talenta PUBLISHER

Data Science : Journal Of Computing And Applied Informatics
Journal homepage: https://jocai.usu.ac.id

The Evolution of Cybercrime and Its Impact on Various Sectors

Cindy Aprilia[*1], Robel Amare Gebrewold[2], Mercy Damilola Bamiduro[3], Niurguiana Borisova[4], Anel Mengdigali[5],

[1,2,3,4,5]*EMJMD SE4GD, Vrije Universiteit Amsterdam, Amsterdam, 1081 HV, Netherlands*

ARTICLE INFO

Article history:
Received 12 January 2026
Revised 27 January 2026
Accepted 30 January 2026
Available online 31 January 2026

E-ISSN: 2580-829X
P-ISSN: 2580-6769

How to cite:
C. Aprilia, R. A. Gebrewold, M. D. Bamiduro, N. Borisova, and A. Mengdigali, "The Evolution of Cybercrime and Its Impact on Various Sectors," Data Science: Journal Of Computing And Applied Informatics, vol. V10, no. 1, Jan. 2026, doi: 10.32734/jocai.v10.i1-24471

ABSTRACT

This research undertakes an investigation, into the development of cybercrime and its significant consequences in five crucial industries; Manufacturing, Finance and Insurance, Professional Business and Consumer Services, Energy and Retail and Wholesale. By examining the progression of cybercrime, the study traces its evolution from curious hacking to its present state as a sophisticated global threat. The analysis delves into cyber incidents in these industries exploring how these criminal activities have evolved from simple digital pranks to globally impactful actions. The narrative provides insights into the effects of these crimes and the evolving strategies employed to mitigate risks enhancing our understanding of the ever-changing cybersecurity landscape. This research serves as an introduction to facilitate an exploration laying the foundation for an understanding of past current and emerging trends in cybercrime, within these key sectors. It aims to significantly contribute to the development and strengthening of future cybersecurity approaches and resilience by providing a deep understanding of these trends.

Keyword: History of Technology, Cybercrime, Literature Review, Industries, Cyber-incident

ABSTRAK

Penelitian ini melakukan kajian terhadap perkembangan kejahatan siber serta dampak signifikan yang ditimbulkannya pada lima sektor industri yang krusial, yaitu manufaktur; keuangan dan asuransi; jasa profesional, bisnis, dan konsumen; energi; serta ritel dan grosir. Dengan menelaah perkembangan kejahatan siber, studi ini menelusuri evolusinya dari aktivitas peretasan yang bersifat eksperimental hingga kondisi saat ini sebagai ancaman global yang kompleks dan terorganisasi. Analisis ini mengkaji insiden-insiden siber di berbagai sektor tersebut, serta mengeksplorasi bagaimana aktivitas kriminal ini telah berkembang dari sekadar aksi digital sederhana menjadi tindakan yang berdampak secara global. Uraian yang disajikan memberikan wawasan mengenai dampak kejahatan siber serta strategi mitigasi yang terus berkembang, sehingga memperkaya pemahaman kita terhadap lanskap keamanan siber yang senantiasa berubah. Penelitian ini berfungsi sebagai pengantar untuk memfasilitasi eksplorasi lebih lanjut dengan meletakkan dasar pemahaman mengenai tren kejahatan siber di masa lalu, saat ini, dan yang akan datang dalam sektor-sektor utama tersebut. Tujuan akhirnya adalah memberikan kontribusi yang signifikan terhadap pengembangan dan penguatan pendekatan serta ketahanan keamanan siber di masa depan melalui pemahaman yang mendalam terhadap tren-tren tersebut.

Keyword: Sejarah Teknologi, Kejahatan Siber, Studi Literature, Industri, Insiden siber

1. Introduction

1.1. Background

The origins of cybercrime can be traced back to the days of computing when hacking was considered an activity carried out by computer enthusiasts and students to test their skills [1]. However, as technology advanced and the internet became more accessible the landscape of cyber activities also evolved. This led to both positive and negative outcomes. The increasing accessibility of the internet has not just brought advancements but has also created opportunities for malicious activities to thrive. As a result, various industrial sectors have faced challenges in dealing with these developments [2]. Understanding the evolution of cyber activities in relation to advancements has made it evident that both positive and negative consequences arise from technology development and internet accessibility. These consequences shaped the landscape of cyber activities. This highlights the importance of comprehending the associated challenges.

Cybercrime has become a threat that significantly impacts different sectors presenting challenges for organizations and individuals alike [2]. This historical study delves into an exploration of how cybercrime has evolved over time and its implications across five key sectors; Manufacturing, Finance and Insurance, Professional Business and Consumer Services, Energy as well, as Retail and Wholesale.

The choice to investigate this topic arises from the increasing importance of addressing cybercrimes in today's interconnected world. The growing influence of cybercrime, especially across the five industries has led us to delve into its development and the consequences it has on both organizations and individuals. Through an examination of the progression of cybercrime and its impact on these sectors our aim is to gain valuable insights into the challenges faced.

Our study focuses on analysing the effects of cybercrime in each sector by investigating incidents and establishing connections between them. Additionally, we will explore how cybercrime investigations have evolved over time ranging from small scale group attacks to operations sponsored by states. To gain an understanding of forms of cybercrime and the individuals involved in such activities our approach will adopt a storytelling perspective. We will critically evaluate sources from viewpoints taking into account biases present within them.

This study will observe how the evolution of cybercrime has shaped these sectors, the challenges it poses to organizations and individuals within them, and the strategies employed to mitigate these risks. The objective of this study is to provide a comprehensive understanding of the cybercrime landscape and its effects on these sectors, and how these cybercrimes are related from one sector to another through analysis of the incidents in each sector. This introduction serves as a precursor to a detailed exploration of the subject matter, setting the stage for an in-depth analysis of the impact of cybercrime on these sectors.

1.2. Five Sectors Under Scrutiny

Based on Statista's 2022 survey [3] (Figure. 1), we see a significant distribution of cyberattacks across sectors, highlighting the digital menace's pervasiveness. This widespread presence emphasizes not only the array of targets targeted by cybercriminals, but also the varying levels of awareness across businesses. The Statista poll identifies that most of cybercrimes attacked companies in the following sectors: Manufacturing (24.8%), Finance and Insurance (18.9%), Professional, Business, and Consumer Services (14.6%), Energy (10.7%), and Retail and Wholesale (8.7%). Each of these sectors has a significant impact on the global economy, and their vulnerability to cybercrimes is a significant concern.

The manufacturing sector displays an alarming tendency. As an industry that relies heavily on interconnected technology and automation, it is a prime target for cybercrimes. These dangers might range from intellectual property theft to production line disruptions, offering both financial and safety problems.

Similarly, the finance and insurance industries, which handle sensitive financial data and transactions, are attractive targets for cybercriminals. Cybercrimes in this sector can result in massive financial losses and erode consumer trust, which is critical to the business resilience.

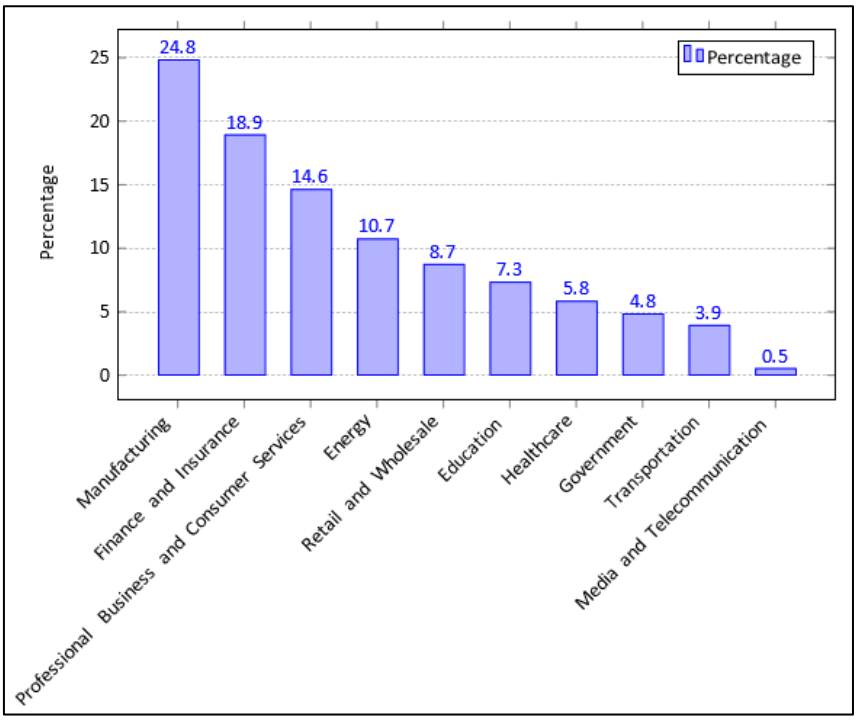

Figure 1: Distribution of cyber-attacks across worldwide industries in 2022 [3]

The Professional, Business, and Consumer Services sector, which includes a diverse range of activities, faces distinct problems. Because of its diversity, this sector is subject to a wide range of cyber threats, including data breaches and phishing schemes, which affect not just businesses but also their clientele.

Vulnerability of energy sectors are particularly alarming because of the possibility of massive disruptions toward both other sectors and general public. Cybercrimes in this sector could lead to widespread power outages or compromise critical infrastructure, underlining the importance of robust cybersecurity measures.

Finally, the Retail and Wholesale sector, which is increasingly reliant on e-commerce, confronts risks such as credit card fraud and personal data breaches. Cybercrime has a direct influence on consumers' trust and financial well-being.

To gain an in-depth understanding of the cybercrime landscape and its effects on these sectors, we dig deeper into the complex nature of cybercrime within these five sectors. These incidents are selected based on their impact, the sophistication of the attack methods used, and their historical significance in the evolution of cybercrime and cybersecurity.

1.3. Historical Research Question

This study aims to understand how cybercrime has changed over time and impacted various sectors. According to the above insights provided by [3], various sectors have been impacted by cyber threats, hence, it's important to investigate the evolution of how cybercrime has shaped these different sectors and how this has historically impacted individuals and organizations.

The world of cyber-attacks has changed over time, posing unique difficulties to various sectors. In addition to understanding the historical evolution of cybercrime, the study also aims to identify historical trends and strategic factors that might strengthen the cybersecurity resilience of these various sectors.

In summary, this research therefore aims to answer the historical research questions;

Main RQ: How has the evolution of cybercrime from its early days to its current transformation impacted various sectors, especially from the perspective of organizations and individuals?

RQ 1: How has the nature of cybercrime evolved within the five sectors?

RQ 2: How has the evolution within the five sectors, which were resulting from cybercrime attacks, impacted organizations and individuals within those sectors?

RQ 3: How have the five key sectors adapted and innovated to address the evolving threat of cybercrime?

Through a comprehensive historical exploration, this research will provide detailed insights into the historical evolution of cybercrime, identifying turning points and transformations while analysing some major incidents across the sectors specifically between 2015 and 2020. It also assesses the implications of cybercrime for organizations and individuals while identifying the important viewpoints to strengthen the measures and practices adopted by organizations to mitigate risks.

2. Methodology

Our research primarily focused on establishing connections between cybercrimes in sectors while examining their political impacts. We chose these sources to identify commonalities among cybercrimes and comprehend their implications from multiple perspectives. Considering the aspects our aim was to provide insights into the development of cybercrime and its effects on different industries.

This research applied a qualitative historical methodology to examine the evolution of cybercrime and its impact on five sectors: manufacturing, finance and insurance, business services, retail and wholesale, and energy. The study relied exclusively on secondary data and focused on identifying temporal patterns and documented incidents across sectors.

Unlike studies limited to peer reviewed literature, this research adopted an inclusive source strategy. Articles, white papers, institutional reports, and reputable news coverage were incorporated provided that they met two primary criteria: first, the source originated from a recognized institution, established media organization, or professional body; second, the publication clearly documented the year of the incident and described the nature of the cyber event. By incorporating a range of materials such as papers, news articles and other media sources we were able to explore cybercrime from angles and gain an understanding of its evolution as well as its specific impacts, on different sectors.

Data elicitation was conducted through structured source collection using Google Scholar and other publicly accessible repositories. Search terms included combinations of “cybercrime,” “sector impact,” “data breach,” “cyber-attack,” and specific industry names. White papers, consisted of selected academic sources authored by cybersecurity experts analysed for their perspectives on the nature and impact of cyber threats.

Institutional data from the Federal Bureau of Investigation were used to obtain further understanding on the chronological and statistical references of cyber incidents. Industry reports were also examined when they provided verifiable incident timelines. News reporting from established outlets such as The Guardian were also included to capture contextual and sector specific accounts of major cyber events. However, we also acknowledged the potential media bias from the sources, particularly in politically sensitive cases.

Data analysis focused on extracting the year of occurrence, type of cyber incident, and affected sector. These variables were organized chronologically to trace developmental trends. By prioritizing incident year and documented impact, the study aimed to map the progression of cybercrime across industries while maintaining source credibility through reliance on reputable publications.

3. Overview of Cybercrime

“Cyber” is a prefix derived from the word “cybernetics,” a term coined by mathematician Norbert Wiener in the 1940s to describe the study of systems within living beings and artificial machines. Since then, the word “cybernetics evolved into the prefix” Cyber-”, which shows the various activities connected to computer networks, information, technology, systems, and the internet.

"Cyber" often encompasses the digital realm of computer networks, information, technology, systems, and the internet [4]. Since the 1960s, the prefix "cyber-" began to be added to words to indicate their association with computers. Some of these words, such as cyberspace, cyberpunk, cybercrime, cyberactivity, and cybersecurity, are few samples of the words still commonly used today. By using the prefix "cyber-", it signifies that the subject being discussed pertains specifically to the online or virtual realm.

Cyberactivity encompasses a range of digitally performed actions aimed at achieving specific goals, as determined by the individuals involved. One of the most famous cyberactivity is hacking. Hacking involves unauthorized access to digital devices and networks, leading to their compromise. Initially, hacking was viewed as light-hearted pranks or playful acts carried out by students or computer enthusiasts to test and improve their skills [1].

Over time, this initially benign activity carried by smart-praised worthy students evolved into something more malicious. The increased accessibility of personal computers expanded the means of unauthorized access beyond hacking. Examples of negative cyber-activities include fraud, unauthorized access, cyberstalking [5], and forgery [6].

The evolution of unauthorised usage of computers attracted government intervention, with the United States of America enacting the Computer Fraud and Abuse Act in the 1980s. This was followed by Germany's Strafgesetzbuch (criminal law code) and the Netherlands' Wet Computercriminaliteit (Law on Computer Crime) in the early 1990s. These laws provided clearer definitions and guidelines for determining the motivation and impact of hacking, as legislative bodies within each legal system shaped the definition of criminal acts [7].

Cybercrime is defined by its "act of crime", which is when digital actions socially, ethically, and legally unaccepted by both law and the general public. So, from the point-of-view of "act of crime" theory, all attacks are bad and criminal. Even the first worm maker (Morris) that made first worm in 1980 had faced multiple backlashes, even though there were no laws legally stating it was a crime at that time yet [8].

Therefore, as our focus on cases between 2005-2020, all attacks are categorized as cybercrimes, either intentional or unintentional. So, precluding any characterization as "Robin-Hood" activities from this perspective.

4. The Birth of Cybercrime

4.1. Birth of Cybercrime: A Historical Perspective

In the 20th century, people lived in two distinct worlds: the physical world and the emerging cyberworld, born out of technological advancements, particularly in Internet technologies. The same 20th century witnessed two industrial eras: the second industrial revolution, which occurred before the digital era, and the subsequent third industrial revolution which commenced with the beginning of the digital age [9].

The concept of cybercrime can be traced back to the mid-20th century with the creation of ENIAC, the world's first digital computer in 1945. However, for nearly two decades after its inception, carrying out cybercrime posed significant challenges. Access to these massive electronic machines was limited to a small number of individuals, and they were not interconnected [10, 11].

As the mid-20th century progressed, criminal activities associated with the second industrial era, such as telephone fraud, utility theft, radio interference, and bank robbery, began to seem outdated. The 1980s witnessed the emergence of several PC viruses, marking the onset of a new era: the third industrial revolution cybercrime. Criminals started to shift their operations into the cyberworld, engaging in activities such as hacking, cyber trespass, data tampering, malware, and spyware [9]. The term "computer virus" was officially defined by Fred Cohen in 1983 during his academic experiments on a Digital Equipment Corporation VAX system. Elk Cloner, targeting Apple II systems in 1982, became the first computer virus discovered in the wild. Subsequently, BRAIN, originating from Pakistan in 1986, evolved into a more extensive and pervasive virus compared to its predecessors [10, 11]. The concept of self-replicating or propagating programs laid the groundwork for the development of more sophisticated forms of cybercrime.

The ethical intentions of individuals involved in activities are brought into question by hacking cultures and cybercrime. Hacking, which involves access to systems, can have varying intentions from positive to negative. On the other hand, cybercrime inherently involves engaging in incorrect activities that harm other digital users, whether intentionally or unintentionally. The historical context of cyber-related words and their acceptance into general public usage lack written sources, making it difficult to explore their origins in depth. However, it is clear that cybercrime is characterized by its "act of crime" where digital actions are socially, ethically, and legally unacceptable. Even early instances of cyber-attacks, like the worm created by Morris in 1980, faced backlash, highlighting the impact such activities have on industry and society. According to the perspective of cybercrime theory, all attacks are considered bad and criminal, including those initially conducted by students for testing purposes in the 1980s, because they have effects on industry as well. Therefore, based on our analysis from 2005 to 2020, no attacks can be classified as "Robin Hood" activities.

Cybercrime encompasses a range of activities, ranging from hacking and fraud to identity theft, cyberstalking, and cyber espionage. Cyber attackers, be they individuals or groups, exploit weaknesses in computer systems and networks to gain entry to information. What sets cybercrime apart from crime is the utilization of methods for carrying out unlawful activities. Cybercrime extends beyond stealing assets; it can also involve causing physical harm or damaging property. For instance, malevolent actors can employ malware to disable infrastructure systems, resulting in destruction and endangering lives.

To summarize, comprehending the implications and historical background of cybercrime and hacking cultures is crucial in understanding how cybercrime has evolved and how it differs from crime.

4.2. Evolution of Cybercrime: From Curiosity to Global Threat

Cybercrime has become an omnipresent threat in the modern digital age, infiltrating every aspect of society from personal data security to national security [12]. The evolution of cybercrime can be traced back to the 1970s when the concept of hacking first emerged as a curiosity and a means for tech enthusiasts to explore the boundaries of the digital world.

Initially, hacking was driven by intellectual pursuits, with early hackers, often referred to as "white hat" hackers, seeking knowledge and understanding of computer systems [13]. However, as technology advanced and access to computers became more widespread, hackers recognized the potential for malicious activities.

In the early 2000s, cybercrimes were characterized by relatively primitive forms of malicious activities, often driven by individual hackers and small groups. However, as digital technologies advanced, so did the methods and capabilities of cybercriminals. The landscape of cybercrime witnessed a transition from isolated incidents of hacking and data breaches to large-scale, coordinated attacks targeting critical infrastructure, government institutions, and multinational corporations [13].

The period also saw the emergence of state-sponsored cybercrime, with governments and their proxies engaging in illegal activities for espionage, sabotage, and geopolitical influence. This posed new challenges for law enforcement and international cooperation in addressing cyber threats [13]. Furthermore, the timeline of cybercrime from 2004 to 2014 was punctuated by high-profile incidents that underscored the growing impact and reach of cyber threats. Notable events such as the Bradley Manning and Edward Snowden leaks, the proliferation of massive botnets, and the industrial-scale espionage allegedly conducted by major powers highlighted the escalating scope and complexity of cybercrimes during this period [13].

As the digital landscape continued to evolve, the methods and tactics employed by cybercriminals became increasingly sophisticated, leveraging advanced technologies and exploiting vulnerabilities in interconnected systems. This evolution necessitated a corresponding adaptation in cybersecurity measures and law enforcement strategies to effectively combat the expanding threat of cybercrime. As technology continued to advance, cybercrime evolved into a sophisticated and pervasive threat. The rise of interconnected systems and digital infrastructure provided cybercriminals with new opportunities to exploit vulnerabilities and target individuals, organizations, and even governments. The arsenal of cybercriminal activities expanded dramatically over the years, encompassing data breaches, identity theft, ransomware, and financial fraud.

5. Evolution of Cybercrime: A Cross-Sectoral Perspective

The evolution of cybercrime across sectors is a dynamic journey shaped by technological developments and the growing integration of digital systems into key infrastructures. Over the years, individuals and businesses have faced significant losses, both monetary and psychological, as a result of cybercrimes [14, 15].

One of the instances of cybercrime targeting an industry emerged in 1986 with the "Cuckoo's Egg" case. Discovered by Clifford Stoll at the Lawrence Berkeley National Laboratory, this case involved Markus Hess, a German hacker who infiltrated numerous U.S. military and industrial networks. Initially detected through a minor accounting anomaly, the investigation revealed Hess's extensive espionage activities. He had gained unauthorized access to networks of defense contractors and research institutions, gathering sensitive data to sell to the Soviet KGB.

This incident served as a wake-up call for industries and governments worldwide, catalyzing the development of more stringent cybersecurity measures. The Cuckoo's Egg case is a landmark in cybercrime history, marking a shift from opportunistic hacking to sophisticated, organized cyber espionage targeting industrial and governmental entities [16].

Also, a Russian hacker named Vladimir Levin in 1994, was able to access $10 million from several large corporate customers of Citibank via their dial-up wire transfer. After this cybercrime, the landscape of cybercrime has evolved significantly since then, with cybercriminals employing increasingly sophisticated methods to carry out their illicit activities [17].

In the following sections, we delve more into the specific evolution of cybercrime in each sector.

5.1. Professional, Business, and Consumer Services Sector

The timeline begins in the 1980s and 1990s when the landscape was marked by worm assaults and the rise of malicious software. These early occurrences, such as the Morris Worm, paved the way for cyber dangers in the Professional, Business, and Consumer Services sector [9]. This early incident made computer network vulnerabilities public and paved the way for subsequent attacks such as the Melissa Worm 1999 and Conficker 2008.

The Melissa worm, created by David L. Smith and reportedly named by Smith for a stripper in Florida, was released in March 1999. The worm also affected Microsoft Word documents which spread through email attachments, resulting in severe disruption and financial loss. This incident highlighted the significance of email security policies and the necessity for organisations to guard against phishing attempts [18].Even though this worm started the new era of phishing, the Melissa worm's purpose was distinct from modern phishing attacks which often have a monetary goal.During the Melissa worm's emergence, hackers were motivated by the excitement of a task and the desire for fame or prestige [19].

Also, the Windows PC virus known as Conficker is one of the most notable worms, because to the large number of victims, resulting from financial losses, and long-term terror. It first appeared in November 2008 and soon gained attention for its vast impact and resilience. Conficker utilizes vulnerabilities in Windows software to seize control of machines and link them to a virtual computer that can be remotely commanded. Despite having control over more than 5 million computers worldwide, Conficker is challenging to eradicate and has persisted as a long-standing problem [20]. Following these incidents, cybercrime has evolved into more dangerous forms.

5.2. Manufacturing Sector

The evolution of cybercrime within the manufacturing sector has undergone a profound transformation over the years, mirroring the broader advancements in technology and connectivity via sensors, artificial intelligence, robotics, and networking technology [21]. In general, manufacturing is transitioning to fully integrated intelligent facilities that can effectively communicate with each other worldwide.

In the early stages, before the widespread adoption of the Internet, manufacturing systems operated in a less interconnected environment. For instance, security threats were often localized, with perpetrators requiring

physical access to facilities [22]. Later, the interconnectedness of sensors, components, machinery, and human involvement has enhanced production speed, efficiency, and facilitate advanced mass customization [23]. However, the introduction of internet connectivity marked a significant shift, exposing manufacturing systems to new vulnerabilities as cybercriminals exploited weaknesses in network security.

As the 2010s unfolded, the manufacturing sector witnessed the rise of ransomware attacks [24]. These malicious campaigns, which involved encrypting critical data and demanding payment for its release, proved highly disruptive to operations. Then, the proliferation of Internet of Things (IoT) devices within manufacturing further expanded the attack surface [25]. Specifically, small and medium-sized manufacturing enterprises (SMEs) are currently grappling with security threats in the digitalized and Internet of Things (IoT) era [23]. Various challenges arise with the implementation of new technologies as the integration of new devices into networks without sufficient caution provides new opportunities for potential attacks [22]. Exploiting vulnerabilities in smart devices and industrial IoT components became a common tactic, illustrating the adaptability of cyber threats in response to technological advancements.

5.3. Finance and Insurance Sector

Cybercrime in the finance and insurance sector has a storied history, marked by incidents that have shaped the industry's approach to digital security. Within the finance and insurance industry there is a story woven around cyber threats. This story reflects the sectors history and its ability to withstand adversaries. It all started in 1994 with the Citibank Hack, which was orchestrated by Vladmir Levin and revealed vulnerabilities, in banking security. Over a period of five months Levins hacking activities led to theft of funds prompting a response from the FBI and his eventual arrest in the UK [26].

In 2011 the RSA Breach dealt a blow by compromising security tokens used for two factor authentication in transactions. This breach undermined trust in a security measure leading to a reevaluation of strategies. The incident of 2008 saw targeting of Heartland Payment Systems, a payment processing network. Not did this breach expose weaknesses in payment infrastructure. It also raised concerns about the reliability of financial transactions serving as a stark reminder that constant vigilance is necessary to protect financial systems and assets [27, 28].

Adding another layer to this narrative is the BTX Hack of 1984 orchestrated by the Chaos Computer Club. Motivated by their mission to highlight security flaws these hackers targeted the Btx system of Hamburger Sparkasse revealing vulnerabilities, within Germanys Federal Post Offices Btx system. Their clever exploit demonstrated their ability to outsmart technology exposing flaws, in the praised innovative means of communication [29].

In times the finance and insurance sector has been contending with breaches and ransomware assaults highlighting its vulnerability to evolving and advanced threats. The continuous advancements, within the finance and insurance sector stand as evidence of the lessons gleaned from cyber incidents and the unwavering dedication to safeguarding financial systems and assets in an ever-shifting digital realm.

5.4. Energy Sector

Cybercrime within the energy sector began concurrently with the introduction and integration of information technology into its operational framework. Initially, these incidents were rare and relatively unsophisticated, often the work of individual hackers or small groups. However, even these early attacks exposed significant vulnerabilities in the energy sector's reliance on digital technology.

With the introduction of the internet and the spread of computer technology in the 1980s, the energy industry began to embrace digitalization for more effective operation and administration. However, this technological embrace created new opportunities for criminal activities, which marks as the beginning of cybercrime in critical infrastructure. One of the earliest known incidents was the 1982 Siberian pipeline sabotage, where a supposed logic bomb caused a massive Soviet pipeline to explode, illustrating the possibility for physical harm by cyber-attacks [30].

As the internet became more commercialised in the 1990s, these activities started evolving, with cybercriminals realising their financial potential in exploiting digital vulnerabilities. The energy sector, which

is growing dependent on digital technologies for control and communication, also became a target. Incidents during this period were rare but served as wake-up calls for the sector. Examples include the exploitation of network protocol weaknesses and the introduction of malware into systems, which result in operational interruptions and data breaches.

The danger in this sector continued to increase as the energy sector continued to digitise its operations and embraced Industrial Control Systems (ICS), which are typically of three types: SCADA (Supervisory Control and Data Acquisition), Distributed Control Systems (DCS), and Programmable Logic Controllers (PLC).

The danger got higher when the energy sector continued to digitize its operations and adopted Industrial Control Systems (ICS), which are usually of three types: SCADA (Supervisory Control and Data Acquisition), Distributed Control Systems (DCS) and Programmable Logic Controllers (PLC) [31]. The adoption of these systems leads to vulnerabilities in the energy sector. SCADA systems are used in many essential infrastructure systems like power grids and water treatment plants. These systems are designed to provide real-time data and control over the various components of a power grid, such as generators, transformers, and transmission lines [32].

Over the years, the nature, sophistication, and frequency of cyber attacks on the energy sector have escalated significantly. The motivations of attackers have diversified from mere financial gain to include espionage, political agendas, and widespread disruption. For instance, the late 1990s and early 2000s saw an increase in politically motivated attacks, often attributed to nation-state actors. A key example of this evolution is Stuxnet. This malicious piece of malware not only underscored the potential for significant impact on the physical world through cyber means but also highlighted how digital tools could be weaponized to cause real-world damage, marking a moment in the history of cyber warfare. The Dragonfly campaign further demonstrated the sophistication of attacks targeting crucial energy companies [32].

5.5. Retail and Wholesale Sector

Similarly, before the 1990s, cyber threats to the Retail and Wholesale sector were limited, Illegal activities were mostly localised and used traditional tactics such as shoplifting and physical theft [33]. However, with the growth of technological advances and the rise of e-commerce, cybercriminals moved their attention to online platforms. As a result, data breaches, payment fraud, and online scams targeting customers and financial information have increased in the retail industry [34].

In the early 2000s, as the growth of technology continued to advance, cybercriminals began attacking retail sectors' Point-of-Sale (POS) systems, known as POS attacks which aim to steal card data during transactions. When this data stays in memory, they are scraped and accessed by specially designed malicious software known as POS RAM scraping malware. In recent years, this type of attack has been responsible for massive data breaches at a well-known US retailer [35, 34]. As e-commerce continued to gain more relevance, retail and wholesale sectors also became primary targets for ransomware attacks and large-scale data breaches. Cybercriminals took advantage of weaknesses in databases and networks to steal consumer information for financial gain or launch ransomware attacks to disrupt business operations [36]. In recent years, retailers and wholesalers who rely on interconnected networks and digital platforms have begun to face threats such as supply chain attacks, in which cybercriminals access the systems of suppliers or partners of these retailers [34].

Notably, In 2010, several other types of cyberattack began to surface like social engineering, cybercriminals began to increasingly use advanced social engineering techniques, such as phishing attacks, and malware, to target business employees. This has raised the possibility of internal threats and allowed unauthorised access to private information [37]. It is important to note that many of these cyber attacks are still been used to date.

6. Overview of Cybercrime

As industry increasingly rely on digital technologies and interconnected systems for efficient operation, they become prime targets for cybercriminals [38]. In this section, we explored the technical methodologies employed by cybercriminals and not only the historical incidents themselves. We delve into the fundamental structure of cybercrime, by analyzing the technical methods used by cybercriminals in these various sectors. This reveals the diverse methods or techniques used by cybercriminal who attack digital vulnerabilities.

6.1. Professional, Business, and Consumer Services

Due to the digitalization of the professional, business, and consumer services sector, several cybercrimes have become more popular globally in recent years [39]. In the Professional, Business, and Consumer Services sector, inadequate security measures can leave vulnerabilities, posing significant corporate risks, including data breaches and service disruptions [40, 41]. Riek and Böhme in 2018 found that consumer-sector faces a wide range of cybercrimes, differing in criminals' motivation, methods used, and impact on victims. Some of the most notorious attacking techniques in business sector are described malwares, hacking, privacy breaching, social engineering and employing internal bugs [42].

In the 1980s, this sector was one of the very first to get attacked. Since the dawn of cybercrime, both the technology available and the cybercriminals themselves have not been sophisticated enough to attack other than direct PCs. Therefore, end-user computers installed with consumer applications become the most targeted devices. The attackers were employing malicious software programs, including computer viruses, worms, and Trojan horses [43]. Cybercriminals employed that software for extorting victims, an action which is called as ransomware [41].

Later on, the cybercrime techniques become more sophisticated, and cybercriminals employ the negligence of their users to commit crimes. Attackers employ social engineering, which is the psychological manipulation of people into performing actions or divulging confidential information. There are several famous techniques of social engineering, such as human scams, clicking fraud (individual negligence to click links without prior checking), and spoofing or phishing (redirecting a Web link to an address different from the intended address).

For personal data, the most famous social engineering technique is identity theft. Identity theft is the most prevalent theft associated with fraud, scams, and extortion. Usually, this attack happens both during data transmission and storage when the victims access the phishing website [41].

For company data, attackers usually employ internal software vulnerabilities. Because, hidden bugs or program code defects are a major problem with software. However, it is virtually impossible to eliminate all bugs from large programs. So, hackers might use this vulnerability to attack the victim's systems [43].

Hackers are not shy away from doing direct hacking in this sector too. They hacked the system to get unauthorized access to other people's digital devices. They might add SQL code into the victim's web systems, flooding a victim's network with numerous false communications to crash the network, or eavesdropping on traveling information over a network [43].

However, it needs to be noted that these list of tactics might not be precisely accurate. Since cybercrime is a rare phenomenon and losses are concentrated, a few respondents can form a large part of survey-based estimates, while others may not report because they did not lose anything monetarily. Therefore, this poses challenges in the estimation of costs and sampling of the tactics and victims [42].

6.2. Manufacturing

Insufficient security measures at any stage of the manufacturing process chain can leave vulnerabilities, giving rise to two distinct types of cyber-attacks: the theft of technical data and sabotage attacks [44]. These attacks pose a significant threat impacting both technological assets and operational integrity of the manufacturing sector.

To understand the breadth of cyber threats faced by the manufacturing sector, attack goals can be broadly classified into three categories: piracy, involving unauthorized copying of designs; sabotage, encompassing the introduction of defects or disruptions to cause harm or delay; and counterfeiting attacks, which involve illegal attempts to replicate genuine products [21].

The attack methods within the manufacturing domain are diverse, falling into seven distinct categories including denial-of-service attacks, reverse engineering, data tampering, reliability degradation, side-channel leakage, covert channel attacks, and IP theft [21]. These methods range from blocking access to systems and manipulating data to stealing proprietary information for the development of competing products.

Attack targets in the Digital Manufacturing system fall into two main phases such as design and manufacturing [21]. In the design phase, Computer Aided Design (CAD) software, Stereolithography (STL) file format, and G-code are identified targets susceptible to data tampering or compromise. Whereas, in the manufacturing phase, the targets include physical manufacturing machines, sensors, actuators, and controllers, all crucial components in the feedback loop controlling the manufacturing process.

6.3. Finance and Insurance

The exploration of the aspects of the finance industry takes us on a journey, in time to the world of Traditional Banking Frauds, which were prevalent before the internet era. These frauds encompassed schemes like account takeovers, forgeries and credit scams relying heavily on social engineering techniques to deceive institutions and individuals for unlawful gains [45].

In the Mid 2000s came an era characterized by Sophisticated Malware. This period saw advancements along with cybercriminals developing complex malware to exploit software vulnerabilities. This sophisticated malware from the mid-2000s era infected millions of hosts and raised questions about future malware defense strategies.[46].

The past decade witnessed an increase, in Advanced Persistent Threats (APTs). These targeted attacks were carefully executed with the intention of infiltrating organizations while maintaining secrecy. The attackers sought to gain access without getting detected, employing tactics to bypass existing security measures. [47].

Alongside this rise there was also an emergence of Cryptocurrency and Blockchain exploitation. Cybercriminals exploited vulnerabilities in finance platforms devising schemes to steal cryptocurrency and using exploits to target marketplaces and pilfer funds from wallets and coin exchanges. [48]. During this time period Mobile Banking Threats became a concern. While mobile banking offered convenience in managing finances it also presented cybersecurity risks. Challenges such as hacked Wi-Fi networks, data breaches and insecure data storage posed threats. However mobile banking apps incorporated features aimed at bolstering security measures setting them apart from banking websites. [49].

Furthermore, the narrative continued with the advent of FinTech and the associated risks posed by third party services. The rise of FinTech injected innovation into the landscape. Also raised concerns about its potential impact on financial stability. Due, to their data and higher failure rates compared to traditional institutions FinTechs became recognized as potential risk factors.

Banks acknowledged the risks involved. Made it their duty to comprehend and minimize any issues that may arise from their dealings, with third party entities. They accomplished this by crafting contracts that addressed concerns such, as default and termination risks. The evolution of technology, in the finance industry, highlighted the changing relationship between innovation, risk and adaptability.

6.4. Energy

The history of cybercrime in the energy sector reflects a landscape that has evolved rapidly and dramatically, with implications that extend far beyond the immediate disruptions of service [50, 51]. The energy sector is a diverse sector comprising electricity generation, transmission, distribution, and consumption, as well as the extraction and distribution of fossil fuels and the harnessing of renewable energy sources [52]. Accordingly, cybercrime in the energy sector refers to the array of illegal activities undertaken by individuals or groups targeting computer systems, networks, and digital information assets of entities engaged in energy production, distribution, and management. This includes, but is not limited to, unauthorized access, data theft, service disruption, and sabotage [53, 52]. The impact of such crimes ranges from financial losses due to theft and fraud to significant operational disruptions that can lead to widespread power outages and affect public safety [54]. In severe cases, cyberattacks against critical energy infrastructure can have national security implications, highlighting the intersection between cybercrime and geopolitics.

6.5. Retail and Wholesale

Cybercriminals often target both e-commerce businesses and their customers, exposing them to the constant danger of cyber-attacks [55]. A significant percentage of American retail stores are reported with

vulnerabilities that might be readily attacked. Attackers often target customers' private information, which is the most important asset in e-commerce. They have various techniques which may involve using e-skimming, malware, ransomware, or stealing data from online shop databases [56].

The study by Odero. et al., also highlighted some of the common types of cyber-attacks that are possible at the customer end, among many others, which include Phishing; which is a fraudulent attempt to get private information from someone, such as their PIN numbers or account details. In this deceitful method, a malicious attacker might insert a fake login page for an E-commerce site onto a legitimate website, exploiting any vulnerabilities that might exist. These false E-commerce sites are frequently sent by emails and Individuals who are not aware of this type of cyber threat, fall victim to such. Another is Pharming, which is similar to phishing. It aims to steal customer information, but it works differently. Here, the goal of this cyber-attack is to redirect users to a fake website, when a user inputs a website's domain name into their web browser, it is converted to a numerical address known as an IP address by a DNS server. In summary, a pharming attack occurs when users' IP addresses are manipulated to send them to a fraudulent website. Another common one is password attacks, some tools are used in password attacks to compromise a user's login information, with the aim of gaining unauthorized access to their account. Successful password attacks can result in actions such as cancelling past orders on the customer's behalf or placing fraudulent orders for new items. Attackers also use brute force attacks, which involve trial and error to guess passwords. Attackers try several combinations until they discover the right one. If the attacker knows something about the target consumer, they may easily launch this sort of attack by guessing the password. It entails continuous and automated attempts to reveal passwords using systematic trial and error [36].

Spoofing is a misleading method in which a malicious attacker impersonates a legitimate entity to obtain unauthorized access to a network or take complete control of the network. In essence, it is creating a fake identity to mislead systems or people into providing access or privileges to the impersonator. There is another known as a man-in-the-middle attack, which is a type of cyberattacks where the attackers silently listen and monitor the communication between a consumer and a server and this results in unauthorized access or modification of the data provided [57].

On the other hand, the possible types of cyberattacks from the e-business side could be viruses, which is a harmful program designed to cause significant damage to a system. Generally, it attaches itself to single files or a group of files, resulting in significant losses by consuming additional storage, modifying files and folders, and causing a slowdown in the system's response. Basically, it is malicious software that can interrupt the normal functioning of a computer system and affect its integrity. Adware is also a type of harmful software that is cunningly inserted inside web adverts. If a consumer unknowingly clicks on such an ad, it might lead to fraudulent activity, such as the unauthorized acquisition of customer information. Essentially, adware poses a hazard by abusing internet adverts to engage in misleading and destructive behaviors. Another common cyberattack is Spyware, which operates similarly to an application to steal people's login information. Once it has these credentials, it sends the data to a cyber attacker who is logged onto the network. There is also ransomware, which is a type of malicious software that attempts to pressure the victim into paying a ransom by either threatening to make their data public or limiting access to it until the requested ransom is paid [36, 57, 58].

7. Cybercrime Dynamics: Understanding the Wider Implications

This section delves into the evolving scope and impact of major cybercrimes, analyzing their progression from simple digital mischief to complex, globally impactful activities. It explores how cybercrimes have shifted to target large corporations and political entities, emphasizing the growing sophistication and strategic nature of these attacks. The analysis highlights the intricate relationship between cybercriminal activities and their broader implications on national security, global politics, and corporate vulnerabilities, offering insights into the changing landscape of cyber threats and their far-reaching consequences.

7.1. From Playful Hacking to Serious Threats

In the initial years of the internet, there are several individual forayed into system, infiltrated and playfully tampered them. They viewed it more as digital mischief and challenge, than genuine threats. These activities, though technically breaches of security, were driven by a sense of inquisitiveness.

The earliest known worm in the public was Elk Cloner, in February 1982. Rich Skrenta, a 15-yearold high school student with remarkable programming skills and a profound interest in computers, devised Elk Cloner as a playful prank. Targeting the prevalent Apple II systems, which were the dominant home computers of the era, this boot sector virus infiltrated floppy discs, causing them to become infected. This virus subtly plays trick on booting.

Elk Cloner did not cause any real harm toward computer, but this mark the rampage spreading of computer virus in the wild. Skrenta's footsteps followed by several aspiring, such as Morris' Worm. Morris Worm, also known as the Internet Worm, was unleashed by Robert Tappan Morris Jr., a Cornell University graduate student.

Morris himself claimed it was a harmless exploit to gauge the size of the Internet, but this experiment gone wrong [59]. However, regardless of the initial intention, the worm spread rapidly, aggressively, and conspicuously. The worm spread like wildfire through vulnerabilities in UNIX operating systems, infected around 6,000 computers connected to the early ARPANET. It was infecting systems at a number of prestigious colleges and public and private organizations, and causing significant damage, causing widespread network disruptions and financial losses [8].

This era of digital mischief played a crucial role in shaping the future of cybersecurity. The actions of Skrenta and others like him exposed the vulnerabilities and weaknesses in early digital systems, inadvertently laying bare the necessity for more robust security measures.

They pushed software developers and system administrators to rethink their approach to digital security, highlighting the need for constant vigilance and improvement in protecting against unauthorized access.

Moreover, Elk Cloner Worm did not only initiate fellow aspiring hackers, it was raising the regulator awareness toward computer privacy as well. After Elk Cloner, Congress had then passed the Computer Fraud and Abuse Act, in 1986.

Therefore, different than its predecessor, Morris' handwork was clearly outlawing unauthorized access to protected computers. So, Morris become the first person convicted under the 1986 law, with 400 hours of community service.

In retrospect, the dawn of digital mischief, was a crucial and formative period in the history of the internet. These early digital explorers mostly had benign intentions. It was a time when the lines between curiosity-driven exploration and cybercrime were blurred, a period that laid the groundwork for the more complex and security-conscious digital landscape we navigate today, either from the technical, ethical or legal point of views. By testing the limits of burgeoning digital landscapes, they also set the stage for the evolution of cybercrime into a more serious and consequential domain.

7.2. Cybercrime for Profit: The Financial Motivation

The playful and curious nature of early cyber intrusions soon evolved into more malicious activities, with hackers shifting their focus towards financial gain. Financially motivated cybercrime led to significant security breaches, like the TJX data breach from July 2005 to January 2007. In this breach, 45.6 million credit and debit card details were stolen from TJX Companies Inc. The methods used were not just opportunistic hacks but demonstrated a high degree of planning and technical proficiency [60].

As seen with the this breach, the target scope of cybercrimes expanded, with large corporations becoming prime targets for their vast data repositories. This shift indicated that cybercriminals were seeking bigger payoffs and were willing to invest more time and resources to infiltrate these larger, more secure targets.

Signs of trouble emerged in November 2005 when Fidelity Homestead noticed unusual credit card payments. By October 2006, issues with processing Discover Cards led TJX to hire Cybertrust for an investigation, revealing a data breach. TJX then brought in General Dynamics and IBM for a deeper investigation. The breach, initially believed to have started in May 2006, was later found to have begun in July 2005. It was traced back to vulnerable wireless networks at two Minnesota retailers [61, 62].

In January 2007, TJX publicly acknowledged the breach. Spokesperson Sherry Lang admitted the breach's occurrence but could not confirm its full extent. TJX pledged to enhance security and cooperate with law enforcement. Due to public demand for information, Ben Cammarata made a video message urging customers to monitor their accounts [62].

Further investigation showed the breach exposed more customer data than initially thought and began earlier. TJX was also found non-compliant with Payment Card Industry Security standards [63].

The investigation led to the arrest of key individuals, including hacker Albert Gonzalez and his associate Stephen Watt [64]. They used SQL injections and other tactics to access retail systems, starting with two Marshalls stores in Miami. Gonzalez installed sniffer software to collect data, selling stolen credit card information to Ukrainian card vendor Maksym Yastremskiy.

Gonzalez was arrested in 2008, revealing his plans for large profits from cybercrimes. His conversation records, which the authorities obtained, show that he planned to profit $15 million from a string of data breaches.

The escalation in cybercrime has led to changes in regulatory frameworks and legal responses. In response to large-scale breaches, there has been a push for stricter data protection laws and regulations, such as the General Data Protection Regulation (GDPR) in the European Union It was adopted in 2016 and entered into application on May 25, 2018. The regulation updated and modernized the principles of the 1995 data protection directive. The GDPR defines individuals' fundamental rights in the digital age, the obligations of those processing data, methods for ensuring compliance, and sanctions for those in breach of the rules [65]. Companies have moved from reactive security postures to more proactive, layered security approaches, including employee training, incident response planning, and a greater focus on understanding and mitigating potential risks.

The TJX breach was another moment in the history of cybercrime, highlighting a significant shift in the scale and sophistication of attacks. It represented a new era where large-scale, financially motivated cybercrimes targeting major corporations became increasingly common. This paradigm shift set the stage for similar, even more audacious cyberattacks in the years that followed, illustrating that no sector was immune to these advanced threats.

One notable example following the TJX incident was the massive data breach at Target. This breach not only echoed the same patterns of exploiting weaknesses in corporate networks but also underscored the escalating stakes in the realm of cybersecurity. It demonstrated how cyber criminals were constantly refining their tactics and techniques, aiming at even larger targets with vast customer databases.

The attack method was cunningly simple yet devastatingly effective: hackers gained access through a third-party vendor, then moved laterally within Target's network to siphon off customer credit card data. This breach underscored the growing complexity of supply chain and vendor relationships in the digital age and how these could be exploited by savvy cybercriminals.

Target, one of the largest retail chains in the United States [66, 67], reported in late December 2013 that hackers had stolen data from up to 40 million credit and debit cards from customers who had shopped at Target retail stores nationwide between November 27 and December 15, 2013. On January 10, 2014, Target announced that attackers had also stolen 70 million records containing personal information. The hack had major financial consequences, costing credit card firms over $200 million just for reissuing cards [68].

Fazio Mechanical Services, an HVAC company, is believed to have been the initial entry point for the attackers who breached Target's network. Target's systems were not directly breached; instead, credentials from Fazio Mechanical Services were compromised. Using these credentials, the attackers reportedly gained access to Target's network and proceeded to access sensitive areas including the point-of-sale (POS) systems. It is believed that Fazio Mechanical Services' system was compromised by a Citadel Trojan, which was installed through a phishing attack. Fazio Mechanical Services had access to Target's Ariba external billing system, which is part of the business section of Target's network, and this access facilitated the initial breach [69].

Over a period of two weeks, the hackers gathered a wealth of personal information, including the full names, addresses, phone numbers, and email addresses of roughly 70 million Target customers. Additionally, they

took the credit and debit card information of about 40 million users, exposing them to the risk of identity theft and financial fraud.

The crucial dates in the Target breach are further discussed, the attack began on November 12, 2013, when attackers hacked into Target's computer system. Target's security systems identified the hack, but no action was taken until law enforcement informed them of the breach.

The breach was reported as a result of a multi-stage attack that involved the installation of pointof-sale (POS) malware, specifically a version of BlackPOS, which is designed to infect Windows-based POS systems.

When the security breach was announced, it triggered a wave of angry customers and class action lawsuits from both consumers and the banks and financial institutions who were harmed by the attack. In March 2015, Target agreed to a $10 million settlement in a class action lawsuit by customers who made purchases there during the data breach. Also, Target settled with Mastercard in April 2015, agreeing to pay up to $19 million to financial institutions for data breach expenses. Notably, following the data breach, Target's stock price fell by around 11%. However, the stock price recovered within a few months, and as of May 2015, it was up 24% from its December 2013 peak [69].

Target had security measures in place, including firewalls and network segmentation using Virtual Local Area Networks (VLANs). Six months before the incident, Target had also installed FireEye, a reputable network security system. However, despite these measures, the breach occurred, demonstrating that the security measures were insufficient. Multiple malware alerts were ignored, and some prevention features of the FireEye system were turned off by administrators who were not familiar with it, resulting in a failed early detection of the breach [69].

After the breach, Target's CEO Gregg Steinhafel resigned, and the company appointed a new chief information officer, named Bob DeRodes. Target further announced plans to enhance its security with a $100 million investment, which included upgrading POS machines and deploying chipand-PIN-enabled technology for payment, as well as improving network segmentation, log analysis, and access control [70].

7.3. Dawn of Cyber Warfare

The emergence of Stuxnet marked a defining moment in the annals of cybercrime. Unlike its predecessors, Stuxnet wasn't the brainchild of lone hackers or criminal groups seeking financial gain. It was a sophisticated and meticulously engineered piece of malware, believed to be developed by nation-states. This was not merely a tool for espionage or theft, Stuxnet was a weapon, signaling a paradigm shift in the objectives and methods of cyber operations.

Stuxnet was a highly sophisticated computer worm discovered in 2010 but believed to have been in development since at least 2005. It specifically targeted Iranian nuclear PLCs manufactured by Siemens [71, 72]. Recent revelations include the involvement of a Dutch national named Erik van Sabben, who played a crucial role in the operational deployment of Stuxnet [73]. The operation, led by the United States and Israel, was intended to use Stuxnet as a tool to derail or at least delay Iran's program to develop nuclear weapons.

In 2009 Stuxnet significantly damaged Iran's nuclear program. While it is widely accepted that the Stuxnet worm caused significant disruption to Iran's nuclear program, the exact extent of the damage is blurred. Iran has not disclosed detailed information about the impact of the attack and has denied that the Stuxnet virus caused any delays in its nuclear power program [74]. However, Iranian leaders have indirectly confirmed that malicious software affected their nuclear centrifuges. In November 2010, President Ahmadinejad acknowledged issues with their centrifuges but didn't specifically mention Stuxnet. Saeed Jalili, a top Iranian security official, also admitted to a cyberattack in an interview, saying that Iranian experts had countered it a while ago [75].

The primary motive appears to have been to stop or slow down Iran's nuclear enrichment capabilities, which were seen as a potential threat to regional and global stability. Iran's nuclear program was suspected of being aimed at developing nuclear weapons, despite Iranian claims of its peaceful nature. By choosing a cyberattack, the attackers likely aimed to achieve their objectives without resorting to open military conflict, which would have had far greater geopolitical and human repercussions.

The most direct physical impact of Stuxnet was the damage it inflicted on the centrifuges. It is believed that the Stuxnet worm resulted in the destruction of 984 centrifuges used for uranium enrichment, leading to a reduction in enrichment efficiency by 30% [76]. According to Symantec security firm report, by September 2010, the worm had infected 59% of computers in Iran, which was approximately 60000 computers, also 19% of computers in Indonesia, which was 15000, and 9% in India, it was assessed to have infected almost 5% of the computers worldwide [31, 75].

Determining the precise monetary loss from the Stuxnet worm is challenging because of the attack's strategic implications and the complexity of Iran's nuclear program. Nonetheless, the interference with Iran's nuclear efforts was considerable.

While Stuxnet didn't directly impact society, it undermined the Iranian government's credibility, leading to perceptions of weakness and insecurity both domestically and globally. This attack demonstrated how nations could wield power and influence not through traditional military or diplomatic means, but via cyber operations. It introduced the world to a new form of discreet, remote warfare capable of significantly impacting national infrastructure.

Economically, Iran, under international embargoes, lacked access to the global market for nuclear-related materials. Iran couldn't purchase centrifuges and had to build them domestically, using foreign components. The attack in the international level, temporarily delayed Iran's nuclear program, influencing international relations and demonstrating the potential of cyberweapons, leading to increased global investment in cybersecurity [77].

The revelation of Stuxnet's impact and sophistication accelerated the implementation of more stringent cybersecurity measures across nations. Key proactive measures included adopting the IEC 62443 standard (formerly known as ISA 99), a comprehensive framework for securing ICS networks [72]. Additionally, security standards such as NERC-CIP, ISO/IEC 27001 and ISA/IEC 62443 so as to minimize exposure with the implementation of security controls [78]. In addition to that, there was an increase in cybersecurity awareness programs, for example, conducted awareness campaigns for critical infrastructure workers about the risks of using unknown USB drives, promoting cautious behavior [77].

This attack demonstrated how manipulating data can lead to physical disruptions, showing that control over digital information translates directly into real-world power. This operation went beyond traditional cybercrime, illustrating how data manipulation can achieve strategic geopolitical objectives. Its legacy is seen in the subsequent rise of state-sponsored cyber activities and the strategic importance placed on cyber capabilities by nations worldwide. It transformed the landscape of cybercrime, turning it into an arena not just for criminals, but for warriors and strategists in the service of national interests.

7.4. Geopolitics in the Digital Age

The following year, in July 2014, the JP Morgan Case Data Breach further amplified the sense of urgency and vulnerability. This incident was particularly notable for its scale and the sophistication of the attackers. It was one of the largest data breaches in history, affecting an estimated 76 million households and 7 million small businesses.

The JP Morgan incident hinted at a blend of financial gain and potentially more sinister political motives. The breach involved the compromise of personal data of a vast number of clients, a type of attack that could potentially be used for more than just financial theft but for influence and manipulation as well [79].

In 2014 around the time that JPMorgan Chase experienced a data breach there was also the annexation of Crimea, by Russia, which resulted in sanctions being imposed on them. This source quoted an "unnamed senior intelligence officer" and indicated that the cyber-attack on JPMorgan Chase could have been a response or retaliation to these sanctions [80].

The hackers, rumoured to be Russian cybercriminals, targeted not only JPMorgan Chase but also nine other major financial institutions [81]. The scale of the breach and the sophistication of the attack highlighted the serious threat that cybercrime posed to the finance and insurance sectors. The breach was traced back to Russia, leading to speculation about possible political motivations [80].

This attack brings financial harm to the organizations and privacy risks to their clients. Following the attack and JPMorgan's Securities and Exchange Commission (SEC) disclosure, shares of the company's stock ticked down 0.4% [82].

On the customer side, after this attack, millions of people are threatened because their personal data is in the hands of hackers. Experts launched an aggressive campaign to prevent people from being further scammed by financial scammers. They also urged the companies to raise the client's awareness toward phishing either by emails, letters, or calls [83].

Finally, to prevent further damages, banks were increasing the amount of attack information they shared with each other through the Financial Services Information Sharing and Analysis Center (FS-ISAC), an industry group formed to meet a government directive to share information about cybersecurity threats to protect the nation's critical infrastructure [83].

In the following year, there was another attack on the financial sector, this time in Bangladesh. On the morning of February 5, 2016, The Bangladesh Bank fell victim to a cyber-attack [84], that exploited vulnerabilities in SWIFT (the system's primary electronic payment messaging system). It took some time before the attack was discovered, when an employee of Deutsche Bank (a routing bank) suspected a spelling mistake in an online bank transfer instruction that mistakenly wrote "fandation" instead of "foundation" in the name of an NGO during their transaction attempt. This suspicion prompted them to seek clarification from the Bangladesh bank, ultimately leading to stopping the transaction and preventing what could have been a nearly billion-dollar heist [85, 84, 86]. The investigation after the attacks discovered that the hackers were exploiting vulnerabilities in SWIFT (the system's primary electronic payment messaging system), and these hackers attempted to steal a whopping one billion dollars. Although most transactions were successfully blocked, 101 million dollars still managed to vanish.

After the heist took place, the government of Bangladesh deliberated on taking action against the Federal Reserve Bank of New York to recover the stolen funds. This gave rise to speculation that the claim of a motivated attack may have been influenced by the possibility of a lawsuit [86].

United States' Federal Bureau of Investigation (FBI) identified one suspect named Park Jin Hyok as part of a group called Lazarus from North Korea. It was believed that they used activities as a way to evade sanctions and generate revenue for the nation [84].

This incident served as a wake-up call for the industry, shedding light on the underestimated risks posed by cyber threats within the financial system [85, 84, 86], and emphasizing the need for vigilance and robust security measures. This incident also highlights a trend where state actors employ cybercrimes as a means to achieve political objectives and how the potential economic consequences of incidents can be substantial while also causing damage to public trust and confidence.

7.5. Rising Above Cyber Threats: Wisdom, Courage, and Rapid Response

In March 2019, manufacturing sector witnessed incident of the Norsk Hydro Aluminum ransomware attack. The Norwegian aluminum manufacture faced a crippling attack of a virus called LockerGoga [87]. However, their action to retaliate was a big courageous act to defend toward cyberattack.

The hackers had weaponized one email attachment sent by a trusted customer employee to an employee at Norsk Hydro, three months before the attacks [88]. The attachment has been injected by LockerGoga virus beforehand. The virus disrupted operations by encrypting crucial files and demanding a ransom [87].

The LockerGoga attack was a serious and high-level cybercrime targeting major industrial companies. Along with Norsk Hydro Aluminum manufacturer, later, the ransomware caused disruptions to the IT services of U.S. chemical companies Hexion and Momentive [89].

Ransomware attacks are typically driven by a desire to extort money from the targeted organization, so the LockerGoga attack was desired by financial gain from extorted the targeted organization. The attackers demand payment to restore access to the encrypted data and systems. As a result, the incident incurred significant financial costs for mitigation and posed the risk of revenue loss due to operational disruptions [90].

However, to prevent further attacks in the future, Norsk Hydro Aluminum focused on restoring its systems and operations instead of complying with the ransom demands. Instead, they contacted experts, such as Microsoft's cybersecurity response team and the Norwegian Norwegian National Cyber Security Centre to reclaim their data [88, 91].

The data was saved, but it took a considerable amount of time. To appease clients, they graciously admitted the mistake and decided to run the company manually. They reached out to retired Hydro employees who were familiar with the paper-based methods of manufacturing to pitch in. The production facilities were then able to continue fulfilling simpler orders from clients using a combination of expertise and the few physically printed order forms and procedures for certain parts. In order to keep up with customer orders, the workers worked double shifts to minimize the disruption to clients' own production schedules [91, 92]. This incident highlighted a pattern of disruption that transcended borders. The tactics of cybercriminals emphasizing insidious methods, the vulnerability of interconnected global supply chains.

The impacts of the Norsk Hydro Aluminum ransomware highlight the need to configure email systems for malware scanning and attachment filtering, enhancing the first line of defense against malicious activities [87]. Additionally, organizations must implement awareness and training programs to educate staff on safe email practices and the recognition of social engineering attacks. Moreover, ensuring up-to-date backup systems further becomes crucial to swiftly restore lost data in the event of a cyber incident, enhancing overall resilience against potential disruptions. And the most important factor is the ethic to be brave in front of cybercriminals, willing to receive advice from experts, and daring to take responsibility for customers, which will enhance the trustworthiness of the organization. This turning point paved the way for technological innovations, collaborations, and a renewed commitment to cybersecurity resilience.

In light of prominent cyber-related activities, the EU has established five strategic priorities for cybersecurity, emphasizing resilience, the reduction of cybercrime, coherent defense policies, and the advancement of industrial and technological resources in this field [23]. Thus, the manufacturing sector witnessed a paradigm shift in its cybersecurity policies and regulations, with an emphasis on proactive defense mechanisms.

In the aftermath of the turning point, manufacturing companies embarked on a quest for cyber resilience. Collaborations with cybersecurity experts and government agencies intensified, leading to the integration of advanced technologies such as artificial intelligence and integration of 5G wireless communication networks to address cybercrime-related challenges [22].

7.6. Beyond Reality: Unraveling Cyber Conspiracies

In November 2014, German-owned steel mill, ThyssenKrupp became the unexpected battleground [23]. ThyssenKrupp is one of the globe leading steel manufactures and a key component of Norway's industrial strength [44, 93]. This cybercrime is marked as one of the first known cyberattacks that brought significant harm to an industrial factory [44]. Thus, this incident served as an alarming wake-up call for the manufacturing sector, showcasing the vulnerability of critical infrastructure to cyberthreats.

The attackers on this incident displayed proficiency not only in conventional IT security systems but also in the specialized software integral to overseeing and administering the steel mill's operations [93]. The attackers exploited vulnerabilities in the mill's operational technology, resulting in significant disruptions. Specifically, the attackers seized control of a computer managing the blast furnace and inserted malware, causing the machine to overheat and melt down [87].

According to investigations, the identity nor the motives of the attackers have been confirmed, so the identity of the attacker is subject to various speculations, with hypotheses ranging from cyber-sabotage orchestrated by competitors of the steel mill to the possibility of an assault conducted by a government intelligence agency [44]. Fortunately, despite the failure to point out the perpetuator, that investigations have been able to provide insight into how the attack was executed allowing to eliminate possibility of similar attacks in the future.

Even though the scope of ThyssenKrupp's attack was just only in one company, this early attack caused significant harm to an industrial factory. The attackers exploited vulnerabilities, seizing control of a computer managing the blast furnace and causing it to overheat and melt down [87, 23, 44]. Therefore, ThyssenKrupp's

attack becomes initial warning toward more extreme mysterious cyberattacks with unknown motives and actors.

The most famous following case was WannaCry Ransomware. This attack on Windows software in 2017 took user data hostage in exchange for Bitcoin cryptocurrency [41]. This attack was a seismic event in the world of cybercrime, demonstrating a level of destruction that had rarely been seen before. This attack was not just another footnote in the annals of hacking history; it was a global phenomenon that highlighted the increasingly dangerous and far-reaching capabilities of modern cybercriminals. This attack was affecting over 230,000 computers in 150 countries in 2017 and causing an estimated $4 billion in damages.

WannaCry had an indiscriminate nature. Unlike targeted attacks that focus on specific organizations or individuals, WannaCry spread rapidly and randomly, impacting anyone with vulnerable systems. The victims of WannaCry were extremely varied. It not only targeted individual computers but also attacked small and large corporations, hospitals, government agencies, and other entities that heavily relied on digital systems for their daily operations. Consequently, WannaCry caused widespread disruption, from the shutdown of hospital services in the UK's National Health Service to the offices of ministries, railways, and banks in Russia [94]. This level of disruption was unprecedented and served as a stark reminder of how deeply embedded technology had become in the fabric of society and how vulnerable it could be.

WannaCry was unique not only in its scale but also in its method of operation. The ransomware exploited vulnerabilities in Microsoft Windows operating systems, particularly targeting outdated and unpatched systems. It encrypted data on infected computers, rendering them unusable, and demanded a ransom payment in Bitcoin to unlock the files [95, 96]. This attack method signified a departure from traditional forms of cybercrime, where data theft or website defacement were the norms. Instead, WannaCry leveraged the very existence of data as a bargaining chip, creating a dire sense of urgency and helplessness among its victims.

Therefore, this attack prompted significant changes in technologies and regulations to prevent a recurrence. One such response was the re-enhancement of the EU regulation on the security of networks and information systems (NIS Directive), initially adopted in 2016. The objective is to impose a common level of cybersecurity in the EU on operators of certain essential services and digital services operators [14].

But one point that has made WannaCry particularly notable is the ongoing debate regarding its perpetrator. In an interview with Independent News UK, Edward Snowden claimed that WannaCry was constructed using leaked data from the U.S. National Security Agency (NSA). According to Snowden, after discovering a Windows vulnerability, the NSA developed an exploit for its own offensive purposes instead of reporting it to Microsoft [102]. Another source said that WannaCry was developed using the leaked NSA's cyberweapon, EternalBlue [95] [102].

On the contrary, N. P. Shields [96], a Special Agent ("SA") of the Federal Bureau of Investigation ("FBI"), through his team investigations, found out the perperator was a North Korean team, of which one of the members was Park Jin Hyok. He presented several pieces of evidence to the court, with the most notable ones being the metadata of the PC used for the attack, which showed that the PC was set to UTC+09:00 (Korean time) and had \fcharset129 Rich Text Format tag, which is unique to Korean keyboards.

However, the victims of WannaCry were extremely varied. Both Western Bloc and Eastern Bloc countries were attacked. It would be hard to imagine that if the perpetrator stood on one side, they would attack their own allies. So, there was a third point of view, that the attacker was a private individual or group that did attacks for financial motives. Until the end, the perpetrator for the WannaCry Ransomware attack remains unclear, similar to the situation with ThyssenKrupp Mill.

But, the legacies of these cases are not only the debates about their perpetrators. In the aftermath of these attacks, there was a renewed focus on cybersecurity practices, particularly on the importance of regular software updates and backups. The attack served as a wake-up call to individuals, businesses, and governments worldwide, emphasizing the need for proactive measures to protect against such threats and prompting the need for vigilant network security monitoring and the development of comprehensive cybersecurity strategies.

7.7. Espionage at a Global Scale

Dragonfly's enduring presence exemplifies a wider trend in cybercrime, where the boundaries between criminal acts, espionage, and warfare increasingly overlap. Its complexity and multi-national impact highlighted a clear reality: the world of cybercrime is continuously evolving, growing more sophisticated, efficient, and widespread.

Dragonfly, also known as Energetic Bear, Crouching Yeti, TEMP.Isotope, ALLANITE or DYMALLOY, is a cyber espionage and sabotage campaign that has targeted energy sector organizations primarily in the United States and Europe. The group is believed to be backed by the Russian government [97]. Cyber operations linked to Russia that target international entities are generally conducted or overseen by one of three key Russian agencies: the GRU (Main Intelligence Directorate of the Military General Staff), the FSB (Federal Security Service), and the SVR (Foreign Intelligence Service) [98]. Different names to the campaign are given by different antivirus vendors, for the sake of simplicity, this entity will be referred to as "Dragonfly". The campaign is characterized by its long-term strategic focus, the use of various malware tools, and its ability to remain undetected for extended periods [99].

The Dragonfly group has been active since at least 2011, initially focusing their attacks on aviation and defense companies in the United States and Canada. However, the geographical location and industry focus of victims in the Dragonfly campaign vary according to different reports. Symantec and CrowdStrike highlight the energy sector in Europe and North America as the main targets. In contrast, Kaspersky's analysis reveals a more widespread pattern of activity, including victims in South America, Central and Southeast Asia, and the Russian Federation. Kaspersky's reports also note a significant number of victims in educational and government sectors. During its initial period of activity, the campaign primarily used phishing attacks with malicious attachments to gain initial access to target companies. These attacks often targeted executives and senior employees with emails, involving embedded Flash objects in Adobe PDFs and sometimes in XML Data Package files containing malicious PDFs. The precise origin of the phishing messages, whether all from the same Gmail account or not, remains unclear [98].

By 2013, Dragonfly shifted their attention, launching a new phase of their campaign targeting energy companies in the United States and Europe [100]. Symantec's reports indicate that the campaign began with spear-phishing attempts from February to June 2013. In May 2013, the campaign shifted to a "watering hole" technique, compromising trusted websites to redirect visitors to malicious sites lasting until April 2014. During this period, several ICSs vendors unwittingly hosted legitimate software with embedded malicious content on their websites. This Trojan-infected ICS software distribution continued for nearly a year, from June 2013 to May 2014 [22]. In 2014, Dragonfly had targeted over 1,000 organizations, with 84% of those organizations being in the energy sector mainly in the United States, Spain, France, Italy, Germany, Turkey, and Poland. The malware used the Havex (or Oldrea) malware as its primary tool, and the Karagany RAT as a secondary tool [101].

The group reemerged in 2017 with a new version, focusing on energy companies in Europe and North America, with Symantec identifying at least 20 compromised organizations, mostly in the U.S., Switzerland, and Turkey. In 2018, the U.S. Department of Homeland Security issued an alert about Dragonfly's new campaign against critical infrastructure in the U.S., including the energy, nuclear, water, aviation, and critical manufacturing sectors [32].

For all the group's activity, it is not linked to any single, definitive incident or disruptive event that would garner headlines and attention. Although Dragonfly hasn't yet actively engaged in disruptive activities, the group has established a foundation for serious future attacks. Their persistent and stealthy approach has enabled them to prepare for significant operations without drawing much attention.

From the perspective of the attackers, likely state-sponsored, Dragonfly offers significant strategic advantages. The campaign enables them to gain insights, into how critical infrastructure in target countries operates and where its vulnerabilities lie. This information can be utilized to gain an advantage in matters prepare for conflicts or assert control over energy resources. This campaign highlights the significance of having control over data in order to access and potentially disrupt infrastructures. It shows that having the ability to access and manipulate data can be a tool in international relations.

Furthermore, the ongoing nature of campaigns like this suggests a shift in the goals of cyber operations. The focus is increasingly on long term strategies. Maintaining a presence within targeted systems than immediate disruption or theft. This approach allows for gathering of intelligence future sabotage opportunities and a more significant impact, on geopolitical dynamics.

8. Conclusion

The birth and evolution of cybercrime have had a profound impact on industries. The increasing effectiveness brought about by digitalisation is accompanied by a dual consequence as it also exposes vulnerabilities presenting new opportunities for potential cyber-attacks.

This study has undertaken an extensive exploration into the historical evolution of cybercrime across five sectors such as Manufacturing, Finance and Insurance, Professional Business and Consumer Services, Energy, and Retail and Wholesale. Through an in-depth analysis into major cyber incidents within each sector, we have traced the trajectory of cybercrime, starting from its origins as curiosity-driven hacking to its current manifestation as a sophisticated global threat. In conclusion, it becomes evident that this study serves as a foundational exploration, setting the stage for a more comprehensive understanding of historical, current, and emerging cybercrime trends within the specified five key sectors.

As we continue to rely more heavily on digital technology, the importance of understanding and mitigating the risks associated with cybercrime cannot be overstated. Consequently, this research aspires to make a significant contribution to the development of future cybersecurity approaches and resilience by providing profound ins

9. Acknowledgements

This work was developed as part of the *History of Digital Cultures (XM_0134)* course at *Vrije Universiteit Amsterdam*. The authors acknowledge and grateful of the academic feedback provided during the course.

References

[1] B. Leibowitz, “Hack, hacker, hacking,” TF Peterson, Nightwork: A History of Hacks and Pranks at MIT, 1990.

[2] D. Prince, “Cybersecurity: The security and protection challenges of our digital world,” Computer, vol. 51, pp. 16–19, 2018. [Online]. Available: https://api.semanticscholar.org/ CorpusID:22324168

[3] Statista. (February 2023) Distribution of cyber attacks across worldwide industries in 2022. Accessed: 06 January 2024. [Online]. Available: https://www.statista.com/statistics/ 1315805/cyber-attacks-top-industries-worldwide/

[4] V. Jangada Correia, “An explorative study into the importance of defining and classifying cyber terrorism in the united kingdom,” SN Computer Science, vol. 3, no. 1, p. 84, 2022.

[5] G. Zeviar-Geese, “The state of the law on cyberjursidiction and cybercrime on the internet,” Gonz. J. Int’l L., vol. 1, p. 119, 1997.

[6] U. Nations, “The united nations manual on the prevention and control of computer related crime,” International Review of Criminal Policy, vol. Supplement, pp. 43–44, 1995, supra note 41, paragraphs 20 to 73 in International Review of Criminal Policy, pp. 43–44 (1995).

[7] D. O. Friedrichs, “Crimes of the powerful and the definition of crime,” in The Routledge international handbook of the crimes of the powerful. Routledge, 2015, pp. 39–49.

[8] Federal Bureau of Investigation. (2018, November) Morris worm: 30 years since first major attack on internet. Accessed on 14 January 2024. [Online]. Available: https://www.fbi.gov/ news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218

[9] K.-S. Choi, C. S. Lee, and E. R. Louderback, “Historical evolutions of cybercrime from computer crime to cybercrime,” The Palgrave handbook of international cybercrime and cyberdeviance, pp. 27–43, 2020.

[10] B. Dwan, “The computer virus—from there to here.: An historical perspective.” Computer Fraud & Security, vol. 2000, no. 12, pp. 13–16, 2000.

[11] C. Miles, "Early history of the computer virus," Prof. Dasgupta's History of Computer Science The Center for Advanced Computer Studies University of Louisiana, pp. 1–8, 2012.
[12] V. Babanina, I. Tkachenko, O. Matiushenko, and M. Krutevych, "Cybercrime: History of formation, current state and ways of counteraction," April 12 2021, https://doi.org/10.34069/ai/2021.38.02.10.
[13] P. Grabosky, "The evolution of cybercrime, 2004-2014," January 1 2014.
[14] N. Vandezande, "Cybersecurity in the eu: How the nis2-directive stacks up against its predecessor," Computer Law & Security Review, vol. 52, p. 105890, 2024.
[15] I. Corradini and I. Corradini, "Redefining the approach to cybersecurity," Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology, pp. 49–62, 2020.
[16] C. Stoll, The cuckoo's egg: tracking a spy through the maze of computer espionage. Simon and Schuster, 2005.
[17] D. R. C. T. C. Community, "25 Years Later: Looking Back at the First Great (Cyber) Bank Heist — darkreading.com," https://www.darkreading.com/perimeter/25-years-later-looking-back-at-the-first-great-cyber-bank-heist, 2019, [Accessed 15-01-2024].
[18] Federal Bureau of Investigation. (2019, March) The melissa virus. Accessed on 14 January 2024. [Online]. Available: https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218
[19] E. Mills, "Melissa virus turns 10 − interview with dmitry gryaznov," CNET, March 2009, accessed on 20 January 2024. [Online]. Available: https://www.cnet.com/news/privacy/ melissa-virus-turns-10/
[20] K. C. Laudon and J. P. Laudon, Management Information System: Managing the Digital Firm, 15th ed. Pearson Education, 2017, chapter 8: Securing Information Systems.
[21] P. Mahesh, A. Tiwari, C. Jin, P. R. Kumar, A. N. Reddy, S. T. Bukkapatanam, N. Gupta, and R. Karri, "A survey of cybersecurity of digital manufacturing," Proceedings of the IEEE, vol. 109, no. 4, pp. 495–516, 2020.
[22] F. Khan, "A detailed study on security breaches of digital forensics in cyber physical systems," in 2019 Sixth HCT Information Technology Trends (ITT). IEEE, 2019, pp. 38–43.
[23] M. Heikkilä, A. Rättyä, S. Pieskä, and J. Jämsä, "Security challenges in small- and medium-sized manufacturing enterprises," in *Proc. Int. Symp. Small-Scale Intelligent Manufacturing Systems (SIMS)*, IEEE, 2016, pp. 25–30.
[24] U. J. Butt, M. Abbod, A. Lors, H. Jahankhani, A. Jamal, and A. Kumar, "Ransomware threat and its impact on scada," in 2019 IEEE 12th international conference on global security, safety and sustainability (ICGS3). IEEE, 2019, pp. 205–212.
[25] A. Buja, M. Apostolova, A. Luma, and Y. Januzaj, "Cyber security standards for the industrial internet of things (iiot)–a systematic review," in 2022 International Congress on Human−Computer Interaction, Optimization and Robotic Applications (HORA). IEEE, 2022, pp. 1–6.
[26] FBI, "A byte out of history: $10 million hack — fbi," 2014. [Online]. Available: https://www.fbi.gov/news/stories/a-byte-out-of-history-10-million-hack-011514
[27] J. S. Cheney, "Heartland Payment Systems: Lessons learned from a data breach," *Federal Reserve Bank of Philadelphia, Payment Cards Center*, Discussion Paper 10-1, 2010. [Online]. Available: https://ssrn.com/abstract=1540143
[28] B. Parmar, "Protecting against spear-phishing," Computer Fraud Security, vol. 2012, no. 1, pp. 8–11, 2012. [Online]. Available: https://www.sciencedirect.com/science/article/pii/ S1361372312700076
[29] T. von Randow, "Btx system," https://germanhistory-intersections.org/en/knowledge-and-education/ghis:document-22 , 1984, accessed: November 30, 2023.
[30] S. Colbourn, "An interpreter or two: defusing nato's siberian pipeline dispute, 1981–1982," Journal of Transatlantic Studies, vol. 18, pp. 131–151, 2020.
[31] C. Edwards and I. Press, "An analysis of a cyberattack on a nuclear plant: The stuxnet worm," Critical Infrastructure Protection, vol. 116, p. 59, 2014.
[32] F. B. Khan, A. Asad, H. Durad, S. M. Mohsin, and S. N. Kazmi, "Dragonfly cyber threats: A case study of malware attacks targeting power grids," Journal of Computing & Biomedical Informatics, vol. 4, no. 02, pp. 172–185, 2023.
[33] T. Whitlock, "Forms of crime," The Oxford Handbook of the History of Crime and Criminal Justice, p. 155, 2016.
[34] K. Joshi and K. Akhilesh, "Role of cyber security in retail," Smart Technologies: Scope and Applications, pp. 233–247, 2020.
[35] R. J. Rodriguez, "Evolution and characterization of point-of-sale ram scraping malware," Journal of

Computer Virology and Hacking Techniques, vol. 13, pp. 179–192, 2017.
[36] O. Eunice, B. Dorothy, and O. Omosa, "The impact of cyber attacks on e-businesses," IJCSNInternational J. Comput. Sci. Netw, vol. 8, no. 4, pp. 354–357, 2019.
[37] D. Slater. (2021) 7 new social engineering tactics threat actors are using now. [Online]. Available: https://www.csoonline.com/article/570557/7-new-social-engineering-tactics-threat-actors-are-using-now.html
[38] S. K. Venkatachary, A. Alagappan, and L. J. B. Andrews, "Cybersecurity challenges in energy sector (virtual power plants)-can edge computing principles be applied to enhance security?" Energy Informatics, vol. 4, no. 1, p. 5, 2021.
[39] K. Huang, X. Wang, W. Wei, and S. Madnick. (2023, May) The devastating business impacts of a cyber breach. Accessed: 06 January 2024. [Online]. Available: https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach
[40] B. Sheehan, F. Murphy, M. Mullins, and C. Ryan, "Connected and autonomous vehicles: A cyber-risk classification framework," Transportation research part A: policy and practice, vol. 124, pp. 523–536, 2019.
[41] F. Cremer, B. Sheehan, M. Fortmann, A. N. Kia, M. Mullins, F. Murphy, and S. Materne, "Cyber risk and cybersecurity: a systematic review of data availability," The Geneva Papers on risk and insurance-Issues and practice, vol. 47, no. 3, pp. 698–736, 2022.
[42] M. Riek and R. B¨ohme, "The costs of consumer-facing cybercrime: an empirical exploration of measurement issues and estimates†," Journal of Cybersecurity, vol. 4, no. 1, p. tyy004, 10 2018.
[43] K. C. Laudon and J. P. Laudon, Management Information System: Managing the Digital Firm, 13th ed. Pearson Education, 2014, chapter 8: Securing Information Systems.
[44] S.-Y. Yu, A. V. Malawade, S. R. Chhetri, and M. A. Al Faruque, "Sabotage attack detection for additive manufacturing systems," IEEE Access, vol. 8, pp. 27 218–27 231, 2020.
[45] L. Bielski, "Keeping check fraud in check: Recent report looks at the marketplace of fraud prevention," ABA Banking Journal, vol. 96, p. 48, 2004. [Online]. Available: https://api.semanticscholar.org/CorpusID:221245572
[46] S. Shin and G. Gu, "Conficker and beyond: a large-scale empirical study," in Asia-Pacific Computer Systems Architecture Conference, 2010. [Online]. Available: https://api.semanticscholar.org/CorpusID:9961043
[47] A. Rot and B. Olszewski, "Advanced persistent threats attacks in cyberspace. threats, vulnerabilities, methods of protection," in Conference on Computer Science and Information Systems, 2017. [Online]. Available: https://api.semanticscholar.org/CorpusID:32355481
[48] K. Sigler, "Crypto-jacking: how cyber-criminals are exploiting the crypto-currency boom," Computer Fraud & Security, 2018. [Online]. Available: https://api.semanticscholar.org/ CorpusID:69683850
[49] N. Yildirim and A. Varol, "A research on security vulnerabilities in online and mobile banking systems," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), pp. 1–5, 2019. [Online]. Available: https://api.semanticscholar.org/CorpusID:195884347
[50] "Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets — CISA — cisa.gov," https://www.cisa.gov/news-events/cybersecurity-advisories/ aa20-296a, [Accessed 07-01-2024].
[51] Symantec, "Dragonfly: Western energy sector targeted by sophisticated attack group," 2018. [Online]. Available: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks. [Accessed: Jan. 7, 2024].
[52] S. K. Venkatachary, J. Prasad, and R. Samikannu, "Cybersecurity and cyber terrorism-in energy sector–a review," Journal of Cyber Security Technology, vol. 2, no. 3-4, pp. 111–130, 2018.
[53] D. C. Smith, "Cybersecurity in the energy sector: are we really prepared?" pp. 265–270, 2021.
[54] T. Akhtar, B. B. Gupta, and S. Yamaguchi, "Malware propagation effects on scada system and smart power grid," in 2018 IEEE International Conference on Consumer Electronics (ICCE). IEEE, 2018, pp. 1–6.
[55] I. D'Adamo, R. Gonz´alez-S´anchez, M. S. Medina-Salgado, and D. Settembre-Blundo, "E-commerce calls for cyber-security and sustainability: How european citizens look for a trusted online environment," Sustainability, vol. 13, no. 12, 2021. [Online]. Available: https://www.mdpi.com/2071-1050/13/12/6752
[56] X. Liu, S. F. Ahmad, M. K. Anser, J. Ke, M. Irshad, J. Ul-Haq, and S. Abbas, "Cyber security threats: A never-ending challenge for e-commerce," Frontiers in psychology, vol. 13, p. 927398, 2022.
[57] N. Leena, "Cyber crime effecting e-commerce technology," Oriental Journal of Computer Science &

Technology, vol. 4, no. 1, pp. 209–212, 2011.
[58] A. Rezk, S. Barakat, and H. Saleh, "The impact of cyber crime on e-commerce," International Journal of Intelligent Computing and Information Sciences, vol. 17, no. 3, pp. 85–96, 2017.
[59] T. Hale. (2022, October) One evening in 1988, a college student's prank broke the internet. Accessed on 20 January 2024. [Online]. Available: https://www.iflscience.com/one-evening-in-1988-a-college-student-s-prank-broke-the-internet-65601
[60] U.S. Department of Justice. (2008) Albert gonzalez indictment. Accessed on 20/01/2024. [Online]. Available: https://wayback.archive-it.org/all/20091202110019/http://www.justice.gov/usao/ma/Press%20Office%20-%20Press%20Release%20Files/IDTheft/Gonzalez,%20Albert%20-%20Indictment%20080508.pdf
[61] R. Walker, "Maxxed out: Tjx companies and the largest-ever consumer data breach," Kellogg School of Management Cases, pp. 1–8, 2017.
[62] W. Xu, G. Grant, H. Nguyen, and X. Dai, "Security breach: The case of tjx companies, inc." Communications of the Association for Information Systems, vol. 23, no. 1, p. 31, 2008.
[63] M. J. Culnan and C. C. Williams, "How ethics can enhance organizational privacy: lessons from the choicepoint and tjx data breaches," MIS quarterly, pp. 673–687, 2009.
[64] G. G. Berg, M. S. Freeman, and K. N. Schneider, "Analyzing the tj maxx data security fiasco: lessons for auditors," The CPA Journal, vol. 78, no. 8, p. 34, 2008.
[65] C. Tankard, "What the gdpr means for businesses," Network Security, vol. 2016, no. 6, pp. 5–8, 2016.
[66] T. D. Breach, "A "kill chain" analysis of the 2013 target data breach," 2014.
[67] K. C. Laudon and J. P. Laudon, Management Information System: Managing the Digital Firm, 16th ed. Pearson Education, 2019, chapter 8: Securing Information Systems.
[68] N. E. Weiss and R. S. Miller, "The target and other financial data breaches: Frequently asked questions," in Congressional Research Service, Prepared for Members and Committees of Congress February, vol. 4, 2015, p. 2015.
[69] D. A. McMullen, M. H. Sanchez, and M. O. Reilly-Allen, "Target security: a case study of how hackers hit the jackpot at the expense of customers," Review of Business & Finance Studies, vol. 7, no. 2, pp. 41–50, 2016.
[70] X. Shu, K. Tian, A. Ciambrone, and D. Yao, "Breaking the target: An analysis of target data breach and lessons learned," arXiv preprint arXiv:1701.04940, 2017.
[71] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," Survival, vol. 53, no. 1, pp. 23–40, 2011.
[72] B. Baki´c, M. Mili´c, I. Antovi´c, D. Savi´c, and T. Stojanovi´c, "10 years since stuxnet: What have we learned from this mysterious computer software worm?" in 2021 25th International Conference on Information Technology (IT). IEEE, 2021, pp. 1–4.
[73] *NL Times*, "Dutch man sabotaged Iranian nuclear program without Dutch government's knowledge: Report," 2024. [Online]. Available: http://bit.ly/48nJwsp. [Accessed: Jan. 8, 2024].
[74] BBC-News, "Iran denies Stuxnet disrupted its nuclear programme — bbc.com," https://www.bbc.com/news/technology-11821011, 2010, [Accessed 13-01-2024].
[75] P. Shakarian, "Stuxnet: Cyberwar revolution in military affairs," 2011.
[76] M. Holloway, "Stuxnet worm attack on iranian nuclear facilities. submitted as coursework for ph241," 2015.
[77] M. Baezner and P. Robin, "Stuxnet," ETH Zurich, Tech. Rep., 2017.
[78] C. K. G. Ang and N. P. Utomo, "Cyber security in the energy world," in 2017 Asian Conference on Energy, Power and Transportation Electrification (ACEPT). IEEE, 2017, pp. 1–5.
[79] T. S. Bernard, "Ways to protect yourself after the jpmorgan hacking," NYC Times, 10 2014, accessed on 27 January 2024. [Online]. Available: https://www.nytimes.com/2014/10/04/your-money/jpmorgan-chase-hack-ways-to-protect-yourself.html
[80] The Register, "Jpmorgan cyber-heist: 9 us financial firms snared by 'russian hackers', says report," Oct 2014. [Online]. Available: https://www.theregister.com/2014/10/05/report_says_russians_behind_jpmorgan_chase_cyber_attack/
[81] M. Riley and J. Robertson, "Jpmorgan hackers said to probe 13 financial firms," Bloomberg, 10 2014, accessed on 27 January 2024. [Online]. Available: https://www.bloomberg.com/news/articles/2014-10-09/jpmorgan-hackers-said-to-probe-13-financial-firms
[82] M. McGrath, "Jp morgan says 76 million households affected by data breach," Forbes, 10 2014, accessed on 27 January 2024. [Online]. Available:

https://www.forbes.com/sites/maggiemcgrath/2014/10/02/jp-morgan-says-76-million-households-affected-by-data-breach/

[83] A. Gonsalves, "What to do in the aftermath of the jpmorgan breach," CSOOonline, 10 2014, accessed on 27 January 2024. [Online]. Available: https://www.csoonline.com/article/549450/what-to-do-in-the-aftermath-of-the-jpmorgan-breach.html

[84] BBC, "The lazarus heist: How north korea almost pulled off a billion-dollar hack," Jun 2021. [Online]. Available: https://www.bbc.com/news/stories-57520169

[85] A. U. Islam, "Assessing the economic and political impacts of the bangladesh bank cyber attack," Mar 2023. [Online]. Available: https://www.ijser.org/researchpaper/ Assessing the Economic and Political Impacts of the Bangladesh Bank Cyber Attack.pdf

[86] The Independent, "Spelling mistake stops hackers stealing $1 billion in bangladesh bank heist," The Independent, Mar. 2016, [Online]. Available: https://www.independent.co.uk/news/world/asia/spelling-mistake-stops-hackers-stealing-1-billion-in-bangladesh-bank-heist-a6924971.html

[87] N. E. Oueslati, H. Mrabet, A. Jemai, and A. Alhomoud, "Comparative study of the common cyber-physical attacks in industry 4.0," in 2019 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC). IEEE, 2019, pp. 1–7.

[88] S. Lyngaas, "Why the norsk hydro attack is a 'blueprint' for disruptive hacking operations," cyberscoop, 03 2020, accessed on 27 January 2024. [Online]. Available: https://cyberscoop.com/norsk-hydro-lockergoga-ransomware/

[89] L. Franceschi-Bicchierai, "Ransomware forces two chemical companies to order 'hundreds of new computers.'," Mother Board, March, vol. 23, 2019.

[90] C. Page, "Europol detains hackers behind 2019 norsk hydro ransomware attack," TechCrunch+, 10 2021, accessed on 27 January 2024. [Online]. Available: https://techcrunch.com/2021/10/29/europol-hackers-norsk-hydro/

[91] P. L. Austin, "This company was hit with a devastating ransomware attack—but instead of giving in, it rebuilt everything," Time, 07 2021, accessed on 27 January 2024. [Online]. Available: https://time.com/6080293/norsk-hydro-ransomware-attack/

[92] B. Briggs, "Hackers hit norsk hydro with ransomware. the company responded with transparency," Microsoft News, 12 2019, accessed on 27 January 2024. [Online]. Available: https://news.microsoft.com/source/features/digital-transformation/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/

[93] BBC News. (2014, December 16), "German steel plant hit by cyber-attack". [Online]. Available: https://www.bbc.com/news/technology-30575104

[94] BBC News. (2017, May), "Ransomware cyber-attack: Who has been hardest hit?", accessed on 27 January 2024. [Online]. Available: https://www.bbc.com/news/world-39919249

[95] D. Goodin, "An nsa-derived ransomware worm is shutting down computers worldwide," Ars Technica, 05 2017, published on May 12, 2017, at 8:11 PM. [Online]. Available: https://arstechnica.com/information-technology/2017/05/an-nsa-derived-ransomware-worm-is-shutting-down-computers-worldwide/

[96] N. P. Shields, "Criminal complaint," United States Department of Justice, 06 2018, archived from the original on September 6, 2018. Retrieved September 6, 2018. [Online]. Available: https://www.justice.gov/opa/press-release/file/1092091/download

[97] A. Thomson and C. Rahn, "Russian hackers threaten power companies, researchers say," Bloomberg, July, 2014.

[98] J. Slowik, "The baffling berserk bear: a decade's activity targeting critical infrastructure," in VIRUS BULLETIN CONFERENCE OCTOBER, vol. 2021, 2021.

[99] P. Maynard, K. McLaughlin, and S. Sezer, "Decomposition and sequential-and analysis of known cyber-attacks on critical infrastructure control systems," Journal of Cybersecurity, vol. 6, no. 1, p. tyaa020, 2020.

[100] J. F. Clemente, "Cyber security for critical energy infrastructure," Ph.D. dissertation, Monterey, CA; Naval Postgraduate School, 2018.

[101] K. E. Hemsley, E. Fisher et al., "History of industrial control system cyber incidents," Idaho National Lab. (INL), Idaho Falls, ID (United States), Tech. Rep., 2018.

[102] C. Farand, "NHS cyber attack: Edward Snowden says NSA should have prevented cyber attack," *The Independent*, May 13, 2017. [Online]. Available: https://www.independent.co.uk/news/uk/home-news/nhs-cyber-attack-edward-snowden-accuses-nsa-not-preventing-ransomware-a7733941.html.