers. They know what to do with those files

DOI: https://doi.org/10.54216/JCIM.080204
Received May 21, 2021 Accepted: November 01, 2021

and hard drives. Most of the cyber-attacks take place by insiders, outsiders, organized crime syndicates, company partners, and affiliated groups, according to a "Data Breach Investigations Report" by Verizon[1].

It is important to prevent data breaches after having a huge data breach event considering the increasing threats of mishandling information by hackers. There are various data breach laws in different countries. There are different factors to be considered as per the business location. Notifications regarding what are covered, breach, and penalties will look different as per the location and incidence. Even the most disciplined and careful organizations suffer data breaches at some point. The key here is to establish a proper disaster management plan to deal with potential risks to respond to attacks and contain the damage. It is evident that businesses are constantly under the risk of cybercrime and they should have proper steps to protect their data. They should take proper steps to avoid data breaches in future and following consequences.

5. Conclusion

All in all, both the cybercrime rate and frequency have increased and will rise up as a result of their past progress. In addition, ransomware is going through a great change as part of data breach incidents. Hackers just used to encrypt data and ask for ransom in the past. But it is recommended for companies to invest properly in their backup and restore plans with their IT team to avoid paying the ransom. These days, hackers are adding the element of data breach extortion as their next step and their ransom demand has been increased to "buy silence" and prevent the leak of sensitive data. The key here is to stay ahead with changing times and evolve data security plans.

6. Future Scope

It is really hard to predict the future of cyber-attacks as confidence of cyber criminals is increasing to evade detection. They have permeated almost every part of large organizations and they might be very efficient to spread ransomware and expand their reach to small fishes and even people to their repertoire for their attack. They can easily spread their "small-dollar" attacks with rising automation to mobile and personal devices while being profitable.

In order to counter these attacks, companies should conduct cyber security risk assessment annually, either with third-party services or in-house IT staff. They can focus on the most prevalent types of cyber-attacks that could wreak havoc to their company and determine the risk levels. They can determine their acceptance levels to deal with existing levels of risk if they are willing to invest in further resources. In addition, anti-ransomware programs are also effective to thwart these attacks. These are relatively cheap and they can help save a lot of resources in an organization. Finally, organizations should also determine whether third-party vendors are prepared with their cyber security plans before contracting the services.

[1]2021 Data Breach Investigations Report. Retrieved https://www.verizon.com/business/resources/reports/dbir/.

DOI: https://doi.org/10.54216/JCIM.080204
Received May 21, 2021 Accepted: November 01, 2021

References

[1] Lohrmann, D. (2021). Cyber Attacks: Is the 'Big One' Coming Soon? *Government Technology.* Retrieved 5 October 2021, from **https://www.govtech.com/blogs/lohrmann-on-cybersecurity/cyber-attacks-is-the-big-one-coming-soon.html.**

[2] Vaughan-Nichols, S.J. (2021). SolarWinds: The more we learn, the worse it looks. ZDNet. Retrieved from https://www.zdnet.com/article/solarwinds-the-more-we-learn-the-worse-it-looks/.

[3] Novet, J. (2021). Microsoft's big email hack: What happened, who did it, and why it matters. CNBC. Retrieved from https://www.cnbc.com/2021/03/09/microsoft-exchange-hack-explained.html.

[4] World Economic Forum. (2020). *The Global Risks Report 2020*. World Economic Forum. Retrieved from https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf.

[5] Hwang, J., & Choi, K. S. (2021). North Korean Cyber Attacks and Policy Responses: An Interdisciplinary Theoretical Framework. *International Journal of Cybersecurity Intelligence & Cybercrime*, *4*(2), 4-24.

[6] Miller, T., Staves, A., Maesschalck, S., Sturdee, M., & Green, B. (2021). Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems. *International Journal of Critical Infrastructure Protection*, *35*, 100464.

[7] Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248.

[8] Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*.

[9] McShane, M., Eling, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, *24*(1), 93-125.

[10] Cook, J. (2020). "British Airways fined £20m for data breach affecting 400,000 customers". *The Telegraph*. ISSN 0307-1235.

[11] The Wired (2018). Marketing Firm Leaked Database With 340 Million Records. Retrieved 11 October 2021, from https://www.wired.com/story/exactis-database-leak-340-million-records/.

[12] What to Do Right Now after the Equifax Hack | Mindsight. (2017). Retrieved 11 October 2021, from https://gomindsight.com/insights/blog/right-now-equifax-hack/.

[13] Hackett, R. (2021). What to Know About the Ashley Madison Hack. Fortune. Retrieved 11 October 2021, from https://fortune.com/2015/08/26/ashley-madison-hack/

[14] Robiah, Y., Rahayu, S. S., Shahrin, S., Faizal, M. A., Zaki, M. M., & Marliza, R. (2010). New multi-step worm attack model. *arXiv preprint arXiv:1001.3477*.

[15] Cost of Cybercrime Study | 9th Annual | Accenture. (2021). Retrieved 11 October 2021, from https://www.accenture.com/us-en/insights/security/cost-cybercrime-study.

[16] Keeper Security (2021). 2019 Ponemon Report. Retrieved 11 October 2021, from https://www.keepersecurity.com/ponemon2019.html.

DOI: https://doi.org/10.54216/JCIM.080204
Received May 21, 2021 Accepted: November 01, 2021

[17] 2021 Must-Know Cyber Attack Statistics and Trends - Embroker. (2021). Retrieved 11 October 2021, from https://www.embroker.com/blog/cyber-attack-statistics/

[18] Global Ransomware Damage Costs Predicted To Exceed $5 Billion In 2017. (2018). Retrieved 11 October 2021, from https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/.

[19] INTRUSION Inc. (2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Retrieved 11 October 2021, from https://www.globenewswire.com/news-release/2020/11/18/2129432/0/en/Cybercrime-To-Cost-The-World-10-5-Trillion-Annually-By-2025.html.

DOI: https://doi.org/10.54216/JCIM.080204
Received May 21, 2021 Accepted: November 01, 2021